Examensarbete

HÖGSKOLAN I SKÖVDE

INFORMATIONSSÄKERHET HOS SME:S

En kvalitativ studie om hur små och medelstora företag inom e-handel arbetar med informationssäkerhet

INFORMATION SECURITY AT SME:S

A qualitative study about how small and middle-sized enterprises in e-commerce work with information security

Examensarbete inom informationsteknologi
Grundnivå 30 Högskolepoäng
Vårtermin 2023

Mattias Erixon

Handledare: Jesper Holgersson
Examinator: Joeri van Laere

Sammanfattning

Informationssäkerhet är en viktig del i företagens arbete för att säkerställa att informationen som lagras inte används på fel sätt eller hamnar i fel persons händer. Numera finns det en uppsjö av standarder och verktyg som kan användas för att göra arbetet lättare. Trots dessa underlättande tjänster misslyckas många företag med att implementera informationssäkerhetsåtgärder. Små och medelstora företag är i synnerhet utsatta på grund av deras ringa storlek samt brist på kapital.

Denna studie har tagit reda på hur små och medelstora företag inom e-handel arbetar med informationssäkerhet med hjälp av en kvalitativ intervjustudie tillsammans med en induktiv analys. Totalt har fyra respondenter från fem olika företag runt om i Sverige intervjuats. Respondenterna som datan samlats in från har haft olika roller, men alla har haft någon form av ledande roll på respektive företag.

Resultatet som tas fram senare i rapporten presenterar insamlat material uppdelat i tre områden. Dessa områden är informationssäkerhetspolicy, personalfrågor och säkerhetsåtgärder. Svaren som samlas in inom dessa områden visar både likheter och skillnader till tidigare litteratur. De tyder på att SME:s inom e-handel har brister inom vissa delar av deras säkerhetsarbete, medans andra delar fungerar bättre.

Nyckelord: Informationssäkerhet, informationssäkerhetspolicy, små och medelstora företag, SME, e-handel.

INNEHÅLLSFÖRTECKNING

1 Inledning

Informationssäkerhet handlar om skydd av all information som hanteras på en organisation. För att säkerställa detta kan ett företag ta till olika åtgärder för att se till att informationen som lagras behåller sin konfidentialitet, integritet samt tillgänglighet (Whitman & Mattord, 2021). I dagens moderna samhälle kan denna uppgift vara svår att lösa, men i takt med ökad digitalisering finns det många digitala verktyg och tjänster för att underlätta detta arbete.

Informationssäkerhet kan tolkas som ett begrepp som endast går att applicera på mjukvara och hårdvara. Detta är inte fallet. Den mänskliga faktorn spelar en stor roll också. Vare sig någon är en anställd på ett företag eller en användare som nyttjar en produkt eller tjänst, finns det alltid en risk att personen utsätter sig själv eller sitt företag för attack. Det har dels att göra med avancerade metoder som illvilliga personer använder sig av för att komma åt information. Det har också att göra med människors brist på medvetenhet om just säkerhetsfrågor och vad konsekvenserna kan bli vid fel användning av digitala verktyg och tjänster (Tu & Yuan, 2014).

Små och medelstora företag (SME) är otroligt viktiga för näringslivet. Enligt European commision (2020) är nio av tio företag i EU SME och står för två av tre av alla jobb som finns tillgängliga i unionen. I Sverige är denna siffra ännu högre och svenskt näringsliv (u.å) menar att 99,9% av alla företag i Sverige är SME. Alhamari & Duncan (2020) visar på en trend att ledningen för SME:s ofta missbedömer de risker som finns riktade mot företagen, och att det leder till att onödiga risker tas. Precis som stora företag blir SME också utsatta för attacker som riktar sig mot företagens tillgångar, men konsekvenserna blir ofta större för SME:s eftersom de ofta inte har de resurser och tillgångar som krävs för att motarbete dem.

Frågan som denna studie kommer undersöka är därför hur små och medelstora företag inom e-handel arbetar med informationssäkerhet. Genom att undersöka den frågan kommer studien att ha en stor betydelse för att presentera och förstå de utmaningar som företag inom den storleken har med informationssäkerhet. Genom att analysera och identifiera möjliga risker som finns tillsammans med de säkerhetsåtgärder som företagen redan applicerar, kan det bidra till att skydda företag och organisationer från potentiella hot.

2 Bakgrundskapitel

Detta kapitel kommer ge läsaren en övergripande förståelse för ämnet informationssäkerhet och för små och medelstora företag. De delkapitel som kommer presenteras är informationssäkerhet, CIA-triaden, standarder, små och medelstora företag, hur SME:s arbetar med informationssäkerhet och hot mot SME:s. Kapitlets inledning kommer förklara begreppet informationssäkerhet och kapitlets avslutning kommer skildra SME:s och hur de arbetar med informationssäkerhet samt de hot som finns.

2.1 Informationssäkerhet

Varje organisation, oavsett verksamhet och storlek, har information som de vill hålla skydda. Informationen kan skilja sig beroende på vad det är för typ av företag, men generellt sett är det information om kunder, försäljningar samt produkter/tjänster (Whitman & Mattord, 2021). Definitionen av informationssäkerhet är skyddande av informationens konfidentialitet (confidentiality), riktighet (integrity) och tillgänglighet (availability). Detta kallas även för CIA-triaden och har varit standarden för datorsäkerhet sedan konceptet dator kom fram. Kan säkerheten för dessa tre delar i en organisation säkerställas, medför det ett stort värde för organisationen (Whitman & Mattord, 2021). Utöver CIA-triaden består även informationssäkerhet av skydd av information och dess kritiska komponenter. Dessa komponenter består bland annat av systemen och hårdvaran som används. Även datasäkerhet och nätverkssäkerhet går under namnet informationssäkerhet (Whitman & Mattord, 2021).

I takt med att datorer uppkom har dessa präglats med problem gällande säkerheten kring deras användande. Grunden för just begreppet säkerhet är att det till en början finns en tillgång som ägaren vill skydda. Detta kan i princip vara vad som helst av värde, fysiskt (något som går att ta på) eller icke-fysiskt (något som inte går att ta på, som till exempel lagrad information på en hårddisk). Inom ämnet informationssäkerhet är tillgången oftast information. För att hantera och skydda informationen används IT och andra stöd (Oscarsson, 2001).

Informationssäkerhet, som går att härleda från namnet, är i grund och botten säkerheten av all form av information som hanteras. Användningsområdena är däremot desto flera. Enligt Tu och Yuan (2014) är hanteringen av IS är en systematisk process som effektivt hanterar informationssäkerhetsrelaterade hot samt risker inom en organisation. Det är viktigt att förstå att IS inte endast handlar om att skydda data från till exempel hackare. Även den mänskliga faktorn måste finnas i åtanke. Detta innefattar bland annat medvetenhet och träning inom säkerhet för de anställda. Tu och Yuan (2014) skriver i sin artikel att om säkerhetsåtgärder inom informationssäkerhet utformas på korrekt sätt, leder det till framgång för informationssäkerhetshanteringen (Tu & Yuan, 2014). Även Åhlfeldt & Huvala (2014) lyfter fram detta i sin artikel att säkerhetsåtgärder för informationen ska baseras primärt på organisationens verksamhetsmål samt syfte.

2.2 CIA-triaden

Konfidentialitet, riktighet och tillgänglighet en vital del i arbetet för hantering av informationssäkerhet (MSB, 2016). Oscarsson (2001) hävdar i sin tur att många definierar informationssäkerhet utifrån dessa tre beståndsdelar. På engelska heter dessa: confidentiality, integrity och availability. Ofta kallas dessa tre begrepp för CIA-triaden som är en förkortning av begreppen. Enligt Samonas & Coss (2014) menar att dessa tre begrepp inte bara format förståelsen för informationssäkerhet men också i praktiken när nya kontroller utvecklas för att säkerställa säkerheten. För personer som arbetar med informationssäkerhet är CIA inte ett magiskt sätt för att skydda all känslig information. Däremot ger det dem ett stöd för att kunna identifiera och förstå hot som relaterar till den information som finns.

Vid utveckling av varje ny policy och process måste denna triad tänkas på och implementeras för att skydda ett datorsystem (Merkow & Breithaubt, 2014).

2.2.1 Confidentiality

Begreppet confidentiality (konfidentialitet) härstammar från det latinska ordet *confidere*, vilket betyder ”att ha fullt förtroende och tillit”. Denna beskrivning speglar på sättet som begreppet används i praktiken. För att upprätthålla kontroll över informationens konfidentialitet är det av prioritet att se till att korrekt auktoritet ges till rätt person. Confidentiality kan även definieras som förmågan att genomföra en uppgift, med hänsyn till uppgiftens informationsinnehåll och vem det är som har tillgång till den informationen (Samonas & Coss, 2014).

Säkerhetskontrollen för att se till att konfidentialitet existerar sker genom att det finns åtkomstkontroller på plats. När någon gör en förfrågan om att ta del av en viss typ av information eller en process måste en säkerhetsprocess finnas på plats för att kunna hantera denna förfråga på rätt sätt. Beroende på vilka policys och regler som finns på plats samt hur mjukvaru- och hårdvaruskyddet ser ut, påverkar detta hur kraftfull tillämpningen av åtkomstkontrollen är (NIST, 2002).

Ett exempel på en praktisk tillämpning av en kontroll för att säkerställa konfidentialitet är enligt Chai (2023) någon form av verifikation att personen som försöker ta del av någon information är den korrekta personen. Användarnamn och lösenord används i princip överallt, men normen börjar i dagsläget luta mer mot tvåfaktorsauktoriseringar. Det är även möjligt att inkorporera biometriska verifikationer i sitt arbete för att säkerställa sin konfidentialitet (Chai, 2023).

Vid förlust av konfidentialitet kan detta leda till att information som inte är till för allmänheten att ta del av läcks ut. Detta i sin tur kan leda till att företaget eller dess anställdas säkerhet utsätts för risker. Beroende på vilken typ av organisations information som inte hålls konfidentiell, kan detta leda en nationell säkerhetsrisk.

Utöver att informationen sprids kan påföljderna av detta vara att organisationen ”tappar ansiktet” samt att allmänhetens syn på företaget förändras åt ett sämre håll. Förlust av konfidentialitet kan även leda till olika typer av rättsliga påföljder (NIST, 2002).

2.2.2 Integrity

Ordet integrity på engelska översätts till det svenska ordet integritet eller riktighet. Riktighet innebär att innehållet i den informationen som lagras och erhålls är korrekt samt autentisk och därmed inte förvrängd på något sätt (MSB, 2016). På samma sätt som informationen måste vara riktig måste den också vara konsistent, både internt och externt. Detta är för att göra det svårare och förhindra att personer med auktoritet gör ändringar som de inte borde göra i ett system. Ett exempel på en sådan ändring kan vara att en person som har korrekt auktoritet att göra förändringar på tabellerna i en databas som hen gör utan tillåtelse från ledningen. Med detta sagt är strävan självklart också att göra det svårare och förhindra för personer utan korrekt auktoritet att göra förändringar på datan som lagras. Ett exempel som datans riktighet kan förändras av en extern part är om en hackare injicerar skadlig kod genom något av en organisations applikationer som till exempel email-service eller webbsida. Är hackaren i detta fall tillräckligt skicklig kan attacken se ut som en legitim uppdatering (Srinivasan, 2016).

När informationen som en organisation lagrar i sina system är riktig och äkta påvisar detta att företaget är seriöst och att deras system går att använda för de ändamål som de är tilltänkta att genomföra. Detta gör att de intressenter som har skapat systemets krav som till exempel andelsägare, ägare samt kunder ser att det fungerar som det ska (Samonas & Coss, 2014).

Det finns flera säkerhetskontroller för att upprätthålla informationens riktighet. Den första kontrollen är att korrekt autentisering ges till korrekt person. För att kontrollera en hävdad identitet finns går att använda lösenord, identifikationsnummer samt digitala certifikat i form av kort eller taggar. För att förhindra att data ändras i databaser kan dataägaren som har ansvar över databasen ge tillgång till ett fåtal anställda som har förtroende att göra förändringar (NIST, 2002).

Så fort data blir tillagd, borttagen eller modifierad på ett felaktigt eller illvilligt sätt är integriteten i princip förlorad. Felaktigt kan i denna kontext också innebära att någon har gjort ett misstag. Skadan är redan skedd. Om dataintegriteten är förlorad och denna används i företagets dagliga arbete kan detta leda till bedrägerier och att fel resultat tas fram. I de fall som data används för beslutsstöd för ledningen kan det leda till att helt fel beslut tas. Vid attacker på ett system kan en attack mot dataintegriteten vara ett första steg, för att sedan angripa systemets konfidentialitet och tillgänglighet. Data med integritet är därför a och o när det kommer till ett systems tillförlitlighet (NIST, 2002).

2.2.3 Availability

Ordet availability på engelska översätts till det svenska ordet tillgänglighet. Tillgänglighet i den här kontexten betyder att informationstillgångar ska kunna utnyttjas när de är tänkta att göra det, i en tidigare bestämd utsträckning. Detta innebär att de även ska finnas tillgängliga inom en given tidsram (MSB, 2016). Tillgänglighet av information i denna kontext betyder med att datan ska gå att komma åt även vid angrepp mot ett system, som vid till exempel en denial-of-service-attack eller DoS. Det finns andra typer av attacker också, men en DoS-attack riktar sig mot just tillgängligheten av ett system eller en sida. I delen om riktighet framkom det att det var viktigt att korrekt person gör korrekt ändringar i till exempel en databas. Korrekt ändringar är även viktiga när det kommer till tillgängligheten av information. I de fall som uppdateringar måste göras på en applikation eller system är det av största betydelse att dessa sker på korrekt sätt. Om uppdateringen inte verkställs på rätt sätt kan det leda till att applikationen slutar fungera. Datan blir då inte längre tillgänglig. Egentligen krävs det inte att någon modifierar ett system för att få det att sluta fungera. Det kan räcka med att en oförsiktig person snubblar över en sladd till en server för att få den att tappa ström och därmed tillgängligheten. Oavsett anledning kan konsekvenserna bli detsamma (Srinivasan, 2016).

Organisationer förlitar sig mer och mer på sina IT-system. I de fall som systemen är kritiska för att slutanvändarna ska kunna genomföra en uppgift, av någon anledning, ligger nere hindrar det organisationen för att bedriva sin verksamhet. En organisation som inte kan bedriva sin verksamhet tjänar inte hellre några pengar. Även om inte hela systemet blir otillgängligt uppstår fortfarande förluster vid förlust av enstaka funktioner. Arbetstiden för de anställda som arbetar med systemet maximeras inte. Utöver bortfall av tillgången till information för slutanvändare kan ett avbrott i ett system även innebära att personal måste sättas in/hyras in för att lösa problemet, vilket ytterligare ökar kostnaden för organisationen (NIST 2002).

2.3 Standarder

2.3.1 Vad är en standard?

En standard är ett dokument som är tänkt att vara en gemensam accepterad lösning för återkommande problem som kan uppstå i en verksamhet i en specifik bransch. Målet med dagens standarder är att skapa enhetliga och öppna rutiner som alla inom den berörda verksamheten kan enas om. En standard ska inte ses som ett verktyg som ska appliceras till 100% i en verksamhet, eftersom standardens natur är ”one-size fits all”, vilket innebär att standardens innehåll ska passa alla verksamheter inom samma bransch. En standard är däremot fördelaktigt att använda eftersom den kan bidra till att öka kvaliteten på arbetet, undvika misstolkningar samt att en organisation slipper skapa nya lösningar på ett problem varje gång de uppstår. Fördelarna med att använda en

standard kontra att inte använda en är att det skapar kostnadseffektiva processer, det höjer företagets säkerhet och kvalitet, etablerar en hög lägstanivå samt att det ger en trovärdighet både lokalt och globalt (SiS, u.å.).

2.3.2 ISO-27000:2018

Denna standard innehåller en överblick för hur säkerhetsarbetet ska gå till inom området informationssäkerhet. Standarden innehåller även en ordlista med centrala begrepp som definierar de teorier som används inom informationssäkerhetsdomänen. ISO-27000 är applicerbar på alla typer och storlekar på organisationer. Det spelar ingen roll om organisationen är en vinstinriktad, icke vinstdrivande eller statlig, alla kan dra nytta av samt tillämpa den i sin verksamhet. Alla dessa företag samlar in, lagrar, bearbetar och överför information av olika slag. Denna hantering av information skapar en risk för dessa organisationer, vare sig det är attacker med ett illvilligt uppsåt att stjäla/förstöra eller om det sker något fel vilket leder till att information förstörs eller läcks ut. Det finns även en fysisk aspekt av att ett organisation hanterar information. Inkorrekt lagrad information kan leda till att den förstörs av till exempel brand eller översvämning (SiS, 2018).

2.3.3 ISO-27001:2022

Denna standard bygger vidare från ISO-27000 och innehåller krav för hur en organisation ska göra för att upprätta, införa, upprätthålla och ständigt förbättra ett styrsystem för informationssäkerhet. För en organisation innebär implementeringen av ett sådant styrsystem att det måste skräddarsys beroende på vilka krav, behov samt vilket syfte som verksamheten har. Som denna rapport tidigare beskrivit under rubriken confidentiality, integrity och availability är en stor del av syftet med informationssäkerhet att upprätthålla att informationen som finns i en organisation är konfidentiell, riktig samt tillgänglig. När implementeringen av styrsystemet är gjort på ett korrekt sätt och dessa tre krav är uppfyllda, bidrar detta till ett ökat förtroende för verksamheten hos intressenter att potentiella risker hanteras på ett sätt som är passande.

För att styrsystemet som utvecklas för organisationen ska fungera med maximal prestanda måste det vara väl samordnat med de processer som organisation arbetar efter i sin verksamhet. Detta innebär även att när nya processer, system samt säkerhetskontroller av olika slag utvecklas och/eller implementeras, måste de vara utgå ifrån det styrsystem som finns på plats (SiS, 2022).

2.3.4 ISO-27002:2022

Denna standard innehåller information om hur säkerhetsåtgärder ska bestämmas och hur de ska användas för att hantera risker som finns i ett styrsystem för informationssäkerhet. Denna standard bygger därför vidare från ISO-27001:2022. Eftersom standarden även innehåller allmänt accepterade säkerhetsåtgärder inom informationssäkerhet, kan den användas för att hjälpa organisationer att fastställa och genomföra dessa. Med ett hänsynstagande till varje organisations unika potentiella farliga situationer kan detta dokument fungera som ett stöd för att utveckla olika specifika riktlinjer som passar in just på den organisationen (SiS, 2022).

2.4 Små och medelstora företag

Kategorin mikro, små och medelstora företag (SME) är företag vars antal anställda inte överskrider 250. Den årliga omsättningen får inte heller vara större än 50 miljoner euro, vilket är cirka 556 miljoner svenska kronor. SME:s är ryggraden av den europeiska ekonomin. Under året 2013 stod 21 miljoner SME:s för 88,8 miljoner jobb i EU. Dessa företag står därför för en stor del av antalet jobb som skapas inom unionen samt för den ekonomiska tillväxten. Nio av tio företag är SME:s och genererar två av tre arbeten (European commision, 2020).

Företagen som inkluderas i kategorin SME:s skiljer sig lite från varandra. Mikroföretag är företag som har färre än tio anställda samt att dess omsättning och eller totala balansen måste vara under två miljoner euro. Småföretag måste ha under 50 anställda samt dess omsättning och eller årliga balans är under tio miljoner euro (European commision, 2020).

I Sverige skiljer sig procentandelen för SME:s lite från hela EU. År 2019 var 99,9% av alla företag i Sverige små och medelstora. Detta innebär att 1 149 000 av 1 150 000 företag är SME:s. Det finns tre miljoner personer i Sverige som arbetar på privata företag och 65% av de personerna arbetar på något av dessa företag. År 2018 stod SME för 60 procent av den totala omsättningen i näringslivet (Svenskt näringsliv, u.å.).

Enligt SCB (2017) stod e-handelsföretag år 2016 för 21% av den totala omsättningen från svenska företag. Denna siffra var något lägre för hela EU där genomsnittet låg på 16%. När det kommer till hur denna siffra ser ut för företag inom SME-kategorin beror det på hur stort företaget är. E-handel stod endast för 10% av omsättningen hos företag som hade 10–49 anställda. Vid lite större företag inom kategorin för små och medelstora företag (50–249 anställda) stod e-handel för en femtedel (20%) av den totala omsättningen (SCB, 2017).

Murphy & Ledwith (2006) diskuterar de skillnader som finns mellan SME:S och stora företag. Det finns fyra delar i dessa företag som skiljer dem åt. Dessa är struktur, procedurer, processer och personal. När det kommer till struktur är det ledningen som ser väldigt annorlunda ut mellan SME:s och stora företag. SME:s har få eller inga lager av

ledning medan stora företag har flera lager. Det är även värt att notera att det finns en stor skillnad i nivån av standardisering. SME:s har en låg nivå av standardisering och deras procedurer är dominerade av personer. Stora företag har en hög nivå av standardisering och deras procedurer är dominerade av system (Murphy & Ledwith, 2006). Berisha & Pula (2015) presenterar ytterligare delar där SME:s skiljer sig från stora företag. Stora skillnader verkar finnas hos de anställdas utbildning och arbetsuppgifter. Stora företag är dominerade av anställda som har examen från högskola vars arbetsuppgifter är specialiserade (Berisha & Pula, 2015). Små och medelstora företag har inte samma nivå av anställda med högskoleexamen och deras arbetsuppgifter är bredare, vilket kräver att de har mer övergripande kunskaper, kontra de anställda som arbetar på stora företag. Berisha & Pula (2015) beskriver ungefär samma sak när det kommer till skillnaderna av de finansiella resurserna som även Murphy & Ledwith (2006) presenterade. Berisha & Pula (2015) menar att de finansiella skillnaderna mellan SME:s och stora företag är att SME:s förlitar sig på att familjen kan stötta företaget samt självfinansiering. Stora företag å andra sidan har en diversifierad ägarstruktur samt tillgång till anonym kapitalmarknad (Berisha & Pula, 2015).

Det finns även en skillnad mellan de företag som klassas som SME (mikro, små och medelstora företag). Pett et al. (2012) genomförde en studie där bland annat IT-kompetens jämfördes mellan företag i dessa storlekar. Resultatet de kom fram till var att kompetensen kring IT var ungefär samma hos små och medelstora företag, men att mikroföretag hade en märkbar lägre kompetens. Enligt Pett et al. (2012) kan denna tydliga skillnad mellan mikro och små och medelstora företag bero på att mikroföretag ständigt arbetar på ”kanten” mellan överlevnad och förlust, vilket innebär att större små SME:s lyckas bättre i deras verksamhet eftersom de har tillräckligt med resurser för det (Pett et al., 2020).

2.5 Hur SME:s arbetar med informationssäkerhet

Vid jämförelse mellan stora företag och företag som klassas som SME, går det se att SME:s generellt sätt har en mindre komplex uppbyggnad. Detta leder till att dessa företag är mer flexibla och kan anpassa sig till förändringar på ett bättre sätt. Däremot kan det i sin tur betyda att de möter större utmaningar än större företag. Det beror på att SME:s inte applicerar aktiviteter för riskhantering i deras verksamhet (Falkner & Hiebl, 2015). Enligt Hoppe et. al., (2020) är detta en direkt orsak av att dessa företag inte har de resurser som krävs. I stället fokuserar SME:s på deras kärnverksamhet, vare sig det är utveckling, försäljning eller produktion. De resurser som finns kvar efter det kan läggas på olika informationssäkerhetsprocesser men i de flesta fall räcker inte det.

Alhamari & Duncan (2020) menar att SME:s har ett stort problem med riskhantering. Det finns olika anledningar till att detta är fallet, men det enligt Alhamari & Duncan (2020) har det att göra med det finns en brist på både resurser och tillgångar samt en otillräckliga processer för att stötta riskhanteringsarbetet. Riskerna ökar även för SME:s

på grund av att de ofta applicerar billiga lösningar med minimala informationssäkerhetsstandarder. Det tillsammans med att de strategier och prioriteringar som SME:s har ligger bakom de risker som dessa företag utsätts för.

2.6 Hot mot SME:s

Enligt Niranjanamurthy & Dharmendra (2013) har e-handelsföretag en större risk att bli attackerade än andra hemsidor samt att konsekvenserna för en attack blir större ifall data förloras eller ändras på något sätt.

Niranjanamurthy & Dharmendra (2013) har identifierat tre typer av säkerhetshot som finns mot e-handelsföretag. Dessa är: denial of service-attacker (DoS), otillåten tillgång samt stöld och bedrägerier. Det finns två typer av DoS-attacker. Den första typen är något som kallas för email-bombing eller e-mailbombning. Det går ut på att en hackare skickar tusentals med e-mails till en dator eller nätverk i syfte att försöka förhindra åtkomst i någon form. Det är även möjligt att placera något som kallas för ”mjukvaruagenter” som i ett system som skickar ut många förfrågningar till systemet. Detta kallas även för DDoS eller distributed denial of service. Metoden för att genomföra en sådan attack är att placera flera mjukvaruagenter i flera system och samtidigt få dem att skicka förfrågningar mot det tänkta målet för attacken. Den andra typen av DoS-attack är virus. Ett datorvirus är en mjukvara som är designad att föröka sig själv och som genomför saker i ett system som är oönskat. Pinzon (2008) menar att distributionen av datorvirus sker via e-mail. Detta innebär att en anställd på företaget får ett e-mail med till exempel en länk som leder till nedladdning av skadlig kod. Denna skadliga kod kan installera olika typer program som kan spionera eller till exempel logga tryck på tangentbordet för att stjäla lösenord och andra känsliga uppgifter. Niranjanamurthy & Dharmendra (2013) fortsätter med att skriva att även worms eller datormaskar samt trojanska hästar är inräknat i virus. En datormask är en speciell typ av virus som sprider sig själv genom internet och kommer in via företagets internetuppkoppling. Enligt Onwubiko & Lenaghan (2007) används datormaskar för att genomföra DoS- eller DDoS-attacker. Dessa typer av attacker stör företagets system och kan göra att de blir oåtkomliga. Dessa typer av attacker påverkar företagets konfidentialitet, riktighet och tillgänglighet starkt (Onwubiko & Lenaghan, 2007). En trojansk häst är ett virus som är ”utklätt” till ett legitimt program. Syftet med en trojansk häst är alltså att lura en användare att köra programmet. Det möjliggör för attackeraren att till exempel skapa en felaktig order hos ett e-handelsföretag som ser korrekt ut och som kommer från ett korrekt klientsystem. När den ordern skickas till servern är det väldigt svårt att se ifall ordern är korrekt eller på något sätt falsk (Niranjanamurthy & Dharmendra, 2013).

Pinzon (2008) beskriver liknande problem som små och medelstora företag står inför när det kommer till säkerhetshot. Pinzon (2008) har identifierat de hot som anses vara mest skadligt mot datasäkerheten hos SME:s. Utöver datorvirus är även automatiserat

utnyttjande av känd sårbarhet i ett system väldigt farligt för SME:s. Det automatiserande utnyttjandet av kända sårbarheter handlar i de flesta fall inte om att ett företag blir angripet direkt och fokuserat av angriparen, utan det sker på ett mer passivt tillvägagångssätt. De allra flesta hoten i denna kategori använder sig av mjukvara som söker igenom webben och letar efter hål i säkerheten som kan utnyttjas. Pinzon (2008) fortsätter med att förklara att SME:s har en större risk att råka ut för denna typ av attack ifall företag inte regelbundet uppdaterar Windows på deras maskiner, eftersom Windows är det vanligaste sättet som angriparna hittar säkerhetshål i.

Enligt Niranjanamurthy & Dharmendra (2013) är det näst största säkerhetshotet som finns mot e-handelsföretag otillåten tillgång/åtkomst. Detta innebär att aktör har otillåten tillgång eller åtkomst till system, applikationer eller data. Detta kan antingen ske passivt eller aktivt. Sker det på ett passivt sätt innebär det att kommunikation inom företaget avlyssnas och på så sätt kan hemligheter som det företaget har avslöjas. Det är även möjligt för en aktören som genomför attacken att använda känslig information som avslöjas för att skada företaget genom att läcka ut den. Det aktiva tillvägagångssättet går ut på att modifiera system eller datan som finns i dem samt att ändra data som skickas mellan parter inom företaget. Ändringar på datan som skickas kan vara att syftet med meddelandet byts, till exempel att ett möte med en kund avbokas eller att en förhandling fördröjs. Det är även möjligt att låtsas att meddelandet kommer från en person trots att denne inte skickat i väg det (Niranjanamurthy & Dharmendra, 2013).

Det tredje största säkerhetshotet är stöld och bedrägerier. Stöld av data går ihop med hoten som berör otillåten åtkomst. Det räknas även som stöld ifall mjukvara kopieras på ett otillåtet sätt från ett företags servrar. När det kommer till bedrägerier räknas det som bedrägerier så fort datan som har blivit stulen används eller modifieras på något sätt. Företag är däremot inte endast utsatta för stölder av mjukvara eller data, utan fysiska stölder är också ett problem som existerar. I denna aspekt är det främst stölder av hårdvara, i synnerhet laptops, som är det största problemet (Niranjanamurthy & Dharmendra, 2013).

Konsekvenserna av typerna av säkerhetshoten i detta kapitel kan vara att ett företag som blir utsatt kan förlora stora mängder pengar på grund av dem. En studie som Onwubiko & Lenaghan (2007) refererar till hade 313 respondenter från SME:s som var villiga att ge svar på hur stora finansiella förluster de hade på grund av hot som påverkar datorsäkerheten. Resultatet som kom från studien visade på att 74,3% av de totala förlusterna kommer från endast fyra typer av attacker. Dessa är: datorvirus, obehörig åtkomst, stölder av laptop/telefon samt stöld av proprietär information (Onwubiko & Lenaghan, 2007).

Enligt Alhamari & Duncan (2020) är cybersäkerhet något som små och medelstora företag kraftigt missuppfattar som stora hot. Nu för tiden sker merparten av informationsutväxling mellan företagens anställda genom ”online networks”. Alhamari & Duncan (2020) hittade fem vitala perspektiv inom cybersäkerhetsåtgärder. Dessa är:

hot, beteenden, praxis, medvetenhet och beslutsfattande. Små till medelstora företag är ofta under cyberattacker som försöker stjäla eller förstöra data, eventuellt neka åtkomst till den. Trots detta hittar Alhamari & Duncan (2020) tendenser som visar på att det finns en stor naivitet när det kommer till att ta detta hot på allvar. Enligt Alhamari & Duncan (2020) menar experter inom området menar på att cyberattacker är det största hotet som ett företag har, oavsett storlek, vilket företag med denna storlek misslyckas att identifiera. Alhamari & Duncan (2020) skriver även i sin rapport att företagens anställda ofta är en brist när det kommer till cybersäkerheten med tanke på deras beteende. Anställda negligerar fastställda policies rörande information, organisationens guidelines samt regler som finns i företaget. Däremot är det inte bara de anställdas fel att det uppstår luckor i säkerheten. Forskningen visar på att personer i ledar- eller chefsroller bidrar till företagens risk att bli utsatta av cyberangrepp eftersom de ofta, utan att veta innebörden av sina handlingar, utsätter sina företag för risker. Genom mindre igenomtänkta metoder som påverkar organisationernas säkerhet, data, integritet och aktuella motmedel mot angrepp negativt. Slutligen som nämnt tidigare har företag i denna storlek generellt sett en mindre förståelse av de hot som kan påverka deras verksamhet. Enligt Alhamari & Duncan (2020) är verkställande chefer alltid beslutsfattare i någon utsträckning. När det kommer till informationssäkerhet och de strategier och policys som organisationen har för detta område, stämmer det för de flesta SME:s att det är den verkställande direktören (CEO) som är direkt involverade i implementeringen av beslut gällande cybersäkerhet (Alhamari & Duncan, 2020).

Enligt Alhamari & Duncan (2020) borde SME:s, med tanke på deras andel av marknaden samt deras benägenhet att råka ut för cyberattacker, lägga mer resurser på att hantera risker gällande cybersäkerhet och informationssäkerhet. I en studie gjord av den brittiska regeringen svarade 333 representanter från 612 SME:s att de blev råkade ut för cyberattacker under året 2018. Enligt rapporten finns det flera tekniska åtgärder för att försöka lösa detta problem, men ännu finns det fortfarande en begränsad kunskap och uppmärksamhet kring dessa lösningar. Detta är speciellt sant från ledande roller i en organisations perspektiv (Alhamari & Duncan, 2020).

3 Problemområde

Detta kapitel redovisar materialet som ligger till grund för problemområdet. Därefter presenteras studiens frågeställning samt de avgränsningar som gjorts. Kapitlet avslutas med studiens förväntade resultat.

3.1 Problembakgrund

Enligt Neama et.al. (2013) är det tack vare en revolution inom informationsteknologin under detta millenium, har antalet e-handelstjänster ökat dramatiskt i antal. Cramer-Flood (2022) presenter att år 2021 sålde e-handelsbolag runt om i världen för strax under fem triljoner amerikanska dollar. Detta är en siffra som endast förväntas att stiga de kommande åren.

Anledningen till att denna uppsats har genomförts är på grund av några faktorer. Företag som faller inom SME-kategorin står för nio av tio arbeten inom EU och genererar två tredjedelar av alla de arbeten som finns inom unionen (European commision, 2020). Enligt SCB (2017) står e-handelsföretag för en betydande del av den totala omsättningen som SME:s står för. För mindre SME:s kommer 10% av omsättningen från e-handel medan den siffran är på 20% för medelstora till stora SME:s (SCB, 2017). E-handelsföretag och SME:s generellt har en stark hotbild mot sig när det kommer till attacker som främst ämnar sig att stjäla eller förstöra information. Ifall attacker av denna typ lyckas leder det till stora finansiella förluster för företaget (Niranjanamurthy & Dharmendra, 2013; Pinzon, 2008; Onwubiko & Lenaghan, 2007). Alla dessa faktorer tillsammans bildar en anledning till att genomföra en intervjustudie med svenska små och medelstora företag för att undersöka hur de arbetar med informationssäkerhet och vad de gör för att förhindra att dessa attacker lyckas.

Trots att det finns bevis på att SME:s är hotade finns det enligt Alhamari & Duncan (2020) en tendens som visar på att personer med ledarroller underskattar säkerhetshot i en stor utsträckning. Det leder i sin tur att problem uppstår eftersom hot, risker och sårbarheter inte tas på det allvar som det borde (Alhamari & Duncan, 2020). Eftersom forskning visar på att personer med ledarpositioner inte tar säkerheten på allvar finns det ett incitament att genomföra en undersökning om hur arbetet faktiskt går till på dessa typer av företag. En studie kan ge både beslutsfattare och intressenter information om hur hantering av informationssäkerhet ser ut samt vad de borde tänka på och vad de bör undvika.

I en studie gjord av Hoppe et. al. (2020) presenterar författarna resultatet av en undersökning de gjorde som skickades ut till 37 företag som klassades som SME:s. Undersökningen kom fram till att dessa SME:s visade på allvarliga brister när det kommer till deras hantering av risker som hotade deras cybersäkerhet. Dessa brister leder till att SME:s misslyckas med att skapa en adekvat kontext för riskhantering, som i sin tur leder till brister som genomsyrar hela riskhanteringsprocessen. Falkner & Hiebl (2015) fortsätter diskussionen kring riskhanteringsprocessen och belyser att det finns

en avsaknad av forskning som fokuserar på SME:s strategier när det kommer till riskhantering. De menar att ytterligare empiriska undersökningar av dessa företag hade kunnat ge en bättre förståelse om de problem de möter i sin verksamhet.

Enligt Alhamari & Duncan (2020) kan undersökningar om hur SME:s hanterar cybersäkerhet leda till en minimering av hot och risker som drabbar dessa företag, inte minst de företag vars affärsmodell är att bedriva e-handel.

3.2 Syfte och frågeställning

Rapportens frågeställning är: ”Hur arbetar små och medelstora företag inom e-handel med informationssäkerhet?”. Genom att undersöka denna fråga kommer rapporten att presentera de fynd som samlas in genom en kvalitativ metod. Vid färdigställd rapport är syftet att kunna informera beslutsfattare och intressenter om de utmaningar och risker som små- och medelstora företag inom e-handel står inför när det gäller informationssäkerhet.

3.3 Avgränsningar

Forskning tyder på att SME:s ofta är utsatta för hot och attacker men lägger inte ner speciellt mycket resurser på att ha en väl fungerande informationssäkerhet. Vare sig det beror på en brist av resurser eller mindre bra styre är det ändå ett faktum. Därför kommer den här studien att ämna att bedriva forskning som ska ta reda på hur företag i SME-storleken arbetar med informationssäkerhet. En färdigställd rapport kan sedan användas till att fler företag kan skydda sig bättre.

För att få en helhetsbild för hur svenska företag som säljer produkter på nätet krävs det att väldigt många företag inom denna bransch undersöks. Eftersom denna uppsats är en kandidatuppsats måste orimligt mycket tid läggas på att hitta företag i olika storlekar samt undersöka hur de arbetar med informationssäkerhet. För denna uppsats finns inte den tiden eller resurser och därför är arbetet avgränsat mot endast små och medelstora företag. Samma princip gäller för varför denna rapport endast valt att inrikta sig mot företag som arbetar med e-handel. Det finns väldigt många små och medelstora företag i Sverige och många av dem arbetar med arbetsprocesser och metoder som författaren till denna uppsats inte har någon erfarenhet av. Ytterligare en anledning till att endast e-handel valts som inriktning är att det är en form av handel som inte är speciellt gammal, men som är extremt relevant tack vare dess utveckling de senaste åren.

3.4 Förväntat resultat

Det resultat som denna rapport förväntas att lyfta fram är en mer detaljerad inblick i hur svenska SME:s inom e-handel arbetar med informationssäkerhet. När undersökningen

är gjord förväntas denna uppsats kunna presentera hur arbetet ser ut och om det är/inte är tillräckligt för att hålla informationen säker.

4 Metod

Detta kapitel presenterar vilka forskningsmetoder som användes för att genomföra rapporten samt motivationen till det valet. Kapitlet avslutas med en förklaring till hur studiens intervjufrågor är formulerade.

4.1 Val av forskningsmetod

För att kunna genomföra denna vetenskapliga studie och ha en chans att kunna besvara rapportens frågeställning var ett val tvunget att göras gällande forskningsmetod för att kunna ge ett svar på frågeställningen: *”Hur arbetar små och medelstora företag inom e-handel med informationssäkerhet?”*.

Två vanliga forskningsmetoder är en kvalitativ metod och en kvantitativ metod. Starrin et al. (1996) lyfter fram de skillnader som finns mellan de två metoderna. Den kvalitativa ansatsen är något som kallas för ”teorigenererande”. Detta innebär att den ansatsen ska användas för att skapa en teori baserat på den data som samlas in. Datan som kommer samlas in för att genomföra denna metod kommer att vara bred och ska vara öppen för tolkning. Detta är någonting som en kvalitativ metod tillåter medans en kvantitativ enkätstudie inte tillåter (Starrin et al.,1996). Den kvantitativa metoden beskriver Starrin et al. (1996) som ”hypotesprövande”. I denna kontext betyder hypotesprövande att författaren i detta fall har en hypotes och utifrån den skall ämnet undersökas för att sedan ha underlag för att acceptera eller förkasta hypotesen.

Anledningen till att en kvalitativ metod har valts är på grund av den kvalitativa metodens egenskaper och att de tillåter insamling av data som möjliggöra för en beskrivning av ämnet på ett mer djupgående och detaljerat sätt (Patton, 2002).

4.2 Datainsamling

Berndtsson et al. (2008) menar att det finns två typer av intervjuer. Dessa är öppna och stängda intervjuer. Den öppna intervjun är en intervjutyp där forskaren inte har någon (eller väldigt liten) kontroll över de exakta problemen som kommer diskuteras i intervjun. Syftet med intervjun är klart (i alla fall för personen som gör intervjun) men intervjuns genomförande samt frågor är inte planerade i förtid. Syftet med en sådan intervju är att ställa öppna frågor och på så sätt få respondenten att ”öppna upp”. En stängd intervju har å andra sidan, i förväg, förberedda frågor som kommer ställas under intervjun. Om denna typ av intervju följs till punkt och pricka tillåts inga tilläggsfrågor utöver de frågor som är nedskrivna (Berndtsson et al., 2008). Enligt Denscombe (2017) finns det även semistrukturerad intervjuform. Den semistrukturerade intervjun fungerar ungefär som en blandning mellan den öppna och den stängda intervjun. Intervjuledaren har förberedda frågor och/eller ämnen som hen vill ta upp i intervjun. Däremot tillåter den semistrukturerade intervjun att intervjuledaren kan vara flexibel i

ordningen som dessa punkter tas upp, och kanske det viktigaste, låta respondenten själv utveckla idéer och prata bredare om de problem som lyfts fram av intervjuledaren.

Efter noga undersökning av för och nackdelar för de tre olika sätten att genomföra intervjuerna på, föll valet på användningen av semistrukturerade intervjuer på grund av att de tillåter följdfrågor som kan ge mer ”uttömmande” svar.

Datainsamlingen som kommer ligga till grund för den här rapporten kommer ske genom en kvalitativ vetenskaplig metod som kommer innefatta intervjuer. Intervjuerna kommer vara semi-strukturerade. Anledningen till att genomföra semistrukturerade intervjuer är på grund av att respondenten kan sitta på information kan vara svår att extrahera med hjälp av frågor som är formulerade i förtid. Enligt Patton (2002) tillåter semistrukturerade intervjuer att intervjuledaren kan ställa följdfrågor till respondenten ifall något uppstår i intervjun intervjuledaren vill veta mer om. Denna typ av intervju möjliggör intervjuledaren att försöka få så djup förståelse av ämnet som möjligt.

Datan som samlas in från intervjuerna kommer transkriberas, sammanställas och sedan analyseras.

4.3 Analys

För att kunna generera en teori utefter frågeställningen måste datan som samlas in analyseras på något sätt. Detta kommer att göras med en tematiskinduktiv analys. Berndtsson et al. (2008) menar att för kvalitativ forskning är en induktiv analys något som borde tolkas som en standard. En tematisk induktiv analys innefattar att den insamlade datan genomgås och analyseras noga för att därför kunna upptäcka mönster eller teman från varje respondent. Den tematiska induktiva analysmetoden möjliggöra för analytikern som bedriver analysen att kunna urskilja, analysera samt återge för de mönster och teman som samlats in.

Enligt Streefkerk (2023) innehåller den induktiva analysen tre steg. Det första steget är observation. För denna studie innebär observation den datainsamling som skett genom de semi-strukturerade intervjuer som gjorts. Frågorna som ställs i intervjuerna har formulerats för att få in så mycket relevant information om ämnet som möjligt. När all datainsamling är gjord går den induktiva analysen vidare till nästa steg som är att leta mönster i den data som samlats in. Patton (2002) utvecklar denna beskrivning och menar att den induktiva analysen betyder att hitta mönster, teman och kategorier i datan. Dessa fynd görs genom att analytikern (författaren) interagerar med den insamlade datan.

Dessa mönster och tendenser kommer sedan användas för att komma fram till om de är till exempel en engångsföreteelse eller om det finns någon tendens till en genomgående trend. När mönstren är hittade har de använts för att skapa en teori. Denna utarbetade

teori kommer sedermera att ligga till grund för de fynd som presenteras i analysen och slutsatsen.

4.4 Etik

Denna rapport har följt och kommer följa de forskningsetiska principer som Vetenskapsrådet (2018) tagit fram. Dessa är:

- **Tillförlitlighet**

  Denna princip ämnar sig att säkerställa forskningens kvalitet som kommer visa sig i rapportens design, metod, analys och utnyttjande av resurser (Vetenskapsrådet, 2018).

- **Ärlighet**

  Denna princip handlar om att utveckla, genomföra samt rapportera om forskning på ett öppet, rättvist och objektivt sätt (Vetenskapsrådet, 2018).

- **Respekt**

  Denna princip handlar om att ha respekt för kolleger, forskningsdeltagare, samhälle, ekosystem, kulturarv och miljö (Vetenskapsrådet, 2018).

- **Ansvarighet**

  Denna princip handlar om ansvar för forskningen från idé till publicering samt för dess vidare konsekvenser (Vetenskapsrådet, 2018).

Innan varje intervju kommer de forskningsetiska principerna förmedlas till personerna som intervjuas. De kommer meddelas om vad intervjun kommer handla om samt vilket syfte som den kommer att tjäna i rapporten. Samtycke gällande inspelning av ljud frågades även för att möjliggöra för transkribering i efterhand. Eftersom intervjun är helt frivillig att delta i kommer även frågan ställas ifall de samtycker till att svara på de frågor som ställas. Om fallet skulle vara så att de, av någon anledning, skulle vilja avbryta intervjun i förtid kommer även intervjupersonerna informeras att hen skulle få göra det när som helst. För att bibehålla respondenternas och företagens anonymitet och konfidentialitet ska det förklaras att identiteter och annan känslig information kommer ersättas med kodifierade identifierare i texten och i transkriberingen. Någon identifierbar information kommer heller delas med någon obehörig part. Innan intervjuerna kommer intervjuledaren förmedla strävan efter att behandla deltagarna med respekt och att vara lyhörd för deras önskemål och behov under forskningsprocessen. Slutligen ska intervjuledaren göra det klart för respondenten att det finns en möjlighet för denne att höra av sig till intervjuledaren efter studien är

slutförd för att ta del av de resultat som presenteras om de skulle vara intresserade av det.

4.5 Intervjufrågor

Studiens intervjufrågor som kommer användas för insamling av data är baserade på standarderna ISO-27001:2022 och ISO:27002:2022. Enligt ISO-27000:2018 är syftet med hela ISO-27000-serien att tillhandahålla en överblick för hur säkerhetsarbetet ska gå till inom området informationssäkerhet. Med övergripande innebär det att den ska vara applicerbar på alla typer av organisationer oavsett storlek (SiS, 2018). Detta innebär att informationen som står i dessa standarder kommer vara relevant för verksamheterna som kommer undersökas. Från standarderna ISO-27001:2022 och ISO-27002:2022 har relevanta delar valts för att formulera intervjufrågorna. Dessa delar har valts genom att leta efter brister som lyfts fram i tidigare litteratur och hitta motsvarande del i standarderna. Detta har medfört att frågorna både har en förankring i vetenskaplig litteratur samt i en övergripande omfattning från standarderna.

Det skulle vara möjligt att endast formulera frågor baserat på den litteratur som presenterats i bakgrundskapitlet. Där redovisas många viktiga delar för hur SME:s bedriver säkerhetsarbete som till exempel typiska brister och hot som de utsätts för. Däremot fanns det en brist på litteratur som visade hur SME:s inom e-handel arbetade med informationssäkerhet. Risken fanns att de fynd som presenterades i dessa texter inte skulle vara relevant för detta specifika forskningsområde och därför gjordes antagandet att inte endast formulera frågor utefter den litteraturen.

5 Genomförande

Detta kapitel presenterar hur den planerade metoden genomfördes i praktiken.

5.1 Etablering av kontakt med respondenter

Majoriteten av respondenterna till intervjuerna har hittats via webbsidor på internet. Till en början försökte eventuella respondenter hittas på LinkedIn, som fungerar som sociala medier för yrkesaktiva personer. För denna rapport var LinkedIn inte helt optimal för att hitta kandidater att intervjua eftersom rapporten kräver företag med relativt strikta kriterier gällande storlek och omsättning, vilket inte fanns med på LinkedIn. Därför försökte författaren hitta ett alternativ till detta. Svea bank publicerar varje år en lista med de e-handelsföretag som ökat mest i omsättning de senaste året. Denna sida var perfekt för denna rapport eftersom majoriteten av de företag som presenteras ligger inom de givna kriterierna

I Sverige finns det väldigt mycket e-handelsföretag och den allra största majoriteten av dessa omsätter mindre än 500 miljoner kronor och har färre än 250 anställda. Detta gjorde det enkelt att hitta väldigt mycket företag att skicka ut förfrågningar till, eftersom de företag som inte faller in i den kategorin är välkända som författaren kände till och därför kunde undvika. Minoriteten av respondenterna har hittats via författarens egna kontakter. Kriterierna är dock desamma.

5.2 Urval

Urvalet som tillämpas på en studie är helt beroende av vad syftet med studien är (Lundén, 2020). Syftet med den här studien är att ta reda på hur små och medelstora e-handelsföretag arbetar med informationssäkerhet. För att kunna besvara den frågan på bästa sätt är det viktigt att intervjua de personer som kan ge informationsrika svar på de frågor som ställs. Därför har ett strategiskt urval använts i denna studie. Det strategiska urvalet innebär att de personer som intervjuas har mycket erfarenhet och kunskap inom det ämne som undersöks (Lundén, 2020).

De kriterier som personen på företaget var tvungen att ha för att ha var kunna delta i studien var att personen har något form av ansvar för säkerhetsfrågor.

Författaren till denna rapport har skickat ut förfrågningar till e-handelsföretag som klassas som SME:s. Eftersom det var svårt att direkt kontakta den person som var ansvarig för de frågorna på företaget, har kundtjänsten kontaktats i de flesta fall. Företagens kundtjänst har sedan antingen skickat vidare ärendet till ansvarig person eller skickat tillbaka en mailadress tillhörande ansvarig person till författaren.

5.3 Genomförandet av intervjuer

Intervjuerna genomfördes under loppet av cirka fyra veckor. Tack vare att tillfällena för intervjuerna var spridda tillät det att svaren som samlades in kunde transkriberas och granskas innan det var dags för nästa intervju. Detta tillvägagångssätt skapade en större förståelse för de svar som varje respondent gav. Varje intervjutillfälle genomfördes med hjälp av samtalsprogrammet Microsoft Teams. Detta val gjordes för att merparten av de företagen som intervjuades endast använde teams för att ha möten på distans. Mötena genomfördes med att båda parter hade sin webbkamera på, vilket möjliggjorde för iakttagelse av ansiktsuttryck och kroppsspråk. I samtliga intervjuer deltog endast intervjuledaren (författaren) och en respondent. Intervjuledaren ställde alla frågor som var bestämda sedan tidigare och vid behov ställdes följdfrågor för att försöka få respondenten att utveckla sitt svar.

Tack vare att tid fanns mellan varje intervju utökades kvaliteten på nästkommande intervju. Det gav författaren tid att djupare analysera varje enskild intervju ner på djupet för att få en bredare förståelse av de svar som samlades in samt vad som hade gått bra och vad som gått dåligt. Dessa kunskaper kunde sedan inkorporeras vid senare intervjuer för att ställa relevanta följdfrågor samt känna igen eventuella mönster.

Från en början var strategin att intervjua minst fem företag och därför ha med fem respondenter i studien. Detta visade sig vara en miss från författarens sida eftersom företagens villighet att svara på frågor om informationssäkerhet överskattades. Cirka 200–250 förfrågningar skickades ut till företag med olika storlekar och i olika branscher men endast fyra var villiga att ställa upp på intervju. Trots bakslaget gällande antalet respondenter utdelade de intervjuer som blev av viktig information som skapade en bra grund för analys. Respondenterna som ligger till grunden för det insamlade empiriska materialet har alla bra erfarenheter samt mycket ansvar i respektive företag. Det går på grund av detta anse att den data som samlats in räcker för att ge ett tillräckligt vetenskapligt underlag för rapporten.

6 Materialpresentation & analys

Detta kapitel presenterar det material från den data som samlats in från intervjuerna. För att öka kapitlets läsbarhet har även analysen skrivits med i detta kapitel. Analysen av varje tema kommer sist i vardera delkapitel, det vill säga efter materialpresentationen. De teman som finns i detta kapitel grundar sig på de frågor som ställts till varje respondent som i sin tur är uppdelade i tre delar som är baserade på olika standarder. Det första temat är informationssäkerhetspolicy och det grundar sig på ISO-27001:2022. Det andra temat är personalfrågor och är grundat på ISO-27001:2022 och ISO-27002:2022. Det tredje temat är säkerhetsåtgärder och är grundat på ISO-27002:2022.

6.1 Respondenter

Den huvudsakliga insamlingen av data till denna studie har skett genom intervjuer med fem SME:s som arbetar med e-handel. Totalt har fyra respondenter svarat på intervjufrågorna och det beror på att respondent 4 (R4) är e-handel och IT-ansvarig för två företag. På grund av både önskemål samt etiska överväganden är både företagen, respondenterna samt eventuell känslig information i svaren anonyma. För att ge en bättre förståelse för varje företag ges en kort beskrivning nedan om varje företag samt respondent.

Respondent 1 (R1)

Denna respondent är VD för ett företag med cirka 15 anställda som omsätter omkring 100 miljoner varje år. Respondenten har arbetat med företaget sedan 2010 och sedan 2016 som VD. Företagets e-handel fokuserar sig inte mot slutkonsument utan har endast en B2B-handel. De har haft verksamhet sedan 2010.

Respondent 2 (R2)

Denna respondent är VD för ett företag med cirka 65 anställda som omsätter omkring 200 miljoner varje år. Respondenten har 30 års erfarenhet av e-handel och 20 års erfarenhet som VD för ett e-handelsföretag.

Respondent 3 (R3)

Denna respondent är IT-utvecklingschef på ett företag med ungefär 50 anställda och som omsatte 178 miljoner förra året. Respondenten har tre års erfarenhet i sin nuvarande post, men har arbetat i branschen i cirka 20 år.

Respondent 4 (R4)

Denna respondent är e-handel och IT-ansvarig för två företag med åtta respektive fem anställda. Det första företaget F1 omsätter ungefär 32 miljoner kronor medans det andra företaget F2 omsätter cirka 17 miljoner. Respondenten har nio års erfarenhet av e-handel.

6.2 Empiriskt material

Detta delkapitel presenterar de svar som gavs av de respondenter som valde att delta genom att svara på frågorna i intervjuerna. Materialet är uppdelat baserat på de frågor som ställdes. Intervjumallen kan hittas i bilaga 1.

6.2.1 Grundläggande information om företag och respondent

Innan den huvudsakliga intervjun började ställdes några inledande frågor kring lite grundläggande information av företaget. Den första frågan som ställdes var **”Hur många anställda har företaget?”.** Ingen av respondenterna förutom R4 kunde/ville svara med ett exakt nummer utan svarade antingen ”ungefär” eller ”cirka” när de svarade på frågan. Respondent 1 svarade: ”Cirka 15 stycken” (R1), respondent 2 svarade: ”Cirka 60–65 årsanställda” (R2), respondent 3 svarade: ”Vi är ungefär 50 anställda” (R3) och respondent 4 svarade: ”[Företag 1 (F1)] har åtta anställda och [Företag 2 (F2)] har fem anställda.

Därefter ställdes frågan **”Hur mycket omsätter företaget varje år?”.** Även på denna fråga var det ingen respondent som hade ett exakt svar som hen var säker på att det stämde. Ingen av respondenterna tvekade eller förmedlade att de inte ville svara den exakta siffran. Respondent 1 svarade: ”100 miljoner ” (R1), respondent 2 svarade: ”Ääh, 200 miljoner säger vi” (R2), respondent 3 svarade: ”Förra året var det nog 178 miljoner” (R3) och respondent 4 svarade: ”F2 omsatte 17 förra året och F1 omsatte ungefär 32” (R4).

Sedan ställdes frågan **”Hur länge har företaget bedrivit e-handel?”.** Precis som de två föregående frågorna var det ingen respondent som kunde ge ett tveklöst svar på den frågan. Alla svar var ungefärsvar och uppskattade av respondenten. Respondent 1 svarade ”…nu måste jag tänka efter, 2010 kanske” (R1), respondent 2 svarade ”2000 skulle jag säga slarvigt” (R2) och respondent 3 svarade ”…jag tror vi fyller tio år så vi säger tio till tolv år då kanske” (R3). R4 svarade: ”F1 har bedrivit e-handel sedan 2014 och F2 har sen 2018” (R4).

Efter dessa grundläggande frågor om företaget ställdes frågor om respondenten själv. Frågan som ställdes var **”Hur många års erfarenhet av e-handel har du?”** och **”Vad har du för huvudsaklig arbetssyssla?”**. Svaren på den här frågan skiljde sig ganska

mycket från varandra. Respondent 1 svarade att hen haft posten som VD sedan 2016, men att hen arbetat med e-handel sedan 2010. Hen påpekade dock att det inte var hens ”core” utan att hen i stället är utbildad ekonom och revisor från början, men på grund av VD-posten måste hen även hantera säkerhetsfrågor på företaget. Hen sade förklarade detta som: ”Jag är ju inblandad i allting egentligen på en övergripande nivå” (R1). Respondent 2 svarade ”I e-handel? Då har jag väl 1984 till nu då ungefär” (R2). Hen svarade även att har 30 års erfarenhet av att vara VD för e-handelsföretag. Respondent 3 svarade att hen arbetat inom IT-branschen i 20 år, men att hen har erfarenhet som IT-utvecklingschef tio år. Respondent 4 svarade att hen har arbetat med e-handel och varit IT-ansvarig sen 2014 då F1 skapades.

6.2.2 Informationssäkerhetspolicy

Frågorna som ställdes inom detta delkapitel är baserade på ISO-standarden 27001:2022. Det kapitel som rör frågorna i standarden är kapitel 5 som är ledarskap. Det aktuella delkapitlet är 5.2 som heter informationssäkerhetspolicy.

Den första frågan som ställdes inom detta område var **”Har företaget någon informationssäkerhetspolicy?”**. Alla förutom R2 kunde inte svara på ett självsäkert sätt på denna fråga.

R1 svarade på frågan genom att säga att de har några styrdokument och att ”ibland har vi ju tvingats skriva en miljöpolicy” (R1). Hen fortsatte med att säga att hen ansåg att det fanns delvis en sådan policy i deras anställningsavtal., men att det berodde på gentemot vem. Intervjuledaren ställde då följdfrågan **”Har ni ett dokument som hanterar informationssäkerhet som är överskridande för hela er verksamhet?”** Svaret som R1 gav till den frågan var: ”Nej, det har vi inte” (R1). Eftersom R1 pratade om en anställningsavtal som ett svar till om företaget hade en informationssäkerhetspolicy ställdes följdfrågan: **”Men du sa att ni hade någon form av policy gentemot anställda, vad var det?”**. R1 svarade på den frågan med:

”Det skriver man ju alltid ett anställsavtal, men det är ju ganska mycket som egentligen följer enligt lag. Du har ju inte rätt att prata om vad som händer på ett företag oavsett om jag skrivit det eller inte.” (R1).

R1 fortsätter med att säga att en ”informationspolicy” finns i anställningsavtalet. Hen sade med att hen skickar ut ett varningsmejl ungefär varannan månad för att öka medvetenheten hos de anställda om att inte klicka på konstiga länkar de får på mejl. Någon annan form av policy eller process gällande informationssäkerhet verkade inte finnas hos företaget som R1 representerade.

R2 var väldigt självsäker när hen svarade på frågan **”Har företaget någon informationssäkerhetspolicy?”**. Hen svarade att de har många policys, men inte en informationssäkerhetspolicy. För att ta reda på mer information om detta ställdes följdfrågan: **”Okej, hur kommer det sig att ni inte har någon informationssäkerhetspolicy?”.** R2 svarade på denna följdfråga som följande:

”Vi tycker väl att vi är så pass outsourcade åt det företaget som sköter det här åt oss har vi så nära arbete med så vi har aldrig skrivit någon egen sådan utan vi arbetar nära dem.” (R2).

Efter det svaret ställdes en följdfråga till R2: **”Och när du menar outsourcing, har ni något IT-företag som löser det eller hur menar du?”.** R2 svarade på denna fråga genom att gå in på detalj om de plattformar som företaget arbetar med när det kommer till IT. Bolaget där R2 är VD för har tre plattformar där all deras verksamhet sker. Ett system kallade R2 för ”funktions-IT” där all deras kommunikation sker och där informationen finns lagrad på servrar. Det är R2:s personliga kompis som driver det företaget. Sedan har de ett affärssystem som är grunden till alla affärer, leverantörer och kunder. Den tredje plattformen de har är deras webbsystem för kunder som är uppbyggt av ett företag som ligger geografiskt nära R2:s bolag.

”Så dom tre företagen har vi ju lagt vårt liv i händerna på. Du har ju rätt i det du gör och jag förstår ju hur den här intervjun kommer bäras. Så ta det här som att nu möter du ett gammalt företag som litar väldigt mycket på parterna dom jobbar med.” (R2).

Detta svar gjorde att intervjuledaren blev intresserad av vad R2 faktiskt tycker om den här lösningen. En följdfråga ställdes: **”Ser du något problem med det sättet att arbeta på, när det kommer till säkerhet?”.** R2 svarade på denna fråga med att säga att hen inte ser något problem med det hela. Däremot har R2 träffat revisorer som tittat på hur situationen ser ut, och att deras råd har varit att bolaget måste dokumentera mer och skriva avtal och ”sånt där naturligtvis” (R2). Intervjuledaren bad om konkreta exempel på vad det skulle innebära, och R2 svarade på det med att de endast skrivit enkla standardavtal med deras parter. Hen fortsatte med att det förmodligen skulle innebära ”SLAR” och att ha avtal på plats som kan hantera avtalsbrott samt ”just för informationsbiten så att det inte missbrukas på något sätt” (R2).

Precis som R1 var R3 något tvekande när hen svarade på frågan **”Har företaget någon informationssäkerhetspolicy?”**. Först svarade respondenten: ”Ja, det skulle jag väl vilja säga att vi har” (R3). När följdfrågan **”Och ungefär vad innehåller den policyn?”**

ställdes var svaret mer osäkert. Först svarade R3 att de har dels en policy för email och en policy för de enheter som används för att sköta sitt arbete. Hen gick vidare med att säga att det finns i personalhandboken vad en anställd får göra och inte göra med bolagets telefoner och datorer samt hur de får bete sig på sociala medier. Intervjuledaren ville få reda på om bolaget hade ytterligare policies kring säkerhet och ställde följdfrågan: **”Har ni någon ytterligare policy för hur hanteringen ska gå till utöver just devices och email?”**. På den frågan svarade R1 att det finns en lång text om hur man ska förhålla sig till när man representerar företaget samt att de aktivt arbetar för säkerhet på deras arbete. R3 skickar ut fingerade phising-mail till de anställda som kan råka ut för sådana. Efter säkerhetstestet är gjord följs dessa upp med en utbildning.

”Och så följer vi upp med utbildning har vi, det har vi gjort sen förra året. Och så så det har vi liksom vi som många har nog intensifierat vårat säkerhetsarbete en del. För det är faktiskt, det är rätt svårt när man är ett litet bolag att hänga med.” (R3).

Just nu håller bolaget som R3 arbetar på med årets utbildning och tanken är att det ska ske på en årlig basis.

Därefter ställdes frågan: **”Om ni ser att det finns behov att uppdatera någon policy inom det här, gör ni det då?”**. R3 svarade med: ”Ja, men det skulle vi göra absolut” (R3). För att fördjupa det svaret ställde intervjuledaren följdfrågan: **”Har ni gjort det innan?”**. R3 svarade att hen aldrig uppdaterat dem, men att hen kollat igenom de policies som fanns i personalhandboken och ansåg att de inte behövde uppdateras. Andra rutiner som är mer ”processnära” som till exempel löpande, årliga rutiner för att gå igenom och rensa konton. Dessa gås igenom på en kvartalsbasis. Resterande uppdateringar av policies sker mer ”ad-hoc” eftersom bolaget är så pass litet. Hen menade med att det är lite mjukare regler med att uppdatera dokument i ett företag i den storleken till skillnad till ett stort företag.

”Det är mjukare och man behöver [vara] inte lika officiell i när man uppdaterar dokument och sådär eftersom vi bara är några få personer som liksom, ja ändrar vi någonting så behöver man bara prata ihop sig.” (R3)

R4 svarade att de faktiskt har en informationssäkerhetspolicy för F1, trots storleken på företaget. Policyn handlar främst om GDPR och hur företagen ska hantera inlogg, filhantering och lagring samt hur företagen delar information mellan olika parter. För F2 menade R4 att det är ”mycket mer generellt, kanske inte en IT-säkerhetspolicy utan det är mer GDPR-policy att ha på webben” (R4). Följdfrågan: **”Hur kommer det sig att F2**

inte har någon informationssäkerhetspolicy?” ställdes till R4. Hen svarade då att ”de hade vi inte till F1 heller innan” (R4). Hen förklarade att de varken haft tid eller fokus på att göra en sådan.

Enligt SiS (2022) är meningen med ISO-27001:2022 att införa ett ledningssystem för organisationer och därför upprätthålla företagets konfidentialitet, riktighet och tillgänglighet. Utan en välskriven informationssäkerhetspolicy kan detta leda till missförstånd gällande hur processer ska utföras på arbetet och därmed utsätta ett företag för risker. När frågan ifall företaget som respondenterna arbetade på hade en informationssäkerhetspolicy ställdes var de flesta svar till en början relativt kortfattade och svarade i princip antingen ja eller nej. Ett undantag för detta var R4 som verkade ha en bra förståelse för vad en sådan policy är samt vad den innehåller. Hen talade om att den främst handlar om GDPR och hur företaget ska hantera inlogg, filhantering, lagring samt hur information ska delas. De andra respondenterna hade inte samma välutformade policy eller kunskap som R4 hade. R1 svarade att hens bolag hade en informationssäkerhetspolicy, men efter en följdfråga blev det tydligt att hen egentligen inte visste vad en sådan policy skulle innebära. R1 hänvisade till anställsavtalet vilket i sig inte är en informationssäkerhetspolicy. Samma ovisshet gällande vad en informationssäkerhetspolicy innebär eller ska innehålla verkade vara en genomgående trend från alla respondenter, förutom R4. R2 svarade att hen lagt hela sitt liv i händerna på tre IT-företag som sköter dessa typer av frågor åt dem, men R2 har ingen egen kunskap. Däremot verkar det inte som att denna outsourcing är tillräcklig för att skydda R2:s företag eftersom hen själv talade om att revisorer har sagt att bolaget måste dokumentera mer och skriva avtal. R3, precis som R1, menade att de hade en informationssäkerhetspolicy, men på närmare undersökning visade det sig att den policyn endast handlade om e-mail samt vad de anställda får göra med de enheter de får tilldelade av företaget.

Enligt Alhamari & Duncan (ÅRTAL) finns det ett missförstånd från små och medelstora företags sida när det kommer till säkerhet. Missförstånd och underskattning av risker gör att SME:s blir väldigt utsatta. Trots dessa hot och risker visar Alhamari & Duncan (2020) på att personer med ledarroll i SME:s inte tar detta på största allvar och därför riskerar dessa företag att bli skadade. Respondenterna som lämnat allt empiriskt material till denna studie har någon form av ledarroll på respektive företag. Respondenterna är antingen verkställande direktör, IT-utvecklingschef eller ansvarig för IT och e-handel. Detta går därför att tolkas som att den trend som Alhamari & Duncan (2020) påvisade, även stämmer för den här studien, trots att omfattningen, såklart, är mindre.

6.2.3 Personalfrågor

Frågorna som ställdes inom detta delkapitel är baserade på ISO-standarderna ISO-27001:2022 samt 27002:2022. Delkapitlet som används från 27001:2022 är 7.3 (medvetenhet). De delkapitel som använts från ISO-27002:2022 är 6.1 och 6.3

(bakgrundskontroll respektive medvetenhet och utbildning inom informationssäkerhet).

Den första frågan som ställdes av intervjuledaren var: **”Har ni någon bakgrundskontroll på nyanställda?”**. På denna fråga var det endast R1 som visade på någon form av en ordentlig bakgrundskontroll som görs på företaget. Resterande respondenter förlitade sig på de nyanställdas ”vänner” samt referenser från tidigare arbetsplatser. R1 svarade: ”Jag gör ju lite, UC och referenser. Men jag tar inte registerutdrag.” (R1). UC i detta fall är en tjänst som gör det möjligt att kolla upp en persons ekonomiska data, eller med andra ord, en kreditkontroll. Däremot gör R1 inte något utdrag från belastningsregistret vid anställning av en ny person. Intervjuledaren försökte leda konversationen in på varför detta är fallet. R1 svarade att hen tyckte att det är ”lite svårt” (R1). Hen är medveten om att det är lagkrav inom vissa branscher men att för hennes bolag finns det andra sätt att sålla bort oönskade kandidater, som till exempel betyg. R1 sa sedan att det finns vissa fall då hen faktiskt kollat upp en person som hen skulle anställa och hittade en dom på den personen. Det visade sig att personen hade en fortkörningsbot och att R1 ansåg att: ”Det är ju en [person] som anställningsbar skulle man ju kunna tycka” (R1). R1 fortsatte att det egentligen spelar roll för vilken tjänst personen söker till. Är tjänsten till kontoret och det finns tre kandidater tycker R1 att man kan lägga ner mer tid på dem, men är det anställda till lagret så kan man sålla bort de personer som ”bara har det minsta på sig” (R1). Eftersom bolaget som R1 är VD för ligger i en medelstor stad i Sverige, har R1 lite koll på de personer som arbetar på företaget utan att göra en regelrätt bakgrundskontroll.

”Som till exempel med [ANSTÄLLD] så har jag ju lite koll på hans familj att han kommer från lite ordnade omständigheter, så det kan ju också ses som någon form av bakgrundskoll.” (R1)

Hen dividerade även kring huruvida en person ska få en andra chans eller inte.

”Man kan ju tycka så att människor ska få andra chanser så länge det inte är brott mot andra människor. För det vore ju förfärligt om man inte fick en andra chans om man gjorde ett brott i sin ungdom.” (R1)

Slutligen försökte R1 rättfärdiga sitt val att inte ha en ordentlig bakgrundskontroll genom att säga att deras verksamhet inte handlar om rikets säkerhet. Deras verksamhet skulle inte skadas så mycket ifall en konkurrent till exempel skulle få information om att företaget precis fått in en ny produkt.

När frågan **”Har ni någon bakgrundskontroll på nyanställda?”** ställdes till R2 blev svaret att det är lite olika beroende på vilka tjänster som personen söks till. I de fall som personer söks till kontoret använder de sig av rekryteringsbyråer. Dessa gör en bakgrundskontroll åt R2:s bolag och det innefattar att de gör ett utdrag från personen i frågas brottsregister. Däremot när en person anställs till företagets lager ser processen annorlunda ut. R2 sa då att ofta kommer personer in dit som halvt känner någon som redan arbetar där, och att det då blir en sämre bakgrundskontroll. Intervjuledaren ställde då följdfrågan **”Har ni någon form av bakgrundskontroll till de lite lightare tjänsterna?”**. R2 svarade: ”inte annat än liksom om du berättar att det är din kompis så frågar vi dig vem kompisen är och så” (R2). Intervjuledaren ställde följdfrågan **”Okej, så ni anställer bara kompisar då? Har jag förstått det rätt?”.** R2 svarade att det delvis blir mycket så. Men det handlar endast om de som företaget själva anställer. Resterande arbetskraft hyrs in från bemanningsföretag. Några av dessa inhyrda personer blir sedan anställda och då ”har man ju i princip gjort den bästa undersökningen man kan för [då] har man jobbat ihop” (R2).

R3 svar på frågan: **”Har ni någon bakgrundskontroll på nyanställda?”** var väldigt kortfattad. Svaret var: ”Nej. Eller ja, det beror på. Vi tar ju referenser från andra tidigare arbetsgivare” (R3). Intervjuledaren ställde följdfrågan: **”Men inget sånt här brottsregister eller kreditkontroll?”**. R3 svarade nej.

R4 svarade på liknande sätt som R2. De gör ingen bakgrundskontroll eftersom R4 anställer personer ”som vi redan har en relation till” (R4). Till F1 anställer de inte mycket folk utifrån, så det blir så att de flesta de anställer känner de redan sen tidigare och att de redan vet vem personen är. Till F2 säger R4 att det är en lite bredare rekryteringsprocess, men att de inte heller där gör något utdrag från något register. Till både F1 och F2 menar R4 att de tar minst två referenser från tidigare arbetsgivare.

Därefter ställdes frågan: **”På vilket sätt introduceras nyanställda?”**. Här hänvisade både R2, R3 och R4 till personalhandboken som är aktuell för vardera arbetsplats. R1 svarade att hen brukar gå igenom anställningsavtalet tydligt med den nyanställde. Enligt R1 står det i anställningsavtalet att allting som händer på företaget är hemligt och att man inte får säga vad som helst. R1 fortsatte med att säga att hen brukar tala om för de nyanställda att de är ett börsbolag vilket innebär att de kan komma att ta del av hemlig information som de inte får dela vidare. Sist sade R1 att anställningsavtalet även innehåller ”lite information om hur vi lagrar data och lite så om såna saker” (R1).

R2 svarade att det är extremt olika hur nyanställda introduceras på bolaget. Det beror på vilket avdelning som den nya personen kommer till, eftersom de har både kontor och lager. Hen fortsatte med att säga att de har personalhandböcker och ”lite såna bitar, allmänna” (R2). Anställs en person till kontoret är det en avdelningschef som står för introduktionen. Vid anställning till lagret får den nyanställde en handledare som talar om hur saker och ting går till. Intervjuledaren ställde då en följdfråga till R2 **”Men de anställda som arbetar med just känsliga uppgifter, introduceras de på något**

speciellt sätt?". R2 svarade med att de har en kundtjänst i flera länder och att där finns det ett ”informationsbehov”. Personen som hanterar den kundtjänsten har tillgång att nyttja flera olika verktyg och till exempel titta på en kunds adress, men den personen får inte berätta den informationen för någon annan.

”Det är ju nästan det känsligaste vi har idag, privata personuppgifter. Identiteter överlag” (R2)

R3 var precis som på föregående fråga väldigt kortfattad när hen svarade på frågan om hur nyanställda introducerades till arbetsplatsen. Eftersom R3 redan talat om att det finns någon form av introduktion inskriven i personalhandboken frågade intervjuledaren: **”Du nämnde den här personalhandboken men informeras de nyanställda på något annat sätt om informationssäkerhetspolicyn?”**. R3 svarade: ”Det är nog bara i den. Sen får man sin information vid de årliga genomgångarna” (R3).

R4 svarade på frågan: **”På vilket sätt introduceras nyanställda?”** med att svara att det går via närmsta chef och att det är chefen som introducerar dem till de rutiner och dokument som finns. När det kommer till informationssäkerhetspolicyn får den nyanställde en personalhandbok där alla policies som personen måste veta. Enligt R4 innehåller personalhandboken: ”syftet med IT-policyn, ansvar, fysisk säkerhet, vid stöld, anmälning, e-post, lösenord och granskning av IT-system” (R4).

Därefter ställdes frågan **”Utbildas anställda för ökad medvetenhet gällande informationssäkerhet?”**. R1 och R3 gav svar som tyder på att de har någon form av utbildning för sina anställda. R2 svarade bara att de inte hade någon utbildning för att öka medvetenheten hos sina anställda och R4 svarade att de inte hade någon annan utbildning utöver informationssäkerhetspolicyn. R1 nämnde på en tidigare fråga att hen skickar ut fingerade mail med länkar i sig för att se vilka som klickar på dem. På denna fråga utvecklade hen svaret lite. R1 menar att de ganska ofta får mail som ser ut som att det kommer från antingen R1 eller någon annan på företaget som uppmanar mottagaren att sätta över pengar på ett visst konto. R1 sade dock att ”jag kan säga att det är ganska lätt att genomskåda, men det är ändå viktigt att vara medveten om att det händer ofta” (R1). R1 fortsatte att det är ganska upptäcka sådana mail eftersom de ofta inte har någon ordentlig ”sidfot” från företaget och att det inte fungerar att sätta över pengar på ett konto på det sättet som de frågar om, utan det måste finnas ett korrekt underlag för transaktionen och det vet personalen på bolaget.

R3 svarade att hen anser att de har det och att de har en bra ”kultur” på arbetsplatsen. Är det något konstigt mail som dyker upp brukar de anställda skriva på de gemensamma chattarna om det så att alla får reda på det. De anställda vet även att de kan kontakta deras IT-partner ifall de har några frågor. Det är även IT-partnern till företaget som håller i utbildningarna. R3 menar att deras fördelaktiga ”kultur” kommer från att de

gjorde ett stort arbete i samband med att GDPR kom. Hen menar att folk nästan blev rädda när GDPR-lagarna kom vilket gjorde att folk anpassade sig bättre.

Enligt SiS (2022) är standarderna 27001:2022 och 27002:2022 bland annat till för att underlätta ett företags arbete med ledningens och de anställdas medvetenhet gällande informationssäkerhet samt företagen har säkerhetsåtgärder riktade mot personrelaterade hot. I 27002:2022 kapitel 6.1 och 6.3 (bakgrundskontroll respektive medvetenhet och utbildning) står det att syftet med de är att säkerställa att all personal på organisationen är behörig samt lämplig för dennes roll på företaget. Det framgår även att syftet är att säkerställa att personalen och relevanta intressenter känner till sitt ansvar gällande informationssäkerhet.

Svaren på frågan ifall företaget som respondenten arbetar på hade en informationssäkerhetspolicy redovisades under föregående delkapitel (5.3.2 Informationssäkerhetspolicy). Det blev det klart att majoriteten av företagen inte hade en informationssäkerhetspolicy eller att de trodde att de hade en, fast att den inte innehöll de delar som krävs för att kalla den för en sådan. Däremot hade R4 en välformulerad policy. Det kan verka onödigt för ett företag att utbilda anställda för att öka deras medvetenhet när de inte har en policy. Var ifrån kommer information och hur väl passar den ihop med organisationen i så fall? Det är också värt att fundera över hur strukturerad utbildningen blir då. Respondenternas svar på om de har någon utbildning för deras anställda differentierar lite från varandra. R1 och R3 hade ingen informationssäkerhetspolicy men hade ändå någon form av utbildning åt sina anställda, även fast den är relativt minimal. Både R1 och R3 skickar fingerade email till sina anställda för att försöka bättra deras medvetenhet när det kommer till phising-attacker. Även fast detta är ett relativt enkelt sätt att säga att man utbildar sina anställda, gör det ändå nytta vilket Lok (2022) bekräftar. Lok (2022) menar att många seniora cybersäkerhetsspecialister tror att anställda som blivit utsatta för simulerade attacker har en högre chans att upptäcka och rapportera suspekta e-mails kontra de anställda om inte blivit utsatta.

Enligt SiS (2022) är syftet med en bakgrundskontroll att säkerställa att den anställde eller personen som ska bli anställd är behörig och lämplig för den aktuella rollen. Endast R1 och R2 hade något som skulle kunna kallas för en bakgrundskontroll när de anställer nya personer. R1 hade den mest omfattande bakgrundskontrollen. R1 gjorde kreditkontroller samt tog referenser från tidigare arbetsgivare, men inga utdrag från brottsregistret. R2 menade att hade en rekryteringsbyrå som sköter deras bakgrundskontroll, vilket följer temat att bolaget outsourcar mycket arbete som har att göra med säkerhet. Enligt R2 innefattade rekryteringsbolagets bakgrundkontroll bland annat ett utdrag från belastningsregistret, men kunde inte gå in på mer detalj. Enligt Binns & Kempf (2021) kan en anställning av en kriminellt belastad person leda till allvarliga konsekvenser för ett företag. Detta påstående är förmodligen för många inte speciellt förvånande, men en person som är tidigare dömd kan fortfarande vara lämplig men då beror det på vilket brott som begåtts. R1 menade att fortkörning eller

brott begångna under ungdomsåren var förmildrande omständigheter. Trots att det borde vara allmänt känt att det är dåligt att anställa kriminella har varken R3 eller R4 någon ordentlig bakgrundskontroll, vilket är borde tolkas som ett varningstecken. R1 visade även på en viss nonchalans när hen frågades varför hen inte gjorde utdrag från belastningsregistret. Hen svarade att deras verksamhet inte handlar om rikets säkerhet. Det kanske och är förmodligen sant, men ändå för det borde ju ett företag sträva efter egen säkerhet också. Oavsett vilken bransch ett företag arbetar i, finns det alltid sätt som det kan skadas.

6.2.4 Säkerhetsåtgärder

Frågorna som ställdes inom detta delkapitel är baserade på ISO-standarden 27002:2022. Delkapitlet som använts från ISO-27002:2022 är 5.11 (Återlämnande av tillgångar), 5.15 (Åtkomstkontroll), 5.16 (Identitetshantering), 5.17 (Autetiseringsinformation) och 5.18 (Åtkomsträttigheter).

Den första frågan som ställdes inom denna del var **”Vad har ni för rutiner när en anställd slutar?”**. R1, R3 och R4 hade tydliga rutiner medans R2 inte hade några specifika rutiner. R1 ansåg att deras rutiner behöver ses över lite men att de fortfarande har rutiner på plats. Enligt R1 har anställda tillgång till både företagstelefon och företagsdator. Informationen på de enheterna ska inte raderas när den anställde slutar eftersom de innehåller information som är värdefull för bolaget, som till exempel kundinformation och andra kontakter. Deras policy just nu säger att det är tillåtet att radera personlig information som till exempel ”receptsamlingar eller tal till en fest” (R1), men att det inte är okej att använda datorn för mer personligt bruk än så.

R3 svarade att deras IT-partner sköter det som ska göras när en anställd slutar. Detta innebär att de stänger av de konton som den anställde har på office 365 samt att denne blir utloggad automatiskt från de system som är berörda. R3 beskriver processen ”liksom en beställning från avslutande chef som går till vår interna admin och våran IT-partner, så då görs det en rensning liksom på veckobasis ungefär” (R3).

R4 svarade att vid avslut ändrar bolaget personens konto och tar bort dennes accesser till de olika systemen. Eftersom det endast är en person på båda bolagen som använder en egen telefon i arbetssyfte menar R4 att det är enkelt att ”stänga ute” personen som slutar så att personen inte längre har tillgång till något känsligt material. De systemen som används finns bara i de datorer som finns fysiskt på plats i F1 och F2. I affärssystemet menar R4 också att det är väldigt enkelt att ta bort en användare. Även mailen stängs ner automatiskt.

R2 svarade på frågan att de pratar med personen om hur länge deras mail ska hänga kvar samt var den ska gå sen. Intervjuledaren frågade då: **”Om en anställd har en dator, får den personen ta hem den och använda den i privat syfte?”**. R2 svarade ja. Därefter frågade intervjuledaren **”Och hur ser den rutinen ut när den personen**

lämnar tillbaka datorn? Måste personen lämna tillbaka den med alla uppgifter på eller ska hen radera den innan?". R2 svarade: "Där kan jag bara svara att det har vi inte styrt upp utan vi förutsätter ju att man använder sin dator merparten till jobbet då naturligtvis men det som ligger på C-disken, antagligen raderas det" (R2).

Därefter ställdes frågan **"Har ni någon form av åtkomstkontroll?"**. Alla respondenter svarade att de på något sätt har en form av åtkomstkontroll samt att de har möjligheten att tilldela eller ta bort åtkomsten för användarna i systemen. R1 svarade att varje anställd har ett konto till ett fjärrstyrbord som tillhandahålls av deras IT-partner. Det krävs även inloggning för att komma in i deras affärssystem. Tillgång för varje anställd till affärssystemet sköts av R1 själv. R1 fortsätter med: "Jag kan ju styra ner på ganska många olika, så mer detaljartat för olika människor så de inte kan komma åt [vissa delar i systemet]" (R1). R2 svarade att de har olika behörigheter i sitt filsystem, som hen kan sköta. Det vill säga, precis som R1, kan R2 sköta vem som har tillgång till vad i deras filsystem baserat på vilka arbetsuppgifter den anställde har. R3 svarar på ungefär samma sätt som R1 och R2. Hen talar om att bolaget hen jobbar på har både olika konton och roller som kan tilldelas till varje anställd som begränsar den information som den anställde kan komma åt. R4 menar att båda företag hen representerar använder tvåstegsautentisering utöver användarnamn och lösenord vid inloggning till deras system.

Slutligen ställdes frågan **"Hur ser er hantering av autentisering ut?"**. Alla respondenter svarade på denna fråga att de hade lösenord till deras system och att viss av dem hade tvåfaktorsautentisering. Alla respondenter förutom R1 svarade att de hade brickor eller taggar tillsammans med en kod för att komma in deras lokaler. R1 svarade att de endast hade en kod för att komma in.

ISO-27002:2022 är enligt SiS (2022) till för att hjälpa en organisation att fastställa och vidta säkerhetsåtgärder för att hantera informationssäkerhetsrisker. Utöver detta går dokumentet även att användas för att fastställa och genomföra allmänt vedertagna informationssäkerhetsåtgärder. Kapitel 5.11, 5.15, 5.16, 5.17 och 5.18 i denna standard berör de hot som en organisation kan utsättas för när en anställd slutar gällande återlämning av tillgångar samt kontroller för åtkomst, identifiering och autentisering. Syftet med att den anställde lämnar tillbaka sin tillgångar när denne slutar är att skydda organisationens tillgångar. Alla tillgångar som en anställd kan ha i sin besittning är inte fysiska. För att skydda organisationen mot hot gällande icke-fysiska tillgångar kan andra informationssäkerhetsåtgärder tillämpas, som till exempel kontroller för åtkomst, identifiering och autentisering.

Förvånande nog visade respondenterna på en bättre förståelse för säkerhet när det kommer till de säkerhetsåtgärder de applicerat i sin verksamhet, till skillnad från föregående frågor om informationssäkerhet och personalfrågor. Alla respondenter förutom R2 hade tydliga processer för vad som ska hända med en anställds tillgångar och konton när denne slutar. R1 ville inte att personen raderar information på sin

jobbdator eller jobbtelefon eftersom de innehåller kundinformation som är mycket värdefull för bolaget. R1 är medveten om att den nuvarande policyn fortfarande är lite tunn och att ”den behöver ses över lite”, men det som finns på plats är ett steg i rätt riktning. Enligt Niranjanamurthy & Dharmendra (2013) är otillåten tillgång ett problem för organisationer som arbetar med e-handel. Detta eftersom det ger en aktör illegal åtkomst till ett system. Det möjliggör då för denne att lyssna på kommunikation eller att stjäla information. Det är även möjligt att ändra på information vilket skadar organisationens riktighet. Om en person slutar på ett företag och kontot fortfarande finns kvar och denne har tillgång till detta kan det leda till stora konsekvenser för företaget. Beroende på vad som föregick avslutet på bolaget kan personen ha olika incitament att skada eller stjäla för företaget för sin egen eller någon annans vinning. Därför är det viktigt att ha någon form av skydd mot detta. R3 och R4 har båda processer för detta. R3 menar att den berörda personens office-365 konto stängs samt att hen blir utloggad från alla konton. R4 har en liknande process där personen stängs ute från sitt konto och inte längre har tillgång till det. Exakt vad det innebär gick hen inte in på men det går att anta att använder helt enkelt tas bort. R2 har å andra sidan ingen egentlig process för att skydda företaget när en anställd slutar. Hen menade att de kommer fram till hur länge mailen ska följa med personen och vem den ska gå till senare. Det svaret kan tolkas som lite underligt eftersom en mailadress vanligtvis är personlig. Det finns en risk att respondenten misstolkade frågan, men intervjuledaren ställde ingen följdfråga baserat på det svaret. R2 sade med att de inte hade någon rutin gällande vad en anställd får göra med sin jobbdator utanför arbetet. Hen sade ”Där kan jag bara svara att det har vi inte styrt upp utan vi förutsätter ju att man använder sin dator merparten till jobbet då naturligtvis…” (R2). Om nu personen har tillgång till olika system eller andra tillgångar på den datorn, och det inte är uppstyrt hur saker och ting ska gå till vid avslut kan det leda till stora problem för företaget.

När det kommer till generell åtkomstkontroll och processer för autentisering menade att respondenter att de hade det. På företaget där R1 arbetar varje anställd på ett fjärrskrivbord där tillgången till filerna går att tilldelas eller återkallas av R1 själv. R2 och R3 har en liknande lösning där de anställda får tillgång till de filer de behöver i sin arbete. R4 svarade att både företagen hen hade ansvar över hade tvåfaktorsautentisering och lösenord vid inloggning till systemen. Tvåfaktorsautentisering hade endast R3 och R4. Rezanov & Kuchuk (2022) menar att det inte alltid räcker att endast ha lösenord för att skydda sina konton på olika webbsidor. Därför är det en bra idé att använda tvåfaktorsautentisering, vilket två av fyra använde. Anledningen till att de andra företagen inte använde tvåstegsautentisering är okänt.

7 Resultat

Detta kapitel presenterar resultatet och besvarar studiens frågeställning.

Resultatet i denna studie har kommit från frågeställningen ”Hur arbetar små och medelstora företag inom e-handel med informationssäkerhet?”. För att kunna besvara den frågeställningen har personer med ansvar över e-handel på SME:s inom e-handel intervjuats. Genom frågorna som ställts i intervjun har denna frågeställning kunnat besvaras.

Intervjuerna inledde med grundläggande frågor om företaget som respondenten arbetade på. Dessa frågor var inte direkt kopplade till informationssäkerhet, men användes för att dubbelkolla att de företag som intervjuades föll inom de kriterier som fastställts tidigare.

7.1 Sammanfattning av svar

Följande tabell visar sammanfattningen av de svar som kommer presenteras i delkapitel 7.2 till 7.4.

Frågeställning:

Hur arbetar små och medelstora företag inom e-handel med informationssäkerhet?

Informationssäkerhetspolicy	Ett företag hade en informationssäkerhetspolicy. Resterande företag var medvetna om brister, men hade ingen policy för att täcka upp dessa.
Personalfrågor	Två av företagen hade knapphändig utbildning av sina anställda gällande informationssäkerhetsfrågor. Bakgrundskontroller genomfördes på två företag, men inga utdrag gjordes från brottsregistret.
Säkerhetsåtgärder	Alla företag hade åtkomstkontroller på plats för att reglera vem som har tillgång till vad. Tre av fyra respondenter hade även processer för vad som ska ske med företagens tillgångar som en anställd har när hen slutar.

7.2 Informationssäkerhetspolicy

Falkner & Hiebl (2015) och Hoppe et. al. (2021) skriver i sina rapporter om problemen som SME:s har med sin informationssäkerhetshantering. De kom fram till att SME:s kan möta mer utmanande problem än större företag och att det är en direkt produkt av att de inte applicerar aktiviteter för riskhantering i sina verksamheter. I stället läggs fokuset på verksamhetens kärnuppgifter som oftast inte innefattar informationssäkerhet. Denna tendens är något som också fångas upp i de svar som respondenterna gav på intervjun om informationssäkerhet.

En informationssäkerhetspolicy kan ses som en grundläggande bit att ha för att kunna ha fungerande informationssäkerhet på en arbetsplats. Utan en informationssäkerhetspolicy kan det leda till att anställda såväl som ledning missförstår processer och andra arbetsuppgifter ska hanteras, och på så sätt utsätta organisationen för eventuella skador. Svaren skiljde sig åt mellan de olika respondenterna, men den allra största majoriteten av dem svarade att de inte hade någon informationssäkerhetspolicy. Endast en respondent talade om att hens bolag hade en sådan policy på plats. En annan respondent menade att de själva inte hade någon egen informationssäkerhetspolicy, men att de outsourcat deras säkerhet till en IT-partner. Däremot nämnde respondenten att de fått kritik av bland annat revisorer om att företaget borde se över sin säkerhet, vilket tyder på att outsourcingen inte riktigt fungerat som den ska.

Utifrån studiens frågeställning går det redan efter de första frågorna komma fram till ett preliminärt svar på den, att företag i den storleken generellt inte lägger ner speciellt mycket tid eller resurser på informationssäkerhet. Samma fenomen är presenterat i Hoppe et. al. (2021) där de skriver att det finns stora problem med säkerhetskulturen. Säkerhetskulturen på ett företag innefattar riskmedvetenhet, kunskap och attityden mot hoten. Bristen inom säkerhetskulturen menar Hoppe et. al. (2021) bidrar till att SME:s misslyckas med att skapa en ordentlig kontext för riskhantering och att det i sin tur skapar problem i hela riskhanteringsprocessen. Som tidigare presenterat visar majoriteten av respondenternas svar att de inte applicerar en informationssäkerhetspolicy i deras verksamhet. Effekterna av detta blir en bristfällig hantering av säkerheten vilket kan medföra negativa konsekvenser för företagen. Detta resultat skiljer sig inte speciellt mycket från tidigare litteratur och säger i princip samma sak som de teorier som dessa texter presenterat.

Däremot är det värt att nämna att respondenterna som inte hade någon informationssäkerhetspolicy ändå var relativt medvetna om att det finns brister i deras sätt att arbeta på. Trots detta hade de fortfarande inget svar på det problemet. Emellertid är medvetenheten om att problem existerar det första steget i att kunna lösa dem

7.3 Personalfrågor

Hur ett företag arbetar med informationssäkerhetsrelaterade personalfrågor ger också en indikation på hur helheten ser ut. För att förhindra att fel person anställs som kan innebära hot för ett företag måste någon form av kunskap kring dessa frågor finnas. Även fast rätt person anställs till rätt position på en organisation är det fortfarande ledningens ansvar att se till så att den anställde sköter sitt arbete på korrekt sätt. Utan korrekt vägledning från chefer kan en anställd omedvetet utföra handlingar som kan utsätta företaget för risker som hade kunnat undvikas om deras medvetenhet om hoten som finns ökats med hjälp av utbildning. Bakgrundskontroll och utbildning av anställda är enligt SiS (2022) viktiga element för att lyckas med sitt arbete med informationssäkerhet.

Falkner & Hiebl (2015) menar att små och medelstora företag sällan erbjuder någon form av utbildning till sin anställda för att utveckla deras kunskaper och färdigheter om informationssäkerhet. Detta innefattar därför även deras medvetenhet och uppfattning om de risker som de och/eller företaget kan råka ut för. Konsekvenserna av denna bristfälliga utbildning visar sig genom att företagen råkar ut för oavsiktlig skada samt bristande efterlevnad av instruktioner från de anställda. Falkner & Hiebl (2015) menar även att ägare och ledning av SME:s verkar vara tvekande till att investera i aktiviteter för att öka anställdas vetande och därför bidra till att hantera risker som beror på avsaknad av kunskap. Respondenternas svar på hur de utbildar sina anställda bekräftar dessa fynd. Två av respondenterna svarade att de utbildade sina anställda för att öka deras medvetenhet om informationssäkerhetsrelaterade frågor. Dessa företag hade ingen informationssäkerhetspolicy och det verkade som att utbildningen de tillhandahöll var sporadiskt planerad och utförd på enklaste möjliga sätt. De två resterande respondenterna hade ingen utbildning för sina anställda, även fast det ena företaget hade en informationssäkerhetspolicy. Svaren som samlats in tyder på en tydlig brist i företagens hantering av medvetenhetsutbildning för sina anställda som påverkar hur dessa företag arbetar med informationssäkerhet. Alhamari & Duncan (2020) skriver att SME:s behöver ytterligare kunskaper om de möjliga sårbarheter som företaget kan utsättas för. Det betyder att de behöver utveckla egna utbildningar eller program med skräddarsytt innehåll som passar just det specifika företaget (Alhamari & Duncan, 2020). Detta är något som företagen som respondenterna representerar inte gör i nuläget, vilket tyder på en brist i informationssäkerhetsarbetet.

Kanske ännu mer alarmerande är att företagen visar på tendenser att inte göra ordentliga bakgrundskontroller innan de anställer någon ny. Två respondenter hävdade att de hade någon form av bakgrundskontroll. Vid djupare analys av detta visade sig att bakgrundskontrollerna bestod av en kreditkontroll från det ena företaget och en outsourcad bakgrundskontroll från det andra. Det var R2 som menade att deras bakgrundskontroll är outsourcad. Däremot kunde R2 inte gå in mer på detalj vad denna kontroll skulle innebära vilket följer linjen att R2 förlitar sig mycket på outsourcad

säkerhet. Resterande två respondenter hade ingen annan bakgrundskontroll förutom referenstagning, vilket är ett dåligt tecken.

Levashina & Campion (2009) menar att det är mindre sannolikt för små verksamheter att genomföra bakgrundskontroller för personer som ansöker till en tjänst till deras verksamhet. Genom att genomföra ordentliga bakgrundskontroller innan en person anställs kan en arbetsgivare förbättra sin anställningsprocess och på så sätt få en person som verkligen passar i den tjänst hen blivit anställd till. Detta gäller för både säkerhet och effektivitet. Binns & Kempf (2020) fortsätter inom detta tema och presenterar deras forskning som de genomfört inom området. De kom fram till att personer med tidigare erfarenhet av att genomföra bedrägerier har en överhängande risk att de kommer göra det igen på en ny arbetsplats. Binns & Kempf (2020) menar även att det är viktigt för företag idag att förstå hur väsentliga bakgrundskontroller är i dagens anställningsprocesser och vilken nytta som de kan bidra till. Trots detta är bakgrundskontroller något som respondenterna har misslyckats att applicera på ett korrekt sätt i sin rekryteringsprocess och kan leda till problem i hanteringen av informationssäkerhet.

7.4 Säkerhetsåtgärder

En annan del som tydligt visar hur ett företag arbetar med informationssäkerhet är vilka åtgärder de implementerar för att hålla deras tillgångar säkra. Onwubiko & Lenaghan (2007) skriver i sin rapport att SME:s har problem med att hantera otillåten åtkomst till deras system och/eller viktig information. Alhamari & Duncan (2020) fortsätter med att förklara att SME:s råkar ut för angrepp genom att de inte applicerar korrekta säkerhetsåtgärder i sitt arbete. Hur SME:s arbetar i praktiken verkar därför skilja sig från vad NIST (2002) påpekar är ett acceptabelt mjukvaru- och hårdvaruskydd. Kontroller för att säkerställa verksamhetens konfidentialitet kräver att det finns åtkomstkontroller på plats. Svaren som respondenterna gav inom detta område var uppfriskande till skillnad från de svar som genererats från tidigare frågor. Svaren skiljde sig också från de resultat som Onwubiko & Lenaghan (2007) och Alhamari & Duncan (2020) presenterat som visade på att SME:s, i stor utsträckning, inte tillämpar korrekta säkerhetsåtgärder för att förhindra åtkomst för personer utan tillåtelse. Alla respondenter svarade att de hade kontroller för att hantera tillgång till deras system och information, samt att de hade en bra uppfattning om deras arbete för att förhindra otillåten åtkomst. Dessa säkerhetsåtgärder hanterade både åtkomstkontroll samt processer för autentisering. Den vanligaste formen när det kommer till åtkomstkontroll hos de intervjuade företagen var att varje anställd hade endast tillgång till de filer eller system som hen behöver i sitt arbete. Detta innebär att chef eller annan ansvarig kan manuellt ställa in de rättigheter som krävs, vilket även innebär att de går att återkallas. Alla respondenter menade även att de hade lösenord till sina system och lokaler. Också nämnvärt är att två av fyra hade tvåfaktorsautentisering vilket är ett väldigt bra verktyg att använda sig av för att hantera informationssäkerhet på ett företag.

Onwubiko & Lenaghan (2007) menar att 74,3% SME:s kapitalförluster kommer från endast fyra kategorier. Två av dessa kategorier är stöld av hårdvara och stöld av skyddad information. SME:s verkar därför har svårt att skydda sig mot sådana attacker. Respondenterna uppvisade en relativt stor förståelse för hur de ska skydda sig mot externa hot via deras säkerhetsåtgärder. Däremot kan stölder av hårdvara och information komma från insidan, både avsiktligt och oavsiktligt. Ett effektivt tillvägagångssätt för ett företag att skydda sig mot sådana hot presenterar SiS (2022) i standarden ISO-27002:2022. Standarden säger att personal eller andra intressenter ska lämna tillbaka tillgångar som tillhör organisationen när anställning eller annat uppdrag avslutas. Syftet med detta är att skydda organisationens tillgångar (SiS, 2007). Svaren som respondenterna i denna studie gav visade på en skillnad från de svar som Onwubiko & Lenaghan (2007) presenterade i sin studie. Alla respondenter förutom en visade på att de hade tydliga processer vad som ska hända med en persons tillgångar och konton när den personen slutar arbeta på den positionen eller på företaget i sin helhet. Detta är något som är positivt eftersom det minimerar de risker som finns med att en anställd fortfarande har tillgång till känslig information efter uppsägning. Det visade sig med att det fanns automatiska processer på plats för att stänga ner personens olika konton. Att eliminera den mänskliga faktorn i denna process minimerar risken att någon ”faller mellan stolarna” och blir bortglömd. Gällande tillbakalämning av tillgångar som till exempel datorer och telefoner ser det också relativt bra ut. Alla förutom en respondent hade tydliga regler eller inte hade några personliga företagsdatorer/telefoner överhuvudtaget.

Baserat på respondenternas svar gällande säkerhetsåtgärder tyder det på att deras arbete med informationssäkerhet lyfts upp på grund av appliceringen av relevanta kontroller.

8 Diskussion

8.1 Metoddiskussion

Studien har använt en kvalitativ metod för att samla in och analysera data. Valet att använda en kvalitativ metod går att diskutera eftersom den har både för- och nackdelar. Datan var samlades in var tvungen att vara bred samt öppen för tolkning, vilket den kvalitativa metoden tillåter. Det möjliggör också för en mer djupgående beskrivning av det ämne som studeras. Problemet med den kvalitativa metoden är att resultaten är svåra att generalisera. Det märks av på denna studie och är dels beroende på metodvalet, dels antalet respondenter. I slutändan var det endast fyra personer som var villiga att ställa upp på intervju. Det går aldrig att helt generalisera resultatet från en kvalitativ metod, men fler respondenter hade ökat studiens trovärdighet. Hade i stället en kvantitativ metod använts hade förmodligen fler företag valt att svara på frågorna, men då hade resultatet haft brist på en djupgående beskrivning och data som var öppen för tolkning.

Valet av att använda semistrukturerade intervjuer i denna rapport visade sig vara positivt för insamlingen av empiriskt material. Att ha haft möjligheten att kunna ställa följdfrågor till varje respondent har tillåtit djupare insikt i verksamheterna och bidrog till information som inte hade övervägts när de initiala frågorna utformades. Därför har semistrukturerade intervjuer lyft denna rapport till en annan nivå än om endast öppna eller stängda intervjuer applicerats för insamling av empiri.

Intervjuerna genomfördes på distans vilket var ett moment som påverkade datainsamlingen. Påverkningen är i sig inte endast negativ, men några extra steg behövdes göras för att intervjuerna skulle bli så bra som möjligt. Inspelningen av intervjun var utmanande eftersom Microsoft teams användes för intervjun. Vid intervjutillfällena gick inte inspelningsfunktionen att starta, vilket förmodligen berodde på att den låg bakom en betalvägg. För att ändå kunna ha inspelat material att transkribera fick andra metoder användas. Respondenters tekniska utrustning var inte heller helt optimal för en intervju på distans. Vissa hade mikrofoner med låg kvalité vilket ledde till att några delar av den inspelade intervjun var svåra eller omöjliga att höra vad som sades. Dessa exempel är bara några nackdelar med valet att ha intervjun på distans. Fördelarna med distansintervjuerna var att det möjliggjorde att intervjua respondenter som befann långt ifrån varandra geografiskt sett. Det hade aldrig varit möjligt på samma sätt ifall fysiska intervjuer använts.

När det kommer till studiens trovärdighet påverkar antalet respondenter den negativt. Även fast den data som samlades in var utförlig och informationsrik, gör antalet respondenter det svårt att säga att studien har en hög trovärdighet med självförtroende. Anledningarna till att företag tackade nej till att bli intervjuade var flera. Ett par menade att de saknade kompetensen för att svara på sådana frågor. Andra verkade kunna svara på sådana frågor men kunde inte ställa upp på grund av hög arbetsbelastning. Några svarade att det står i deras informationssäkerhetspolicy att inte svara på frågor om

deras informationssäkerhetspolicy. Men de allra flesta slutade svara efter några meddelanden i mailkonversationen eller svarade inte överhuvudtaget. Anledningen till att respondenterna svarade (eller inte svarade) på detta sätt kan vara flera, och det finns i nuläget ingen förklaring. För framtida forskning kan det vara värt att se över hur kontakten med företaget tas samt hur frågan är formulerad.

8.2 Samhälleliga aspekter

Målet med denna studie har varit att ta reda på hur små och medelstora företag inom e-handel arbetar med informationssäkerhet. Frågorna som utformats har varit till för att försöka få en så bred bild av företagens informationssäkerhet som möjligt, inom ramen för denna studie. I första hand borde respondenten tillsammans med företaget som hen representerar få en tankeställare när det kommer hur de själva arbetar med informationssäkerhet. Beroende på hur väl de kunde svara på frågorna som ställdes kanske de fick en idé om vad de behöver göra för att förbättra sitt säkerhetsarbete.

En annan aspekt av detta kan vara att utomstående företag, som inte har någon koppling till företagen i denna studie, kan dra nytta av forskningen också. Företag som är ute efter att påbörja eller förbättra sitt arbete med informationssäkerhet kan komma att söka efter information på nätet. När denna studie är färdigställd och publicerad finns det en chans att ett sådant företag hittar den. Det kan leda till att personer i någon form av ledarroll som till exempel beslutsfattare eller eventuella intressenter kan se vilka utmaningar och risker som andra företag möter i sitt arbete, och använda denna studie för sin egen vinning.

8.3 Vetenskapliga aspekter

För att kunna genomföra denna studie var kontakten med företagen ett kritiskt moment som krävdes att mycket tid lades ner. Med tanke på studiens inriktning och hur pass känslig den är var det viktigt att hålla en professionell kontakt med företagen som kan vara intresserade. Fokus lades även på att skicka förfrågningar via mail som väckte intresse hos företagen så att de skulle vara villiga att svara på studiens frågor. Den initiala kontakten med företaget banade sedan väg för studiens metod och resterande arbete.

Resultaten som samlats in kontra tidigare litteratur hade både likheter och skillnader. De tre områden som fokuset låg på i analysen var informationssäkerhetspolicy, personalfrågor och säkerhetsåtgärder. Vid läsning av tidigare forskning inom dessa områden tydde svaren på att SME:s inte hanterar dessa på något vidare sätt. Detta var delvis sant framför allt i de två första områdena (informationssäkerhetspolicy och personalfrågor). Litteraturen menade att SME:s, till en stor del, inte applicerade en informationssäkerhetspolicy i sin verksamhet. Ungefär samma resultat visade sig vid

analys av det empiriska materialet. Även respondenternas svar på hur de hanterar personalfrågor (utbildning och bakgrundskontroller) följde det material som presenterats tidigare. Personer med ledarroll för SME:s prioriterar inte vidare utbildning för sina anställda för att öka deras medvetenhet för informationssäkerhet och bakgrundskontroller är något som sällan används på ett strukturerat sätt. Vid det tredje området (säkerhetsåtgärder) menade tidigare forskning att även det området var något som SME:s hanterade på ett dåligt sätt. Denna studies insamlade material lutar däremot åt ett annat håll. Respondenternas svar visar på att de är medvetna om vilka säkerhetsåtgärder som bör appliceras samt att de praktiskt applicerar de åtgärder i sina verksamheter. Några respondenter svarade till och med att de använde tvåfaktorsautentisering i sina kontroller vilket inte är ett vanligt verktyg att använda för företag i den storleken. De insamlade svaren inom detta område visar därför en relativt tydlig skillnad kontra tidigare litteratur vilket är intressant.

8.4 Etiska aspekter

I samband med att varje intervju inleddes informerades varje respondent om de forskningsetiska principerna som tagits fram av Vetenskapsrådet (2018). Eftersom insamlingen av data var en avgörande del i genomförandet av denna studie lades stort fokus på etiken. Företagen fick veta vad syftet med studien var samt vilket syfte som detta moment skulle tjäna i studien. De blev även informerade om samtycke när det kommer till att delta och om de accepterade att en ljudupptagning gjordes för att möjliggöra transkribering av datan. Kanske viktigast av dem alla var att personuppgifter och uppgifter om företaget som kan anses vara identifierande skulle hållas konfidentiella. Allt material som samlats in har behandlats på ett sätt så att ingen utomstående kan ta del av den i rå form, utan endast i behandlad form i denna studie. Filen som innehåller intervjuns ljudupptagning laddades inte upp till någon server eller extern databas, utan fanns endast lagrad lokalt på författarens egen hårddisk. Efter genomförd transkribering raderades.

8.5 Framtida forskning

En tänkbar inriktning för framtida forskning inom detta område kan vara att ha hårdare kriterier vid val av företag. Denna studie har valt att nischa sig mot e-handelsföretag som finns i kategorin SME. Problemet med den inriktningen kan vara att den fortfarande kan vara för bred för att få ett resultat som är så likt verkligheten som möjligt. Som nämnt i första delkapitlet i bakgrundskapitlet 2.1 (Små och medelstora företag) står SME:s för 99,9% av alla företag i Sverige. Detta är ett otroligt stort spann som med säkerhet kan minskas, även fast det kommer innebära mer arbete för att hitta respondenter. Ett förslag kan vara att fokusera på antalet anställda och därmed ha ett mindre spann. Exempel på detta kan vara 1–10 anställda eller 50–100 anställda. Det går även att ta med båda exemplen för att sedan ställa de mot varandra och se vad som

skiljer dem åt. Eftersom det kommer att krävas mer tid för att hitta företag som har dessa uppdaterade kriterier är det även möjligt att reflektera över ifall det krävs någon inriktning inom en viss bransch, eller om det snäva antalet anställda räcker.

Denna studie fokuserar på flera delar inom informationssäkerhet, och kan därför inte rikta sig in på djupet på alla områden. Det kan vara något som är värt att forska mer om hos SME:s. Exempel på ett sådant område kan vara teknisk säkerhet och kanske mer specifikt IT-säkerhet eller fysisk säkerhet. En sådan studie hade kommit in mer djupare på ett särskilt område och kan ge mer utförliga och tydliga svar om specifika problem som SME:s möter i sin verksamhet.

Referenser

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1–5. IEEE. https://doi-org.libraryproxy.his.se/10.1109/CyberSA49311.2020.9139638

Berisha, G., & Pula, J. S. (2015). Defining Small and Medium Enterprises: a critical review. Academic Journal of Business, Administration, Law and Social Sciences, 1(1), 17–28.

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2007). Thesis projects: a guide for students in computer science and information systems. Springer Science & Business Media.

Binns, C. A., & Kempf, R. J. (2021). Background checks: the theories behind the process. Security Journal, 34(4), 776–801. https://doi.org/10.1057/s41284-020-00260-4

Chai, W. (2023, 1 februari). What is the CIA triad (confidentiality, integrity and availability)?. *Wesley Chai*. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. Hämtad 2023-05-14.

Cramer-Flood, E. (2022, 2 februari). Global ecommerce forecast 2022. https://www.insiderintelligence.com/content/global-ecommerce-forecast-2022. Hämtad 2023-02-01.

Data. (u.å.). I *Nationalencyklopedin.* Hämtad 10 februari, 2023, från https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/data

Denscombe, M. (2017). EBOOK: The good research guide: For small-scale social research projects. McGraw-Hill Education (UK).

European commission. (2020). *SME Definition – user guide 2020.* Doi: 10.2873/677467

Falkner, E. M., & Hiebl, M. R. W. (2015). Risk management in SMEs: a systematic review of available evidence. Journal of Risk Finance (Emerald Group Publishing Limited), 16(2), 122–144. https://doi.org/10.1108/JRF-06-2014-0079

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance (Emerald Group Publishing Limited)*, 22, 240–260. https://doi.org/10.1108/JRF-02-2020-0024

International Organization for Standardization. (2018). *Information technology – Security Techniques – Information security management systems – Overview and vocabulary*. (ISO 27000:2018). https://www-sis-se.libraryproxy.his.se/en/produkter/standardization/vocabularies/information-technology-office-machines-/isoiec-270002018/

International Organization for Standardization. (2022). *Information technology – Cybersecurity and privacy protection – Information security management systems - Requirements.* (ISO 27001:2022). https://www-sis-se.libraryproxy.his.se/en/produkter/information-technology-office-machines/general/ss-isoiec-270012022/

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security controls.* (ISO 27002:2022). https://www-sis-se.libraryproxy.his.se/en/produkter/information-technology-office-machines/general/ss-en-isoiec-270022022/

Levashina, J., & Campion, M. A. (2009). Expected practices in background checking: Review of the human resource management literature. Employee Responsibilities and Rights Journal, 21, 231–249.

Lok. (2022, 28 november). Are phising simulations effective? *Usecure*. https://blog.usecure.io/are-phishing-simulations-effective. Hämtad 2023-04-25

Lundén, M. (2020). *Kvalitativa metoder* [PowerPoint-presentation]. Canvas, Göteborgs Universitet. Hämtad 10 mars, 2023, från https://canvas.gu.se/courses/31832/files/2907245/download?download_frd=1

Merkow, M. S., Breithaupt, J. (2014). *Information Security: Principles and Practices* (2: a utgåvan). Pearson.

Murphy, Alan and Ledwith, Ann (2006) Project Management Tools and Techniques in High-Tech SMEs in Ireland. In: The 14th Annual High Technology Small Firms Conference: May 11-13, 2006 + May 10, 2006 Doctoral Workshop, University of Twente, Enschede, The Netherlands., 10 May 2006 - 13 May 2006, Enschede, The Netherlands.

Myndigheten för samhällsskydd och beredskap. (2016). Terminologi och begrepp inom informationssäkerhet. https://www.diva-portal.org/smash/get/diva2:904740/FULLTEXT01.pdf

National Institute of Standards and Technology (NIST) (2002). Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology. http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/NIST%20-%20800-30R0%20-%20Risk%20Management%20Guide%20for%20IT%20Systems.pdf

Neama, G., Alaskar, R., & Alkandari, M. (2013). Privacy, security, risk and trust concerns in e-commerce. *Proceedings of the 17th International Conference on Distributed Computing and Networking*, 46, 1-6. https://doi-org.libraryproxy.his.se/10.1145/2833312.2850445

Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2(7), 2885-2895.

Onwubiko, C., & Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. 2007 IEEE Intelligence and Security Informatics, Intelligence and Security Informatics, 2007 IEEE, 244–249. https://doi-org.libraryproxy.his.se/10.1109/ISI.2007.379479

Oscarson, P. (2001). Informationssäkerhet i verksamheter : begrepp och modeller som stöd för förståelse av informationssäkerhet och dess hantering i verksamheter. Institutionen för datavetenskap, Univ. Filosofiska fakulteten

Padallan, J. O. (2019). *Cyber Security*. Arcler Press.

Patton, M Q. (2002). *Qualitative Research & Evaluation Methods* (3: e utgåvan). Sage Pulications.

Pett, T.L., Wolff, J.A., & Sié, L. (2012). SME Identity and Homogeneity – Are There Meaningful Differences Between Micro, Small, and Medium-Sized Enterprises? Journal of Marketing Development and Competitiveness, 6, 48–59.

Pinzon, S. (2008, 1 oktober). Top 10 threats to SME data security. WatchGuard Technologies. http://www.safesoft.hu/whitepaper/WatchGuard_White_Paper.pdf. Hämtad 2023-01-20.

Rezanov, B., & Kuchuk, H. (2022). Fast Two-Factor Authentication Method in Systems With a Centralized User's Database. 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Advanced Technology (KhPIWeek), 2022 IEEE 3rd KhPI Week On, 1–5. https://doi.org/10.1109/KhPIWeek57572.2022.9916491

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21-45.

Statistiska Centralbyrån. (2017). E-handel allt viktigare för svenska företag. https://www.scb.se/hitta-statistik/artiklar/2017/E-handel-allt-viktigare-for-svenska-foretag/#:~:text=Den%20visar%20att%2021%20procent,%2Dhandel%2C%20%C3%B6ver%2030%20procent.

Sjölin, M., Henriksson, S. (u.å.). Information. I *Nationalencyklopedin*. Hämtad 10 februari, 2023, från https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/information

Srinivasan, M. L. (2016). *CISSP in 21 Days* (2: a utgåvan). Packt publishing.

Sundström, M. (u.å.) E-handel. I *Nationalencyklopedin*. Hämtad 23 februari, 2023, från https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/e-handel

Svenska Institutet för Standarder. (u. å.). *Vad är en standard.* https://www.sis.se/standarder/vad-ar-en-standard/

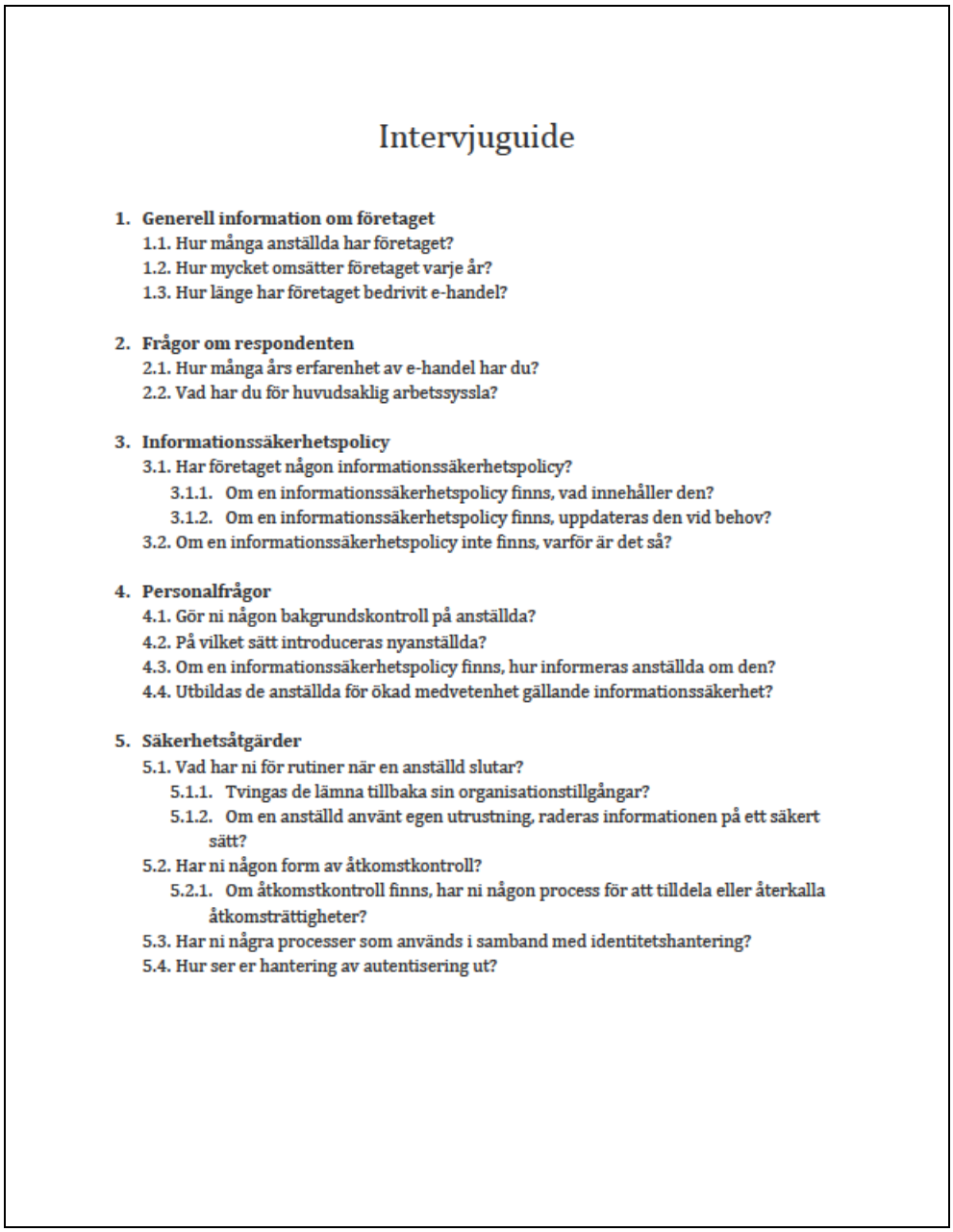
Svenskt Näringsliv (u. å.). SME-kommittén. https://www.svensktnaringsliv.se/sme/

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review.

Vetenskapsrådet (2018). *Etik i forskningen.* https://www.vr.se/uppdrag/etik/etik-i-forskningen.html

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security. Cengage learning.

9 Bilagor



Intervjuguide

1. **Generell information om företaget**
   - 1.1. Hur många anställda har företaget?
   - 1.2. Hur mycket omsätter företaget varje år?
   - 1.3. Hur länge har företaget bedrivit e-handel?

2. **Frågor om respondenten**
   - 2.1. Hur många års erfarenhet av e-handel har du?
   - 2.2. Vad har du för huvudsaklig arbetssyssla?

3. **Informationssäkerhetspolicy**
   - 3.1. Har företaget någon informationssäkerhetspolicy?
     - 3.1.1. Om en informationssäkerhetspolicy finns, vad innehåller den?
     - 3.1.2. Om en informationssäkerhetspolicy finns, uppdateras den vid behov?
   - 3.2. Om en informationssäkerhetspolicy inte finns, varför är det så?

4. **Personalfrågor**
   - 4.1. Gör ni någon bakgrundskontroll på anställda?
   - 4.2. På vilket sätt introduceras nyanställda?
   - 4.3. Om en informationssäkerhetspolicy finns, hur informeras anställda om den?
   - 4.4. Utbildas de anställda för ökad medvetenhet gällande informationssäkerhet?

5. **Säkerhetsåtgärder**
   - 5.1. Vad har ni för rutiner när en anställd slutar?
     - 5.1.1. Tvingas de lämna tillbaka sin organisationstillgångar?
     - 5.1.2. Om en anställd använt egen utrustning, raderas informationen på ett säkert sätt?
   - 5.2. Har ni någon form av åtkomstkontroll?
     - 5.2.1. Om åtkomstkontroll finns, har ni någon process för att tilldela eller återkalla åtkomsträttigheter?
   - 5.3. Har ni några processer som används i samband med identitetshantering?
   - 5.4. Hur ser er hantering av autentisering ut?

Bilaga 1: Intervjuguide

Begrepp	Beskrivning
1. Kontroll	En åtgärd med syfte att modifiera en risk (SiS, 2018).
2. Åtkomstkontroll	Typer av medel som går att ta till för att se till att åtkomst har restriktioner baserat på organisationens krav på säkerhet (SiS, 2018).
3. Hot	En tänkbar orsak till en icke avsedd händelse, som kan leda till att informationssystem eller organisation skadas på något sätt (SiS, 2018).
4. Risk	Effekten av osäkerheten på organisationens mål. Något som varierar från ett väntat resultat (SiS, 2018).
5. Intressent	En organisation eller en person som på något sätt kan bli påverkad av, påverka eller på något annat sätt anse sig vara påverkad av ett beslut eller aktivitet som en organisation gör (SiS, 2018).
6. Attack	Ett försök att förstöra, avslöja, stjäla, få obehörig tillgång till material eller använda en tillgång på ett obehörigt sätt (SiS, 2018).
7. Informationssäkerhet	Ett sätt för att säkerställa konfidentialitet, riktighet och tillgänglighet (SiS, 2018).
8. SME	Small and middle-sized enterprises eller små och medelstora företag (European commision, 2020).

Bilaga 2: Centrala begrepp