Examensarbete

HÖGSKOLAN
I SKÖVDE

FYSISK SÄKERHET

Skydd av IT-utrustning och information

Examensarbete i Datalogi med inriktning mot
Nätverks- och Systemadministration
Grundnivå 15 högskolepoäng
Vårtermin 2012

Jenny Danielsson

Handledare: Marcus Nohlberg
Examinator: Rose-Mharie Åhlfeldt

Fysisk säkerhet

Skydd av IT-utrustning och information

Examensrapport inlämnat av Jenny Danielsson till Högskolan i Skövde, för Högskoleexamen vid Institutionen för kommunikation och information. Arbetet har handletts av Marcus Nohlberg.

2012-05-30

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Sammanfattning

Informationssäkerhet handlar om att skydda sin information och bevara informationens tillgänglighet, riktighet, konfidentialitet samt spårbarhet. Fysisk säkerhet inom informationssäkerhet innebär att skydda sina informationstillgångar mot fysiska hot. Fysiska hot kan orsakas av exempelvis strömförsörjning, naturkatastrofer och mänsklig åverkan. Problemet med fysisk säkerhet är att den oftast är förbisedd och att den inte anses lika viktig. Det finns flera standarder och riktlinjer med rekommendationer om vad som bör ses över inom informationssäkerhet och däribland just fysisk säkerhet. Denna rapport visar hur väl förberedda verksamheter inom den offentliga sektorn är för de rekommendationer som finns angivna av ISO-standarden 27002 rörande fysisk och miljörelaterad säkerhet inom informationssäkerhet. En intervjuundersökning har genomförts för att få svar på detta. Ett stort TACK riktas till handledare Marcus Nohlberg för vägledning och stöttning samt till de personer som ställt upp på en intervju.

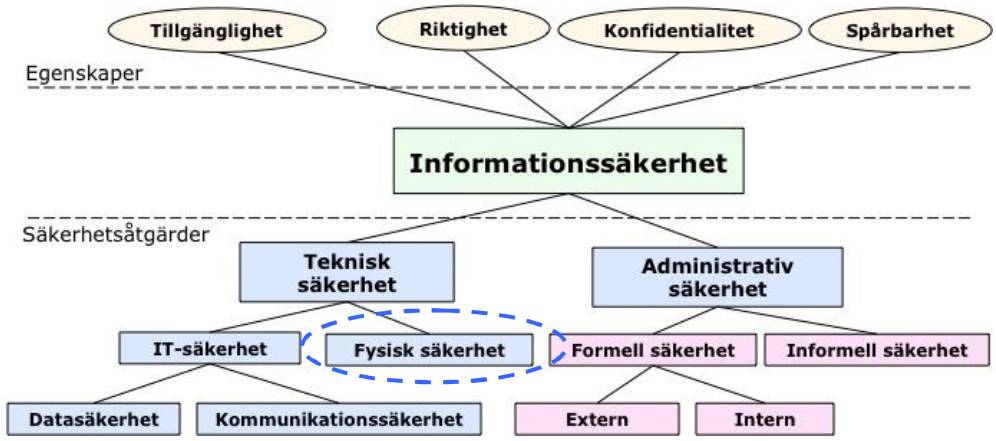
Nyckelord: Informationssäkerhet, Informationstillgångar, Fysisk säkerhet, Fysiska hot, ISO-27002.

Innehållsförteckning

1 Introduktion

Säkerhetsarbetet inom informationssäkerhet i en verksamhet inkluderar många faktorer som kan ses i nedanstående modell där fysisk säkerhet är en av byggstenarna för att uppnå fyra egenskaper. Egenskaperna som information bör uppnå förklaras nedan och dessa egenskaper kan åstadkommas med hjälp av säkerhetsåtgärder. Dessa säkerhetsåtgärder är dels administrativ säkerhet som handlar om hur den administrativa delen av säkerheten sköts, som att ha en säkerhetspolicy samt att det är viktigt att göra en riskanalys för att bli medveten om vilka hot som finns i ens närhet. Det finns både formell och informell administrativ säkerhet då säkerhetsarbetet inte bara påverkas av vad verksamheten vill och behöver göra. Det finns också formella lagar och regler som måste efterföljas. Tekniska säkerhetsåtgärder handlar dels om IT-säkerhet som inkluderar hur nätverket bör skyddas och hur säkerheten i en dator fungerar. Teknisk säkerhet handlar också om fysisk säkerhet vilket innebär hur information skyddas mot fysiska hot. Den fysiska säkerhetsdelen kommer beröras i denna rapport.

Allsopp (2009, s. 1) skriver *"that security is only as strong as the weakest link in the chain"*. Översatt innebär detta att säkerheten inte är starkare än dess svagaste länk och därför bör samtliga säkerhetsåtgärder ses över för att få så lite brister i skyddet som möjligt. Att ha brister i skyddet av information innebär att hot kan realiseras.



Figur 1 Informationssäkerhetsmodellen (Åhlfeldt, R-M., Spagnoletti, P. & Sindre, G., 2007). Då denna rapport handlar om fysisk säkerhet har denna del ringats in i blå streckad linje.

Med informationssäkerhet önskas fyra egenskaper uppnås som kan ses i Figur 1.

Bowin (2007, s. 10-13) skriver följande om de fyra egenskaperna:

- Tillgänglighet innebär att *"informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid"*.
- Riktighet att *"information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning"*.
- Konfidentialitet att *"innehållet i ett informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga"*.

- Spårbarhet att *”möjligheten att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare”*.

Dessa egenskaper uppnås med en mängd olika säkerhetsåtgärder där fysisk säkerhet är en del. Den fysiska säkerheten är viktig att se över av olika aspekter. Dels spelar placering av exempelvis serverrum stor roll då det finns fysiska hot som kan inträffa. En annan orsak till att den fysiska säkerheten inte får glömmas av är att det alltid kommer finnas människor som vill illa. Därför måste informationstillgångar, både inom och utanför verksamhetens lokaler, skyddas från obehörig åtkomst (Anderson, 2008).

Säkerhetsarbetet i en verksamhet kan variera beroende på vilken budget som finns att arbeta med. Då fysisk säkerhet är en del av säkerhetsarbetet inom informationssäkerhet är denna del lika viktig att se över som de övriga delarna. Det stora problemet med fysisk säkerhet är att den inte anses vara lika viktig och nonchaleras. Tankar som ”vi tar det sen” och ”det händer inte oss ändå” uppstår och den fysiska säkerheten blir vilande och energi läggs istället på annat (LabCenter, 2009).

2 Bakgrund

Fysisk säkerhet inom informationssäkerhet handlar om hur informationstillgångar skyddas från fysiska hot. En informationstillgång är alltså där informationen finns, det kan vara en dator, en server eller annan programvara. Information finns i hårdvaran och denna måste skyddas dels från att bli förstörd men även från obehörig tillgång. Säkerhetsmedvetenhet kring IT handlar inte bara om hur nätverket skyddas. Många hot existerar över nätverket som exempelvis virus, trojaner, maskar, avlyssning med mera och skyddsåtgärder som virusskydd, brandväggar och annan mjukvara kan användas för att åtgärda och förebygga dessa hot. Men den fysiska säkerheten kring sin information är också betydelsefull (Pfleeger & Pfleeger, 2006).

En verksamhet bör ha en säkerhetspolicy som är ett övergripande anslag om syftet med säkerhetsarbetet (Pfleeger & Pfleeger, 2006). För att göra sig medveten om vilka hot som finns närmast kan en riskanalys göras.

2.1 Fysisk säkerhet

Fysisk säkerhet är en mekanism inom informationssäkerhet som handlar om skyddsåtgärder utanför datasystemen för att undvika och förebygga fysiska hot (Pfleeger & Pfleeger, 2006).

Många organisationer idag är beroende av information som lagras elektroniskt och varje anställd på ett kontor har oftast en egen bärbar eller stationär dator. Dessa datorer innehåller information som måste skyddas från hot. Inte bara de anställdas datorer måste skyddas utan även de servrar som verksamheten har. På servrarna lagras eventuellt mycket information i olika former så som anställdas inloggningskonton, bilder över verksamheten och annan känslig information som inte får komma i orätta händer. IT-utrustningen måste skyddas från hot.

Enligt Bowin (2007, s. 16) är hot en *”möjlig, oönskad händelse med negativa konsekvenser för verksamheten”*.

Det finns hot som är både avsiktliga och oavsiktliga. Enligt Bowin (2007, s. 16-17) definieras dessa enligt följande:

Avsiktligt hot är *”hot där händelsen orsakas av någon med syfte att skada verksamheten”*.

Oavsiktligt hot är *”hot som existerar trots att illasinnad avsikt saknas”*. Exempel på oavsiktliga hot är misstag orsakat av människor eller naturkatastrofer.

För att skydda sin dator och information mot hot måste skyddsåtgärder väljas och implementeras. Skyddsåtgärder är åtgärder som används för att skydda sig mot hot, det kan vara regler och policys men också tekniska åtgärder i form av övervakning och lås (MSB, 2010a). Oftast när IT-säkerhet diskuteras tänker många på de hot som finns över nätverket, alltså hot som virus och trojaner som datorn kan utsättas för. Tankar går även kring avlyssning av mediet som används, exempelvis avlyssning av kopparkabel. Skyddsåtgärder som virusskydd och brandväggar kan användas för att åtgärda och förebygga dessa nätverkshot men fysiska skyddsåtgärder är även de viktiga. Genom att få fysisk tillgång till en laptop, serverrum eller annan hårdvara som innehåller mjukvara kan hot realiseras.

Pfleeger och Pfleeger (2006) inkluderar fysiska hot så som:

- Naturkatastrofer
- Strömförsörjning
- Mänsklig åverkan

Det finns flera fysiska hot men då dessa inte anses relevanta att tas med i denna rapport har dessa uteslutits. Ett exempel på sådant fysiskt hot som inte tagits med är avmagnetisering. Det vill säga att en magnetisk hårddisk kan utsättas för avmagnetisering vilket orsakar att information raderas (Pfleeger & Pfleeger, 2006). Då naturkatastrofer, strömförsörjning och mänsklig åverkan är de hot som ofta nämns när fysisk säkerhet kommer på tal har dessa valts ut för att beskrivas närmare. Dessa hot är enkla att relatera till och vid djupare kunskap om vad de kan orsaka kan verksamheter inse att fysisk säkerhet kring sina informationstillgångar inte får nonchaleras (LabCenter, 2009).

2.1.1 Naturkatastrofer

Naturkatastrofer innefattar bland annat översvämning och brand och dessa kan inträffa plötsligt och utan förvarning. Översvämningar orsakas av vatten som tar sig in antingen från bottenvåning, taket eller från otäta väggar (Pfleeger & Pfleeger, 2006). Vatten tar sig först in i källare/bottenvåning och fyller sedan på uppåt och vid en storm kan mycket vatten lägga sig på taket och detta kan då brista. Då elektronik förstörs i kontakt med vatten är det viktigt att skydda sin hårdvara mot denna typ av katastrof (Pfleeger & Pfleeger, 2006). Översvämningar kan också orsakas av att en vattenledning eller vattenberedare i byggnaden går sönder. Även om hårdvara går att köpa ny är det innehållet i hårdvaran som är av betydelse. Informationen som finns i hårdvara kan bli förstörd om hårdvaran kommer i kontakt med vatten.

En annan katastrof som brand kan uppstå fort och utan förvarning. Det är kort tid att handla på vilket medför att bränder anses som mer allvarliga (Pfleeger & Pfleeger, 2006). En brand kan uppstå på grund av för hög värme och dålig ventilation kring hårdvaran samtidigt som en brand kan uppstå på annan plats i en verksamhet. Då bränder sprider sig fort kan mycket information förstöras om inte branden släcks i tid.

2.1.2 Strömförsörjning

Hårdvara behöver ström för att fungera och om strömmen bryts av en orsak stängs en maskin av direkt (Pfleeger & Pfleeger, 2006). Om strömmen bryts och hårdvaran stängs ner kan osparad information försvinna. Att strömförsörjning bryts kan orsakas av strömavbrott eller spänningsförändringar. Spänningsförändringar innebär att strömmen inte håller jämnt flöde utan att strömförsörjningen kan variera. Spänningsförändringar kan upplevas genom exempelvis en lampa som blinkar till. Ofta händer inget mer än så men en sådan spänningsförändring kan göra att en hårdvara påverkas eller faktiskt stängs av. En naturkatastrof som åska kan orsaka strömavbrott som i sin tur kan orsaka att hårdvara plötsligt stängs av (Pfleeger & Pfleeger, 2006). Att ha en UPS i sådant fall är att föredra då det kan bli stora konsekvenser om ett helt serverrum stängs ner. En UPS (Uninterruptible Power Supply) kan ses som ett slags batteri som används som backup och tar över om den vanliga strömförsörjningen oväntat slutar fungera (Pfleeger & Pfleeger, 2006).

2.1.3 Mänsklig åverkan

Mänsklig åverkan handlar om förstörelse, stöld och påverkan av information, hårdvara och mjukvara. Sådan åverkan kan orsakas av missnöjda anställda, uttråkad personal eller andra personer som vill förstöra information (Pfleeger & Pfleeger, 2006). Fysiska hot inom mänsklig åverkan handlar bland annat om kontroll av åtkomst samt stöld. Om obehöriga personer kan få fysisk tillgång till informationstillgångar kan dessa på så sätt stjäla och förstöra information. Mänsklig åverkan kan orsakas av både interna anställda och externa, obehöriga personer. Interna anställda kan ha som vilja att förstöra för verksamheten de arbetar på och har åtkomst till mycket information. De kan på så sätt orsaka förstörelse eller stöld utan att egentligen vara mycket tekniskt kunniga. De anses pålitliga och har ofta ett konto för autentisering in till system och är därför svårare att spåra då de har en gällande inloggning (Roy Sarkar, 2010).

För övrigt utgör anställda hot mot den fysiska säkerheten då händelser som inte är avsiktliga kan inträffa, så som att glömma släcka ett ljus eller stänga av vattenkranen i köket. Att skydda information från obehöriga personer blir allt viktigare då det finns personer som kan orsaka skada vare sig det är avsiktligt eller oavsiktligt (Pfleeger & Pfleeger, 2006). Enligt Roy Sarkar (2010) är det lättare att skydda sig mot utomstående genom att använda sig av fysiska skydd, men det är dessvärre svårare att skydda sig mot interna anställda. Interna anställda kan på så sätt utgöra ett stort hot mot informationssäkerheten.

I kommande stycken beskrivs två administrativa åtgärder som en verksamhet bör se över gällande säkerhetsarbetet.

2.2 Säkerhetspolicy

En verksamhet bör ha en säkerhetspolicy som anger hur säkerhetsarbetet ska hanteras och denna bör innefatta fysisk säkerhet. Detta för att fysiska hot kan realiseras mot verksamheten. En säkerhetspolicy är ett övergripande anslag om hur säkerhetsarbetet i en verksamhet ska bedrivas och är ett dokument som klart och tydligt beskriver vad de olika skyddsmekanismerna ska uppnå (Anderson, 2008). En säkerhetspolicy baseras på verksamhetens kunskaper om de hot som finns i närheten och som kan realiseras. Säkerhetspolicyn innehåller rader med uttalanden om bland annat vilka personer policyn gäller för, vilka regler som ska följas och vem som får komma åt vad (behörigheter). En policy kan även ange vad som ska ske om en incident inträffar och vem som är ansvarig för att åtgärda incidenten. Syftet med en säkerhetspolicy är att kommunicera (Anderson, 2008), det vill säga uttrycka påståenden som ska följas av samtliga den gäller för och att alla berörda personer vet vilka regler som gäller.

Säkerhetsarbetet bör innefatta både tekniska och administrativa delar då dessa tillsammans bidrar till ökad säkerhet då brister i skyddet ses över (Goel & Chengalur-Smith, 2010). En säkerhetspolicy behövs för att ange vad som ska göras och uppnås med säkerhetsarbetet. Tekniska delar som virusskydd behövs för att göra nätverket säkrare, men administrativa delar som regler att följa är lika viktigt då interna anställda också utgör hot mot säkerheten.

2.3 Riskanalys

En riskanalys används för att bli medveten om de hot som finns i ens närhet och hur stor sannolikhet det är att de inträffar och vilka negativa konsekvenser de kan få för verksamheten (Pfleeger & Pfleeger, 2006). I en riskanalys är det viktigt att se över vilka hot

som finns över nätverket men det är lika viktigt att inkludera den fysiska säkerheten i riskanalysen. Det vill säga att kartlägga de fysiska hot som finns och sedan göra en uppskattning av hur sannolikt det är att dessa hot realiseras och vad konsekvensen av dessa skulle bli. Konsekvensen av en incident handlar dels om det som kan komma att förstöras. Det innefattar både kostnader för fysiska tillgångar som exempelvis kostnaden av en ny server, samtidigt som konsekvensen kan bli att informationen i hårdvara förstörs.

Säkerhet handlar om frågan: Säker mot vad och för vem, i vilken miljö? (Anderson, 2008).

En riskanalys ska resultera i medvetenhet av risker. Alltså hot som kan komma att hända, hur stor sannolikhet det är att de inträffar samt vad konsekvensen skulle bli (MSB, 2011c). En riskanalys inkluderar även delen att ta fram lämpliga åtgärdsförslag (MSB, 2011c). Med det menas att se över vilka åtgärder som behövs för att eliminera sannolikheten att ett hot inträffar. En åtgärd kan exempelvis vara att installera UPS för att undvika att en server stängs av vid ett fysiskt hot som strömavbrott orsakat av åska.

2.4 ISO-27002 och gapanalys

En gapanalys innebär granskning av en verksamhets säkerhetsarbete. Vid en sådan analys jämförs verksamhetens befintliga skydd med de rekommendationer som finns i en standard (MSB, 2011a). En gapanalys syftar till att ange gapet mellan standardens rekommendationer och de skyddsåtgärder som verksamheten tillhandahållit (MSB, 2011a). Detta gap ger en bild av säkerhetsarbetet i verksamheten och det finns många standarder som verksamheter kan använda sig av för att granska sitt säkerhetsarbete. Arbetet med informationssäkerhet kan ske utifrån en standard men också utifrån ett ramverk. Vad som skiljer dessa åt förklaras i nedanstående stycke.

2.4.1 Standarder och ramverk

MSB (2011d, s. 4) skriver: *”Alla verksamheter behöver säker information”*. För att uppnå säker information kan en verksamhet arbeta utifrån en standard så som ISO-27002 som anger rekommendationer om vad som bör ses över inom informationssäkerhetsarbetet. Serien ISO-27000 innehåller flera standarder för just informationssäkerhet där ISO-27002 är en standard. ISO-27000 är en serie standarder som tagits fram av ISO/IEC där organisationer har samlat in erfarenheter av arbete med just informationssäkerhet (MSB, 2011d). Standarderna i sig anger vad en verksamhet bör göra inom arbetet med informationssäkerhet. MSB (2010b) skriver följande om standarder: *”De anger krav och riktlinjer som är användbara för alla typer av organisationer. Verksamheter får möjligheter att arbeta utifrån beprövade erfarenheter och då enklare skapa förutsättningar för bättre säkerhet”*.

För att arbeta med informationssäkerhet kan ett ledningssystem för informationssäkerhet (LIS) införas. LIS handlar om hur informationssäkerhet i en verksamhet styrs. MSB (2011d, s. 4) skriver: ”*Alla organisationer har ett ledningssystem, eller ett ”system” för att leda verksamheter. Det handlar helt enkelt om hur ledningen styr verksamheten”*. Den engelska benämningen för LIS är Information security management systems (ISMS) och är alltså standarderna ISO-27000 (ISO, 2011). I denna rapport betecknar LIS standarden ISO-27002 då detta arbete bygger på rekommendationer som finns angivna av just denna standard.

Istället för att följa och arbeta utifrån en standard kan verksamheter också följa Ramverket för informationssäkerhet. Ramverket kan användas som stöd för informationssäkerhetsarbetet vid införandet eller vid förbättring av LIS och ramverket har utgått från standarder i serien ISO-27000 (MSB, 2011d). Ett ramverks syfte är att hjälpa verksamheter att tolka information från en standard för att lättare kunna införa LIS i verksamheten. Ramverket innehåller då mallar och andra dokument som en verksamhet kan använda till arbetet med LIS. MSB (2011d, s. 12) skriver följande om Ramverket för informationssäkerhet: *”Ramverket beskriver en process och riktar sig till den som ska arbeta med informationssäkerhet i en verksamhet. Ramverket bygger på standarderna i 27000-serien”.*

Tidigare fanns även ett koncept inom informationssäkerhet som Krisberedskapsmyndigheten utvecklat. BITS står för Basnivå för informationssäkerhet och rekommendationerna inom detta koncept var mer inriktat på IT- och systemsäkerhet medan standarder i 27000-serien har mer fokus på just informationssäkerhet (MSB, 2011d).

Det finns även utbildningsprogram inom informationssäkerhet för att öka kunskapen hos användare i en verksamhet. Ett utbildningsprogram som MSB tillhandahåller är DISA som står för Datorstödd informationssäkerhetsutbildning för användare. Detta utbildningsprogram kan användas i en verksamhet för att ge användare förståelse för vad informationssäkerhet är (MSB, 2010c).

Det finns olika delar att granska i en verksamhet där vissa anses som mer kritiska än andra. I denna rapport anges de rekommendationer som ISO-standarden 27002 har angett gällande fysisk och miljörelaterad säkerhet och dessa rekommendationer är tänkta att verksamheter ska se över och möjligtvis rikta sig efter. Standarden ISO-27002 innehåller flera krav och riktlinjer över delar som verksamheter bör se över gällande sitt säkerhetsarbete. Standarden inkluderar delar som säkerhetspolicy, hantering av tillgångar, personal och säkerhet, styrning av åtkomst med flera (MSB, 2011b). En del som standarden anger är fysisk och miljörelaterad säkerhet och dess rekommendationer som bör ses över i en verksamhet.

2.4.2 Fysisk och miljörelaterad säkerhet

I detta stycke beskrivs de rekommendationer som ISO-27002 angett att se över inom delen fysisk och miljörelaterad säkerhet (MSB, 2011b). Alla dessa punkter bidrar till informationssäkerhet då hot mot den fysiska säkerheten kan realiseras om inte skyddsåtgärder finns.

De rekommendationer som finns inom detta område ligger indelat under *säkrade utrymmen* och *skydd av utrustning*.

Målet med säkrade utrymmen är att undvika att obehöriga personer tar sig in i utrymmen där information finns att tillgå. Ett annat mål är att säkrade utrymmen ska skydda mot fysiska hot och skador som kan komma att uppstå (MSB, 2011b).

Målet med skydd av utrustning är att försöka förhindra att information stjäls, förstörs eller påverkas av obehöriga personer eller av fysiska hot. Detta handlar om att skydda sin utrustning, både inom och utanför verksamhetens lokaler, dels från obehörig åtkomst. Ett annat mål är att avveckla utrustningen på lämpligt sätt så att information inte kan kommas åt av obehöriga efter att utrustning har slängts eller återvunnits (MSB, 2011b).

Säkrade utrymmen inkluderar följande enligt MSB (2011b):

- Skalskydd
- Tillträdeskontroll
- Skydd av kontor, rum och faciliteter
- Skydd mot externa hot och miljöhot
- Arbete i säkra utrymmen
- Allmänhetens tillträdes, leverans- och lastutrymmen

Skalskydd innefattar golv, väggar och tak för att skydda informationstillgångar mot fysiska hot. Det vill säga säkrade utrymmen där utrustning finns som måste skyddas. Detta skydd anser MSB (2011b) vara en kritisk säkerhetsåtgärd då det är lättare att stjäla och skada utrustning om skalskydd kring utrymmet saknas. Skalskydd innebär att ha en eller flera säkerhetsspärrar för att ta sig in i vissa utrymmen. Genom att ha flera spärrar skyddas utrustningen som så att den inte görs tillgänglig direkt om någon tar sig igenom första spärren. Ett låsbart rum är exempel på skalskydd då låset tillsammans med väggar och dörrar utgör ett säkrat utrymme. Ibland kan även andra åtkomstkontroller behövas tillsammans med skalskydd för att förhindra obehörig åtkomst (MSB, 2011b). Saknas skalskydd kring informationstillgångar kan information lättare utsättas för fysiska hot.

Tillträdeskontroll innebär behörighetskontroll, det vill säga att endast behöriga personer ska få tillgång till säkrade utrymmen. Denna faktor anses som en kritisk säkerhetsåtgärd av samma orsak som föregående rekommendation (skalskydd). Om obehöriga personer får komma in i säkrade utrymmen kan utrustning och information skadas eller stjälas (MSB, 2011b).

Skydd av kontor, rum och faciliteter innebär att utrymmen bör placeras med fysisk säkerhet i åtanke. Detta anses inte som någon kritisk säkerhetsåtgärd men det är bra att tänka på då obehöriga ska hållas borta från utrymmen där behandling av information sker. Detta för att obehöriga inte ska kunna utnyttja informationstillgångar och påverka befintlig information. Om utrymmen placeras utan fysisk säkerhet i åtanke kan obehöriga personer ta sig till platser där informationstillgångar finns och på så sätt utgöra ett fysiskt hot mot informationssäkerheten (MSB, 2011b).

Skydd mot externa hot och miljöhot anses vara en kritisk säkerhetsåtgärd då detta handlar om att skydda verksamheten mot naturkatastrofer så som brand, åska, översvämning, jordbävning och upplopp. Dessa hot anses kritiska då en katastrof kan uppstå plötsligt och utan förvarning och kan innebära att information och utrustning kan förstöras. Naturkatastrofer kan inte bara innebära hot mot den fysiska säkerheten utan kan också vara farliga för personal. Om fysiska katastrofer inträffar kan information lagrad i hårdvara förstöras och på så sätt bli otillgängligt för verksamhetens fortsatta arbete (MSB, 2011b).

Arbete i säkra utrymmen innebär att det bör finnas fysiskt skydd samt regler och riktlinjer för hur arbete får utföras inom ett säkrat utrymme. Detta är viktigt för säkerheten kring personal och information. Att ha klara regler för vad som gäller i ett visst utrymme är att föredra för att exempelvis undvika att information görs tillgänglig eller avslöjas för obehöriga. Detta anses dock inte som någon kritisk säkerhetsåtgärd men är en del av arbetet för att upprätthålla fysisk säkerhet gällande informationssäkerhet (MSB, 2011b).

Allmänhetens tillträdes, leverans- och lastutrymmen är den sista delen under säkrade utrymmen. Denna anses inte som kritisk men är bra att se över då det handlar om huruvida exempelvis lastutrymmen övervakas. Då det kommer in obehöriga personer vid sådana utrymmen bör informationstillgångar skyddas så att dessa personer inte får åtkomst till tillgångarna. Om tillgångar inte skyddas eller övervakas kan obehöriga, obevakat ta sig in på områden där vistelse inte får ske och på så sätt utgöra fysiskt hot mot information och utrustning (MSB, 2011b).

Skydd av utrustning inkluderar följande enligt MSB (2011b):

- Placering av skydd och utrustning
- Tekniska försörjningssystem
- Kablageskydd
- Underhåll av utrustning
- Säkerhet för utrustning utanför egna lokaler
- Säker avveckling eller återanvändning av utrustning
- Avlägsnande av egendom

Placering av skydd och utrustning innebär att utrustningen ska skyddas och placeras på bästa sätt för att undvika att obehöriga personer får åtkomst till utrustningen. Dessutom bör utrustningen skyddas från miljörelaterade och fysiska hot. Detta anses inte som en kritisk säkerhetsåtgärd men om utrustningen inte skyddas från dessa hot ökar sannolikheten att information förstörs om ett hot realiseras (MSB, 2011b).

Tekniska försörjningssystem handlar om att skydda utrustning från fysiska hot som strömavbrott och spänningsförändringar. Då tekniska system som hårdvara behöver ström hela tiden för att fungera är det bra att se över vad som händer om exempelvis ett strömavbrott inträffar. Detta är ingen kritisk säkerhetsåtgärd men om strömmen plötsligt bryts till en hårdvara kan information komma att förloras. Dessutom kan informationstillgången skadas och informationen i resursen blir otillgänglig under en viss tid (MSB, 2011b).

Kablageskydd handlar om att se över vilken form av kablar som används. Då kablar används för överföring av data kan trafik över dessa kablar avlyssnas av obehöriga. Detta är ingen kritisk säkerhetsåtgärd men då avlyssning kan ske innebär detta ett hot mot verksamheten då information kan komma att läsas av obehöriga (MSB, 2011b).

Underhåll av utrustning innebär att utrustning som används bör underhållas för att fortsätta tillhandahålla tillgänglighet och riktighet. Tillgänglighet och riktighet är två egenskaper informationssäkerhet ska uppnå. Detta anses inte som en kritisk säkerhetsåtgärd men om utrustning inte underhålls kan denna sluta fungera och informationen blir då otillgänglig (MSB, 2011b).

Säkerhet för utrustning utanför egna lokaler handlar om vad som sker när arbete utanför verksamhetens lokaler inträffar. Detta är ingen kritisk säkerhetsåtgärd men bör ses över. Många anställda tar med sina laptops hem och fortsätter arbeta och det är då bra att vara medveten om de risker som kan inträffa på platser utanför verksamhetens lokaler. Detta för

att arbete på annan plats medför säkerhetsrisker då information och informationstillgångar kan stjälas eller läsas och spridas av obehöriga. Stöld är ett fysiskt hot som orsakas av mänsklig åverkan. Om inte säkerheten utanför egna lokaler ses över kan information komma i orätta händer om exempelvis en laptop stjäls från en anställd. Utrustning som används utanför verksamhetens lokaler innefattar både laptops, mobiltelefoner, kalendrar och andra dokument (MSB, 2011b).

Säker avveckling eller återanvändning av utrustning handlar om att ta bort all information från utrustning som inte ska användas längre. Dels utrustning som ska avvecklas och slängas, och dels utrustning som ska återanvändas. Att ta bort viktig, känslig information från utrustningen är viktigt då ingen annan ska kunna läsa det. Denna säkerhetsåtgärd anses vara kritisk då risken för att känslig information kommer i orätta händer ökar om inte informationen tas bort på ett säkert sätt. Genom att ge obehöriga personer fysisk tillgång till lagringsmedium kan åtkomst till information ges om inte denna tagits bort. Därför är det också viktigt att tänka på vart utrustning slängs när den inte ska användas längre. Att slänga en hårddisk i en container som innehållet inte blivit raderat på ökar risken för att en obehörig person tar upp och läser denna (MSB, 2011b).

Avlägsnande av egendom hänger ihop med föregående punkt (säker avveckling eller återanvändning av utrustning) och innebär att utrustning inte ska slängas om inte informationen på utrustningen först blivit borttagen. Detta är ingen kritisk säkerhetsåtgärd men risken ökar för att information avslöjas för obehöriga om informationen inte raderas innan (MSB, 2011b).

3 Problem

Problemet är att fysisk säkerhet lätt kan glömmas av när säkerhet kring IT är i fokus. Det finns många hot som existerar kring IT, både fysiska som nätverksbaserade. Ofta underskattas den fysiska säkerheten då tankar som ”det händer inte oss” och mer energi läggs istället på hot som relaterar till nätverket, så som virus, trojaner och annan skadlig kod (SearchSecurity, 2005).

Erbschloe (2005, s. 2) skriver *”physical security is important for several reasons”*.

Erbschloe (2005) menar att fysisk säkerhet är minst lika viktig som nätverkssäkerhet. Mycket energi läggs på nätverkssäkerheten och den fysiska säkerheten kan lätt falla bort. Fysiska hot som bränder och sabotage kan vara svårare att återhämta sig från jämfört med vad en attack över nätverket kan vara och därför bör den fysiska säkerheten ses över och undersökas (Erbschloe, 2005). Som systemadministratör är det viktigt att vara medveten om den fysiska säkerheten inom informationssäkerhet för att kunna undvika att fysiska hot realiseras. Att ha koll på vem som är inne i ett serverrum och vad denna person gör är viktigt ur flera aspekter då både interna anställda och externa, obehöriga personer kan utgöra ett stort hot mot informationstillgångarna. En systemadministratör bör ha kunskap om den fysiska säkerheten då informationstillgångar annars kan exponeras för hot. Ett serverrum ska ha god fysisk säkerhet utan att hindra en systemadministratörs arbete och åtkomst ska endast ges till de som är behöriga (Limoncelli, Hogan & Chalup, 2007). Fysisk säkerhet är viktigt ur flera synpunkter. Dels är det kostsamt att skaffa och installera hårdvara så att den fungerar för verksamheten, dels är aktiviteter i en verksamhet beroende av teknologi och går hårdvaran ner över en dag blir verksamhetens arbete lidande (Erbschloe, 2005). En systemadministratör är i en unik position för att kunna upptäcka om ett fysiskt hot realiseras. Detta genom att en systemadministratör kan upptäcka att en hårddisk har stulits eller utsatts för annat fysiskt hot (Allen, 2001).

Frågan är om verksamheter är medvetna om vad fysisk säkerhet innebär kring dess datautrustning. Vet de vad fysiska hot är? En verksamhet bör ha en säkerhetspolicy som övergripande beskriver säkerhetsarbetet i verksamheten (Pfleeger & Pfleeger, 2006). En riskanalys handlar om att identifiera de hot som finns mot verksamheten och hur stor sannolikhet det är att ett givet hot realiseras och vad dess konsekvens i så fall skulle bli. Det är viktigt att inse att fysisk säkerhet bidrar till säkerhetsarbetet och att denna del är lika viktig som de andra delarna att se över. Finns fysisk tillgång till utrustningen kan övriga skydd lätt undvikas. Bara genom att använda ett USB-minne kan mycket information överföras av obehörig person och på så sätt komma i orätta händer. Om en vattenledning i taket ovanför ett serverrum går sönder kan hårdvara och information förstöras. Att skydda serverrummet från obehörig tillgång och naturkatastrofer anses viktiga i en standard som ISO-27002 (MSB, 2011b). Om ett hot ändå realiseras är det bra att ha någon form av kontinuitetsplanering som anger vad som ska hända. Så som att ha backuper på en annan geografisk plats kan vara bra att tänka på då en brand faktiskt kan förstöra ett helt serverrum. En backup innebär att ha en kopia av den data som anses viktig att lagra. Det bör finnas information om hur anställdas laptops ska skyddas från exempelvis stöld och sabotage då en laptop är lätt att plocka med sig om obehörig tillgång ges (MSB, 2011b).

Är den fysiska säkerheten kring information och datautrustning något som verksamheter lägger ner tid på? Om inte verksamheter är medvetna om den fysiska säkerheten medför det

brister i skyddet av information. Detta är ett problem då verksamheten ökar sannolikheten att hårdvara och innehållande information förstörs om en incident inträffar. Den fysiska säkerheten kan lätt nonchaleras (LabCenter, 2009).

Om brist i skyddet saknas kring fysisk och miljörelaterad säkerhet ökar risken för att hot realiseras. Genom att göra en gapanalys och jämföra det befintliga säkerhetsarbetet i verksamheten med riktlinjer enligt ISO-27002 kan en verksamhet få en uppfattning av hur deras säkerhet ligger till och vad som möjligtvis bör förbättras enligt riktlinjerna (MSB, 2011a). I denna rapport kommer ett mindre antal verksamheter intervjuas för att se hur väl granskat deras säkerhetsarbete är kring miljörelaterad och fysisk säkerhet, jämfört med vad rekommendationerna som MSB (2011b) anger utifrån standarden ISO-27002.

Jones (2005, s. 4) skriver följande:

"Physical security is important – leaving the data center unlocked leaves your servers as open to attack as leaving the firewall open; allowing someone to walk away with a server's removable hard drive defeats the purpose of file-and-folder security, password management, and network security.

(...)

However, the physical security of data is often overlooked."

Här visas tydligt, som i flera andra böcker och artiklar, att fysisk säkerhet faktiskt är viktigt att se över och får inte glömmas bort. Oavsett hur bra nätverkssäkerhet en verksamhet har kan denna förbises om en attackerare får fysisk tillgång till hårddisken (Jones, 2005).

3.1 Problemprecisering

Den huvudsakliga frågan i denna rapport är:

Hur väl förberedda är verksamheter inom den offentliga sektorn för de rekommendationer som finns angivna av standarden ISO-27002 kring fysisk och miljörelaterad säkerhet rörande informationssäkerhet?

Vissa verksamheter kan möjligtvis vara certifierade enligt ISO-27002 och bör då efterfölja de rekommendationer som angetts i standarden. Andra verksamheter kanske följer en annan standard och är inte medvetna om de riktlinjer som MSB (2011b) enligt ISO-27002 tar upp kring fysisk och miljörelaterad säkerhet.

3.2 Avgränsning

I denna rapport kommer ett mindre antal verksamheter inom den offentliga sektorn, i detta fall kommuner, att intervjuas. Anledningen till att kommuner har valts ut är att kommuner är en viktig instans i dagens samhälle. En kommun ansvarar för lagring av information åt många förvaltningar och omsorger som både hanterar konfidentiell och icke-konfidentiell information. Att skydda informationen mot hot anses viktigt för att informationen inte ska komma i orätta händer eller förstöras. En kommun som hanterar information åt både skolor, vård- och omsorg samt andra förvaltningar måste skydda informationstillgångarna mot hot, däribland fysiska hot. Denna rapport handlar om hur kommuner riktar sig efter de rekommendationer som finns i ISO-27002 om fysisk och miljörelaterad säkerhet.

Kommunerna har en egen IT-avdelning och frågan är hur den fysiska säkerheten ser ut kring skyddet av informationstillgångar.

Ytterligare en anledning till att denna undersökning kommer att rikta sig till kommuner är att det kan bli svårt att jämföra de svar som fås från kommuner med svar från andra verksamheter (exempelvis företag). Att hålla sig inom ett område känns relevant för att få ett bra resultat.

3.3 Förväntat resultat

Ett förväntat resultat med detta arbete är att få en bild av hur några kommuner i en offentlig verksamhet hanterar fysisk säkerhet inom informationssäkerhet. Resultatet syftar till att visa hur verksamheter tänkt kring de olika rekommendationerna som ISO-standarden anger som viktiga att se över. Genom en intervju med respektive kommun kommer medvetenheten kring den fysiska säkerheten inom informationssäkerhet förhoppningsvis att öka. Detta arbete kommer även att uppmuntra verksamheter att följa de rekommendationer som finns i standarder och andra koncept.

Ett annat resultat som förväntas är att se hur väl litteraturen stämmer överens med praktiken. I litteratur står det att den fysiska säkerheten ofta är förbisedd och lätt nonchaleras. Hur det är i praktiken återstår nu att se.

4 Metod

Det finns olika metoder som kan användas för att undersöka hur väl verksamheter efterföljer de rekommendationer som MSB enligt ISO-27002 anger. Då detta handlar om hur säkerhetsarbetet kring fysisk säkerhet bedrivs inom verksamheter måste verksamheter inkluderas i undersökningen.

En ren *litteraturundersökning* där vetenskap om säkerhetsarbetet i verksamheter fungerar är inte att föredra då arbetet i sig grundar sig på att förstå och ta reda på hur verksamheter ställer sig till de rekommendationer ISO-27002 anger. Det kan vara svårt att finna information i litteratur om detta och därför kommer kontakt tas med ett antal verksamheter istället. Nedan ses olika metoder för tillvägagångssätt samt val av metod vid denna undersökning.

Det finns två typer av undersökningar; kvalitativ och kvantitativ (Trost, 1994). Kortfattat innebär kvalitativa undersökningar att sammanfattade och enkla frågor framställs och att den utvalda svarsperson ger mycket information som svar. Dessa undersökningar ger innehållsrik information och intressanta svar att bearbeta (Trost, 1994). En kvalitativ undersökning kan användas om ökad förståelse önskas inom ett område. Enligt Trost (1994, s. 22) handlar kvantitativ undersökning om frågeställningen *”hur ofta, hur många eller hur vanligt”* någonting är. Denna kvantitativa metod kan exempelvis användas då någonting ska beräknas.

4.1 Enkätundersökning

En metod som *enkätundersökning* skulle kunna användas för en sådan här undersökning. En enkät skickas till en verksamhet och en person inom området blir tilldelad att svara på innehållande frågor. En enkät består av ett antal frågor där angivna svar kan kryssas i och personen i fråga får kryssa i det alternativ som stämmer mest överens med hur säkerhetsarbetet ser ut i verksamheten. En enkät kan bestå av få eller många frågor och kan på så sätt ta olika lång tid att besvara (Kylén, 2004). Redan definierade svar som ska kryssas i av användaren är bra då vissa personer har dålig handstil. Personen som ska tolka svaren behöver inte lägga energi på att förstå det som står utan kollar bara vilket alternativ som är ikryssat (Trost, 1994). Vid en enkätundersökning måste ett urval göras för att begränsa vem enkäterna ska skickas till. Antalet deltagande i enkätundersökningen utgör underlag för vidare analys och det är därför viktigt att ett minimun antal svar fås på enkäten (Trost, 1994).

Innan en enkät skickas ut, eller i samband med att enkäten skickas, bör det finnas en inledning till varför enkäten är viktig, vad den ska användas till och resultera i. Detta för att skapa intresse att vilja besvara frågorna i enkäten (Kylén, 2004).

Denna metod kommer inte att implementeras i denna rapport. Detta på grund av att svaren kan bli kortfattade då de inte säger mer än det alternativ som redan var fördefinierat. Det är svårt att ställa följfrågor vid en enkätundersökning då frågorna måste vara klara innan en enkät skickas ut. Om inte en enkät riktas till en större grupp urval kan mycket bortfall ske vilket bidrar till dåligt underlag för undersökningen (Trost, 1994).

4.2 Intervjuer

En annan metod är att genomföra *intervjuer* med verksamheter. Intervjuer genomförs med en utvald person från verksamheten som är kunnig inom området. Ett antal förberedda frågor ställs till denna person för att få reda på information om ämnet och intervjuaren antecknar svaren som sedan behövs för vidare undersökning (Kylén, 2004).

En intervju kan vara både korta och långa, allt från fem minuter till flera timmar och tiden intervjun varar anpassas till området intervjun handlar om. Vissa intervjuområden är väl avgränsade och tar då inte så lång tid att få information om medan andra områden är bredare och behöver mer tid för undersökning. En vanlig tid för intervju är en timma (Kylén, 2004).

Intervjuer kan antingen vara öppna och ostrukturerade eller strukturerade. I en öppen och ostrukturerad intervju ställer intervjuaren frågor som intervjuobjektet kan berätta fritt om för att där i ge svar på den fråga som ställdes. Detta ger mycket information att bearbeta för att få ut ett svar på frågan. Strukturerade intervjuer är inte lika fria som ostrukturerade. I en strukturerad intervju ställs klara och tydliga frågor för att få mindre långa, berättande svar och därmed mindre information att bearbeta för att komma fram till svaret på frågan. En strukturerad intervju bygger på färdiga frågor som ska besvaras klart och tydligt. En strukturerad intervju styrs och läggs upp av intervjuaren medan en ostrukturerad intervju mer styrs utifrån intervjuobjektet (Kylén, 2004). Vid en ostrukturerad intervju kan en *intervjuguide* användas. En intervjuguide består av fyra till sex huvudområden som ska täckas in i intervjun och dessa punkter bör visas för den intervjuade. Detta för att det ska finnas ett stöd till intervjun och inte glömma av vad det är intervjun ska syfta till. Vid en strukturerad intervju används en *frågelista* istället för en intervjuguide. En frågelista består av färdiga frågor som ska ställas till den intervjuade. Dessa frågor ger svar som antecknas ner av den som intervjuar (Kylén, 2004).

Vid en kvalitativ intervju ska personen som intervjuar tänka på att ställa frågor som ger berättande svar. Detta för att få mycket information som underlag till arbetet. Innan en intervju måste frågor som tystnadsplikt avgöras, det vill säga om arbetet intervjun ligger som grund till ska anses vara hemligt eller inte. Kan namnet på den verksamhet som har valts att intervjua publiceras eller hemlighetshållas? (Trost, 1997).

En intervju kan bedrivas på olika sätt; *parintervju*, *gruppintervju* samt *panelintervju* (Kylén, 2004). En parintervju innebär att det är två personer som närvarar, det vill säga en som intervjuar och en som blir intervjuad. Vid en gruppintervju är det en person som intervjuar flera personer, detta innebär en intervjuare och flera intervjuade. Vid en gruppintervju intervjuas flera personer som är kunniga inom områden som anses relevanta för undersökningen. En panelintervju är tvärtom mot gruppintervju, alltså flera personer som intervjuar och en person som blir intervjuad. Tanken med en panelintervju är att flera personer ska kunna anteckna och bättre förstå det som intervjuobjektet säger då alla intervjuare inte hör samma saker (Kylén, 2004).

4.3 Val av metod

Då en intervju ger innehållsrika svar på frågor kommer denna metod implementeras i denna rapport (Trost, 1997). På grund av arbetets omfattning kommer ett mindre antal verksamheter (fem kommuner) intervjuas för att ta reda på hur väl de följer de rekommendationer som anges i ISO-standarden 27002 angående fysisk och miljörelaterad

säkerhet. Intervjuerna syftar till att se hur kunniga och väl medvetna verksamheter är gällande den fysiska säkerheten och hur de gjort för att uppnå de rekommendationer som finns angivna i standarden ISO-27002.

Då denna rapport syftar till att ge ökad förståelse för hur fysisk säkerhet implementeras i kommuner kommer kvalitativa intervjuer ske. Detta eftersom kvalitativa intervjuer handlar om att förstå och finna mer information om ett ämne (Trost, 1997).

Detta arbete kommer förhoppningsvis påverkas positivt av metoden *intervju*. Då den fysiska säkerheten inom informationssäkerhet ska undersökas på utvalda kommuner är det viktigt att få ut nyttig information som går att analysera. Då intervjuer ger mycket svar att bearbeta känns detta som en mer relevant metod för att uppnå ett intressant resultat av detta arbete. Intervjuer kan ske i form av möten eller per telefon men då det är svårt att gå in på djupet vid en telefonintervju kommer ett möte ske med respektive kommun i denna undersökning (Kylén, 2004). Intervjuerna med kommunerna kommer att vara av typen parintervju samt strukturerade då klara och tydliga frågor kommer ställas som intervjuobjektet får svara på. Valet att använda strukturerade intervjuer beror på att dessa ger specifika svar för området frågorna ställs kring.

4.4 Genomförande

I denna undersökning kommer fem stycken intervjuer att ske, en intervju för varje kommun. Intervjuerna kommer ske med olika representanter inom verksamheten. Då intervjuerna med varje kommun skulle bokas ringdes IT-chefen i varje kommun upp. IT-chefen valdes att tala med eftersom det är denna person som har det övergripande ansvaret över den avdelning där känsliga informationstillgångar, så som serverrum, hanteras och skyddas. Det är också IT-avdelningen som ger nyanställda en dator och supportar användare gällande IT-relaterade frågor. IT-chefen i varje kommun har fått bedöma vem som kan berätta om kommunens informationssäkerhet med den fysiska säkerheten i fokus. De representanter som IT-chefen i varje kommun bedömt lämplig för denna undersökning har titel som IT-chef, IT-tekniker samt E-strateg med roll som Informationssäkerhetsansvarig. Att olika personer kommer intervjuas beror på vem som anses ha mest kunskap inom ämnet. Vissa IT-chefer anser att de själva kan mest om den fysiska säkerheten inom informationssäkerhet medan andra IT-chefer anser att detta är en IT-teknikers uppgift att ha koll på. Andra verksamheter har en person som är ansvarig för just informationssäkerhet och IT-chefen anser då att det är lämpligast att intervjua denna person. Oavsett vilken titel intervjuobjektet har så är det IT-chefen i samtliga verksamheter som hänvisat till vilken person som är lämplig att intervjua.

Intervjufrågor som skapas kommer delas in i tre kategorier; *inledning*, *allmänt* och *rekommendationer i ISO-27002*. Detta för att en inledande fråga ger en beskrivning av den person som intervjuas och hur det kommer sig att personen arbetar på just den specifika kommunen. Genom en persons bakgrundsbeskrivning kan en ökad förståelse fås till de svar som framkommer på kommande frågor och vilken relation och kunskap personen har till just informationssäkerhet. Efter den inledande frågan kommer ett antal frågor under kategorin *allmänt* ställas och dessa frågor är tänkta att ge ett underlag till analys av hur medveten kommunen är om standarder inom informationssäkerhet och hur väl den valda standarden efterföljs. Kategorin *rekommendationer i ISO-27002* innehåller en huvudfråga per rekommendation i standarden ISO-27002. Denna kategori har tagits fram för att kunna

besvara den huvudsakliga frågan i denna rapport. Genom att ställa en fråga per rekommendationen ges ökad kunskap om hur väl förberedda kommunerna är kring de rekommendationer som ISO-27002 tar upp angående fysisk och miljörelaterad säkerhet inom informationssäkerhet.

Svaren som framkommer vid varje fråga kommer analyseras närmare för att ge svar på hur väl medvetna kommuner är om standarder då de själva får berätta om den standard de efterföljer. Därefter kommer efterföljande av standarden analyseras då svar på intervjufrågor ger en bild av hur kommunen arbetar med sitt informationssäkerhetsarbete utifrån den valda standarden. En annan punkt som kommer analyseras är vem/vad som påverkar de beslut som tas gällande informationssäkerheten. Påverkas besluten av standardens rekommendationer eller påverkas de istället av något som någon säger? Till sist kommer även framtiden på kommunerna att analyseras. Hur informationssäkerheten är tänkt att vidareutvecklas och hur kommer arbetet i fortsättningen bedrivas. Dessa analyser har tagits fram utifrån de frågekategorier som intervjufrågorna ska vara indelade under och analyserna kommer ske utifrån den information som framkommer vid intervjuerna.

5 Resultat

En intervju har genomförts med respektive kommun för att undersöka hur väl rekommendationerna i ISO-standarden 27002 angående fysisk och miljörelaterad säkerhet efterföljs. Ett antal frågor har formulerats och ställts till en utvald person i respektive kommun och nedan kommer varje fråga presenteras följt av de svar som framkom vid intervjuerna.

Totalt har fem intervjuer genomförts, en intervju per kommun. I varje kommun har intervjun skett med en person som varit kunnig inom ämnet *fysisk säkerhet inom informationssäkerhet*. Titel på intervjuobjektet har därför varierat mellan IT-chef, IT-tekniker samt E-strateg med roll som Informationssäkerhetsansvarig.

5.1 Intervjufrågor och svar

Nedan presenteras varje intervjufråga och under visas den information som framkom vid varje intervju. Ur säkerhetssynpunkt kommer inga namn att nämnas i rapporten utan kommunerna anges: Kommun A, Kommun B, Kommun C, Kommun D samt Kommun E. Om begreppet Person används kommer denna person betecknas med samma bokstav som den kommun personen arbetar på. Denna person betecknar alltså intervjuobjektet på kommunen. Exempelvis tillhör Person A till Kommun A.

Samtliga intervjuer har skett med en kommun och kommunerna kommer inte beskrivas närmare. Detta för att inte hänga ut någon av kommunerna och göra dessa spårbara. Vid varje intervju har information lämnats om att intervjuobjektet inte behöver svara på samtliga frågor och att personen får avbryta när som helst. Subjekten har också informerats om att inga namn kommer nämnas i rapporten, varken intervjuobjektets namn eller kommunens namn.

Samma frågor, totalt 20 stycken huvudfrågor, har ställts vid varje intervju och som en inledning har varje intervjuobjekt fått berätta om sig själv och varför personen just arbetar på kommunen. Efter den inledande frågan ställdes ett antal allmänna frågor inom informationssäkerhet och därefter ställdes en huvudfråga per rekommendation enligt ISO-standarden 27002. Intervjuerna har varierat i tid men samtliga intervjuer har varit mellan en och två timmar.

5.1.1 Inledning, fråga 1

Denna fråga har ställts till varje kommun som en inledning till intervjun.

Inledning:

1. *Kan du berätta om dig själv och din bakgrund och hur kommer det sig att du arbetar här?*

Svaret på denna fråga har varierat. Några personer har utbildning inom området IT och andra personer har ingen utbildning men dock arbetslivserfarenhet och intresse inom ämnet.

Kommun A: Person A är utbildad inom sjukvård och även utbildad lärare. Har arbetat inom vården och därefter som högskolelärare. Personen såg sedan att IT växte mer och mer och tog

därefter högskoleexamen inom Informatik som sedan slutade med en tjänst i denna kommun. Titeln är IT-chef.

Kommun B: Person B har högskoleutbildning inom Datalogistik med inriktning mot systemvetenskapliga kurser och betecknar sig själv som Systemvetare men utan ekonomidelen. Personen har arbetat inom Kommun B en längre tid och har vidareutvecklats och bytt titel flertalet gånger. Nu är titeln E-strateg där en av arbetsuppgifterna är just informationssäkerhet.

Kommun C: Person C som medverkar vid denna intervju har en treårig högskoleutbildning som Systemprogrammerare vilket personen sedan arbetat som en kortare tid efter utbildningen. Efter detta uppstod möjligheten till arbete som IT-samordnare i hemkommunen som personen sökte och fick. Så småningom blev titeln istället IT-chef vilket är titeln idag.

Kommun D: Person D började intressera sig för IT i tidig ålder men har ingen eftergymnasial utbildning inom ämnet. Intresset har hållit sig genom livet och efter gymnasiet fick personen själv utbilda andra inom IT-relaterade ämnen. När tjänsten som IT-tekniker inom kommun D dök upp ansågs denna passande och personen har sedan läst fristående kurser på högskola för att få en mer teoretisk bakgrund.

Kommun E: Person E började sin karriär som reklamägare följt av journalist. Personen har ingen akademisk utbildning men har ett intresse inom IT och stor kunskap om projektledning. Efter arbetet som journalist arbetade personen som IT-chef i en annan kommun som sedan ledde vidare till tjänsten som IT-chef i nuvarande kommun.

5.1.2 Allmänt, fråga 2 – 7

Nedan presenteras de frågor och svar som ställdes till varje kommun om hur de hanterar sitt informationssäkerhetsarbete.

Allmänt:

2. *Vilken/vilka standarder eller riktlinjer arbetar ni utifrån? Kan du berätta om varför ni valt just denna standard?*

Kommun A: Personen på Kommun A berättar att kommunen från början arbetade utifrån FA22 som var framtagen av ÖCB (Överstyrelsen för Civil Beredskap). Person A säger *”alla våra planer och sånt är egentligen i grunden från den tiden”* och syftar till att deras nuvarande planer och dokument bygger på en genomgång som gjordes med hjälp av ÖCB och deras FA22. ÖCB bytte senare namn till MSB. Person A fortsätter berätta *”att det är mycket FA22 och så har vi modifierat lite utifrån BITS och nu tittar vi på det här med LIS då som är den nya ersättaren till BITS”*. Personen förklarar att BITS kan ses som en uppsnyggning av gamla FA22 där BITS ger rekommendationer på en mer detaljerad nivå, så som exempelvis lösenordslängder och hur lång tid det ska ta innan en skärmsläckare går igång på en dator. Vissa av dessa rekommendationer anses dock svårt att kunna tillämpa överallt då en skola inom en kommun inte behöver en skärmsläckare efter kort tid då en föreläsning inte ska avbrytas mitt i, medan en dator på en vårdinrättning inte ska stå öppen för länge innan en skärmsläckare startas. Person A säger *”det är svårt att ha samma principer på två så olika miljöer”*. BITS ersätts nu av LIS som står för Ledningssystem för Informationssäkerhet

och Person A upplever att mycket av den fysiska säkerheten har släppts i LIS och att konceptet nu fokuserar mer på informationssäkerheten överlag. Arbetet med LIS har ännu inte kommit igång men inom kort kommer MSB på besök och informerar om vad som nu ska gälla.

Kommun B: Denna kommun arbetar också utifrån BITS som står för Basnivå för Informationssäkerhet. BITS valdes att arbeta utifrån då det är en vanlig standard inom kommuner. Arbetet med BITS påbörjades kring år 2004/2005 men arbetet blev aldrig klart och togs åter upp igen någonstans mellan 2007 och 2009. Mallarna som använts för säkerhetsarbetet har nu förändrats då BITS har ersatts av en annan standard. Kommunen kommer nu istället följa ett annat koncept från MSB som heter DISA och står för Datorstödd Informationssäkerhetsutbildning för Användare.

Kommun C: Kommun C använder sig av konceptet BITS som är ett verktyg som MSB har tillhandahållit. Arbetet med BITS påbörjades för ungefär två år sedan tillsammans med säkerhetssamordnare men arbetet blev aldrig färdigt. BITS har gåtts igenom men alla dokument som verksamheten behöver har inte ännu tagits fram. Person C berättar att själva ansvaret för IT-säkerheten ligger på IT-enheten och säger att *"vi måste koncentrera oss på driftsfrågor liksom när vi har så begränsade resurser"*. Person C fortsätter sedan med *"IT-säkerheten alltså den, den kommer i andra hand tyvärr"*.

Kommun D: Även denna kommun har baserat sitt säkerhetsarbete på BITS men kommunen kommer nu, i samarbete med en närliggande kommun, att följa efterträdaren LIS. Kommunen följer inte andra ramverk så som ITIL. Hur det kommer sig att kommunen följer just BITS kan personen inte svara på mer än att BITS är en vanlig standard för kommuner att följa och MSB gav rådet till kommuner att följa just BITS.

Kommun E: Precis som tidigare kommuner följer denna kommun konceptet BITS. Person E tycker att BITS fokuserar mycket på rutiner, ger vägledning och hjälper till med formulering och vad som ska täckas in. BITS som nu följs av LIS ska vara med inriktat på just informationssäkerheten och vårda just informationen. BITS har gåtts igenom av kommunen och dokument har skapats utifrån BITS men dessa dokument anses i behov av förbättring.

Allmänt:

3. *Arbetar ni med gapanalyser inom säkerhetsarbetet och hur långt har ni kommit med den?*

Kommun A: En gapanalys inom informationssäkerhet är inte gjort. Person A säger *"nåt så strukturerat som en sån grej är inte gjort"* och fortsätter berätta att den allra första genomgången av säkerhetsarbetet tillsammans med ÖCB:s FA22 var en typ av gapanalys. På den tiden sågs säkerheten över och dokument och planer skapades som sedan har modifierats och uppdaterats allt eftersom.

Kommun B: Person B förklarar att kommunen inte arbetar med gapanalyser men i en del av företagets säkerhetspolicy beskrivs vad som önskas uppnås med informationssäkerhetsarbetet och vad som redan är påbörjat arbete.

Kommun C: Person C är inte helt med på vad som menas med uttrycket gapanalys men då detta förklarats närmare svarar personen *"frågan är om inte det är en gapanalys egentligen*

man gör då när man går igenom det här… det här BITS-programmet". Personen fortsätter berätta att en bedömning har gjorts av hur väl kommunen efterföljer de rekommendationer som BITS tillhandahåller.

Kommun D: Person D berättar att kommunen inte gjort en gapanalys men att detta är tänkt att göras nu när LIS ska införas.

Kommun E: Vad gäller gapanalyser berättar Person E att detta inte är gjort inom kommunen. Personen säger *"inga gapanalyser tyvärr"*.

Allmänt:

4. *Hur är det med stöd från ledningen, politiskt stöd och finansiellt stöd för ert säkerhetsarbete för att kunna vidta skyddsåtgärder för exempelvis fysiska hot?*

Kommun A: Person A förklarar att pengar givetvis är en möjliggörare och ska någonting bli gjort måste säkerhetsfrågorna drivas framåt. Det är ingen annan som kommer och säger till vad som ska göras och inte göras. Person A berättar att det är lätt att driva en fråga framåt när det finns ett underliggande stöd för det. Ett exempel på det i denna kommun är när räddningsverket var på besök och erbjöd ett automatiskt släckningssystem till serverrummet. När politikerna sedan fick denna rekommendation med pris i handen är det svårt att säga nej till en sådan åtgärd då ingen vill ta ansvaret om all information totalförstörs i en brand för att det inte finns ett bra släckningssystem. Person A säger *"har man rätt argument är det inget svårt att få fram pengarna"*. Med andra ord finns stödet där om rätt argument framhävs. Dock måste argumenten vara trovärdiga då det är lätt i ett säkerhetsarbete att lägga på ett lager till, och ett lager till och trovärdigheten sänks då det blir svårt att bevisa att allt detta verkligen behövs.

Kommun B: Person B berättar att *"vi får inga centrala medel för att bekosta infrastruktur kring dem här datacenterhallarna då som vi har, utan det får vi själva bekosta"* och berättar vidare att det finns en katastrofgrupp som arbetar med att säkra upp samhällsviktiga punkter så som elnätet i kommunen. Men det finns inte någon i ledningen som säger vad som behöver göras.

Kommun C: Person C berättar att när det gäller skalskyddet och tillträdeskontroller ligger detta ansvaret på fastighetsavdelningen. Dessa skydd har det gjorts en satsning på med stöd från ledningen och därmed kunnats få fram pengar till.

Kommun D: Person D säger *"det har blivit jättemycket bättre, det här har ju vart totalt bortprioriterat under liksom 90-talet, även början av 2000-talet"* och menar att elektronik och IT inte ansågs lika viktigt då. Under 2006/2007 gick Krisberedskapsmyndigheten (nuvarande namn är MSB) ut och erbjöd stöd för kommunen att se över den fysiska säkerheten inom IT-säkerheten. Under denna tid åtgärdades många brister som kommunen då hade genom ombyggnationer och införande av flertalet säkerhetsåtgärder så som automatiskt släckningsutrustning i serverrummet. Brister och åtgärder rekommenderades av Krisberedskapsmyndigheten som kommunen köpte. Person D menar att stödet från ledningen ökade då en utomstående myndighet visade klart och tydligt alla brister som fanns och de åtgärder de kunde erbjuda.

Kommun E: Stöd från ledningen finns och Person E ingår i kommunkontorets ledningsgrupp där flertalet möten hålls per månad där bland annat säkerhetsarbetet tas upp. Politiskt stöd finns upplever IT-chefen. Finansiellt finns det stöd för säkerhetsarbetet men Person E förklarar att det är en balansgång med vad pengarna ska läggas på då det finns flertalet projekt som måste drivas i kommunen och allt kostar pengar.

Allmänt:

5. *Vad skulle du vilja ändra på och möjligtvis förbättra med ert befintliga säkerhetsarbete?*

Kommun A: Kring just den fysiska säkerheten finns det några saker som skulle kunna förbättras i denna kommun. Person A berättar att det i stadsnätet finns en del korskopplingsskåp som i sig inte är fysiskt säkra. Korskopplingsskåp innehåller både kablar och switchar som används för att koppla samman ett nät och för att kunna ge anslutning till kommunens platser. Person A säger *"där skulle jag önska att tillträdesskyddet var bättre och kanske att de vore larmade"*. Tyvärr anses detta svårt då det är många olika lokaler att se över. En annan sak som Person A skulle vilja förbättra säkerheten kring är fiberkablarna i marken. Säkerheten kring dessa skulle önskvärt kunna förbättras då en kabel kan grävas av.

Kommun B: Person B önskar vidareutveckla en nuvarande modell som de har för informationsklassning. Person B säger att *"vi har tagit datainspektionens definition bara då och sagt att känsliga personuppgifter är det här och om vi ska hantera dem krävs en tvåfaktorsinloggning, mer än så har vi inte gjort"* och fortsätter berätta om att det finns en matris för informationsklassning men att det är svårt att säga hur olika system och information ska hanteras. Personen nämner även att det vore önskvärt att utbilda personal om just informationssäkerhet för att uppmärksamma frågan. En annan punkt är att göra en systemsäkerhetsanalys som handlar om vilka krav som finns avseende sekretess, tillgänglighet, lagstiftning och informationens riktighet på den information som finns i systemet. Person B säger *"skulle vilja att kommunledningen då liksom sätter ner foten och säger att de här 10 systemen, eller 8 eller 12, dem är samhällsviktiga, på dem måste vi ha järnkoll"* och menar att det är svårt för IT-enheten själva att göra bedömningen om vilka system som är viktigare än andra.

Kommun C: Inom informationssäkerhetsarbetet skulle det önskas mer tid och mer resurser berättar Person C. Den del som är i störst behov av att utvecklas är just den administrativa delen, att få nedskrivet säkerhetsarbetet i formella dokument. Person C menar att det krävs bra underlag för att kunna få mer resurser till säkerhetsarbetet och anser att detta underlag kan förbättras bara dokument skapas.

Kommun D: Person D skulle vilja att säkerhetsarbetet kring informationstillgångarna blev mer kontinuerligt. Med detta menar personen att det ofta görs analyser av ett system som sedan sätts in i en pärm och ingenting mer händer – ingen åtgärd görs för de brister som upptäcks vid analysen. Personen önskar också vara mer verksamhetsnära. Med detta menar personen att kommunens olika verksamheter borde upplysas mer om vilka risker de kan utsättas för och sedan försöka göra en plan för att undvika att dessa risker inträffar.

Kommun E: För att täcka upp brister i dokument har Person E försökt öka dialogen med verksamheten. Men detta menar personen att medvetandegöra personalen och användare

om deras eget ansvar för en informationstillgång. Detta är dock en ständigt pågående dialog. Person E skulle också vilja förbättra de dokument som finns som skapats utifrån BITS då dessa inte är i önskat skick.

Allmänt:

6. *Kan du berätta om verksamhetens säkerhetspolicy? Inkluderar den riktlinjer om fysisk säkerhet kring era informationstillgångar?*

Kommun A: Det finns en säkerhetspolicy inom kommunen och denna är från början utformad från FA22. Säkerhetspolicyn har uppdaterats mycket genom åren och därför hänvisas den nu till BITS istället. I kommunen finns det tre nivåer av säkerhetspolicyn där en är en övergripande nivå som mer beskriver ansvar och roller. Nästa nivå anger *vad*, alltså konkreta mål och visioner och den sista nivån anger *hur*. Den sista nivån *hur* finns i två versioner, en komplett och en mer sammanfattad version som är till för användarna. Versionen för användarna är som en säkerhetsinstruktion. Säkerhetspolicyns olika nivåer innehåller lite om just fysisk säkerhet då det finns beskrivet om just skalskydd men för övrigt inte så mycket mer.

Kommun B: Kommunen har en säkerhetspolicy som är framtagen med hjälp av BITS dokument. Säkerhetspolicyn är indelad i fyra delar där en del är en övergripande policy som sätter ramarna för övrig policys. Under den övergripande policyn finns fyra underliggande instruktioner som arbetats fram. En av dessa är riktad och anpassad till användare. I denna står allmänt om informationssäkerhet och vilket ansvar användarna har samt vart de kan vända sig för att få support. Då skolan i kommunen har eget ansvar för datorer och en extern leverantör kan kommunen inte ställa samma krav på dessa användare. Av denna orsak har en annan instruktion tagits fram till de användare som finns inom skolans värld. Den tredje underliggande instruktionen är riktad till systemägare, systemansvariga, IT-samordnare samt chefer och handlar om hur verksamhetssystemen förvaltas och sköts. I denna instruktion finns angivet vem som ansvarar för vilket system och vilka skyldigheter som finns. Den fjärde och sista instruktionen är riktad till support- och driftpersonal på IT-avdelningen och beskriver hur driftmiljön ska hanteras och dokumenteras. I denna instruktion finns bland annat riktlinjer om just den fysiska säkerheten. Om den sista instruktion säger Person B *”det här var ju den som var klart jobbigast (...) det är sånt där som man inte riktigt har koll på men som man måste ha koll på”*.

Kommun C: Kommunen har ingen säkerhetspolicy ännu. Detta är dock tänkt att utvecklas med hjälp av BITS eller det nya konceptet som ersätter BITS.

Kommun D: Det finns en säkerhetsinstruktion som endast riktar sig till slutanvändare. Denna instruktion innehåller kortfattade punkter för att medvetandegöra användaren om enklare saker som bör tänkas på. En instruktion är exempelvis att inte lämna en dator öppen utan att denna ska låsas om datorn ska lämnas för en stund. Ingen mer policy än detta finns ännu men kommer förmodligen utvecklas under arbetet med LIS. Person C säger *”idag är det ju mer så säga ett de facto arbetssätt att vi jobbar utifrån ett visst sätt, hur vi liksom hanterar hur vi jobbar med det här men ja försök, försök att hitta det dokumenterat verkligen”*.

Kommun E: Person E säger *”i kommunen finns en säkerhetspolicy som är antagen, och den är ju antagen av kommunledningsgruppen, förvaltningschefsgruppen för några år sedan (…) problemet med den typen av policys, det är att det, det är väldigt få som vet vad det innebär, det är mycket fackord och ganska långgående förpliktelser”.* Person E menar att en säkerhetspolicy och dokument finns men att de inte följs på grund av att användare inte förstår det som står och arbetssättet blir då annorlunda. Säkerhetspolicyn är fem år gammal och anses nu inaktuell. Framtida policys kommer förmodligen skapas utifrån MSB:s nya rekommendationer.

Allmänt:

7. *Hur har en riskanalys gjorts över de hot som verksamheten kan utsättas för?*

Kommun A: En risk- och sårbarhetsanalys gjordes för många år sedan men även i fjol gjordes en analys där olika scenarier och risker har bedömts. Många av dessa scenarier har kretsat kring serverrummet men riskerna blir antingen orimliga eller anses väldigt viktiga. De risker som ansetts ha hög sannolikhet har åtgärdats. Risk- och sårbarhetsanalysen i denna kommun är gjord utifrån ett dokument som MSB ligger bakom. Person A säger vid intervjun att *”mitt jobb har ändrats från IT med litet i och stort T, till stort I och litet t. Vi pratar mindre och mindre teknik och mer och mer informationssäkerhet”*.

Kommun B: En riskanalys har inte gjorts ännu, men detta ska göras inom kort.

Kommun C: En riskanalys igår i arbetet med BITS men på denna kommun är ingen riskanalys gjord ännu.

Kommun D: Person D berättar att en kollega har gjort en riskanalys i viss mån där information samlats in från olika representanter i kommunen för att bedöma ett givet scenario. Denna riskanalys har mer riktats till vad som händer om tillgängligheten av informationstillgångarna försvinner och hur allvarlig denna otillgänglighet anses av olika förvaltningar beroende på olika system.

Kommun E: Det pågår diskussioner om olika säkerhetsfrågor inom kommunen men ingen riskanalys har gjorts på ett strukturerat sätt. Person E säger *”samtidigt som det är väldigt lätt att komma åt informationen fysiskt, så drivs ju utvecklingen mot att hela tiden göra det enklare”* och menar att information ska vara tillgängligt både från en surfplatta och en mobiltelefon.

5.1.3 Rekommendationer i ISO-27002, fråga 8 – 20

Nedan presenteras de frågor som riktar sig efter varje rekommendation i ISO-standarden 27002 kring fysisk- och miljörelaterad säkerhet inom informationssäkerhet. En huvudfråga per rekommendation har ställts till kommunerna.

Skalskydd:

8. *Hur arbetar ni för att ta fram skalskydd kring laptops respektive serverrummet?*

Kommun A: I skolans värld hanteras bärbara medel ganska fritt. Person A säger att *"vi fokuserar mer på informationen är på prylen"*. Inom kommunen finns en matris med informationsklassning och anses informationen konfidentiell ska sådan information lagras på servrarna och får inte bäras iväg men det finns inga direkta skalskydd som fysiskt hindrar från att bära iväg en laptop. Kring serverrummet finns brandsäkra dörrar och väggar. Den svaga punkten är att det finns små källarfönster till serverrummet men dessa ska vara säkrade både genom glaset och genom galler. Skalskydden togs fram med hjälp av rekommendationer från räddningsverket.

Kommun B: I regel finns inga extra skalskydd mot laptops förutom de skydd som byggnaden i sig omges av. Kommunen har utsatts för inbrott så på grund av den anledningen får inte laptops förvaras synligt efter arbetsdagens slut. På skolor finns säkerhetsskåp där laptops läggs in efter dagens slut. Gällande serverrummet finns det dokumenterat vad som bör finnas i och runt serverrummet. Det finns angivet i en policy vad serverrummet ska ha skydd mot och de skalskydd som finns är brandsäkra.

Kommun C: Det finns inga speciella skalskydd kring laptops. Anställda som har ett eget kontor har givetvis skalskydd men det är många anställda i kommunen som inte har egna kontor och dessa laptops skyddas inte på något annat sätt. Skalskyddet kring serverrummet består av brandsäkra dörrar och väggar. Person C berättar att fastighetsavdelningen skött upphandlingen av skalskydd.

Kommun D: Kring laptops finns inga skalskydd där laptops fysiskt kan låsas in efter arbetsdagens slut. Serverrummet är en egen brandcell vilken består av både brandsäkra dörrar och väggar. Valet av skalskydd har påverkats av Krisberedskapsmyndigheten som gjorde en stor genomgång av säkerheten på denna kommun.

Kommun E: Det finns inga speciella skalskydd kring laptops i kommunen förutom de personer som har eget kontor. Serverrummet omges av dörrar och väggar men Person E är osäker på om rummet består av brandsäkra sådana. Personen kan inte svara på hur skalskydden har arbetats fram.

Tillträdeskontroll:

9. *Finns det något behörighetssystem för att undvika otillåten fysisk åtkomst och hur har ni arbetat för att komma fram till detta?*

Kommun A: Person A berättar att det finns ett passagesystem vid ytterdörrarna till fastigheten. Dagtid är ytterdörrarna olåsta och öppna men efter kontorstid är de stängda och låsta. Till serverrummet finns passagesystem där det även loggas vem som går in och ut ur serverrummet. Behörighet till serverrummet är tilldelat efter befattning då inte vem som helst ska kunna ta sig in dit. Passagesystemet togs fram innan Person A började arbeta på kommunen.

Kommun B: Person B berättar att det finns tillträdeskontroller i form av nycklar och kort och att det är driftchefen som ansvarar för vem som får åtkomst till serverrummet. För åtkomst till serverrummet används en tvåfaktorslösning som inkluderar kort plus kod. Utdelning av nycklar och kort är den säkerhetsansvariges uppgift att ha koll på och den tekniska förvaltningen ansvarar för behörighetssystemet och framtagningen av detta.

Kommun C: Till serverrummet finns tillträdeskontroller i form av kortläsare och endast personer med behörighet kommer in till detta rum. Hur passagesystemet utvecklades kan Person C inte svara på då fastighetsavdelningen ansvarar för detta system och fortsätter säga att det är *”i mångt och mycket leverantörerna som på nåt sätt driver, driver fram, ja den här utvecklingen”* och menar att kommunen lyssnat på det som rekommenderats.

Kommun D: Det finns passersystem till serverrummet där endast behöriga personer kommer in. Behörighetssystemet består av en nyckelbricka samt individuell kod vilket tillsammans utgör en tvåfaktorslösning. Hur det kom sig att passersystemet valdes kan inte personen svara på då det är den tekniska förvaltningen som ansvarar för detta.

Kommun E: Passerkort används för att komma ner i källaren där serverrummet finns och därefter behövs passerkortet igen för att komma in i själva serverrummet. Detta är dock ingen tvåfaktorslösning som är önskvärt, det vill säga både kort plus kod. Samma behörighetssystem används också för att ta sig in till själva kommunkontoret. Olika behörigheter tilldelas utefter befattning.

Skydd av kontor, rum och faciliteter:

10. *Hur har placering av serverrum tänkts över?*
    a. *Hade ni fysisk säkerhet i åtanke då?*
    b. *Tänker ni på något särskilt när ni bygger nya kontor som ska innehålla informationstillgångar?*

Kommun A: Serverrummet ligger i källaren och varför kan intervjuobjektet inte svara på då beslutet togs före personens tid inom kommunen. Även om placering av kontor, rum och faciliteter finns i tankarna är det svårt att bibehålla detta i slutändan. Person A svarar *”man tänker på det säkert, försöker tänka på det, men det är inte en prioriterad fråga och dessutom så hinner verkligheten ikapp och då är det andra argument som går före”*.

Kommun B: Serverrummet har placerats med fysisk säkerhet i åtanke. Även i denna kommun finns serverrummet i källaren men åtgärder har vidtagits för att det ska vara så säkert som möjligt. Vad gäller fysisk säkerhet och placering av nya kontor kan Person B inte uttala sig om detta.

Kommun C: På placering av serverrummet svarar Person C att det inte tänkts över och säger *”inte ur ett säkerhetsperspektiv, det har det inte. Utan det är mest det att man har hittat en lämplig lokal”*. Serverrummet ligger i källaren även i denna kommun. Vid nybyggnation av kontor och placering av informationstillgångar säger Person C att *”man tänker ju tanken alltså, det gör man, men sen om man liksom kan åstadkomma nånting egentligen det är, det är ju kanske lite mer tveksamt då”*.

Kommun D: Placeringen av serverrummet kan inte Person D svara på då detta fanns på samma plats innan personen började arbeta inom kommunen. Serverrummet finns beläget i källaren. Vad gäller placering av nya kontor tänks detta över för vissa förvaltningar. Kontor inom förvaltningar som hanterar ytterst känslig information byggs med specialgjorda fönster för att minska insynen till kontoret. Person D säger att det beroende på förvaltning tas hänsyn till placering.

Kommun E: Placering av att ha serverrummet i källaren har inte tänkts över med fysisk säkerhet i åtanke. Hur exakt kommunen tänkte kan inte Person E svara på då det fanns på samma plats innan personen började på kommunen. Nya kontor byggs sällan och personen vet inte om placering tänks över med just fysisk säkerhet i åtanke.

Skydd mot externa hot och miljöhot:

11. *Kan du berätta om hur ni arbetar för att skydda era informationstillgångar mot fysiska hot så som översvämningar och bränder? Har det arbetats fram riktlinjer för vad som ska göras om en sådan katastrof inträffar?*

Kommun A: Det har vidtagits en hel del åtgärder för att skydda informationstillgångarna mot fysiska hot. Vattenledningar i tak och i väggar kring serverrummet är borttagna för att minska riskerna för en översvämning inuti byggnaden. Det finns klimatanläggning i serverrummet för att hålla det i rätt temperatur samt släckningssystem om något börjar brinna. Det finns även en gas som tar bort syret i serverummet och därmed kväver en brand. Dessutom finns brandsäkra dörrar och väggar. Det finns en del riktlinjer beskrivet i en katastrofplan och det mesta bygger på vad som händer så länge en brand är hanterbar. Det har mer skissats på hur kommunen återställer sig efter en katastrof för att snabbt fungera igen. Mer arbete är pågående.

Kommun B: Det finns dokumenterat vad serverrummet ska ha skydd för och åtgärder har vidtagits för att skydda informationstillgångar från fysiska hot. Det finns brandsäkra dörrar och väggar och släckningsmedel som tar bort syret i rummet så att en brand istället för att spridas, släcks i tid. Det finns klimatanläggning i form av vattenkylningssystem i serverracken så att temperaturen inte ska bli för hög. I serverracken finns även ett eget släckningssystem. Riktlinjer för hur en katastrof hanteras finns i en så kallas krisberedskapsplan men då detta hanteras av en annan avdelning kan Person B inte gå in närmare på det.

Kommun C: Det finns brandsäkra dörrar och väggar till serverrummet samt fuktvarnare som larmar om fukt uppstår i rummet. Klimatkontroll i form av kylningssystem och släckningssystem som inte förstör elektronik finns. Kommunen satte själva upp krav för vad som behövdes i serverrummet och efter leverantörers rekommendationer valdes ett lämpligt brandsläckningssystem. För övrigt finns brandsläckare och brandvarnare uppsatta i byggnationer inom kommunen. Det finns inga nedskriva riktlinjer för vad som ska göras om en katastrof inträffar.

Kommun D: Utöver att serverrummet är en egen brandcell finns även klimatkontroll, fuktlarm och automatiskt släckningssystem. Om en katastrof ändå inträffar finns en generell krisberedskapsplan men denna innehåller inga direkta riktlinjer för just informationssäkerheten. Detta är tänkt att arbetas fram enligt LIS.

Kommun E: I kommunhuset finns en kylanläggning som även förser serverrummet med kyla. Det finns på så sätt klimatkontroll i rummet som ser till att det inte blir för varmt. Person E kan inte svara på vad det finns för någon släckningsutrustning i serverrummet. Runt om kontor finns det utplacerade brandsläckare som även kan användas till elektronik. Det finns inga nedskriva riktlinjer för vad som ska göras om en katastrof inträffar.

Arbete i säkra utrymmen:

12. *Har ni arbetat med riktlinjer för hur arbete får utföras i ett säkrat utrymme så som serverrummet?*

Kommun A: Det finns riktlinjer för detta och dessa har arbetats fram med hjälp av FA22 och har sedan hängt med. Ingen person går in obevakat i serverummet och IT-enheten lämnar inte någon ensam i serverrummet om de inte anses pålitliga. Många leverantörer har varit med länge och anses därmed pålitliga. Nu för tiden minskar behovet av att vara i serverrummet rent fysiskt sett då många istället använder sig av fjärrstyrning.

Kommun B: Personen berättar att det inte finns några nedskriva riktlinjer för detta men att varje person som ska in i serverrummet behöver ett kort med tillhörande kod. Kommer en leverantör får denna ett kort att använda som sedan lämnas tillbaka. På så sätt ökar kontrollen över vem som befinner sig i serverrummet.

Kommun C: Person C svarar *"vi har inga speciella riktlinjer, det har vi inte"* men säger också att detta är tänkt att arbetas fram. Dock är det endast behöriga personer som kommer in i serverrummet via kortläsarna och dessa personer vet hur utrustningen ska hanteras. Andra personer som släpps in i serverummet är kända leverantörer som kommunen länge haft en relation till.

Kommun D: Den finns inga riktlinjer för detta nedskrivet och Person D säger att detta mer är ett *"de facto arbetssätt snarare än en formell policy"*. Om en leverantör ska befinna sig i serverrummet får denna person först låna en bricka med kod för att ens komma in i dit. Kommunen försöker även begränsa sig och endast ha de leverantörer som behövs för att så få som möjligt ska behöva tillgång till deras servrar.

Kommun E: Det finns inga nedskriva riktlinjer för hur arbete får utföras i ett säkrat utrymme, endast arbetssätt, men som leverantör har man inte raka spåret ner till serverrummet då det finns passagekontroller på vägen. IT-enheten följer med en ny leverantör ner till serverrummet men är det en leverantör som varit med länge kan denna självständigt arbeta i serverrummet efter att ha fått ett passagekort. Person E säger även att det är sällan nu för tiden som någon måste ha fysisk tillgång till serverrummet då mycket idag går att lösa via fjärrstyrning.

Allmänhetens tillträdes, leverans- och lastutrymmen:

13. *Har ni tagit fram någon form av övervakningssystem kring era informationstillgångar? Varför har ni detta?*

Kommun A: Det finns inget övervakningssystem i form av någon kamera eller liknande i serverrummet eller vid ingången till serverrummet. Person A berättar att det nu för tiden är väldigt sällan någon behöver fysisk tillgång till serverrummet då åtkomst till servrar istället sker via fjärrstyrning. För övrigt finns larm som larmar om något plötsligt inträffar, så som en klimatförändring i serverummet.

Kommun B: Det finns övervakningssystem som övervakar kommunikationsutrustningen i kommunen, det vill säga ett system som larmar om en kabel grävs av. Detta används för att undvika större problem om en katastrof inträffar och att personer hinner reagera i tid. Det finns även andra larm i serverrummet som upplyser om klimatet i rummet förändras. Det finns inga kameror i serverrummet.

Kommun C: Även i denna kommun finns inget övervakningssystem i form av en kamera som bevakar vem som befinner sig i serverummet. Om något annat inträffar i serverummet så som om en server går ner eller om kommunikationen över nätverket förändras får driftsenheten larm om detta.

Kommun D: Denna kommun har larm som går till det tekniska kontoret om något i serverrummet beter sig onormalt. Det vill säga att om exempelvis fuktnivån stiger eller om rummet blir för varmt så larmas detta. Det finns även en rörelsedetektor i serverrummet men ingen kameraövervakning. Person D förklarar att rörelsedetektorn förmodligen finns där för att känna av om inbrott sker och dörren bryts upp utan att använda passersystemet.

Kommun E: Det finns en kamera i serverrummet men denna förmodas att ta ner. Den sattes upp då det var mer spring till och från serverrummet men i dagens läge anses kameran onödig då många servrar går att fjärrstyra istället. Tekniker får larm om serverrummet blir för varmt eller om en annan klimatförändring sker.

Placering av skydd och utrustning:

14. *På vilket sätt har ni tänkt över hur era informationstillgångar och valda skyddsåtgärder placerats för att minimera risken för fysiska hot? Används några särskilda skyddsmetoder kring laptops?*

Kommun A: När det gäller datorer är det inget speciellt som tänkts över gällande placeringen av dem. I serverrummet har servrarna centraliserats så att dessa informationstillgångar ska finnas samlade på samma ställe. Person A säger att kommunen *”resonerat så att vi försöker bygga upp så mycket säkerhet som möjligt kring serverrummet”*. Det finns inga särskilda skyddsmetoder kring laptops i allmänhet.

Kommun B: För att ta sig in i serverrummet måste tre dörrar måste passeras med kort och kod. Serverrummet är byggt för att vara så säkert som möjligt och laptops ska plockas bort från fönster och synliga platser efter arbetsdagens slut. Övrig tanke på placering kan Person B inte svara på.

Kommun C: Placering vad gäller skydd har inte tänkts över på något speciellt sätt så vitt Person C vet. Det är fastighetsavdelningen som har skött placering av exempelvis brandskydd och behörighetskontroller men givetvis har IT-enheten varit med i diskussionen kring skydd i serverrummet. Alla servrar har centraliserats till serverrummet så dessa ska finnas samlade på ett och samma ställe.

Kommun D: Servrarna har centraliserats till ett ställe – serverrummet. Detta för att minska sårbarheten mot dessa och genom att ha en känslig punkt kan denna påkostas mer. All utrustning är stöldmärkt och tanken med detta är att avskräcka en attackerare från att stjäla kommunens utrustning. Inga övriga skyddsmetoder används kring laptops förutom, som i

samtliga kommuner, att anställda ombeds att lagra all information på servrarna och inte lokalt för att försvåra tillgängligheten till informationen om datorn blir stulen.

Kommun E: Person E förklarar att fastighetsavdelningen har mer koll på placering och berättar att dagens utrustning blir alltmer bärbar vilket försvårar den fysiska kontrollen. Person E nämner också att molntjänster (tjänster som köps av andra) ger sämre kontroll över den fysiska säkerheten kring den tjänst som köps och trygghetskänslan faller. Inom kommunen finns inga extra skydd för laptops.

Tekniska försörjningssystem:

15. *Vad händer om strömförsörjning till era informationstillgångar plötsligt slutar fungera?*
    a. *Om åtgärder finns, gäller dessa endast specifika informationstillgångar så som serverrum?*
    b. *Hur många laptops finns i verksamheten?*
    c. *Hur många stationära datorer finns i verksamheten?*
    d. *Om strömförsörjningen plötsligt slutar fungera, finns det åtgärder för dessa datorer också?*

Kommun A: Det finns en UPS som tar över och klarar att driva serverrummet i ungefär 20 minuter. Därefter tar dieselkraft över så serverrummet ska aldrig kunna bli utan ström. I verksamheten finns många laptops och ännu fler stationära datorer. Hälften av de stationära datorerna är tunna klienter vilket innebär att information lagras direkt på en server och inte lokalt på datorn. Om strömmen bryts av exempelvis ett strömavbrott fortsätter serverrummet att fungera men stationära datorer i stadshuset stängs av och kan startas igen när reservkraften/dieselkraften går in. Laptops som har eget batteri fortsätter fungera men de laptops som inte finns i stadshuset kan få problem att komma åt stadshusets nät då omkopplingsställen på vägen dit står utan ström. Då reservkraften fungerar för stadshuset kan stationära datorer på annan plats i kommunens omnejd inte startas förrän den ordinarie strömmen kommer tillbaka.

Kommun B: Det finns en UPS som är för hela stadshuset och dieselkraft som tar över efter en viss tid. Detta innebär att serverrummet aldrig går ner. I verksamheten finns många stationära datorer och något färre laptops. Kommunen ansvarar inte för skolans datorer då skolorna själva gör det. Precis som i föregående kommun är det främst stationära datorer som drabbas vid ett strömavbrott då laptops fortsätter på sitt eget batteri. UPS:en testas regelbundet så att den fungerar när den behövs.

Kommun C: I serverummet finns en UPS som hanterar spänningsförändringar. Om ett strömavbrott sker tar UPS:en över så att serverrummet aldrig ska gå ner. Utöver denna åtgärd finns ett dieselkraftverk som går igång snabbt och kan leverera ström till resten av kommunhuset. Det finns ungefär dubbelt så många stationära datorer som det finns laptops i verksamheten. Givetvis stängs stationära datorer i huset av vid ett strömavbrott men då dieselkraften går igång inom kort kan dessa datorer snabbt startas upp igen. Laptops har egna bärbara batterier och stängs därmed inte av vid ett strömavbrott.

Kommun D: Kommunen har UPS:er som tar över om ström till serverrum, korskopplingsrum samt lokaler plötsligt bryts. Efter kort tid tar ett dieselverk över som kan tillhandahålla ström till kommunhuset. Inom kommunen finns många laptops men antalet

stationära datorer är det dubbla. Med åtgärder som UPS och dieselkraft blir serverrummet aldrig utan ström. Laptops fortsätter fungera på sitt eget bärbara batteri och de stationära datorerna i kommunhuset stängs av under kort tid men kan startas igen när dieselkraften tar över strömförsörjningen. Stationära datorer på andra platser än kommunhuset får vänta tills den ordinarie strömmen kommer tillbaka.

Kommun E: I serverrummet finns en UPS och därefter finns ett dieselaggregat som driver hela kommunhuset. Serverrummet går aldrig ner då UPS:en tar över direkt och följs av dieselkraften. I kommunen finns både laptops och stationära datorer och antalet stationära datorer är något större än antalet laptops. Det är endast de stationära datorerna som påverkas av ett strömavbrott men de datorer som finns i kommunhuset kan startas igen när dieselkraften går igång.

Kablageskydd:

16. *Hur gör ni för att skydda kablar mot fysiska hot?*
    a. *Arbetar ni medvetet med att använda kablageskydd?*
    b. *Tänker ni på det vid upphandlingar?*

Kommun A: Kablageskydd finns inom kontor och om ett kontor byggs sätts det alltid in kanaler för el och andra kablar. Kablar som anses mer känsliga, så som fiberkablar i stadsnätet, är inte skyddade på något särskilt sätt. Med det menas att en kabel kan grävas av och på så sätt orsaka problem.

Kommun B: Person B svarar att *”vi följer de föreskrifter som finns i byggnormer för kabelförläggning i fastighet respektive mark. Byggnormerna använder vi också vid upphandlingar då när vi upphandlar installationer men vi gör inga tillägg”*.

Kommun C: Inom kontor finns kabelkanaler men den sista biten av kabeln från kabelkanalen till utrustningen är synlig och utan skydd. I serverrummet finns inga speciella kablageskydd men detta anses inte lika känsligt då endast behöriga personer kommer in i rummet. Kommun C arbetar inte medvetet med skydd av kablar mer än kabelkanaler i kontor.

Kommun D: Kablar som kommer upp ur mark och som går in till fastigheter skyddas med kablageskydd som är av kraftig metall. Kablar som kommer in i fastigheter skyddas men kablar inom byggnaden skyddas desto mindre. I varje kontor finns kabelkanaler men dessa är främst avsedda för elkablar så att dessa inte hänger löst. Kablageskydd är inget som prioriteras vid upphandlingar.

Kommun E: Kablar mellan nätverksenheter är inte synliga förutom i något undantag. Kabelkanaler används i kontor men kommunen försöker gå mot ett nätverk där kablar behövs allt mindre och kommunen satsar mer på det trådlösa nätverket. Förövrigt finns det inget speciellt tankesätt för att skydda kablarna mot fysiska hot.

Underhåll av utrustning:

17. *På vilket sätt sker det underhåll av era informationstillgångar? Så som uppdateringar, borttagning av damm i hårdvara.*

Kommun A: Det sker underhåll med jämna mellanrum för att uppdatera och uppgradera servrar i serverrummet. Det finns dock inga nedskrivna riktlinjer för detta men arbetssättet är att underhåll ska ske kontinuerligt. Städning av serverrummet och bortplockning av damm och annan smuts görs av IT-enheten själva då ingen obehörig städerska ska komma in i rummet.

Kommun B: Underhåll av informationstillgångarna sker under fyra lördagar per år då system stängs ner mellan 22.00 på fredagen till 06.00 på lördagen. Alla mjukvaruuppdateringar samt hårdvaruförändringar sker under dessa underhållslördagar. Person B säger *"finns ingen underhåll av damm i hårdvara och så vidare utan vi byter hårdvara med 3-5 års mellanrum och då krävs ingen åtgärd mot damm i hårvara"*.

Kommun C: Borttagning av damm i serverummet sker inte rutinmässigt då serverrummet anses relativt dammfritt. Uppdatering av mjukvara sköter IT-enheten själva men dessa underhåll sker inte under en särskild avsatt tid utan mjukvaruuppdateringar sker när de dyker upp. Det finns inga nedskriva riktlinjer för underhåll av utrustning.

Kommun D: Det finns inga dokumenterade riktlinjer för underhåll av utrustning. Mjukvaruuppdateringar sker regelbundet och borttagning av damm sker i samband med reparationer, uppgraderingar eller ominstallationer av datorer. Underhåll är mer ett arbetssätt som tillämpas vid behov och är inget som sker regelbundet.

Kommun E: IT-avdelningen har en egen dammsugare som ibland kommer fram för att hålla damm i serverrummet borta då en städerska inte är behörig att komma in i ett serverrum. Person E säger att *"ibland får vi in datorer som det är ett under att de inte brunnit upp"*. Det finns inga riktlinjer för när underhåll av hård- och mjukvara ska ske.

Säkerhet för utrustning utanför egna lokaler:

18. *Vad finns för regler och riktlinjer för huruvida arbete får ske utanför era egna lokaler? Får informationstillgångar tas med hem för fortsatt arbete och vilka regler gäller för detta?*

Kommun A: Viss typ av information får inte visas för andra och denna information får heller inte tas med hem. Det finns riktlinjer för hur information får hanteras och hur denna hanteras beror på vilken informationsklassning informationen har. Är informationen inte konfidentiell får den tas med hem för fortsatt arbete.

Kommun B: Arbete får ske utanför egna lokaler men riktlinjer finns för detta. Det är användarens närmaste chef som bestämmer om arbete får ske på annan plats än arbetsplatsen. Användaren själv ansvarar för att datorn inte kommer i kontakt med obehöriga och att datorn förvaras på ett säkert sätt för att undvika stöld. Även att informationen skyddas från brand och insyn. Användaren måste själv ta ansvar för att vara uppkopplad mot kommunens stadsnät för att filerna inte ska lagras lokalt på datorn. Ska externa personer komma åt interna system måste godkända metoder enligt kommunen, så som VPN, att användas. VPN är en anslutningsmetod som kan användas för att ansluta en enhet som befinner sig utanför verksamhetens nät.

Kommun C: Person C berättar att informationstillgångar får tas med hem efter arbetsdagens slut men det finns inga regler eller riktlinjer för detta. Finns ingen nedskriven policy som användarna måste rätta sig efter.

Kommun D: Arbete får ske utanför egna lokaler om användarens närmaste chef medger detta och riktlinjer finns enligt den instruktion för slutanvändare som kommunen har. Reglerna som står i detta dokument är kortfattade och gäller för användare när de befinner sig på arbetsplatsen men också på annan plats. Dessa regler kommer förhoppningsvis att uppdateras enligt rekommendationer i LIS.

Kommun E: Det finns riktlinjer för hur arbete får ske utanför egna lokaler och dessa är delvis dokumenterade. Ska arbete ske på distans måste detta ske genom kommunens två erbjudna kanaler där den ena är en erbjuden anslutning via VPN. Laptops får tas med hem efter arbetsdagens slut men en riktlinje säger att anställda inte ska lagra filer lokalt utan filer ska sparas ned via någon av dessa två kanaler.

Säker avveckling eller återanvändning av utrustning:

19. *Har ni arbetat fram några speciella rutiner för avveckling, utbyte eller återanvändning av hårdvara? Hur kom ni fram till dessa rutiner?*

Kommun A: Hårddiskar som används i administrativa arbeten plockas ut ur datorerna och skickas till leverantör för att förstöras och tar bort information. De skickas för ”degaussing” som innebär avmagnetisering. Om en laptop ska återanvändas installeras datorn om. Vad gäller egna konton, så som e-postkonton, raderas dessa några veckor efter att en person slutat. Dessa rutiner anses som en självklarhet i branschen så dessa rutiner är inte framtagna med hjälp av någon standard utan anses mer som en principsak.

Kommun B: Datorer som ska avvecklas eller återanvändas samlas i ett låst skåp och sedan köps en tjänst från en leverantör som ansvarar för att ta bort all information på hårddisken. Tidigare borrades ett hål i hårddisken om den inte skulle användas mer men Person B säger *”vi tänker så hela tiden, om vi inte kan göra en sak billigast och bäst då ska vi inte göra den utan då köper vi tjänsten istället”*.

Kommun C: Stationära datorer som ska avvecklas skickas till en leverantör som tar bort informationen på dessa hårddiskar. Om en laptop ska avvecklas slås hårddisken manuellt sönder innan den läggs i elektronikskroten. Ska en dator återanvändas installeras maskinen om och på så sätt skrivs befintlig information över. Det finns inga skriftliga rutiner för avveckling, återanvändning eller utbyte av hårdvara men detta arbetssätt är framtaget då viss information inom kommunen kan vara sekretessbelagd och inte får komma i obehöriga händer. All information ska i regel finnas lagrad på servrar men då det kan finnas något sparat lokalt i datorn antogs detta arbetssätt.

Kommun D: Person D säger *”återigen mycket en fråga om arbetssätt och de facto rutiner”* och menar att de rutiner som finns kring avveckling, återanvändning och utbyte finns inte nedskrivet någonstans. De datorer som återanvänds installeras om och städas innan de lämnas ut på nytt. Utrustning som inte kan återanvändas får hårddisken urplockad och sedan hamras denna sönder innan den läggs till elektronikskroten. Om en server ska avvecklas

skickas denna komplett i en låst bur till leverantör för professionell hantering och borttagning av information.

Kommun E: Det finns rutiner för hur utrustning ska avvecklas, återanvändas eller bytas ut. När det gäller utrustning där det kan finnas sekretessbelagd information förstörs dessa hårddiskar av IT-avdelningen själva. Övrig IT-utrustning som ska avvecklas samlas in och läggs i en container som står i ett låst utrymme dit ett fåtal personer har nyckel till. En leverantör hämtar sedan containern och förstör utrustningen. Person E säger också *"nu när jag hör mig själv så kan jag ju inte säga att vi har full koll"* och syftar på om exempelvis en användare har tagit med en gammal dator hem. Dessa rutiner har resonerats fram. Oftast återanvänds ingen utrustning och därför finns inga klara rutiner för detta.

Avlägsnande av egendom:

20. *På vilket sätt kontrolleras det att information är borttagen från en informationstillgång innan den slängs eller återanvänds? Finns rutiner för detta och hur har dessa arbetats fram?*

Kommun A: När en hårddisk skickas för avmagnetisering återfås ett skrotningsintyg från leverantören som ett kvitto att informationen på hårddisken är borttagen. Innan rutinen fanns med att skicka hårddiskar för avmagnetisering borrades ett hål i varje hårddisk. Men detta blev ohållbart då det är tidsödslande. Person A säger även att *"det största problemet idag egentligen det är, vet du vad det är? Det är hårddiskar i skrivare"* och menar att dessa ofta glöms av. En skrivare lagrar det som skrivs ut vilket innebär mycket information.

Kommun B: Kommunen har ett avtal med leverantören som ansvarar för borttagning av information och i avtalet är det förmodligen specificerat att leverantören ska kontrollera att informationen faktiskt är borttagen.

Kommun C: Det sker inga kontroller för att se om informationen faktiskt är borttagen. Kommunen anser att informationen är borttagen efter att rutinerna i föregående fråga gåtts igenom.

Kommun D: Då hårddiskar installeras om innan de återanvänds sker inga övriga kontroller då informationen ska vara överskriven. Hårddiskar som avvecklas hamras sönder och då styrkortet förstörs anses hårddisken obrukbar. För övrigt sker inga fler kontroller. Vad gäller de servrar som skickas för professionell avveckling kan Person D inte svara på hur detta kontrolleras. Person D säger *"om inte vi längre kan se informationen enkelt så räknar vi med att då krävs det så pass extraordinära åtgärder"* och menar att informationen ska vara svår att återställa efter en ominstallation.

Kommun E: Utrustning hanteras olika beroende på varifrån den kommer. Om en dator kommer socialförvaltningen hanteras dessa annorlunda då dessa kan innehålla känslig information. Dessa datorer förstörs och slås sönder. Övriga datorer som skickas till en för leverantör borttagning av information fås det inget kvitto på att utrustningen faktiskt är förstörd. För övrigt finns det inga riktlinjer för hur sådant kontrolleras. Person E avslutar hela intervjun med att säga *"jag ser ju att det finns en risk i att fysisk säkerhet kommer lite i skymundan"* och fortsättar med att leverantörer oftast pratar om mjukvarubaserade säkerhetslösningar.

6 Analys

I kapitel fem visas de resultat som framkom vid intervjuerna med respektive kommun. I detta kapitel kommer resultatet analyseras på bästa sätt för att se hur medvetna kommuner är om den standard de använder sig av, hur väl denna standard efterföljs och vem som egentligen påverkar de beslut som tas kring vilka skyddsåtgärder som införts. Det kommer även diskuteras kring hur framtidstänket ser ut och vad som egentligen kommer hända hos kommunerna just inom informationssäkerhet. Dessa rubrikindelningar har tagits fram med hjälp av intervjufrågornas kategorier och svar. Då intervjufrågorna är kategoriserade under *inledning*, *allmänt* samt *rekommendationer i ISO-27002* har frågor under dessa kategorier valts att analyseras under olika rubriker. För mer information om hur intervjuerna genomförts kan detta läsas under avsnitten 4.4 och 5.1.

Frågor under kategorin *allmänt* och *rekommendationer enligt ISO-27002* ger ett underlag för vidare analys av hur väl den valda standarden efterföljs. Frågor om säkerhetspolicy, riskanalys och en fråga per rekommendation skapar en bild av hur kommunens informationssäkerhetsarbete ligger till. En fråga per rekommendation i ISO-27002 ger underlag till att analysera hur väl förberedda kommunerna är för dessa rekommendationer som i sin tur kan ge svar på den huvudsakliga frågan i denna rapport. Rubriken som innehåller information om vem som påverkar de beslut som tas anses intressant då många frågor har besvarats oklara med hur kommunen faktiskt tänkte gällande ett beslut. I många fall är det inte den valda standarden som påverkar att ett visst beslut tas. Rubriken där framtidstänket analyseras har tagits fram på grund av att många kommuner nämner redan i början av intervjun att informationssäkerhetsarbetet är tänkt att förbättras med en ny, kommande standard. Eftersom arbetet med exempelvis Ramverket för informationssäkerhet inte kommit igång ännu anses detta som något som ska göras i framtiden.

6.1 Analys av intervjuobjekten

Intervjusubjekten har olika bakgrund. Tre av fem personer har en akademisk, eftergymnasial utbildning inom IT. Beteckningen på utbildningarna varierar mellan de tre personerna men då även åldern mellan personerna är olika är detta förståeligt. Utbildningsnamn ändrar sig med tiden. Resterande två personer har ingen akademisk utbildning inom IT men har ett gediget intresse för ämnet och är självlärda genom erfarenhet. Den ena av dessa personer har dock läst fristående kurser på högskola för att få en mer teoretisk bakgrund till sitt arbete.

Genom att samtliga intervjuobjekt har ett gemensamt intresse – IT, har medvetenheten kring vad informationssäkerhet handlar om varit relativt hög. Framförallt har tre av fem personer läst kurser på högskola inom informationssäkerhet och har då en teoretisk förklaring till varför detta är viktigt. Övriga två personer har kunskaper om vad ordet informationssäkerhet innebär genom arbetslivserfarenhet och fristående högskolekurser.

6.2 Medvetenhet kring standarder

Samtliga kommuner känner till och har på något sätt en relation till konceptet BITS. Det ska dock förtydligas att BITS *inte* är en standard utan ett koncept med rekommendationer som Krisberedskapsmyndigheten arbetat fram (MSB, 2011d). Anledningen till att kommunerna arbetat utifrån BITS är att detta koncept har rekommenderats av MSB till just kommuner. Det visar sig att alla fem kommuner har arbetat utifrån BITS men vissa kommuner har inte

kommit lika långt i arbetet som andra kommuner har gjort. Personen på Kommun A kan berätta mycket om FA22 som var ramverket kommunen följde innan BITS kom in i bilden. Varken FA22 eller BITS är standarder inom informationssäkerhet. Samtliga kommuner är medvetna om vad BITS är, men det är dock inte självklart för alla vad BITS egentligen anger i sina rekommendationer. Detta kan bero på att kommunerna kommit olika långt med sina säkerhetsarbeten.

Två av fem intervjuade nämner att BITS-konceptet fokuserar mycket på rutiner och vägledning och att LIS kommer ha mer fokus på informationssäkerheten där det upplevs att den fysiska säkerheten har släppts en aning. I detta fall är det Ramverket för informationssäkerhet som intervjuobjekten syftar på vilket är ett ramverk som MSB står bakom och rekommendationer i detta ramverk baserar på LIS vilket innebär standarder i ISO-27000. Ett ramverks syfte är att hjälpa verksamheter att tolka information från en standard för att lättare kunna införa LIS i verksamheten (MSB, 2011d).

Vad gäller Ramverket för informationssäkerhet har intervjusubjekten svårt att uttala sig om detta då informationssäkerhetsarbetet ännu inte kommit igång utifrån detta ramverk.

MSB (2010b) skriver följande om standarder: *”De anger krav och riktlinjer som är användbara för alla typer av organisationer. Verksamheter får möjligheter att arbeta utifrån beprövade erfarenheter och då enklare skapa förutsättningar för bättre säkerhet.”* Att vara medveten om en standard anses bra då en standard kan vara användbar för säkerhetsarbetet i en verksamhet. I undersökningen som gjorts visar det sig att fem av fem kommuner är mer eller mindre medvetna om konceptet BITS. Dock är det inte varje intervjuobjekt som kan uttala sig och berätta om vad BITS innebär. Dessutom är inte BITS en standard utan ett koncept. Efterträdaren LIS anser intervjusubjekten som ny och därför är de ännu inte medvetna om vilka rekommendationer LIS står för. Det ska dock förtydligas ännu en gång att det är Ramverket för informationssäkerhet som baserar på LIS de intervjuade syftar till då det är MSB:s ramverk kommunerna tänkt att numera följa. Skillnaden på att följa en standard och ett ramverk är att ett ramverk endast har standarder som utgångspunkt i sina rekommendationer och föreskrifter. Standarder i sig har arbetats fram utifrån erfarenheter av arbete med just informationssäkerhet (MSB, 2011d).

6.3 Efterföljande av standard

Ingen av kommunerna följer någon standard inom informationssäkerhet men samtliga kommuner arbetar utifrån tidigare Krisberedskapsmyndighetens koncept BITS och det varierar i kommunerna hur väl detta koncept efterföljs. Inom en av kommunerna baserar många dokument på FA22 som sedan har verklighetsanpassats och uppdaterats med hjälp av rekommendationerna och dokumenten i BITS. En annan kommun har samtliga dokument, så som säkerhetspolicys och säkerhetsinstruktioner, framtagna med BITS som stöd. De övriga tre kommunerna har påbörjat säkerhetsarbetet med BITS men har inte alla dokument som BITS föreslår framtagna och de dokument som finns är ofta föråldrade och i behov av uppdatering. I en kommun togs BITS upp men arbetet blev aldrig färdigt och en av orsakerna till detta är att det finns begränsade resurser.

Syftet med en säkerhetspolicy är att kommunicera (Anderson, 2008), det vill säga uttrycka påståenden som ska följas av samtliga den gäller för och att alla berörda personer vet vilka regler som gäller. Vad gäller arbetet med säkerhetspolicys har detta varierat bland kommunerna. Två kommuner har arbetet fram säkerhetspolicys som är uppdaterade och

anpassade efter dagens behov och en av dessa kommuner säger att den policy som inkluderar fysisk säkerhet var svårast att ta fram. Person B säger: *”det här var ju den som var klart jobbigast (...) det är sånt där som man inte riktigt har koll på men som man måste ha koll på”*. En kommun saknar helt en säkerhetspolicy och i en annan kommun finns endast en säkerhetsinstruktion för slutanvändare men denna instruktion är inte antagen som säkerhetspolicy. Den sista kommunen har en säkerhetspolicy men denna anses föråldrad och inte uppdaterad. Av denna information kan slutsatsen dras att arbetet med en säkerhetspolicy skulle kunna förbättras och förhoppningsvis kommer detta göras utifrån Ramverket för informationssäkerhet.

Mycket inom den fysiska säkerheten tyder på arbetssätt istället för dokumenterade rutiner, precis som Person D säger: *”idag är det ju mer så säga ett de facto arbetssätt att vi jobbar utifrån ett visst sätt, hur vi liksom hanterar hur vi jobbar med det här men ja försök, försök att hitta det dokumenterat verkligen”*.

För att få stöd från ledning, politiskt stöd och finansiellt stöd för sitt säkerhetsarbete instämmer samtliga intervjuobjekt att detta finns om rätt argument läggs fram. Som Person A säger: *”har man rätt argument är det inget svårt att få fram pengarna”*.

En naturkatastrof som åska kan orsaka strömavbrott som i sin tur kan orsaka att hårdvara plötsligt stängs av (Pfleeger & Pfleeger, 2006). För att skydda sina informationstillgångar mot naturkatastrofer bedöms samtliga kommuner ha vidtagit de åtgärder som behövs för att minimera riskerna att information förloras. I tre av fem kommuner finns inga nedskriva riktlinjer för vad som ska ske om en katastrof inträffar. I de övriga två kommunerna finns det riktlinjer för detta nedskrivet men detta har en annan avdelning inom kommunen ansvar för.

En orsak till att den fysiska säkerheten inte får glömmas av är att det alltid kommer finnas människor som vill illa. Därför måste informationstillgångar, både inom och utanför verksamhetens lokaler, skyddas från obehörig åtkomst (Anderson, 2008). I fyra av fem kommuner finns det någon form av säkerhetsinstruktion dokumenterat som anger regler för hur arbete får ske utanför verksamhetens egna lokaler. Dock är det upp till användarna själva att ta ansvar för att dessa regler efterföljs.

Vad gäller placering av serverrum och nybyggda kontor med fysisk säkerhet i åtanke säger intervjuobjekten så här:

”man tänker på det säkert, försöker tänka på det, men det är inte en prioriterad fråga och dessutom så hinner verkligheten ikapp och då är det andra argument som går före” (Person A, Kommun A).

”inte ur ett säkerhetsperspektiv, det har det inte. Utan det är mest det att man har hittat en lämplig lokal” (Person C, Kommun C).

Sammanfattningsvis följer ingen av kommunerna en standard inom informationssäkerhet och är heller inte medvetna om vilka rekommendationer en standard som ISO-27002 tar upp. De koncept eller ramverk som kommunerna arbetar utifrån följs till viss del. Framförallt två av kommunerna är mycket medvetna om informationssäkerheten i deras verksamhet och de kan själva peka på brister som finns. I de övriga tre kommunerna upplevs säkerhetsarbetet komma i andra hand då det är svårt att prioritera mellan olika projekt. Personen C säger: *”vi måste koncentrera oss på driftsfrågor liksom när vi har så begränsade resurser”* och fortsätter med *”IT-säkerheten alltså den, den kommer i andra hand tyvärr”* medan Person A

säger: *”mitt jobb har ändrats från IT med litet i och stort T, till stort I och litet t. Vi pratar mindre och mindre teknik och mer och mer informationssäkerhet”*.

6.4 Vem/vad som påverkar besluten

Samtliga intervjuobjekt har svårt att uttala sig i de flesta frågor om vad som påverkar de beslut som tas. I de flesta fall påverkas inte besluten av det koncept som kommunen arbetar utifrån. Beslut påverkas mer av att en utomstående, tredje part gör en undersökning på kommunen och därefter bedömer vilket skydd som rekommenderas. När det gäller passagesystem för tillträdeskontroll säger Person C: *”i mångt och mycket leverantörerna som på nåt sätt driver, driver fram, ja den här utvecklingen”*. Ett annat intervjusubjekt svarar att en tredje part ansvarar för borttagning av information på hårddiskar som ska avvecklas och att beslutet har påverkats av kommunens tankesätt. Person B säger: *”vi tänker så hela tiden, om vi inte kan göra en sak billigast och bäst då ska vi inte göra den utan då köper vi tjänsten istället”*.

Sammanfattningsvis upplevs det att det inte är det valda konceptet eller någon annan standard som påverkar beslut som tas kring den fysiska säkerheten inom informationssäkerhetsarbetet. Ofta är det ”sunt förnuft” och rena principer som anses självklara i branschen som påverkar arbetssättet och kommuner litar på det som leverantörer rekommenderar.

6.5 Framtid

Eftersom BITS nu är föråldrat ersätts detta koncept av MSB:s Ramverk för informationssäkerhet som i sig baserar på LIS. LIS är alltså standarder i serien ISO-27000 där bland annat standarden ISO-27002 finns med. Fyra av fem kommuner har tänkt följa Ramverket för informationssäkerhet i framtiden. Ramverket är precis som BITS ingen standard men ramverket bygger dock på rekommendationer som anges i standarden ISO-27002. Den femte kommunen har tänkt titta på DISA som också kommer från MSB. DISA är inte heller en standard utan är ett utbildningsprogram som kan användas för att utbilda användare om just informationssäkerhet (MSB, 2011d). Vid intervjuerna med kommunerna är det mycket arbete som ”är tänkt att göras” och förhoppningsvis blir detta arbete gjort när arbetet med Ramverket för informationssäkerhet kommer igång.

7 Slutsatser

Denna rapport syftar till att visa att den fysiska säkerheten inom informationssäkerhet är minst lika viktig som övriga delar inom säkerhetsarbetet. Allsopp (2009, s. 1) skriver *"that security is only as strong as the weakest link in the chain"* och detta är viktigt att komma ihåg då brister i skyddet någonstans kan orsaka att information förloras.

ISO-standarden 27002 anger flera rekommendationer som en verksamhet bör se över kring den fysiska och miljörelaterade säkerheten. Denna rapport har visat hur några verksamheter inom den offentliga sektorn har gjort och hur arbetet är strukturerat för att tillgodose dessa rekommendationer. Nedan ges det svar på den huvudsakliga frågan i detta arbete och därefter tolkas slutsatser utifrån de resultat och analyser som har presenterats tidigare i rapporten gällande förhållandet mellan en standard och en kommun.

7.1 Problemprecisering – Svar

Den huvudsakliga frågan som denna rapport är tänkt att besvara är:

Hur väl förberedda är verksamheter inom den offentliga sektorn för de rekommendationer som finns angivna av standarden ISO-27002 kring fysisk och miljörelaterad säkerhet rörande informationssäkerhet?

Enligt den information som framkommit vid intervjuerna följs en del av de rekommendationer som ISO-27002 tar upp. Utifrån de frågor som ställts till kommunerna framkommer det att minst tre av fem kommuner är förberedda för dessa rekommendationer: *skalskydd*, *tillträdeskontroll*, *skydd mot externa hot och miljöhot*, *arbete i säkra utrymmen*, *tekniska försörjningssystem*, underhåll av utrustning, *säkerhet utanför egna lokaler* samt *säker avveckling eller återanvändning av utrustning*.

Dock är det få av dessa punkter som mer än tre av fem kommuner har nedskriva och dokumenterade rutiner och riktlinjer för. Många rutiner i en verksamhet är arbetssätt och inte dokumenterade instruktioner. Exempelvis under *skydd mot externa hot och miljöhot* är det endast två av fem kommuner som har nedskrivna riktlinjer för vad som ska göras om en naturkatastrof skulle inträffa.

Följande rekommendationer är mer oklara om kommunerna är förberedda för: *skydd av kontor, rum och faciliteter*, *allmänhetens tillträdes, leverans- och lastutrymmen* (ingen kamera, men larm), *placering av skydd och utrustning*, *kablageskydd* samt *avlägsnande av egendom*. Detta kan bero på att någon annan avdelning ansvarar för dessa frågor inom kommunen. Vad gäller kablageskydd finns kabelkanaler i samtliga kommuners kontor men kablar utanför byggnaden finns det sämre skydd för, därav hamnar denna punkt här.

Sammanfattningsvis är det åtta av tretton rekommendationer enligt ISO-standarden 27002 som minst tre av fem kommuner är förberedda för.

Några avslutande ord är Person E som säger: *"jag ser ju att det finns en risk i att fysisk säkerhet kommer lite i skymundan"* och syftar på att många leverantörer idag har mycket fokus på mjukvarubaserade säkerhetssystem. Detta stämmer överens med litteraturen där Jones (2005, s. 4) skriver *"However, the physical security of data is often overlooked"*.

Minst tre av fem kommuner är förberedda för över hälften av rekommendationerna i ISO-standarden 27002 men även om en kommun är förberedd för några rekommendationer är det oftast genom arbetssätt och sällan genom dokumenterade riktlinjer. Det är bra att följa någon typ av standard för att inte missa sådant som faktiskt är viktigt och som bör ses över kring den fysiska säkerheten inom informationssäkerhet.

7.2 Standarder

Utifrån de resultat som framkommit vid intervjuerna och den analys som gjorts av denna information kan slutsatsen dras att ingen av kommunerna efterföljer en standard. En standard som ISO-27002 innehåller rekommendationer som bör ses över inom en verksamhet men ingen av kommunerna nämner en standard som denna. De intervjuade pratar istället om konceptet BITS och dess efterträdare som är Ramverket för informationssäkerhet men nämner inte att ramverket faktiskt baserar på LIS och de rekommendationer som standarden ISO-27002 tar upp. Denna kunskap saknas hos intervjusubjekten men kunskapen om ramverket kommer förmodligen att öka då arbetet med detta sätter igång. Även om inte Ramverket för informationssäkerhet är en standard fokuserar detta ramverk mer på just informationssäkerheten då ramverket baserar på en standards rekommendationer.

Det är svårt att dra slutsats kring hur väl den valda standarden efterföljs inom en kommun då ingen kommun faktiskt efterföljer en standard. Samtliga kommuner arbetar utifrån ett koncept som Krisberedskapsmyndigheten skapat och arbetet med detta koncept (BITS) har kommit olika långt inom kommunerna på grund av tid och resurser. Givetvis påverkas arbetet med konceptet av storleken på kommunen då större kommuner oftast har mer tid och resurser att lägga på just informationssäkerhetsarbetet.

Det som skulle önskas påpekas i detta arbete är att uppmana kommuner att ta sig tid och faktiskt läsa in sig på vilka rekommendationer en standard anger inom informationssäkerheten. Även om varken tid eller resurser finns till att åtgärda samtliga rekommendationer ökas ändå kunskapen om vad en standard anser som viktiga delar att se över kring sin information. Att bara vara medveten om vad en standard är och vad en standard tar upp i sina rekommendationer kan öka kunskapen om vilka brister som finns kring informationstillgångarna, både i det fysiska skyddet samt i övriga skydd.

8 Diskussion

I detta kapitel diskuteras det kring resultatet av detta arbete och även om hur denna undersökning påverkar etiska, samhälleliga och vetenskapliga aspekter. Det ges även svar på hur den valda metoden för denna undersökning har påverkat resultatet på den huvudsakliga frågan i denna rapport. Avslutningsvis ges exempel på fortsatt undersökning inom ämnet *fysisk säkerhet inom informationssäkerhet*.

8.1 Resultat

Detta arbete ger endast en bild av hur säkerhetsarbetet kring den fysiska säkerheten inom informationssäkerhet sköts inom några kommuner och av resultaten att döma så finns det punkter som kommunerna skulle behöva arbeta mer med. Något som tydligt visat sig ha brister är just dokumentation av viktiga säkerhetspunkter. Mycket inom kommunernas hantering av information sker utifrån arbetssätt och faktiskt inte dokumenterade riktlinjer. Att beslut påverkas mer av en tredje, utomstående leverantör visar att kunskap hos kommunen saknas kring vad för typ av skydd som bör finnas kring informationstillgångarna. Om en kommun var mer medveten om rekommendationer som en standard inom informationssäkerhet tar upp skulle kommunen lättare kunna diskutera kring vilka skydd som faktiskt behövs innan en tredje part kopplas in. Kort och gott skulle medvetenheten om standarder behöva ökas inom kommuner för att på så sätt kunna leda informationssäkerhetsarbetet framåt. Av resultat att döma är det ofta så att säkerhetsarbetet påbörjas men stannar sedan upp vilket medför att brister i skyddet av information finns.

8.2 Etiska aspekter

Arbetet visar endast en bild av hur några verksamheter i den offentliga sektorn hanterar säkerhetsarbetet kring just den fysiska säkerheten inom informationssäkerhet. Ingen av kommunerna gör rätt eller fel då varje kommun bedriver sitt säkerhetsarbete på bästa sätt för deras egen skull. Denna undersökning syftar inte till att påverka lagar och regler utan syftar mer till att öka medvetenheten kring standarder och vad de faktiskt är bra för. Undersökningen syftar också till att upplysa verksamheter inom den offentliga sektorn att standarder inom informationssäkerhet kan bidra till säkrare information då en standard anger rekommendationer om delar som en verksamhet bör se över kring sin informationshantering. Detta arbete visar endast en del inom arbetet med informationssäkerhet då fler delar än just fysisk och miljörelaterad säkerhet finns att se över enligt en standard som ISO-27002.

8.3 Samhälleliga aspekter

Denna undersökning har utförts på kommuner som är en viktig instans i dagens samhälle. I undersökningen har det visat sig att det finns en del punkter enligt ISO-27002 som kommunerna skulle behöva förbättra i det fysiska skyddet kring sin information. Att utveckla det fysiska säkerhetsarbetet i form av administrativa dokument innebär att mer tid och mer resurser måste avsättas för att få detta arbete gjort. Kommuner hanterar information åt flera viktiga förvaltningar i samhället och information måste hanteras utefter hur konfidentiell informationen är. Information får inte komma i orätta händer och kommunerna måste arbeta för att information hela tiden finns tillgänglig till behöriga personer. Ingen kommun som medverkat i denna undersökning efterföljer någon standard inom informationssäkerhet.

Kommunerna har blivit uppmuntrade att följa konceptet BITS men ingen påtryckning om att vara standardiserad inom informationssäkerhet verkar ha funnits. Då information blir mer och mer känslig i dagens samhälle skulle det kanske vara intressant att införa standardisering inom informationssäkerhet i kommuner. Att följa en standard visar att verksamheten har sett över sitt säkerhetsarbete och åtgärdat de brister som funnits enligt rekommendationer som standarder anger. Givetvis innebär sådant här arbete att mer resurser och mer tid måste spenderas på just informationssäkerhetsarbetet och som det framkommer i undersökningen så finns pengar om rätt argument framförs. Hur information hanteras påverkar kommunens medborgare då konfidentiell information inte får avslöjas för obehöriga. Om exempelvis information innehållande personuppgifter avslöjas för utomstående parter innebär detta ett brott mot Personuppgiftslagen då personuppgifter måste hanteras på ett visst sätt. Om brister i det fysiska skyddet av information finns kan information göras tillgängligt för obehöriga personer. Att ha dokumenterade riktlinjer för hur information får hanteras fysiskt sett och att faktiskt utbilda personal om just informationssäkerhet skulle vara bra för verksamheter inom den offentliga sektorn då användare lättare kan förstå varför den fysiska säkerheten inom informationssäkerhet är viktig.

8.4 Vetenskapliga aspekter

Utifrån undersökningen kan lärdom dras att standarder är bra att följa då de anger rekommendationer inom flera säkerhetspunkter i hanteringen av information. Kommunerna som bidragit till resultatet i denna undersökning har visat att förbättringar inom det fysiska skyddet av information kan göras och medvetenheten kring standarder skulle kunna ökas. Det andra verksamheter kan dra lärdom av är att alltid se över samtliga delar inom informationssäkerhetsarbetet och faktiskt dokumentera vad som sker och vilka regler som ska gälla. De resultat som visas i detta arbete stämmer även överens med existerande forskning då forskningen säger att den fysiska säkerheten kommer i skymundan och att den faktiskt glöms av. Resultaten har visat att några kommuner inom den offentliga sektorn har vidtagit åtgärder i delar av det fysiska skyddet av information men att dessa åtgärder oftast inte är dokumenterade. Att ha klara och tydliga riktlinjer och regler för hur information hanteras skulle kunna förbättras genom att ha detta nedskrivet i form av policys och övriga säkerhetsinstruktioner. Som intervjuobjekten sagt är det ofta en utomstående, tredje part som bidragit till att vissa beslut tagits. En leverantör fokuserar ofta på mjukvarubaserade säkerhetslösningar vilket bidrar till att det fysiska skyddet av information kommer i andra hand. Något som kunde gjorts bättre i detta arbete är att tydliggöra för kommunerna att LIS, som intervjuobjekten talat om, faktiskt inte är en ny standard. LIS är standarder i ISO-27000 och dessa standarder har funnits sedan längre tillbaka. Kommunerna som anger att de ska följa LIS i framtiden menar MSB:s Ramverk för informationssäkerhet som baserar på LIS. Det andra verksamheter kan lära sig av detta arbete är just skillnaden mellan ett ramverk och en standard och få en tydligare bild av vad de själva faktiskt arbetar utifrån. Då information idag hanteras elektroniskt är det viktigt att lägga tid och resurser på just informationssäkerheten.

8.5 Metodval

Den valda metoden som använts för att undersöka hur väl verksamheter inom den offentliga sektorn efterföljder de rekommendationer som finns ISO-standarden 27002 angående fysisk och miljörelaterad säkerhet är intervjuer. En intervju valdes för att en intervju ger innehållsrika svar på frågor (Trost, 1994).

Undersökningen har varit en strukturerad, kvalitativ parintervju. En parintervju innebär att intervjun skett mellan en intervjuare och en intervjuad. Kylén (2004) skriver att en frågelista används vid strukturerade intervjuer. Detta har också genomförts i undersökningen då totalt 20 stycken huvudfrågor sammanställdes som sedan varje intervjuobjekt fick svara på. Innan mötet med varje intervjuobjekt skickades frågorna ut via mail till dessa personer. Detta för att personerna själva bett om att få frågorna i förväg så att förberedelse inför intervjun kunde ske.

Metoden intervju har påverkat resultatet i denna rapport positivt då berättande svar och ökad förståelse har getts via svar på de frågor som ställdes vid intervjuerna. Det gick bra att skicka frågorna innan intervjun till respektive intervjuobjekt då personerna hann förbereda sig för de frågor som skulle komma att ställas. Att spela in varje intervju har varit mycket bra då det är svårt att hinna med att skriva ned all information som sägs. Den inspelade informationen gav mycket underlag att använda vid sammanställningen av resultatet.

En nackdel med intervjuer är att en intervju är oerhört beroende av att intervjuobjektet kan ta sig tid att ställa upp på en intervju. För att undersökningen ska klara av den tidsomfattning som ges i projektet måste intervjuobjekten kunna ställa upp på en intervju inom snar framtid. I detta fall har alla intervjuobjekt varit tillmötesgående och tagit sig tid för en personlig intervju.

8.6 Fortsatt arbete

Informationssäkerhet är ett arbete som aldrig tar slut och som hela tiden behöver uppdateras och förnyas. Som det visade sig i denna undersökning är det endast två kommuner som har uppdaterade säkerhetspolicys. En kommun har en kortfattad säkerhetsinstruktion för slutanvändare och en annan kommun har ingen säkerhetspolicy alls. Den femte kommunen har en säkerhetspolicy men denna anses föråldrad. I intervjuerna med personerna för varje kommun är det oklart om säkerhetspolicyn inkluderar fysisk säkerhet och gör den det så är det mycket lite. Denna undersökning har också visat att samtliga kommuner nu ska lämna arbetet med BITS och införa ett annat ramverk istället. En fortsättning på detta arbete är:

- Att undersöka hur informationssäkerhetsarbetet bedrivs utifrån MSB:s Ramverk för informationssäkerhet. I denna rapport talar kommuner om att efterträdaren till BITS är Ramverket för informationssäkerhet och att detta ramverk är tänkt att införas i kommunen. Hur ser informationssäkerhetsarbetet i kommunerna ut i framtiden? Har Ramverket för informationssäkerhet införts och har detta haft någon betydelse för informationssäkerhetsarbetet inom kommunen?

Referenser

Allen, J. H. (2001) *The CERT Guide to System and Network Security Practices*. US: ADDISON-WESLEY, Pearson Education.

Allsopp, W. (2009) *Unauthorised Access – Physical Penetration Testing For IT Security Teams*. Tillgänglig på Internet: http://site.ebrary.com.libraryproxy.his.se/lib/hiskovde/docDetail.action?docID=10325810 [Hämtad 12.02.03]

Anderson, R. J. (2008) *Security Engineering* (2:a upplagan). US: Wiley Publishing, Inc.

Bowin, J. (red.) (2007) *Terminologi för Informationssäkerhet* (3:e upplagan). SE: SIS Förlag AB.

Erbschloe, M. (2005) *Physical Security for IT*. US: Elsevier Digital Press.

Goel, S. & Chengalur-Smith, I. N. (2010) *Metrics for characterizing the form of security policies*. *The Journal of Strategic Information Systems*, 19, (4), 281-295.

ISO (2011) *ISO/IEC 27000:2009.* Tillgänglig på Internet: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933 [Hämtad 12.05.11]

Jones, D. (2005) *The Definitive Guide To Securing Windows in the Enterprise*. US: Realtimepublishers.com, Inc.

Kylén, J-A. (2004) *Att få svar*. SE: Bonnier Utbildning AB.

LabCenter (2009) *Svenska IT-säkerhetshandboken 1.0*. SE: Pagina Förlags AB.

Limoncelli, T. A., Hogan, C. J. & Chalup, S. R. (2007) *The Practice of System and Network Administration* (2:a upplagan). US: RR Donnelley.

MSB (2010a) *Informationssäkerhet och säkerhet i IT-produkter.* Tillgänglig på Internet: http://www.informationssakerhet.se/Sakra-IT-produkter/Informationssakerhet-och-sakerhet-i-IT-produkter/ [Hämtad 12.01.18]

MSB (2010b) *Standarder*. Tillgänglig på Internet: http://www.informationssakerhet.se/Stod-i-arbetet/Standarder/ [Hämtad 12.02.08]

MSB (2010c) *Datorstödd informationssäkerhetsutbildning för användare (DISA).* Tillgänglig på Internet: http://www.informationssakerhet.se/Stod-i-arbetet/DISA-Utbildning-informationssakerhet/ [Hämtad 12.05.06]

MSB (2011a) *Gapanalys*. Tillgänglig på Internet: http://www.informationssakerhet.se/Documents/Ramverket/Gapanalys.pdf [Hämtad 12.02.07]

MSB (2011b) *Gapanalys – Checklistan*. Tillgänglig på Internet: http://www.informationssakerhet.se/Documents/Ramverket/GAP-analys%20checklista.pdf [Hämtad 12.02.07]

MSB (2011c) *Riskanalys*. Tillgänglig på Internet:
http://www.informationssakerhet.se/Documents/Ramverket/Riskanalys.pdf
[Hämtad 12.02.08]

MSB (2011d) *Introduktion till Ramverket*. Tillgänglig på Internet:
http://www.informationssakerhet.se/Documents/Ramverket/Introduktion%20till%20Ramverket.pdf [Hämtad 12.05.06]

Pfleeger, C. P. & Pfleeger, S. L. (2006) *Security in Computing* (4:e upplagan).
US: Prentice Hall, Pearson Education, Inc.
Avsnitt 1.3, 8.1-8.4.

Roy Sarkar, K. (2010) *Assessing insider threats to information security using technical, behavioural and organisational measures*.
Information Security Technical Report, 15, (3), 112-133.

SearchSecurity (2005) *Definition physical security.* Tillgänglig på Internet:
http://searchsecurity.techtarget.com/definition/physical-security [Hämtad 12.01.17]

Trost, J. (1994) *Enkätboken*.
SE: Studentlitteratur, Lund.

Trost, J. (1997) *Kvalitativa intervjuer* (2:a upplagan).
SE: Studentlitteratur, Lund.

Åhlfeldt, R-M., Spagnoletti, P. & Sindre, G. (2007) Improving the Information Security Model by using TFI*. In Proceedings of the 22tn IFIP TC-11 International Information Security Conference (SEC 2007).* Sandton, South Africa, May 14-16, 2007. pp 73-84. ISBN: 13:978-0-387-72366-2, eISBN: 13:97-387-72367-9, ISSN: 1571-5736.