LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Cybersäkerhet med medarbetare i fokus

En kvalitativ studie om medarbetares cybersäkerhetsbeteenden inom svenska SME

Kandidatuppsats 15 hp, kurs SYSK16 i

Författare: Hanna Laremark
Maja Vigh

Handledare: Markus Lahtinen

Rättande lärare: Niki Chatzipanagiotou

Cybersäkerhet med medarbetare i fokus: En kvalitativ studie om medarbetares cybersäkerhetsbeteende inom svenska SME

ENGELSK TITEL: Cybersecurity with employees in focus: A qualitative study on employees' cybersecurity behavior within Swedish SMEs.

FÖRFATTARE: Laremark och Vigh

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: Maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 56

NYCKELORD: Cybersecurity, Bottom-up, Human factors, Cybersecurity Strategy, Motivational factors, Social norms, Cybersecurity frameworks

SAMMANFATTNING (MAX. 200 ORD):
Antalet cyberattacker har ökat markant sedan förändringar i det geopolitiska läget och som resultat under och efter Covid19 pandemin. För svenska SME kan en välfungerande cybersäkerhetskultur vara avgörande för företagens överlevnad. Därmed har en kvalitativ undersökning i form av semistrukturerade intervjuer genomförts hos 5 svenska SME:er i Skåne. Intervjuernas primära syfte är att undersöka hur cybersäkerhetsbeteenden kan främjas hos medarbetare inom olika sektorer, där medarbetarna inte har IT-säkerhetsrelaterade roller, samt undersöka hur svenska SME förmågor ser ut i arbetet med erkända tekniska ramverk. Resultatet visade att företag i mellanstorlek, hade en mer utvecklad cybersäkerhet genom en etablerad IT-avdelning. Resultatet visade även att motivation och mänskliga faktorer såsom ett ansvar, möjlighet till utveckling, beröm, trivsel och en hållbar arbetsbörda, kan ha en inverkan på cybersäkerhetsarbetet. Brist på kunskap och självförtroende i samband med cyberhot/cybersäkerhet var en framträdande upptäckt. Det framkom även att majoriteten av företagen inte inkluderar anställda i framtagandet av cybersäkerhetspolicyer. Ingen av företagen använde Zero Trust eller NIST som uttalade strategier, trots att företagen använde

delar av dessa ramverk. Slustasen blir att organisationer som tar hänsyn till organisationskultur, kompetens och mänskliga faktorer, samt inkluderar medarbetare i sin cybersäkerhetsstrategi kan utveckla en mer robust och hållbar cybersäkerhetspraxis.

Innehåll

Definitioner

Tabell 1.1: Definitions tabell

Begrepp	Definition
Ransomware attacker (RW)	Ransomware, "utpressningsattacker", är ofta virus som drabbar organisationer, där delar av informationen från en verksamhet blir otillgänglig. Angriparna hoppas därefter att organisationen ska betala en lösensumma för att få en dekrypteringsnyckel eller återfå informationen (Myndigheten för samhällsskydd och beredskap, 2023).
Malware attacker (MA)	Syftar till hårdvara, fast programvara, mjukvara som avsiktligt inkluderas eller infogas i ett system för ett skadligt syfte (NIST, n.d.). Malware innefattar virus, maskar och spionprogram (European Parliament, 2022).
Social Engineering threats (SET)	Exploatering av mänskliga fel görs för att få tillgång till information eller tjänster. Manipulering används för att få användare att öppna skadliga utskick eller webbplatser, för att få tillgång till system eller tjänster. Exempelvis är phishing (mail) eller smishing (textmeddelande) förekommande attacker inom SET (European Parliament, 2022).
Threats against data (TAD)	TAD riktar in sig på datakällor för att få obehörig åtkomst och avslöjande. Exempelvis är dataintrång (avsiktligt) samt dataläckor (oavsiktligt) två hot inom denna kategori (European Parliament, 2022).
Desinformation (DIS)	Spridande av missledande information görs med avsikten att skada. Desinformation kan skada företags rykten och ledningens trovärdighet (Lella et al. 2022).
Supply chain attacker (SCA)	SCA har som mål att påverka relationer mellan organisationer och leverantörer. Detta syftar till två attacker, en mot leverantören och en mot kunden. Exponeringen för dessa attacker har ökat på grund av invecklade system och det stora antalet leverantörer som finns, vilket kan vara svårt att överblicka (Europaparlamentet, 2022).

Figurer

Tabeller

1 Introduktion

Sedan Covid-19-pandemin och invasionen av Ukraina har antalet IT-attacker ökat inom EU (European Parliament, 2022). Phishing-attacker är det vanligaste tillvägagångssättet för hackare att få sin första tillgång till ett system. Nya tillvägagångssätt inom SET liknar attack-beteendet under Covid-19, men fokuserar nu istället på Ryssland-Ukraina-konflikten (Lella et al., 2022). Konsekvenserna av cyberattacker som utförts mellan 2021 och 2022 drabbade organisationer ur flera aspekter:

- **Ekonomiska förhållanden:** Nya finansiella kostnader, såsom skada för nationell säkerhet eller lösensumma vid ransomware-attacker.
- **Rykten:** Negativ publicitet eller att organisationer blivit offer för cyberhot.
- **Digitala förhållanden:** Korrupt data eller otillgängliga system.
- **Psykiska förhållanden:** Medarbetare, patienter eller kunder som skadas (Lella et al., 2022).

Cyberattacker sker i allt större utsträckning, och även Sverige har påverkats. Attacker mot myndigheter, offentliga organisationer och den privata sektorn har blivit allt fler. Ett närliggande exempel är Tietoevry. SVT (2024) skriver att Tietoevrys svenska datacenter blev utsatt för en ransomwareattack, vilket påverkade bland annat företag som Rusta, Filmstaden och Anticimex. Vidare påverkades även 120 myndigheter, däribland Vellinge kommun och Lunds universitet (SVT, 2024). Attacken påverkade betydande delar av svensk näringsverksamhet, såsom privata företag, myndigheter och offentliga organisationer (SVT, 2024). Trots att attacken inte var riktad mot en myndighet, kan "leverantörer till offentlig sektor" drabbas, vilket var fallet för Tietoevry. Utöver attacker mot svenska datacenter eller företag kan även organisationer med IT-system som drivs av företag från utlandet påverkas, om dessa utländska system utsätts för cyberattacker. År 2021 utsattes det amerikanska mjukvaruföretaget Kaseya, vilket resulterade i att 800 av Coops kassor och självbetalningskassor inte kunde användas (SVT, 2021). Samarbetet mellan företag i olika länder är därmed en allt mer betydande faktor som påverkar IT-säkerheten för svenska företag.

Europaparlamentet beskriver att de vanligaste cyberhoten 2022 inkluderar bland annat: ransomwareattacker, malwareattacker, social engineering-hot, hot mot data, desinformation och leverantörskedjeattacker (European Parliament, 2022). Enligt en studie av Sakib et al. (2023) visar deras resultat att människor delar känslig information via offentliga wifi-nätverk, klickar på länkar som skickas till deras e-post, inte använder tvåstegsverifiering, använder vanliga lösenord, återanvänder sina lösenord för flera konton och laddar ner mjukvara från obehöriga källor. Dessa beteenden kan leda till ransomwareattacker. SET-tekniker används ofta för att utföra sådana attacker. Organisationer kan påverkas av cyberattacker på grund av mänskliga fel, systemfel och otillräcklig cybersäkerhet (Sakib et al., 2023). Dessa mänskliga faktorer inom organisationen kan därmed resultera i cyberattacker.

1.1 Problemområde

Små och medelstora företag (SME) i Sverige påverkas av det ökade antalet cyberattacker och hanteringen av cybersäkerhetsfrågor inom näringsverksamhet kan genomföras på olika sätt. SME definieras enligt EU genom bland annat antalet anställda i företag. Ett mellanstort företag innefattar upp till 250 anställda, litet företag innefattar upp till 50 anställda och mikroföretag innefattar upp till 10 anställda (Commission Recommendation 2003/05/06). Enligt Barlette et al. (2015) fattas beslut om riktlinjer och strategier från en top-down-approach där högsta ledningen vidarebefordrar besluten till medarbetarna inom SME. På liknande sätt fungerar det inom informationssäkerhetsarbete, som beslutas av de högsta verkställande cheferna i SME. Osborn och Simpson (2018) förklarar att beslutsfattare inom SME kan ha fler roller i organisationen, vilket i sin tur kan påverka deras kunskaper om informationssäkerhet, som kan återspeglas i deras beslut. Inom svenska företag finns en varierad strategihantering av cybersäkerhet. Enligt Statistiska centralbyrån (2019) förmedlas information om medarbetarnas ansvar inom IT-säkerhet på tre sätt: 49 % genom kontrakt (anställningsavtal), 26 % genom obligatoriska kurser eller material, och 44 % genom frivillig utbildning/intern information.

Att upprätthålla god säkerhet inom ett företag kan vara en utmaning. Därför har hjälpmedel i form av tekniska ramverk som NIST och Zero Trust utvecklats för att stödja organisationer i deras arbete med cybersäkerhet. NIST är anpassningsbar för organisationer oavsett storlek eller sektor (National Institute Security Technologies, 2024). Globala konsultföretag som Deloitte har publicerat riktlinjer kring Zero Trust och hänvisar till att implementeringen ska ske steg-för-steg (Buck et al., 2021). Microsofts Microsoft Azure och Microsoft 365 Security har även utvecklat Zero-Trust-baserade lösningar, vilket även Google Corp har (Sarkar et al., 2022). Trots att ramverken är välanvända finns det utmaningar med att applicera dem; exempelvis är de komplexa och resurskrävande, särskilt för SME med begränsade resurser och erfarenhet, samt att det finns en avsaknad av tekniska detaljer. När det gäller Zero Trust finns det dessutom få detaljerade fallstudier, publicerade rapporter och forskning som belyser erfarenheter av att använda och implementera detta ramverk (Fernandez & Brazhuk, 2022).

Corradini (2020) betonar att vi ofta tenderar att glömma bort att organisationer är uppbyggda av människor och vikten av att ge medarbetare rätt förutsättningar för att identifiera och agera vid risker. Vid framtagandet av program och strategier som främjar medvetenhet kring cybersäkerhet, är det viktigt att ta hänsyn till både kognitiva, sociala och emotionella aspekter, eftersom medarbetarna är de som ska följa policier och agera informationssäkert i sitt dagliga arbete (Corradini, 2020). Vidare förklarar Young et al. (2017) att medvetenhet kring cybersäkerhet inte alltid räcker för att förebygga attacker. Att förändra mänskliga beteenden är en betydligt mer komplex process, och kortvariga fördelar vinner oftast över de långsiktiga (Young et al., 2017). I denna studie undersöks medarbetare inom olika sektorer, där de har olika roller och de skiljer sig även i sina ansvarsområden. Det gemensamma för medarbetarna i denna studie är att medarbetarna inte har roller relaterade till cybersäkerhet. Samspelet mellan organisationens cybersäkerhetsarbete och medarbetarna är därmed avgörande för en välfungerande säkerhetskultur. Det är även detta kunskapsgap som ligger till grund för våra forskningsfrågor i studien.

1.2 Forskningsfråga

Den primära forskningsfrågan för denna undersökning är följande:

1. *Hur kan cybersäkerhetsbeteenden främjas hos medarbetare inom olika sektorer som inte har IT-säkerhetsrelaterade roller?*

För att göra en djupare analys av efterlevnaden av dagens tekniker inom cybersäkerhetstrategier används en sekundär forskningsfråga i undersökningen:

2. *Hur ser svenska SMEs förmågor ut att arbeta med erkända tekniska ramverk?*

1.3 Syfte

Syftet med uppsatsen är att undersöka hur medarbetare som inte har cybersäkerhetsrelaterade roller arbetar med IT-säkerhet inom svenska SMEs. Vi kommer även att undersöka hur svenska SME arbetar med erkända tekniska ramverk, då dessa ramverk ska vara anpassningsbara för alla företag. Vi kommer att ställa undersökningens resultat i relation till följande aspekter: Motivation-, mänskliga faktorer, organisationskultur, tekniska ramverk, decentralisering och centralisering. Målet med uppsatsen är att stödja svenska SME i utvecklingen av cybersäkerhetsstrategier genom att plocka fram de faktorer som påverkar medarbetarnas arbete och beteende gentemot IT-säkerhet. Uppsatsens bidrag är att ge exempel på hur SME kan engagera medarbetare, främja proaktiva cybersäkerhetsbeteenden och bygga en starkare säkerhetskultur.

1.4 Avgränsningar

Vi avgränsar oss till att enbart studera SME-företag med kontor i Skåne. Urvalet omfattar endast ett företag inom vardera sektor (life science, mödravård, juridik, energi och IT-sektorn). Resultatet är därmed inte garanterat applicerbart på andra företag inom samma sektorer. Vidare avgränsar vi oss till att studera medarbetare som inte har en roll inom IT-säkerhet. Dessutom speglar resultatet inte en större bild än företag inom Sveriges gränser.

2 Litteraturgenomgång

I detta kapitel behandlas teorier, ramverk och litteratur som ligger till grund för vår studie. Kapitlets delar syftar till motivationsfaktorer, mänskliga faktorer, organisationskultur, tekniska ramverk och centralisering/decentralisering. Syftet är att skapa en förståelse för hur medarbetarna agerar gentemot hot i en organisation, vilka faktorer som påverkar medarbetarnas riskhantering eller varför medarbetare begår misstag. Vidare syftar litteraturgenomgången till att skapa kunskap om organisationer, roller, ansvar och möjligheter att delta i beslutsfattning, vilket är aspekter som skiljer sig mellan medarbetarna som undersöks i kapitel 4.

2.1 Motivation

2.1.1 Protection Motivation Theory - PMT

Protection Motivation Theory (PMT) utvecklades av Rogers (1975) och är en teoretisk ram inom psykologi och beteendevetenskap, som syftar till att förstå varför människor vidtar skyddsåtgärder mot hot och risker. PMT har genom åren anpassats för olika sammanhang, varav ett är informationssäkerhet (Boss et al., 2015). Enligt Rogers (1975) utför människor två processer när de står inför ett hot, dvs en hotbedömning och en hanteringsbedömning. Hotbedömningen innebär att individen bedömer hur pass allvarligt hotet är, hur stor sannolikheten är att det inträffar samt hur pass stor risken är att personligen påverkas av hotet. Vidare syftar hanteringsbedömning till tre faktorer: Den första faktorn innefattar tron individen har på att föreslagen skyddsåtgärd kommer att mildra eller hindra hotet. Den andra faktorn innefattar tron individen har på sin egen förmåga att genomföra skyddsåtgärden. Den tredje faktorn innefattar vilka hinder eller kostnader som upplevs stå i vägen för att utföra skyddsåtgärden. Enligt PMT motiveras en individ att vidta åtgärder om denne bedömer hotet som allvarligt, känner sig sårbar och tror på sin förmåga att kunna skydda sig själv från hotet (Rogers, 1975).

2.1.2 Herzbergs tvåfaktorsteori

Herzberg (2003) menar att människan har två olika behov, vilket är hygienfaktorer och motivationsfaktorer. Baserat på arbetssituationen som människan befinner sig i, kan dessa behov antingen tillfredsställas eller skapa ett missnöje. Hygienfaktorer inkluderar grundläggande behov som är kritiska för människans överlevnad såsom lön, belöningssystem och interpersonella relationer. Dessa aspekter kan påverka hur en anställd genomför arbetet. Genom att uppfylla dessa behov kan motivationen och tillfredsställelsen höjas hos medarbetaren, men om dessa behov inte uppfylls kan det resultera i missnöje (Herzberg, 2003).

Herzberg (2003) menar att det andra behovet, dvs motivationsfaktorer inkluderar inre faktorer hos individen såsom prestationer, eget ansvar, uppskattning och möjlighet till utveckling. Vid

en tillfredsställelse av dessa faktorer höjs också motivationen och bidrar till att en medarbetare vill göra ett så bra arbete som möjligt. Det skapas däremot inte ett missnöje om dessa faktorer inte uppfylls, istället bidrar det till att medarbetaren inte känner sig tillfredsställd.

2.1.3 General Decision-Making Style - GDMS

Scott och Bruce (1995) har tagit fram General Decision Making Style (GDMS), som är ett ramverk som har i syfte att beskriva hur människor resonerar när de fattar beslut. Ramverket inkluderar följande fem kategorier:

Rationell stil: Denna stil innebär att individen utgår från faktiska bevis och objektiva kriterier när de ska fatta beslut. Individen har ett logiskt och metodiskt tillvägagångssätt.

Intuitiv stil: Denna stil inkluderar individer som fattar beslut baserat på sina insikter eller magkänsla. Vidare görs det ingen omfattande analys av alternativen.

Beroende stil: Stilen innebär att individen gärna lutar sig mot andra och andras åsikter när denne står inför beslut. Oftast beror detta på att individen tvivlar på sin egen förmåga.

Undvikande stil: Stilen innebär att beslutsfattandet skjuts upp eller undviks på grund av osäkerhet eller rädsla för dess konsekvenser.

Spontan stil: Denna stil inkluderar de individer som fattar beslut snabbt och impulsivt, utan att se över alternativ eller konsekvenser.

2.1.4 Motivering för valet av teorier

Protection Motivation Theory

PMT är en betydelsefull teori för att förstå hur individer motiveras att skydda sig mot hot. Med hänsyn till dagens organisationers cybersäkerhet, där hoten både ökar och blir mer avancerade, erbjuder PMT en ram för att utforska de kognitiva processerna bakom anställdas skyddsbeteenden. Genom att analysera faktorer som: hur medarbetare förhåller sig till cybersäkerhet, deras upplevda sårbarhet samt deras tilltro till sin egen förmåga att hantera risker och hot, erhöll vi viktiga insikter. Dessa insikter berör de motivationsaspekter som påverkar anställdas benägenhet att vidta åtgärder vid hot inom svenska små och medelstora företag (SME).

Herzbergs tvåfaktorsteori

Herzbergs tvåfaktorsteori fokuserar på hygienfaktorer och motivationsfaktorer som båda är kritiska i organisationers arbetsmiljö. Teorin används för att utvärdera hur olika faktorer som rör arbetsplatsen och arbetsmiljön påverkar anställdas engagemang i arbetet. Anledningen till att Herzberg tvåfaktorsteori är betydelsefull för studien är att den appliceras i en cybersäkerhetsaspekt. Genom att identifiera hygienfaktorer (såsom arbetsförhållanden) och motivationsfaktorer (såsom uppskattning, eget ansvar och möjlighet till utveckling) kunde vi göra en bedömning för hur dessa element påverkar cybersäkerhetsbeteende och den övergripande säkerhetskultur inom små och medelstora företag. Med tanke på att medarbetares beteende gentemot cybersäkerhet kan påverkas av arbetstillfredsställelse och

motivation, hjälper denna teori att identifiera vilka faktorer som kan förbättra eller förhindra goda cybersäkerhetsbeteenden.

GDMS - General Decision–Making style

GDMS erbjuder insikter i individers beslutsprocesser, vilket är avgörande i samband med cybersäkerhet där beslutsfattande kan påverka organisationers cybersäkerhet avsevärt. Att förstå de anställdas beslutsstilar hjälper till att utforma regler som kan mildra riskbeteenden. GDMS är betydelsefull för studien, eftersom teorien används för att kategorisera de anställdas beslutsstilar när de ställs inför cybersäkerhetsrelaterade beslut. Genom att förstå huruvida medarbetares stilar är rationella, intuitiva, beroende, undvikande eller spontana, kan beslutstilarna analyseras om huruvida dessa påverkar organisationers cybersäkerhetsarbete.

Teoriernas bidragande

Integrationen av dessa teorier gjorde det möjligt att analysera medarbetarnas beteende ur flera perspektiv. Detta multiteoretiska tillvägagångssätt gav en djupare förståelse för de mänskliga faktorer som påverkar cybersäkerhetsbeteenden och gjorde det möjligt att dra en slutsats som tog hänsyn till flera faktorer då relationen mellan cybersäkerhet och människa är komplex. Studien kunde därigenom ge en mer holistisk syn på hur man främjar en starkare cybersäkerhetskultur inom SME.

2.2 Mänskliga faktorer

Enligt (European Parliament, 2022), orsakas 60% av alla dataläckor med komponenter av SET där exploatering av mänskliga fel görs för att få tillgång till information. Corradini (2020) menar att det är en grundläggande princip att studera mänskliga faktorer och hur människan interagerar med system. Vidare är detta viktigt för att förstå bakomliggande faktorer till varför cyberolyckor sker så att man kan förebygga att misstag sker. Hon lyfter även fram att mänskliga fel som sker på grund av för hög arbetsbelastning, distraktion, okunskap eller bristande medvetenhet samt organisatoriska problem, bör betraktas som de främsta anledningarna till varför cyberattacker sker.

Kanki och Hobbes (2023), har tagit fram en forskningsrapport där de hänvisar till piloten Dupont (1997) som myntade begreppet “the dirty dozen”, som syftar till 12 faktorer som orsakar att människor begår fel (Kanki & Hobbes, 2023). Dirty dozen består av följande 12 faktorer: dålig kommunikation, distraktion, för lite kunskap, bristande samarbete, stress, sömnbrist, press, för lite resurser, brist på medvetenhet, sociala normer, brist på självsäkerhet och självtillfredsställelse Dupont (Kanki & Hobbes, 2023).

2.3 Organisationskultur

2.3.1 Socialpsykologiska faktorer

Vidare menar Allport (1954) att människors beteende påverkas av andra människors närvaro eller inställning till saker och ting. Han hävdar att människor inte bara påverkas av andra människors närvaro, utan också av sociala normer och påtryckningen att följa dessa, vilket kan påverka beteende och agerande. Konformitet är ett socialpsykologiskt begrepp som framkom under ett experiment genomfört av Asch (1955). Konformitetsexperimentet bevisade att människor oftast tenderar att anpassa sig efter gruppens förväntningar och normer, trots att det strider mot sin egen sinnes uppfattning (Asch, 1955). Vidare genomfördes ett annat socialpsykologiskt experiment av Milgram (1963) som resulterade i flera observationer och slutsatser om mänskligt beteende och lydnad. Lydnadsexperimentet bevisade att människor kan utföra handlingar som strider mot deras inre moral och åsikter om de påverkas av en högre auktoritet (Milgram, 1963).

Corradini (2020) menar att socialpsykologiska faktorer kan påverka medarbetarnas beteende i både positiv och negativ riktning. Hon beskriver en organisation som en social omgivning där människor ser vad andra gör och hon menar därmed att ett positivt ledarskap kan påverka organisationen i en positiv riktning. Däremot om ledningen visar eller uttrycker att de inte är uppmärksammar cyberhot, riskerar medarbetarna att ta efter samma beteende, vilket istället tar organisationen i en negativ riktning. Hon betonar också att vi ofta tenderar att glömma bort att organisationer är uppbyggda av människor och vikten av att ge medarbetare rätt förutsättningar att identifiera och agera när risker uppstår. Under framtagandet av program som främjar medvetenheten om cybersäkerhet är det viktigt att både tänka på kognitiva, sociala och emotionella aspekter (Corradini, 2020).

2.3.2 Efterlevanden av Säkerhetspolicyer

Beautement et al. (2009) menar att medarbetare gör en slags kostnadsnyttoanalys som avgör om de kommer att följa cybersäkerhetsregler eller inte. Med kostnadsnyttoanalys menas inte ekonomiska åtagande. Den upplevda kostnad/nytto-analysen syftar till medarbetarens psykiska, kognitiva press, skamsenhet, missade möligheter och press att möta deadlines, som gör att medarbetarna väljer att ignorera vissa policies. Enligt Corradini (2020) kan utformningen av policyer vara komplicerad, vilket leder till att medarbetare helt enkelt inte förstår dem eller anser att de inte är relevanta för deras arbetsuppgifter. Därför är kommunikation särskilt viktig. Enligt Chang och Lin (2007) har diskussioner om cybersäkerhetspolicyer i informella sammanhang en annan inverkan än kommunikationsmetoder såsom att skicka ut ett mail eller hålla en formell konferens.

2.4 Tekniska ramverk (Zero Trust Architecture och NIST)

Som tidigare nämnt är Zero Trust och NIST två omtalade och välanvända ramverk, men när dessa ramverk ska appliceras medkommer en del utmaningar. Exempelvis är NIST komplext och resurskrävande, särskilt för SME med begränsade resurser och erfarenhet (Benz & Chatterjee, 2020). Angående Zero Trust finns det dessutom en avsaknad av tekniska detaljer, få detaljerade fallstudier, få publicerade rapporter och forskning som belyser erfarenheter av att använda och implementera detta ramverk (Fernandez & Brazhuk, 2022). Teerakanok et al. (2021) menar även att att en av de största utmaningarna för Zero Trust är bristen på kvalificerad arbetskraft som förstår konceptet och teknologierna som är involverade i en Zero-Trust arkitektur, vilket kan vara en utmaning för vissa företag. Vidare är Zero-Trust inte lämplig för alla organisationer, eftersom ramverket inte är kompatibelt med vissa äldre system eller applikationer (Mutabazi et al., 2023). NIST CFS saknar även specificerade rekommendationer för att minimera risker baserat på en organisations uppmätta svagheter (Benz & Chatterjee, 2020).

Detta talar för att det finns ett kunskapsgap då det finns få fallstudier, tekniska detaljer och forskning som belyser erfarenheter av att använda och implementera Zero Trust. Vidare har vissa företag brist på kvalificerad arbetskraft som förstår konceptet och teknologierna av Zero Trust. Även NIST saknar rekommendationer för organisationer med uppmätta svagheter och ramverket kan både vara komplext och resurskrävande. Detta anser vi gör det aktuellt att undersöka och analysera svenska SMEs förmågor för att arbeta med dessa erkända tekniska ramverk.

2.4.1 Zero Trust? - En introduktion

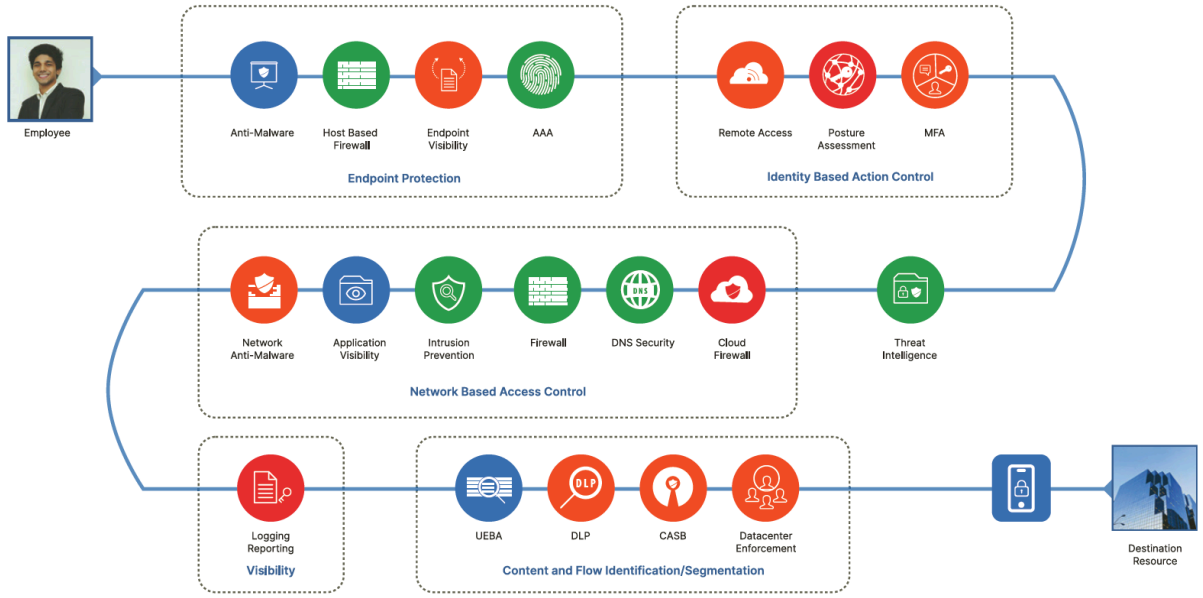
Zero Trust eller ZTA är ett säkerhetskoncept som blivit väl omtalat de senaste åren på grund av covid-19 pandemin och det ökade antalet cyberattacker. Detta eftersom många människor behövde arbeta hemifrån vilket ökade användningen av enheter och nätverk som användes utanför företagens kontrollsystem. Denna digitala transformation har lett till att den traditionella perimetermodellen blivit allt mer inaktuell. Fler människor som arbetar hemifrån, som använder sina egna enheter och den ökade användning av molntjänster har bidragit till att det inte längre går att betrakta det företagsnätverket som den primära säkerhetsgränsen (Madsen, 2024). Därmed utvecklades Zero Trust som Madsen (2024) beskriver med talesättet "Tillit är bra, men kontroll är bättre". Med Zero Trust ges åtkomst efter noggrann verifiering, och all kommunikation måste vara krypterad (Madsen, 2024).

Madsen (2024) beskriver Zero Trust som ett urval av verktyg och system som är utformade för att möjliggöra säkerhetsstrategier för digitala miljöer. Detta flyttar försvaret från statiska, nätverksbaserade gränser till att fokusera på användare, tillgångar och resurser vilket beror på att användarens plats inte längre betraktas som den främsta komponenten för resursens säkerhetsställning (Rose et al. 2020).

Det finns enligt Shore et al. (2021), inte enbart en gemensam definition av Zero Trust, däremot relateras koncepten Just-in-time access (JITA), Just-enough access (JEA), tokenisering, kryptering och åtkomstkontroll, ofta till ramverket. JITA innebär att åtkomst

enbart tillåts i realtid och vid behov, vilket förhindrar att rättigheter missbrukas. JEA är en kompletterande metod som innebär att en användare enbart får de rättigheter och den tid som är nödvändig för att genomföra en uppgift. Vidare används tokenisering och kryptering för att förhindra att känsliga uppgifter exponeras. Vid åtkomstkontroller läggs stor vikt på att utveckla dynamiska policies för att de enkelt ska kunna ändras eller uppdateras och därmed mer effektivt hantera risker i realtid (Shore et al. 2021).

Nedan visas ett diagram utvecklat av Madsen (2024) som beskriver hur ett Zero Trust flöde kan se ut. Bilden nedan visar hur en användaren valideras genom hela flödet innan denne får åtkomst till en applikation.



Figur 2.1: Zero Trust flöde (Madsen, 2024).

I en publikation av NIST skriven av Rose et al. (2020), definieras Zero Trust med hjälp av sju stycken grundprinciper:

1. Alla datakällor och datatjänster betraktas som resurser.
2. All kommunikation är säkrad oavsett nätverksplats.
3. Åtkomst till enskilda företagsresurser beviljas på en per-session-basis.
4. Åtkomst till resurser regleras av en dynamisk policy som inkluderar det observerbara tillståndet av klientidentitet, applikation/tjänst och den begärda tillgången. Policyn kan även omfatta andra beteendemässiga och miljömässiga attribut.
5. Företaget ser över och mäter integriteten och säkerhetsställningen för alla ägda och associerade tillgångar.

6. All autentisering och auktorisering av resurser är dynamisk och strikt genomförd innan tillträde tillåts.

7. Företaget samlar så mycket information som möjligt om det aktuella tillståndet av tillgångar, nätverksinfrastruktur och kommunikationer och använder det för att förbättra sin säkerhetsställning.

2.4.2 Kritisk analys - Zero Trust

Avsaknad av fallstudier

Fernandez och Brazhuk (2022) menar i en kritisk analys av Zero Trust, att det finns få rapporter och forskning som lyfter fram erfarenhet av att använda och bygga en Zero Trust arkitektur. De rapporter som finns tillgängliga beskriver implementationen av arkitekturen, men dessa är mer övergripande beskrivningar och saknar detaljerade fallstudier. Flertalet större bolag erbjuder lösningar för att inför Zero Trust inom organisationer, men informationen som delas är relativt begränsad. Dessa vägledande dokument saknar tekniska detaljer, men även hur en organisation ska gå tillväga steg för steg. Istället beskrivs en generell bild av bolagens approach till Zero Trust (Fernandez & Brazhuk, 2022).

Policyinstanser kan leda till inneffektivitet

I en artikel skriven av Shore et al. (2021) lyfts en komplexitet fram, vilket orsakas av att Zero Trust skiljer sig från traditionella åtkomstkontroller. Zero Trust har en dynamisk tillitsbedömning för att reglera och motivera åtkomst som styrs av en policyinstans. Alla åtkomstbeslut baseras alltså på en rad olika policyer med regler och villkor för vem som får åtkomst. Ett potentiellt problem med detta skapas om det finns ett fel i policyinstansen, vilket kan leda till konsekvenser för effektiviteten. Det argumenteras därmed att åtkomstbeslut bör baseras på mer tillförlitliga säkerhetsmekanismer för att förebygga ineffektivitet.

Vidare benämner Shore et al. (2021) att den största utmaningen när ett företag ska implementera Zero Trust är att undvika användaravbrott. Teerakanok et al. (2021) nämner också i sin artikel att arbetsflödet inom en organisation kan påverkas om tillits-nivåerna för åtkomsten till IT-resurser är för restriktiva. De menar att det är en utmaning för organisationen att bestämma en lämplig tillitsnivå för varje resurs. Om nivån är för låg kan det leda till konsekvenser för säkerheten och om den är för hög kan det leda till ineffektivitet i medarbetarnas arbete (Teerakanok et al., 2021).

Vad säger svenska företag och myndigheter om Zero Trust?

I en studie skriven av Nordgren et al. (2023) har intervjuer genomförts hos olika svenska företag och myndigheter, där frågor ställts gällande arbetet med Zero Trust. Första frågorna ställs i syfte att ta reda på deras inställning till Zero Trust. En av respondenternas svar på frågan “Hur skulle du vilja beskriva termen Zero Trust?” är följande:

> Det finns en teoretisk och en praktisk sida med att säga Zero Trust. I teorin är det en väldigt bra grej att ha att sträva emot, för då får jag i min roll en mycket enklare vardag egentligen [...] Men det kan bli för mycket att kräva det av medarbetare, eller sådana som agerar i nätverket som behöver bandbredden eller behöver nyttja den. Så det är en balansgång, att ligga på rätt säkerhetsnivå så att folk ändå kan jobba effektivt om man kan säga så (Nordgren et al. 2023, p.27).

Vidare baserat på respondenternas svar i frågan “Upplever ni att det mest är myndigheter eller företag som går mot Zero Trust-lösningar?” (Nordgren et al. 2023, p.29), verkar det som att företag som arbetar i molnet eventuellt går mer mot Zero Trust, medan en respondent inom den offentliga sektorn inte berört ämnet alls och inom den privata har det börjat diskuteras. På frågan “Har ni implementerat Zero Trust eller har ni funderat på att göra det?” (Nordgren et al. 2023, p.30) visar resultatet att det finns en variation i hur långt företag och myndigheter har kommit i implementationen av Zero Trust. Majoriteten har dock börjat implementera och har som ambition att gå mer mot arkitekturen. Vidare i frågan “Vilka hinder har ni upplevt i arbetet med implementeringen?” (Nordgren et al. 2023, p.32), svarar samtliga respondenter att de upplevt någon form av hinder. En myndighet nämner att det krävs otroligt mycket arbete då hela arkitekturen ska byggas om, medan ett annat företag nämner att kostnaderna har varit det största hindret. Ett företag nämner även att alla system och leverantörer inte har varit mogna eller mottagliga för att implementera Zero Trust. Två andra företag ansåg att den mänskliga faktorn och de anställda har varit ett hinder. Detta i form av brist på teknisk kompetens, men även att människan i sin natur är lat och bara vill att allt ska fungera. Zero Trust blir därmed för komplext.

2.4.3 NIST (National Institute of Standards and Technology) - Cybersecurity Framework

NIST Cybersecurity Framework (NIST CSF) utformades genom ett initiativ från Vita Huset (2014). Syftet med ramverket var att utveckla ett cybersäkerhets ramverk för att mildra risker inom cybersäkerhet för industrier, som i sin tur skulle kunna påverka ekonomisk och nationell säkerhet. NIST CSF baseras på expertis från hundratals säkerhetsexperter och deltagare från privata sektorn som tillsammans etablerade ramverket (The White House, 2014). Ramverket hjälper organisationer oberoende storlek eller sektor, att hantera samt minimera sina cyberrisker (National Institute Security Technologies, 2024).

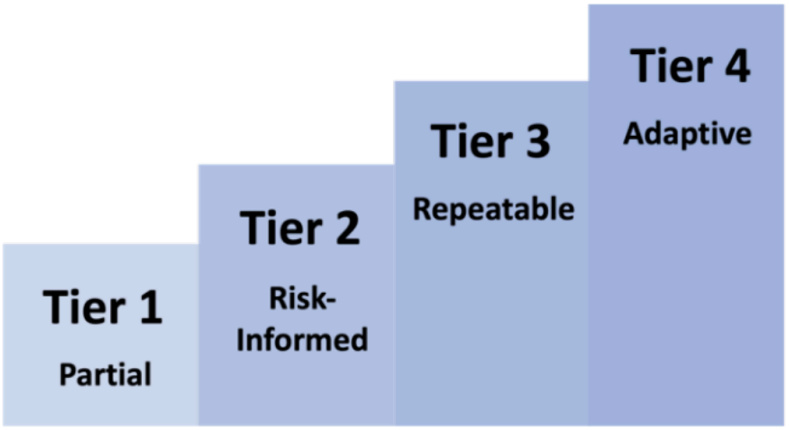
Ramverket baseras på tre komponenter: CSF core, CSF organizational profiles och CSF tiers.

CSF Core baseras på 5 funktioner som beskriver de önskade resultaten som ska förstås av medarbetarna oberoende av deras cybersäkerhetskunskaper. CORE syfte är att stödja de ansvariga för riskhantering i en organisation genom att förbereda, förebygga, upptäcka samt hantera incidenter. De 5 funktionerna innefattar: granskning, identifiering, skydda, svara och återhämtning av potentiella cyberattacker. Funktionen “skydda” ger resultat i form av bland annat medvetenhet och träning, autentisering och tillgångskontroll i organisationer. Sammantaget innefattar CORE riskhantering med hjälp av strategier, översikt av tillgångar såsom mjukvaror, hårdvara, tjänster, analyser av avvikelser för möjliga intrång och rapportering.

CSF Organizational Profiles fungerar som en utvärdering för organisationers säkerhetsläge och hur det önskade säkerhetsläget för en organisation skulle se ut. Därmed görs en identifiering av den nuvarande profilen, den önskade profilen, skillnaderna mellan profilerna och en handlingsplan för att uppnå målen.

CFS tiers fungerar som indikator för en organisations hantering och granskning av cybersäkerhet. Tiers förklarar hur efterlevnaden av cybersäkerhet ser ut, vilket tillåter organisationer att identifiera sig inom ett spann av 4 olika nivåer. Tiers 4 nivåer baseras på cybersäkerhetshantering samt granskning. Tiers nivåer innefattar: delvis hantering, risk informerad, repetitiv hantering och anpassad hantering. “Delvis hantering” brister i sin

hantering kring cybersäkerhet medan “Anpassad hantering” har fullt fungerande cybersäkerhet (National Institute Security Technologies, 2024).



Figur 2.2: CSF Tiers för cybersäkerhet risk governance and management (National Institute Security Technologies, 2024)

2.4.4 Kritisk analys NIST CSF

NIST CSF är en välanvänd metod inom hantering av cybersäkerhet och en metod som ska vara anpassningsbar till organisationer oberoende sektor och storlek (National Institute Security Technologies, 2024). Däremot upplevs ramverket bristande ur 3 aspekter:

1. Det är komplext och resurskrävande, särskilt för SME med begränsade resurser och erfarenhet. Vidare krävs det att medarbetarna lär sig ett nytt vokabulär för att genomgå det omfattande ramverket.
2. NIST CFS saknar även specificerade rekommendationer för att minimera risker baserat på en organisations uppmätta svagheter.
3. Ytterligare kritik är avsaknaden av tydliga betygskriterier, då IT-ledare bedömer sig själva mot standarder, där betyg som accepteras saknas. Det blir därmed en svårighet att mäta effektiviteten av cybersäkerhetsstrategier (Benz & Chatterjee, 2020).

2.5 Decentralisering och centralisering

2.5.1 Definition decentralisering och centralisering

En centraliserad struktur syftar till när beslutsfattande sker från ledningen och arbetet är ordnat i hierarkier. En centraliserad struktur kan även kallas traditionell struktur. Organisationen är högfungerande, där ledning fokuserar på inputs, parametrar tillhörande inputs och regler. Medarbetarna rapporterar till chefer och medarbetarna har ett primärt fokus på arbetet. Organisationen fungerar väl då medarbetarna uppfyller regler, processer som finns och följer ledarskapet. Ledningen har ett primärt fokus på resultat, framgången av kundnöjdhet och produkten. Policier och system är utformade för att skydda mot förändring och för att försäkra sig om att bibehålla riktlinjer, samt roller utan ifrågasättning. Nackdelen med centraliserad approach är att problem inte uppmärksammas till ledning och när ett problem upptäcks kan det vara försent (Norton & Fox, 1997).

I en decentraliserad struktur är makten fördelad i organisationen och organisering av arbete sker genom projekt eller produkter. Beslutsfattandet ges till medarbetarna i organisationen, vilket gör medarbetaren ansvarig för resultatet gällande kostnader, processer, strategier och kvalitéer. En decentraliserad struktur kan vara en nackdel då alla medarbetare kanske inte har samma vilja att delta eller involvera sig med detta ansvar, vilket kan bero på organisationen (Norton & Fox, 1997).

2.5.2 Decentralisering och centralisering i arbetssätt samt riskhantering

Bakos och Dumitrașcu (2021) genomförde en riskhanteringsstudie, där företag undersöktes i 3 följande faktorer: teknikrelaterade-, operationella risker, personalresurser och en kontext av föränderliga miljöer. Slutsatsen definierar tre brister i identifiering av risker, vilket innefattade: centraliserat arbetssätt, linjärt tänkande och brister i tidsaspekten till agerande. Bakos och Dumitrașcu (2021), argumenterar för ett decentraliserat arbetssätt, anpassningsbara metoder och inkludering av tidsaspekten i riskhanteringsprocessen. De menar att stärka samarbetet mellan olika nivåer gällande beslutsfattaning skulle vara fördelaktigt, då det skapar en mer flexibel riskhanteringsstrategi (Bakos & Dumitrașcu, 2021).

2.5.3 En mindre kontrollerade strategi

I en studie av Pham et al. (2017) poängterar undersökarna att medarbetare inte vill ta emot information om cybersäkerhetspolicyer, istället vill medarbetare vara med och forma policyer. Orsaken till viljan att forma cybersäkerhetspolicyer grundar sig i att medarbetarnas intresse, tillfredsställelse och nöje inom IT-säkerhet. Detta skiljer sig från chefer som vill att medarbetarna upphåller en passiv efterlevnad av poliycs. Därmed uppstår en klyfta mellan

IT-experter/chefer och medarbetarna åsikter om cybersäkerhet. Vidare upplevde medarbetarna att deras nuvarande IT-säkerhetspolicyer och dess uppgifter (som de inte varit med och utformat), som en distraktion och tidskrävande (Pham et al., 2017).

Vidare i Marquet (2013) förklarar en kapten för en kärnkraftsdriven ubåt, sina insikter med en social kultur där människor var följeslagare istället för att individuellt ta ledning. En kultur där människor är följeslagare påverkade medarbetarna negativt och resulterade i en låg moral och att stora misstag gjordes. Kaptenen genomförde därefter en förändring i sättet han styrde sitt skepp och fann att metoden att ge besättningen ägarskap och kontroll gjorde att de själva kunde identifiera behovet av att förändra sina tankesätt. Majoriteten av resultaten i dessa fall var önskade utfall. Corradini (2020) menar också att involvering och interagera med medarbetarna kring säkerhetsproblem kan öka motivationen genom att skapa en känsla av delaktighet då de medarbetarna får vara med och påverka organisationens strategi.

2.6 Litteraturgenomgång sammanfattning

Motivation och mänskliga faktorer

Vad som påverkar medarbetares arbete benämns i flera delar av litteraturen. Dels benämns Herzbergs hygienfaktorer som belöningssystem och interpersonella relationer, samt nämns även motivationsfaktorer som ansvar och utvecklingsmöjligheter. Dessa faktorer skapar missnöje eller motivation, vilket formar hur medarbetare genomför sitt arbete. Vidare anser vi att motivation eller missnöje kan ha en inverkan i hur en anställd hanterar risker eller hot på arbetsplatsen. I hantering av risker nämns i litteraturen att människor gör en analys gällande sårbarhet och allvaret av risken, en så kallad “hot bedömning” och en “hanteringsbedömning”. Om en anställd upplever missnöje anser vi att sättet att hantera risker kan påverkas. Missnöje eller motivation anser vi även har kopplingar till stress, press, organisationskultur och ledarskap. I litteraturen benämns även hur människor fattar beslut, baserat på kunskap och direktiv (rationell stil), beroende stil (ta hjälp av andra) etc. Dessa beslutstilar anser vi har kopplingar organisationskulturen, om en anställd som agerar i en beroende stil, kan ta hjälp av sina kollegor, eller har goda interpersonella relationer i arbetet.

Organisationskultur, Tekniska ramverk, Decentralisering och Centralisering

Ramverk som Zero Trust och NIST CSF, är välanvända runt om i världen. Zero Trust kan beskrivas som “Never Trust Always Verify”, vilket innebär att alla tillgångsförfrågningar ska antas komma från ett osäkert nätverk i syfte att skydda verksamheten. Koncept som Just In Time Access, Just Enough Access och kryptering är andra definitioner kopplade till ramverket. Zero Trust lägger betydande vikt vid det tekniska, såsom datakällor och datatjänster, säkrad kommunikation, hantering av åtkomster till enskilda företags resurser, klienthantering och applikationer. Ytterligare metoder inom Zero Trust mäter och granskar tillgångar, samt autentisering och auktorisering av resurser. NIST kan beskrivas som ett komplext ramverk med olika delar. NIST Core granskar, identifierar, skyddar, svarar tillgångar såsom mjukvaror, hårdvara, tjänster. NIST Organization Profiles analyserar gapet mellan företagets nuvarande cybersäkerhetsituation och företaget cybersäkerhetsmål. Slutligen innefattar NIST tiers en indikator som bedömer hur väl ett företag har anpassat sitt arbete till cybersäkerhetsaspekten.

Decentraliserade organisationsstrukturer kännetecknas av en fördelad makt, beslutsfattande och ansvar mellan medarbetarna. Medarbetarna kan fatta beslut gällande processer, strategier och kvalitéer. En centraliserad organisationsstruktur kännetecknas av att beslutsfattande sker från ledningen och regler samt policyer beslutas om från ledningen. Organisationsstrukturen anser vi är relaterad till medarbetarnas motivation och deras sätt att hantera risker.

Tabell 2.1: Undersökningsmodell

Huvudområde	Aspekter	Litteratur
Motivation	- Uppfattning av hot och risker - Hygien- och motivationsfaktorer - Resonemang vid beslut	Rogers (1975); Boss et al. (2015); Herzberg (2003); Scott och Bruce (1995);
Mänskliga faktorer	- Stress, press och distraktion	European Parliament, (2022); Corradini (2020); Kanki & Hobbes (2023);
	- Arbetsbörda	
Organisationskultur	- Sociala normer och Auktoritet	Allport (1954); Asch (1955); Milgram (1963); Corradini (2020); Beautement et al. (2009); Chang och Lin (2007)
	- Policier och dess förståelse	
Tekniska ramverk och tekniker	- Tekniska ramverk: Zero Trust-Architecture och NIST	Madsen (2024); Rose et al. (2020); Shore et al. (2021); Fernandez och Brazhuk (2022); Teerakanok et al. (2021); Nordgren et al. (2023); National Institute Security Technologies (2024); The White House (2014); Benz och Chatterjee (2020)
	- Kontinuerlig utbildning - Organisationens verktyg	
Decentralisering och centralisering	- Möjlighet att påverka strategier	Norton och Fox (1997); Bakos och Dumitrașcu (2021) (2021); Pham et al. (2017); Marquet (2013); Corradini (2020); Barlette (2015); Osborn och Simpson (2018);
	- Medarbetarnas inflytande inom organisationen	

Delar av teorin tas upp i flera områden i vår undersökningsmodell. När fenomen har tagits upp flertalet gånger har vi gjort vår egen avvägning vid kategorisering. I övrigt har undersökningsmodellen följts genom uppsatsen.

3 Metod och genomförande

I detta avsnitt presenteras och motiveras metodvalen som gjorts för studien, vilket baserats på undersökningsteorier och egna överväganden. Vidare motiveras urvalet i studien, strategin för genomförande av intervjuer samt valet av intervjufrågor. Slutligen presenteras och diskuteras tillvägagångssättet för bearbetning av data samt aspekter som validitet, reliabilitet och etik.

3.1 Metodik för litteraturgenomgång

Den empiriska metoden har i avsikt att gå från tankevärlden till en praktisk undersökning, dvs empiri. Tankevärlden innefattar olika uppfattningar, beskrivningar och förklaringar om olika fenomen, som genom empirin kommer att undersöka om dessa beskrivningar överensstämmer med verkligheten (Jacobsen, 2002). Beskrivningar av fenomen som använts i denna undersökning syftar till vår litteraturgenomgång. Metoden som användes för informationsinsamlingen av litteraturgenomgången, gjordes baserat på akademiska artiklar, journaler, E-böcker, böcker och webbsidor. Sökmotorer som använts för teorier baseras på akademiska artiklar, journaler och E-böcker, hos LUBsearch och Google Scholar. För informationsinsamling av tekniska ramverk och strategier har webbsidor som NIST, Europaparlamentet och olika myndigheter använts. Vidare har böcker för metodik och uppsatsskrivande lånats av Lunds Universitets bibliotek. Ytterligare, har nyhetsartiklar från Svt använts för att få information om aktuella händelser inom cybersäkerhet. I de akademiska artiklar som använts har vi använt oss av förstahandskällor för att stärka trovärdigheten. Vissa av källorna är mellan 20-50 år gamla, vilket beror på att vi har sökt i akademiska artiklar som hänvisat till dessa äldre förstahandskällor, som vi istället använt. Exempelvis Protection Motivation Theory av Rogers 1975. Genom vår användning av flertalet källor har vi hittat samband mellan olika källors information och hittat information som upprepats. Detta anser vi stärker och skapar en trovärdighet för informationen som presenterats i vår litteraturgenomgång. Genom de samband som upptäckts, utvecklades sökord som upprepande gånger använts under litteraturgenomgången. Dessa sökord innefattar cybersecurity, NIST CFS, Zero Trust, human factors, protection motivation theory, motivational factors, criticism, decentralisation, centralisation, Herzberg och risk-management. Majoriteten av sökmetodiken har gjorts på engelska, då det är det språk med flest forskningsartiklar inom vårt ämne.

3.2 Metodval

Metodval för denna studie är en kvalitativ metod. Valet av en kvalitativ studie grundar sig i dess öppenhet, där undersökaren inte ställer fasta frågor med förutbestämda svarskategorier, detta bidrar till att kvalitativa studier har hög intern giltighet och flexibilitet (Jacobsen, 2002). En korrelation som kvalitativa ansatser medför är sambandet mellan individer och en kontext, vilket är det som vår undersökning baseras på. Individer, dvs medarbetare inom olika sektorer och i kontexten av organisationers cybersäkerhetsarbete.

Vidare baseras valet av kvalitativ studie på att vår problemställning är explorativ och riktar sig till få undersökningsenheter. Fördelarna med en explorativ problemställning är att den går in på djupet och kan ta fram nyanserad data (Jacobsen, 2002). Utformningen är intensiv och används för att göra en ingående analys av ämnet, genom att hitta ett stort antal variabler hos ett få antal enheter (Jacobsen, 2002). En intensiv uppläggning lyfter fram fler nyanser och variabler vilket är i enlighet med studiens syfte. Vi vill få en tydligare bild av hur svenska SME inom olika sektorer driver sitt säkerhetsarbete, samt hur medarbetarna arbetar med cybersäkerhet. Genom att använda sig av intensiv uppläggning ökar den interna giltigheten. Nackdelen med en intensiv utformning är att det inte går att generalisera, då den intensiva utformningen blir mer kontextbaserad (Jacobsen, 2002). För att öka generaliserbarheten riktar sig vår studie till olika sektorer med ett urval av undersökningsenheter med olika roller. Sambanden vi sedan upptäcker mellan undersökningsenheterna och deras svar, anser vi stärker generaliserbarheten, vilket bidrar till att undersöka hur cybersäkerhetsbeteenden främjas hos medarbetare och hur svenska SME arbetar med erkända tekniska ramverk.

3.3 Urval

Urvalet av undersökningsenheter var ändamålsorienterat, vilket innebär att vi valde sektorer och företag som förväntades ge den mest relevanta och användbara informationen för att svara på forskningsfrågorna och uppnå studiens syfte. Ändamålsorienterat innebär att urvalet fastställer vilken information vi får (Jacobsen, 2002). Det fanns flera kriterier för vårt urval. Första kriteriet innefattade bredd och variation, där ville vi få information från medarbetare inom olika sektorer och därmed grupperade vi dem enligt sektorerna. Sektorerna vi valde innefattade sjukvård-, IT-, energi-, juridik- och life-science-sektorn. Det andra kriteriet var information, dvs att valet av undersökningsenheter hade god kunskap om ämnet vi behandlar (Jacobsen, 2002). Det andra kriteriet, "god kunskap”, innebär i vår undersökning att respondenterna är förstahandskällor och förklarar sina upplevelser om cybersäkerhet. Avsikten med undersökningen är inte att intervjua experter inom IT-säkerhetsområdet, istället syftade vi till att undersöka medarbetare med andra ansvarsområden. Undersökningsenheterna innefattade medarbetare med olika befattningar, t.ex. chefer och anställda, då dessa var medarbetare som behandlades i vår teori. Undersökningsenheterna hittades genom googlesökningar om företag i Lund och Malmö. Totalt kontaktades 23 företag och detta gjordes via mail. Vidare användes hemsidan allabolag (n.d.) för att kontrollera att företagens antal anställda innefattade ett SME. Vidare var vårt urval baserat på utvalda SME med kontor i Skåne. Anledningen till att vårt urval baserades på SME i Skåne, grundar sig i att vi ville göra besöksintervjuer i så stor utsträckning som möjligt och Skåneregionen passade vår undersökning ur ett tidsmässigt och resursmässigt perspektiv. Vidare följde vi EUs definition av SME i antal anställda, där mellanstort företag innefattade upp till 250 anställda, litet

företag som innefattade upp till 50 anställda och mikroföretag som innefattade upp till 10 anställda (Commission Recommendation 2003/05/06).

Tabell 3.1: Deltagande i studien

Respondent	Företag	Sektor	Roll	Storlek (Antal anställda)	Plats	Tid
R1	F1	Energi	HR-specialist	50 (litet)	Zoom	24 min
R2	F2	IT	IT-Konsult	80 (mellan)	Zoom	32 min
R3	F3	Life-science	Projektledare/VD	115 (mellan)	Besöksintervju	22 min
R4	F4	Mödravård	Barnmorska/Delägare	20 (litet)	Besöksintervju	16 min
R5	F5	Advokatbyrå	Chefssekreterare	10 (mikro)	Besöksintervju	23 min

3.4 Intervjuer

Semistrukturerade intervjuer baseras på ett skript med färdiga frågor, men erbjuder samtidigt möjligheten att ställa följdfrågor för att få djupare information (Wengraf, 2001). Semistrukturerade intervjuer användes även i vårt fall och det gav en flexibilitet i intervjuerna. Med andra ord följdes frågorna i intervjuguiden, men tack vare att semistrukturen skapades möjligheten att ge en mer nyanserad bild. Följdfrågorna/de öppna frågor kunde tack vare inspelning, samt transkribering följas och går att hitta i appendix 1-5. Vi valde att göra individuella intervjuer, då vi hade få undersökningsenheter som undersöktes. Vidare var syftet att i första hand hålla besöksintervjuer och i andra hand användes videosamtal via Zoom. Vi valde att göra individuella intervjuer då detta mäter samtliga deltagare på ett likvärdigt sätt (Jacobsen, 2002). Den begränsade tidsaspekten och datamängden som uppkom av kvalitativa intervjuer passade besöksintervjuer och videointervjuer bra. Ytterligare fördel med besöksintervjuer var den personliga kontakten, öppna stämningen, samt att besöksintervjuerna passade bra för öppna frågor. Anledningen till att vi undvek telefonintervju är att undersökningsenheten har lättare för att ljuga i dessa (Jacobsen, 2002).

Som visas i intervjuguiden (3.4.2 Intervjuguide) följde intervjufrågorna en viss struktur, vilket baserades på undersökningsmodellen och de teman som vi funnit i litteraturen. Intervjuguiden användes för att försäkra oss om att samma tema togs upp vid varje intervju. Undersökningsmodellens 5 huvudområden delades in i 2 teman i intervjuguiden. Denna uppdelning skapade ett flyt under intervjuernas gång, där frågor inom olika områden inte blandades.

Tabell 3.2: Tematisering av undersökningsmodell

Huvudområde:	
Motivation	Individbaserade frågor
Mänskliga faktorer	
Organisationskultur	Organisationsbaserade frågor
Tekniska ramverk och Tekniker	
Decentralisering och centralisering	

3.4.1 Motivering av intervjufrågor

Introduktion

Intervjun introduceras med att förklara de etiska aspekterna i undersökningen. De etiska aspekterna är baserade på vetenskapsrådets rekommendationer. Vidare, frågade vi undersökningsenheterna om tillåtelse att spela in intervjun. Utöver detta förklarade vi hur intervjun var strukturerad. Dessa aspekter genomfördes för att säkerställa att respondenterna skulle känna sig trygga. Den inledande frågan gällande respondentens roll i företaget, samt respondentens arbetsuppgifter, ställdes i syfte för att förtydliga att respondenten är en lämplig deltagare för vår undersökning. Arbetsuppgifter och roller har tidigare frågats efter i kommunikationen inför intervjuerna.

Individbaserade frågor

I första delen av intervjun ställdes frågor baserade på litteraturgenomgångens avsnitt om motivationsteorier och det individuella beslutsfattandet. Syftet med dessa frågor var att få en djupare bild av hur medarbetarna upplever sin förståelse gällande cybersäkerhet och hur medarbetarna bedömer sin förmåga att hantera hot. Exempelvis frågan: “Om du misstänker att du blir utsatt för en cyberattack på arbetet, hur hade du gått tillväga för att hantera detta? Tror du på din egen förmåga att hantera ett hot?” Vidare, undersökte vi om den anställda hade inflytande över sitt arbete och möjlighet att utvecklas inom sin roll. Syftet med denna frågan var att undersöka om organisationer erbjuder en möjlighet för sina medarbetare att utvecklas och om medarbetarna har inflytande, eftersom dessa förklarades vara motivationsfaktorer enligt litteraturgenomgången. Utöver detta ställdes en fråga om arbetsbörda och arbetsmiljö som baserades på litteraturgenomgångens avsnitt om mänskliga faktorer. Syftet var att ta reda på om medarbetarna upplevde stress och press, vilket skulle kunna resultera i misstag som kan ha en korrelation till cybersäkerhetsattacker. Detta gav oss också en möjlighet att avgöra hur bra medarbetarna trivdes på sina arbetsplatser, eftersom trivsel också kan vara en motivationsfaktor.

Organisationsbaserade frågor

Andra delen av intervjun inleddes med att undersöka organisationskulturella faktorer som kommunikation och samarbete. Vidare undersöktes även hur ledningen skulle gå tillväga vid ett cyberhot. Syftet med frågor gällande kommunikation var att skapa en förståelse för om cybersäkerhet var en uppmärksammad risk inom organisationen och hur aktivt organisationen arbetar med säkerhet. Vidare ställdes frågor kring om företagen hade några utbildningar relaterade till cybersäkerhet. Syftet var att undersöka om utbildning hade en inverkan på medarbetarnas kunskap och medvetenhet om cybersäkerhet. Vidare ställdes en fråga om de tekniska ramverken som Zero Trust eller NIST ingår i företagens strategier. Dessa ramverk har behandlats i litteraturgenomgången och utger sig för att vara anpassningsbara för olika företag oberoende storlek och sektor. Denna fråga var av största vikt, just p.g.a att ramverken är välanvända runt om i världen. Sedan ställdes en fråga gällande centralisering och decentralisering, genom att undersöka om det fanns utrymme för medarbetarnas input gällande företags cybersäkerhetspolicyer. Den slutliga frågan undersökte om respondenterna visste vilka de största utmaningarna var idag inom sina organisationers cybersäkerhetsarbete. Denna fråga undersökte om det fanns några upplevda brister i organisationernas cybersäkerhet.

Summering

Efter att intervjuerna genomfördes, gick vi igenom vilka frågor som besvarats och frågade om respondenten skulle vilja lägga till något. Därefter förklarades möjligheten att avsluta medverkan och kort nämndes de etiska principerna, samt tackades respondenten för sin medverkan.

3.4.2 Intervjuguide

Tabell 3.4: Intervjuguide

Tema	**Intervjufrågor**
Personfrågor	● Berätta om din roll i företaget och vilka arbetsuppgifter du har?
Motivation	● Hur mycket inflytande känner du att du har över ditt arbete i nuläget, hade du velat ha mer eller mindre? ● Känner du att du har möjlighet att utvecklas inom ditt arbete och att du får beröm för dina prestationer? Alt. *(Hur ser utvecklingsmöjligheterna ut i ditt arbete och hur ser uppmuntran till prestationer ut?)*

	● Är företagets cybersäkerhetspolicy något som du behöver ha i beaktande för att genomföra ditt arbete och på vilket sätt? ● Om du misstänker att du blir utsatt för en cyberattack på arbetet, hur hade du gått tillväga för att hantera detta? Tror du på din egen förmåga att hantera ett hot? ● Känner du att du har kunskap eller verktyg för att hantera ett cyberhot, på vilket sätt då?
Mänskliga Faktorer	● Hur upplever du din arbetsbörda och din arbetsmiljö?
Organisationskultur	● Hur hanteras cybersäkerhet inom verksamheten? a. Dvs har ni outsourcat denna uppgift eller hanteras den internt? ● Förstår du vad verksamhetens cybersäkerhetpolicier innebär? ● Hur kommuniceras cybersäkerhetspolicyer inom din organisation? ● Berätta om en gång när du arbetade tillsammans med dina kollegor för att lösa ett problem. Hur kom ni fram till en lösning? ● Vilka åtgärder vidtar ledningen när en attack sker?
Tekniska ramverk/Tekniker	● Har ni regelbundna utbildningar inom cybersäkerhet och hur ser dessa ut?

	● Har ni några nuvarande strategier eller ramverk i hantering av cybersäkerhet? T.ex. NIST, Zero Trust eller ISO dylikt?
Decentralisering Centralisering	● Hur fattas beslut kring cybersäkerhetsstrategier i din organisation och upplever du att det finns utrymme för medarbetarinput?
Övriga frågor	● Vilka upplever du är de största utmaningarna ni möter i er cybersäkerhetsstrategi idag?

3.5 Bearbetning av data

3.5.1 Förberedelse dataanalys

För att uppfylla en fullständig registrering av data är bandinspelning den mest kompletta formen för hantering av data i kvalitativa studier (Jacobsen, 2002). Denna metod användes när respondenternas svar skulle behandlas. Verktyget som användes för ljudupptagning var applikationen “röstmemon” i våra mobiltelefoner. Vidare förespråkar Jacobsen (2002) att den som intervjuar för anteckningar under intervjun. Syftet med att föra anteckningar är att visa intresse för vad respondenten uttrycker (Jacobsen, 2002). Anteckningar fördes även under samtalen med respondenterna för att samla de primära intryck vi fick. Under samtliga intervjuer förutom den första (Appendix 2) var enbart en av oss undersökare närvarande. Anledningen till att resterande intervjuer kunde göras av en av oss, beror på att vi använde oss av samma intervjuguide och därmed fick vi svar på samma frågor i intervjuguiden. Intervjun med båda av oss närvarande var den första intervjun som gjordes och anledningen till att vi var två i denna intervjun berodde på att vi ville känna oss trygga i de övriga intervjuerna. Vi utförde ingen testintervju innan de riktiga intervjuerna påbörjades. Vidare bestämdes tidpunkt och datum utifrån respondenternas schema.

3.5.2 Transkribering

Analysprocessen innefattar beskrivning, kategorisering och att hitta samband. Första steget i beskrivningsdelen syftar till renskrivning av samtalen med respondenterna (Jacobsen, 2002). Verktyg som Whisper och Goodtape användes inte. Fördelen med tjänster som dessa är att de är tidseffektiva, särskilt om flera transkriberingar skall göras (Jacobsen, 2002). Däremot var intervjuerna i vårt fall relativt korta, mellan 16-32 minuter, därmed fungerade manuell transkribering i vårt fall. Ytterligare anledningen till att vi använde manuell transkribering beror på att vi som intervjuade ville bearbeta information som sammanställts och detta bidrog även till en djupare förståelse för informationen som samlats in. Vidare, om fallet var att vi missat information, skulle vi snabbt upptäcka om vi hade behövt kontakta respondenten igen. Direkt efter att intervjuerna hölls, eller dagen efter, påbörjades transkriberingen. I

transkriberingen togs alla onödiga pauser bort och tilläggsord såsom (liksom, hmm), därmed blir transkriberingen mer innehållsfokuserad. Den asynkrona versionen (textformatet) av materialet användes sedan för att kategorisera och sortera information. En av respondenterna hade en vilja att få transkribering skickad till sig, på grund av sekretess och företagets policyer. Vi skickade därmed transkriberingen till respondenten, som sedan skickade materialet till dennes HR-ansvarig för kontroll. Detta gjordes för att säkerställa att medverkan skulle vara möjlig och om innehållet i materialet kunde vara en del av undersökningen.

3.5.3 Kodning

Kodningen av vår datainsamling är baserat på Alvehus (2019), som skrivit en handbok för uppsatsskrivande med en kvalitativ metod. Han delar in kodningen i tre delar: sortera, reducera och argumentera. Detta var utgångspunkten för hur vi arbetade med vår datainsamling och hur vi framställde ett resultat. Vidare, användes färgkodning som kodning i vår uppsats.

Vidare låg undersökningsmodellen till grund för färgkodningen av transkriberingen:

Tabell 3.5: Färgkodning

Kategori	Färg
Motivation	Blå
Mänskliga faktorer	Grön
Organisationskultur	Lila
Tekniska ramverk/tekniker	Gul
Decentralisering och centralisering	Orange

Sortera och Kategorisera

För att få en förståelse för det insamlade materialet rekomenderar Alvehus (2019) att läsa igenom materialet en gång innan sortering påbörjas. Detta följdes även i vår behandling av intervjuerna. Kategorierna var redan framtagna i undersökningsmodellen och detta låg till grund för vår ursprungliga tematisering. Alvehus (2019) nämner att tematiseringen inte ska fastställas allt för snabbt utan trycker på vikten av att vrida och vända på materialet några gånger först. Detta inträffade även i vårt fall, då tematiseringen ändrades ett antal gånger, för att sedan uppnå en slutgiltig tematisering. Vidare färgkodade vi skribenter varje enskild intervju, därefter jämfördes våran färgkodning, för att sedan diskutera fram en slutliglitig gemensam kodning.

Reducera

Här sållades det kategoriserade materialet för att ta ut det som vi ansåg var viktigast för studiens syfte och forskningsfrågor, som vi sedan ville presentera i empirin. Alvehus (2019) nämner däremot att det empiriska materialet måste presenteras på ett rättvist sätt då det är lätt hänt att urvalet av materialet påverkas för mycket av forskningsfrågan och syftet. Vi var därmed extra uppmärksamma på att även lyfta fram det material som var motsägelsefullt till våra forskningsfrågor, de teorier och den litteratur som lyfts i litteraturgenomgången.

Argumentera

Här menar Alvehus (2019) att skribenterna ska utveckla argument som är baserade på det empiriska materialet. I vår undersökning togs förklaringar fram som överensstämde eller uppkom flera gånger bland respondenterna. Detta låg till grund för att skapa argumenten. Vidare om det fanns motsägelser till dessa argument togs även dessa fram i resultatet då dessa förklaringar är också av hög relevans. Vår undersökning syftade till flera sektorer, därmed var det viktigt att belysa skillnaderna mellan sektorer och respondenter i resultatet. Undersökningsmodellen och intervjufrågorna var baserade på tidigare forskning, därmed underlättade det när argument för olika fenomen skulle behandlas.

3.6 Validitet, Reliabilitet och etik

3.6.1 Validitet

Validitet eller giltighet är en betydande faktor i en kvalitativ undersökningsprocess. Syftet med validiteten är att säkerställa att resultatet som sammanställs är pålitligt. Det är betydelsefullt att förhålla sig kritiskt till datan som samlas in. Det kritiska förhållningssättet baseras på intern giltighet, vilket syftar till frågan om vi har fått informationen vi vill ha. I den kritiska aspekten till den kvalitativa datans validitet finns även extern giltighet, vilket syftar till om datan kan appliceras i andra sammanhang (Jacobsen, 2002). För att upprätthålla god externa giltighet hade vår undersökning ett urval inom flera sektorer, därmed kunde vi upptäcka gemensamma mönster eller avvikande data, vilket uppfyller kravet att kunna applicera datan i andra sammanhang. Däremot kan den externa giltigheten vara begränsad till svenska eller europeiska företag och till SME- storlekar på företag. Den interna giltigheten är även hög, då undersökningen baserades på medarbetarnas upplevelser eller agerande i IT-säkerhetssituationer inom svenska SME. Syftet med undersökningen var inte att intervjua cybersäkerhetsexperter, syftet var istället att se hur medarbetare utan cybersäkerhetexpertis arbetar på ett IT-säkert sätt. Viktigt att ta i beaktande är att undersökningen bara har inkluderat en respondent från varje företag och ett företag från varje sektor. Detta kan orsaka att validiteten brister i en viss utsträckning, då en respondent från ett företag inte räcker för att kunna ge en fullständig bild av det specifika företaget.

Validering av källor syftar till om källorna är de rätta undersökningsenheterna och om de uppger korrekt fakta (Jacobsen, 2002). Vi anser att undersökningsenheterna var rätt för denna undersökning, då de var förstahandskällor som baserade fakta till situationer som de själva har varit med om, därmed var närheten hög. Vidare ansåg vi att det inte fanns motiv för

undersökningsenheterna att uppge oriktig information och därmed ansågs källorna ha en vilja att ange korrekt information. Ytterligare fördel med urvalet av källor var dess oberoende från varandra.

Vidare är litteraturgenomgången betydande för validiteten och generalisering av undersökningen som utförts. Som hjälpmedel för att stärka generaliseringen kan stöd tas från tidigare undersökningar (Jacobsen, 2002). Teorier och modeller som belysts i litteraturgenomgången, såsom tekniska ramverk, centralisering, motivationsfaktorer, etc, bidrar till en ökad generalisering när resultatet för studien sammanställdes.

3.6.2 Reliabilitet

En annan betydande faktor i undersökningsprocessen är reliabilitet eller tillförlitlighet, vilket syftar till om det finns faktorer som påverkar resultatet, t.ex. undersökaren, kontexter och planering. Undersökaren kan exempelvis ha en inverkan på den som intervjuas och vice versa, vilket kan uppkomma under datainsamlingsprocessen. När en undersökare har en inverkan på den intervjuade kallas det för intervjuareffekten (Jacobsen, 2002). Men hänsyn till intervjuareffekten, där intervjuaren kan forma samtalet med olika stimulier, kroppsspråk och talesätt, försökte vi som intervjuare uppträda och agera likadant vid samtliga intervjuer, i ett försök att bidra till reliabiliteten. Vidare kan kontexten (kontexteffekten), dvs platsen där intervjun genomförs påverka. Ett exempel är om intervjun skulle genomföras i ett sammanhang som är onaturligt för den som intervjuas (Jacobsen 2002). Detta togs i beaktande då vi erbjöd respondenterna att genomföra intervjuerna via Zoom och på så sätt kunde respondenterna fritt välja vilken plats som kändes mest lämplig för intervjun. Dessutom, som nämnts tidigare, försökte vi skapa förtroende på olika sätt, genom att följa forskningsetiska principer och anteckna under intervjun för att visa stort intresse för respondenternas svar. Vidare är en planerad eller överraskande kontext något som påverkar resultaten (Jacobsen, 2002). Intervjuerna var planerade, vilket gav respondenterna tid och möjlighet att ställa frågor innan intervjun. Planerade intervjuer var särskilt viktigt då ämnet behandlar cybersäkerhet och organisationer har olika policyer eller sekretess kring detta. En av respondenterna tillhörde en organisation, där intervjuguiden tilldelades till HR-avdelningen för att se över om deltagandet var möjligt med tanke på policyer eller sekretess kring cybersäkerhetsfrågor.

3.6.3 Etik - Forskningsetiska principer

Enligt Vetenskapsrådet (2002) kan det så kallade grundläggande individskyddskravet delas in i fyra krav på forskning. Intervjuerna genomfördes därmed med fyra forskningsetiska principer i beaktande: informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. För att säkerställa att studien uppfyllde samtliga fyra krav, delades en information- och samtyckesblankett ut till varje intervjuobjekt. Information- och samtyckesblanketten innehöll all nödvändig information om studien och intervjun, dessutom innehöll blanketten citat från Vetenskapsrådet för att tydliggöra vissa punkter.

Informationskravet

Enligt informationskravet inleds intervjuer med att berätta om vilka villkor som gäller för intervjubjektets deltagande (Vetenskapsrådet, 2002). Detta gjordes även i vårt fall. Det tydliggjordes att en ljudupptagning av intervjun skulle göras, med verktyget röstmemon och

att transkribering skulle ske för hand. Vidare tydliggjordes, innan intervjun påbörjades, att deltagandet var frivilligt och att intervjuobjektet skulle förbli anonymt genom hela studien. För att ge deltagarna en möjlighet att kontakta skribenterna gällande frågor, uppgavs telefonnummer samt e-post i information- och samtyckesblanketten (bilaga 2). Vidare uppgavs kontaktuppgifter till ansvarig lärare för examensarbetet på Lunds universitet (bilaga 2). Innan intervjun genomfördes fick även samtliga deltagare information om vart de kan läsa den färdigställda uppsatsen.

En annan aspekt är avslöjandet av studiens syfte/forskningsfråga, samt vilka insikter studien hoppas kunna bidra med, som kan äventyra studiens syfte samt validitet. Beslutet togs att avslöja syftet först efter att intervjun genomförts. Deltagarna fick endast information om att undersökningen berörde cybersäkerhet innan intervjuerna påbörjades. Efter intervjuerna fick deltagarna information om vad deras medverkande bidrog med till studien.

Samtyckeskravet

Studien följde samtyckeskravet genom att deltagarna lämnade samtycke innan intervjuerna inleddes, via information- och samtyckesblanketten. Vidare tydliggjordes för intervjuobjekten att de hade rätt att dra tillbaka sitt deltagande i studien om de skulle ångra sig samt deras möjlighet att avbryta intervjuerna när som helst.

Konfidentialitetskravet

I enlighet med detta krav signerade undersökarna en tystnadspliktsförbindelse som placerades i slutet av informationsblanketten. Detta gjordes i syfte för att deltagarna skulle känna sig trygga med att känsliga uppgifter inte kommer att anges utanför studien. Vidare uppgavs även möjligheten för den som intervjuades att inte svara på frågor, med anledning av företagens cybersäkerhet- och sekretesspolicyer. Därmed var det viktigt att poängtera för deltagarna att det fanns en valmöjlighet att inte svara på frågor. Ett exempel på sådan uppgift är t.ex. fråga 9, vilket berör hur personen hade gått till väga vid en attack.

Nyttjandekravet

Enligt detta krav framgick det att respondenternas svar enbart skulle användas för forskningsändamål. Denna information framgick också i information- och samtyckesblanketten.

4 Empiri

I detta avsnitt kommer de empiriska resultaten från intervjuerna att presenteras. Datan kommer presenteras i enlighet med undersökningmodellen.

4.1 Motivation

4.1.1 Uppfattning av hot och risker

Flera av respondenterna förklarade att cybersäkerheten grundar sig hos individen. R2 förklarade att cybersäkerhet, att hålla sig uppdaterad är en del av arbetet att och detta är individens ansvar. Vidare användes ord som medvetenhet och ett konstant tänk i respondentens inställning till cyberhot. R5 förklarade att det är viktigt att alltid ha en kritisk inställning, till exempel när man öppnar mail eller svarar i telefonsamtal. R3 förklarade att de behöver vara extra misstänksamma vid hantering av bluffakturor och att allmän försiktighet gäller vid hantering av mail. R1 förklarade att respondentens organisation borde skapa en formell utbildning, en större medvetenhet, bli mer kritiska och eftertänksamma i olika sorters situationer.

Vidare presenteras respondenternas förklaringar, gällande om de upplever rädsla att drabbas av ett cyberhot. R5 upplevde en viss oro för cyberattacker och detta förklaras i följande:

> *"Ja det klart man känner viss oro i och med att vi arbetar inom en bransch som hanterar känsliga uppgifter. Det är väl främst därför, men det är ingenting jag tänker på dagligen eller ser som en brist i verksamheten. Jag tror att för en sådan här liten organisation är det svårt att hantera det på ett annat sätt."* (Appendix 5, rad 43)

Därav upplevs hotets allvarhet, men samtidigt upplevde R5 en liten sannolikhet att det inträffar. R4 hanterade också känslig information och upplevde att hot som kommer utifrån, skulle kunna slå undan fötterna på en. R4 ger ett exempel:

> "*Ja men det är ju jätte skrämmande om vi skulle bli attackerade såsom Vellinge kommun blev nu t.ex. där hela journalsystemet slås ut och man inte kommer åt någon information. Det är ju medicinskt jätteallvarligt och om det hade drabbat oss eftersom vi har en hög medicinskt säkerhet och att inte komma åt information oerhört besvärligt.*" (Appendix 4, rad 38)

Med detta tolkas det som att R4 upplevde att risken för att ett hot skulle inträffa är stort och att det finns en risk att personligen påverkas av hotet. Vidare blev Vellinge kommun drabbad som en del av Ransomware-attacken mot Tietoevry. R3 förklarade att hoten ökar och att detta blir mer och mer påtagligt. R1 upplevde en rädsla för cyberattacker och förklarade följande:

> "*Även om många är bra på att identifiera spam-mail, utskick i mail, kanske det inte alltid är lika tydligt och det kanske inte inom en snar framtid, kommer att vara lika tydligt att något faktiskt kan vara ett cyberhot."* (Appendix 1, rad 18)

R1, R3, R4 kände därmed en rädsla inför framtida cyberhot. Gällande kunskap om att hantera cyberhot svarade R1 att denne inte har kunskap om detta och är personligen ganska rädd för att det skulle hända. R4 upplevde att respondenten själv inte har kunskap att hantera ett cyberhot. Till R4, ställdes även en följdfråga om de andra anställda har kunskap:

> "*Nej verkligen inte. Det är ju mitt uppdrag, och jag har själv ingen kunskap, så det har inte mina anställda heller.* (Appendix 4, rad 56)

R5 förklarade att respondenten inte heller har kunskap att hantera ett hot rent tekniskt. Istället har respondenten kunskap ur ett praktiskt perspektiv, då respondenten skulle kontakta sin närmaste chef. Likt R4 förklarade R5 att de inte har kompetens gällande cybersäkerhet i organisationen. R5 förklarade att de största utmaningarna är brist på kompetens och resurser. Därmed upplevde R1, R4 och R5 att de inte har kunskap att hantera cyberhot. R2 och R3 svar skiljer sig, då de upplevde att de har kunskap att hantera ett cyberhot.

4.1.2 Hygien- och motivationsfaktorer

R4 uttryckte att organisationen jobbar med personalvård, vilket innebär bland annat firande av födelsedagar och personalresor. R4 förklarade att respondenten har fantastiska kollegor och är i ett bra sammanhang med bra människor. R2 trivdes också bra med sina kollegor. R1, R3, R4 och R5 upplevde beröm för sina prestationer. R5 upplevde bra feedback, möjlighet att utvecklas och möjligheter att få mer ansvar, samt förklarade R5 att arbetsplatsen som positiv. R1, R2 och R5 upplevde därmed möjligheter att utvecklas. R4 prioriterade att medarbetarna ska få möjlighet att gå utbildningar för att få utvecklas inom sina områden. R4 ger personlig feedback för att uttrycka beröm. R2 och R5 förklarar:

"*Jag har alltså stor möjlighet att styra över mina arbetstider och miljö."* (R2, Appendix 2, rad 6)

"Precis, överlag är jag nöjd och tycker att jag får påverka så mycket som jag vill och kan göra på det sättet jag vill i de flesta fall." (R2, Appendix 2, rad 8)

"Jag får också möjlighet att utvecklas. Jag var från början sekreterare och har fått mer ansvar blivit chefssekreterare. Det glömde jag att säga innan, men det gjorde att jag fick mer möjlighet att lära mig mer om bokföring och fakturering och så." (R5, Appendix 5, rad 6)

4.1.3 Resonemang vid beslut

I undersökningen användes olika metoder för hantera cyberhot. Återkommande cyberhot som framkom i undersökningen var: mail, phishingmail och bluffakturor. Även samtal nämndes som ett hot, men detta tolkar vi inte som ett cyberhot.

Mail, phishing mail och bluffakturor hade inträffat hos R1, R3, R5 och samtal hos R1 och R5. Vidare undvek R4 och dennes organisation att jobba i mail. R4 skulle kontakta organisationens supportfunktion ifall en cyberattack skulle ske:

> *"Då hade vi nog kontaktat vår supportfunktion, för att jag tror inte att jag har så stor förmåga att lösa en sådan situation utan då får man kontakta någon som kan detta."* (Appendix 4, rad 36)

Vidare förklarade R1, R2 och R3 att de rapporterar incidenter, till exempel mail till en extern IT-tjänst (R1), intranät (R2) och IT-chef eller IT-avdelning (R3).

R2 och R4 nämnde inte att de hade hanterat ett phishing mail eller behövt rapportera en incident. R2 nämnde däremot vilka åtgärder respondenten hade vidtagit ifall det skulle hända. För mindre incidenter skulle rapportering via organisationens intranät göras. Vid allvarligare attacker finns telefon och mail till IT-säkerhetsansvariga hos R2s organisation som respondenten skulle kontakta.

R5 skulle kontakta sin närmaste chef vid en cyberattack eller om respondenten hade hanterat ett phishing-mail som hade riskerat att skada verksamheten. R5 nämnde även att mail och fakturor som denne identifierar som "bluff" läggs i skräpkorgen. Vidare tolkas det som att R5 själv upplevt phishingmail och bluffakturor:

> *"Det är ganska vanligt att vi får in bluffakturor, eller betalningspåminnelser där man ser att det kommer från en konstig mail."* (Appendix 5, rad 28)

Vidare förklarade R5 att vid större attacker skulle ledningen behöva ta hjälp av en extern IT-aktör, då organisationen inte har en IT-avdelning. Vidare trodde inte respondenten att organisationen har ett IT-avtal gällande organisationens cybersäkerhet i dagsläget. Vid större cyberattacker tror R1 att cyberattacker inkluderas i organisationens krishanteringsplan. R3 förklarade situationen vid akuta attacker:

> *"Är det så att man ser att det är något akut, har vi ett system där vi mailar ut till hela organisationen t.ex. om E-post skickas ut i ens namn utan att det är en själv."* (Appendix 3, rad 34)

4.2 Mänskliga faktorer

4.2.1 Stress, press och distraktion

R1 berättade att respondenten har en bra arbetsmiljö, som består av en hybrid arbetsmodell, som gör att R1 kan jobba hemifrån, vilket R1 upplever som flexibelt. Trots att R1 jobbar mycket hemifrån upplever R1 att det är enkelt att "stänga av".

R3 berättade om sina arbetsupplevelser kopplat till stress, press och distraktion. Arbetsbördan upplever R3 som hög emellanåt, men inte främst i arbetsmängden, vilket förklaras i följande:

> "*Kanske inte mycket i arbetsmängden utan mer att man blir splittrad därför att man sitter i många olika möten och inte riktigt får tid att fokusera på en sak under en längre tidsperiod. Kan man jobba mer än 30-60 minuter på samma sak är man rätt nöjd, men oftast är det någonting som avbryter."* (Appendix 3, rad 15)

Vidare berättar R3, att respondenten ofta får tid för återhämtning, men om respondenten är pressad av olika avdelningar eller ska leverera det kunden förväntar sig, blir respondenten pressad av det. Vidare förklarar R3 att respondenten är stressad i perioder och det påverkar hur respondenten utför arbetet. Stressen kan resultera i följande för R3:

> *"Det kan det absolut göra, ju mer stressad man är gör att man ibland kanske inte hinner göra saker på det sättet man hade velat göra och då får man ta lite genvägar eller nöja sig med det som är tillräckligt bra. Istället för att genomföra det så bra som man hade ambition att göra från början."* (Appendix 3, rad 20)

Vidare berättade R4 att respondenterna har begått misstag pga stress. Detta har även R3 gjort:

> (M) *"Har du någonsin begått ett misstag på grund av stress?"*
>
> (R3) *"Absolut, många gånger!"* (Appendix 3, rad 21-22)

R3 och R5 upplevde ibland ett högt tempo. R2 och R4 upplevde ett genomgående högt tempo.

4.2.2 Arbetsbörda

Gällande arbetsbörda uppfattade R1 och R2 arbetet som flexibelt, där de kan jobba hemifrån och från kontoret. R1 och R2 kunde även styra över vilka tider respondenterna jobbar. R2 poängterade samtidigt att kunden alltid kommer först. R2 förklarade även sin arbetsbörda:

> "*Det går lite i vågor och beror på vilka ambitioner man har och hur mycket man tar sig an. Bitvis blir det lite för mycket, men ibland känns det lugnt. Överlag tycker jag att det är ganska lagom, det är högt tempo, men det är också för att vi vill mycket och är taggade på att testa nya grejer och se hur det går."* (Appendix 2, rad 12)
>
> *"Arbetsbördan är lagom hittills, lite mycket kanske men när jag har tagit upp det med chefer hitintills så har vi löst det."* (Appendix 2, rad 12)

R2, R3, R5 förklarade att arbetsbördan varierar, medan R4 uttryckte att arbetsbördan har varit stor i perioder:

> *"Just nu och de senaste 14 åren har det varit perioder där det har varit alldeles för mycket att göra, det är en del av den här resan."* (Appendix 4, rad 16)

R4 uttryckte också att respondenten trivs på arbetsplatsen, vilket är orsaken till att respondenten orkar den höga arbetsbördan:

> *"Ja, det gör jag! Det har jag alltid gjort och det är det som gör att jag orkar. Jag har fantastiska kollegor och är i ett bra sammanhang med bra människor."* (Appendix 4, rad 20)

R5 förklarade att schemaläggningen mellan sekreterarna ibland inte går ihop, vilket beror på att samtliga sekreterare är studerande:

> *"Där ingen av oss vill arbeta för att det krockar med studier."* (Appendix 5, rad 10)
>
> *"Hur ser deras situation ut nu? Med tentor och finns föreläsningar man kan skippa, så får man ta hänsyn till om det är någon som har skippat en föreläsning tidigare."* (Appendix 5, rad 10)

4.3 Organisationskultur

4.3.1 Sociala normer och auktoritet

Gällande diskussion och kommunikation kring cybersäkerhet nämnde R1 att det diskuteras och informeras om hot som upptäckts mellan kollegor, men att det inte tas på lika stort allvar internt:

> *"Ja men det gör vi. Mina kollegor har fått mail, telefonsamtal. Personligen tycker jag att det är ganska allvarligt att få sådana mail. Men jag upplever inte att det finns lika stor förståelse för det internt eller hos vår IT-avdelning. Men detta kanske är för att det är så vanligt förekommande och att de får frågor om det, flera gånger i veckan."* (Appendix 1, rad 20)

R1 uttryckte att deras cybersäkerhetspolicy skickas ut vid anställningsavtal, som en del av on-boardingen och det är något som de anställda bockar av. Vidare uttryckte R1 att organisationen kan gör mer för att uppmärksamma cybersäkerhet:

> "*För att uppmärksamma cybersäkerhet mer tror jag på en formell utbildning, men också att få in förhållningssätt i det dagliga. Att skapa en större medvetenhet och att bli mer kritisk och eftertänksamma i olika sorters situationer. Och att skapa interna kanaler för att kommunicera och uppmärksamma avvikelser som kan leda till större hot*." (Appendix 1, rad 48)

R2 nämnde att det finns en kontinuerlig diskussion kring cybersäkerhet i organisationens slack-kanaler. Vidare har organisationen konferenser där de går igenom säkerhetsrelaterade saker på olika nivåer. R3 svarade inte uttryckligen att de kontinuerligt kommunicerar kring cybersäkerhet, men nämnde att om det händer saker och ting kommuniceras det till de anställda. R5 nämnde också att det tas upp under början av en anställning:

> *"Ja, inom organisationen har vi tydliga rutiner och instruktioner på hur vi hanterar mail, telefon och hur vi hanterar olika uppgifter, som man får lära sig när man börjar."* (Appendix 5, rad 26)

R4 svarade att de kommunicerar sin policy genom att prata om det och att skapa en medvetenhet. R4 nämnde även att cybersäkerhetspolicyer diskuteras under deras arbetsträffar, som uppkommer några gånger per år, samt diskuteras cybersäkerhet i följande fall:

> *"Vi pratar ofta om det, det händer ju ibland att man råkar öppna någonting som inte skulle ha öppnats och att man lyfter en medvetenhet hela tiden och påminner personalen om att radera sina inkorgar, så det inte ligger en massa som svämmar över."* (Appendix 4, rad 44)

Gällande samarbete och samverkan uttryckte R1 att det finns ett gott samarbete:

> "*Ja absolut, inom min avdelning upplever jag att det finns ett sådant förhållningssätt där man tar hjälp av närliggande avdelningar om man inte har svar på en fråga eller kan lösa ett problem själv.*" (Appendix 1, rad 48)

Även R2 nämnde att de delar med sig av kompetens och att det är en stor del av företaget. Vidare förklarade R2 samarbete och samverkan i följande fall:

> *"Sedan har vi ett möte (en kommitté), där alla får granska och komma med input/ förslag och då kanske vi reviderar så att alla är nöjda med lösningen."* (Appendix 2, rad 16)

Vidare beskrev samtliga respondenter att de arbetar tillsammans när det uppstår problem. R3 uttryckte följande om deras samarbete:

> "*Oftast sitter vi tillsammans och pratar. Man pratar med medarbetare och kanske leverantörer som man har, men även med kunden om hur man kan komma fram till en lösning.* " (Appendix 3, rad. 24)

Även R2 nämnde att de genomgående lyfter en diskussion och vill få mycket input om något har gått fel. R5 tycker att det finns en hjälpsam inställning när det uppstår problem och att medarbetarna är ärliga. R4 nämnde att de tillsammans diskuterar frågor om det uppstår problem eller om de får nya direktiv från Region Skåne. Därmed finns en samarbetskultur hos samtliga respondenters organisationer.

Vidare gällande uppfattningen av brister inom organisationen uttryckte R1 att respondenten saknar riktlinjer för vad som inte får göras på företaget, t.ex. att man inte kollar sin privata mail på jobbdatorn. Detta hade R1 personligen inte gjort, men R1 vet att det förekommer. R1 nämnde att det finns situationer som företaget behöver arbeta mer aktivt med:

> "*Men jag vet t.ex. i och med att jag jobbar med lönehantering, att jag vid flertalet tillfällen fått mail från personer som utger sig för att vara arbetstagare och som begär om att få byta bankuppgifter. Bara en sådan sak kanske man behöver jobba mer aktivt med.*" (Appendix 1, rad 18)

R1 beskrev att respondenten upplever att dagens inställningen till cybersäkerhet som naiv:

> *"I takt med att fler ungdomar inträder på arbetsmarknaden som har mer kunskap om cyberhot, tror jag att man behöver prata mer om det och att det i dag kanske finns ett naivt förhållningssätt gentemot att det skulle hända.*" (Appendix 1, rad 24)

R5 uttryckte att dennes företag inte hade kunnat hantera ett avancerat hot pga resurser, eller att företaget inte har ett system för att hantera hot. R5 är även medveten om att det finns brister i hur företaget hanterar sin cybersäkerhet:

> "*Vi är en väldigt liten organisation, som kanske inte gör så mycket för att hantera cybersäkerheten. Om man tänker på de program vi använder. Vi har liksom en öppen mailadress, där vem som helst kan skicka mail och bilagor till. Vi har en telefon som vem som helst kan ringa, utan någon rutin att kontrollera vem som är på andra sidan. Vår cybersäkerhet bygger på att vi människor är kritiska och att vi har rutiner för att inte lita på vem som helst.*" (Appendix 5, rad 41)

Vidare nämnde R4, som är delägare, att respondenten inte vet vad ledningen skulle vidtagit för åtgärder om en attack skulle ske, men att det är något som borde diskuteras med tanke på vad som hände Vellinge kommun.

4.3.2 Policier och dess förståelse

Till att börja med uttryckte samtliga respondenter att de har någon form av riktlinjer kring cybersäkerhet, däremot hade inte alla organisationer en bestämd cybersäkerhetspolicy. R2 nämnde att de har ett ledningssystem där olika policyer ska följas, men att när de är ute hos kunder är det deras policyer och riktlinjer de arbetar efter. R5 svarade på ett annat sätt att:

> *"Sedan ska jag vara ärlig med att det inte är något vi har en fast policy för. Vi är ett ganska litet företag. Det är inte att vi har en IT-avdelning eller så. Det är mer rutiner vi har för att arbeta mer cyber-säkert. Jag tror inte att vi har en specifik policy."* (Appendix 5, rad. 16)

Det var även en stor variation i respondenternas svar gällande om de förstår organisationens policy och riktlinjer. R3 uppfattade inte att det fanns termer eller begrepp som respondenten inte förstod. Detta uttryckte även R5 trots att företaget inte har någon direkt policy. I frågan om respondenten förstår företagets cybersäkerhetspolicy förklarade R2:

> "*Ja det tycker jag, där har säkerhetschefen och vår CISO varit nere på kontoret och gått igenom för alla anställda vilka regler/ krav som finns och av vilka anledningar de finns samt vart de kan hittas.*" (Appendix 2, rad 22)

Därmed hade R2, R3 och R5 förståelse för sina företags policyer. R4 svarade istället att respondenten inte full förståelse för företagets policyer och riktlinjer. R1 uttryckte sin tolkning av organisationens cybersäkerhetspolicy, men förklarade samtidigt att inte alla i organisationen har en förståelse för policyn:

> *"Hm, jag skulle säga att, ur ett allmänt perspektiv, handlar policyn om att förstå hur man kan jobba med det själv, i ett förebyggande syfte. Vilket skiljer sig från idag då organisationen har ett retroaktivt förhållningssätt. Och jag vet att det är något som kan skapa svår frustration, det här med att man autentiserar sig via Microsoft som många använder många gånger per dag. Att man inte förstår varför man behöver gå in och signera så många gånger."* (Appendix 1, rad. 10)

4.4 Tekniker och verktyg

4.4.1 Tekniska ramverk och Zero Trust-Architecture/NIST

De tekniska ramverk som användes i repsondenternas organisationer innefattar: NIS (R1) och ISO (R2). Ingen av respondenterna uppgav om organisationerna använder sig av NIST, däremot förklarade R4 följande efter att en förklaring av Zero Trust gjorts:

> *"Ja, jag håller med om att vi använder vissa delar av Zero Trust, men det var inte planerat."* (Appendix 4, Rad 60)

I en fråga som inte berör tekniska ramverk förklarade R1 att respondentens organisation använder sig av Microsofts autentisering flera gånger om dagen:

> *"Och jag vet att det är något som kan skapa svår frustration, det här med att man autentiserar sig via Microsoft som många använder många gånger per dag."* (Appendix 1, Rad 10)

R3 förklarade även att deras arbete med Microsoft molnet kräver säkerhetauthenticator. Precis som R1 trodde R3 inte att organisationen använde sig av Zero Trust. R3 förklarar:

> *"Nej vi har inga sådana ramverk, det enda vi har är VPN tunnlar. Allting som går via Office 365 är deras säkerhets authenticator osv, som man behöver identifiera sig om man ska arbeta i molnet på Microsofts plattformar."* (Appendix 3, Rad 54)

Därmed användes Microsoft autentisering hos R1 och R3s organisationer. Vidare användes delar av Zero Trust av R4.

"ISO 27001" användes av R2s organisation, där en extern firma verifierar att organisationen uppfyller de krav som finns för certifieringen. Firman gör även stickprover.

R5 kände inte till att de hade några tekniska ramverk inom cybersäkerhet. Vidare förklarade R5 att de är en liten organisation, som kanske inte kan göra så mycket för att hantera cybersäkerhet.

4.4.2 Kontinuerlig utbildning

I respondenternas svar gällande om de har någon form av utbildning inom cybersäkerhet skiljer sig svaren åt. R2 svarade följande i frågan om utbildning:

> "*Nej, vi har inte regelrätta kurser man ska gå en gång i halvåret, som jag vet att vissa andra företag har. Vi har ju ett mer kontinuerligt arbete där vi håller oss uppdaterade och har en diskussion i våra slack-kanaler. Vi har ju vissa som är relaterade till extern säkerhet och vissa som är mer intern. T.ex. de som sitter i red team/blue team, visar exploits och vad som är nytt och vad man behöver hålla koll på.*" (Appendix 2, rad 35)

R2 förklarade även att organisationen har konferenser gällande cyberhot:

> "*Vi hade en väldigt bra konferens förra året om hardware attacker. Har ni läst något om xz-exploits supply chain attack? Det var en ganska kodtung attack, med ett spännande tillvägagångssätt.*" (Appendix 2, rad 35)

Vidare förklarade R4 att de inte har några regelbundna utbildningar inom cybersäkerhet. Enligt R5s svar kan det tolkas att de inte har formella utbildningar, men att de håller sig uppdaterade med GDPR:

"*Inga utbildningar i sig, eftersom det är en organisation inom juridiken tar vi hänsyn till hur GDPR och annat regleras i lag och liknande. Kommer det något nytt på den fronten ser vi till att det arbetas in i våra rutiner, så att det inte är något som släpas efter.*" (Appendix 5, rad 33)

Det var enbart R3 och R1 som nämnde att de hade någon form av regelbunden utbildning. R1 svarade att de har regelbundna utbildningar digitalt:

> "*Sedan vet jag att de en gång i veckan skickar ut E-learnings till alla inom företaget, som man ska gå in och göra. Med detta tror jag att de vill förmedla att man kanske vissa gånger är en stor risk själv. Så att det handlar mycket om att skapa en medvetenhet och bli mer eftertänksam när man hanterar sin mail.* " (Appendix 1, rad 4)

I frågan om företaget har fler utbildningar svarade R1 följande:

> "*Nej, däremot vet jag att man har pratat om att ha det. Kanske ta ett omtag och använda ett sätt så att man kan följa upp det bättre också. Kanske se vilka som har gjort det?* " (Appendix 1, rad 26)

R3 nämnde också att de har mindre utbildningar med jämna mellanrum:

> "*Men vi har även så kallade micro-utbildningar, som kommer ut med jämna mellanrum där man får en 5 minuters utbildning och sedan får man svara på några frågor och man får även lite tips och råd om hur man ska hantera sin vardag säkert.*" (Appendix 3, rad 38)

4.4.3 Organisationens verktyg

De verktyg som organisationerna använder varierar beroende på sektor.

R1 förklarade att suspekta mail rapporteras in och läggs som ett ärende i deras externa IT-tjänst. Vidare förklarade R1 att medarbetarna autentiserar sig med Microsoft flera gånger dagligen. R2 förklarade att det finns enkla grundregler för hur man bygger säkra system, det finns anställda som är mer specialiserade inom cybersäkerhet i organisationen. R2 förklarade att respondenten själv använder sig av hotmodellering, riskanalys och code-reviews i det egna arbete. Detta förklarades i följande:

> *"När vi bygger något från grunden, så är det säkerhet som vi tänker på. Det ska inte gå att hacka och där finns det enkla grundregler för hur man bygger säkra system."* (Appendix 2, rad 37)

> *"Sedan gör man en hotmodellering eller en riskanalys, där man punktar upp vilka punkter som finns, som kan vara en angreppsyta. Har vi tänkt på det här? Sedan jobbar vi mycket med code-review, dvs att någon annan granskar vad man har byggt."* (Appendix 2, rad 45)

R3 förklarade att organisationen har ett stort fokus på hur de lagrar information, med rätt åtkomst och behörighet. Vidare förklarade R3:

> *"däremot har vi behörighetshantering där vi får en månadsrapport från vår IT-avdelning som visar vem som har access till vissa servrar, ytor och verktyg osv. Och det ser vi över minst en gång i månaden…"* (Appendix 3, rad 44)

R4 förklarade att de regelbundet byter lösenord, har certifikat för inloggning, jobbar så lite de kan i mail och att de har en funktion på datorn som regelbundet rensar mailen. Vidare förklarade respondenten att de arbetar mycket i molnet, de har en installerad hårddisk där de sparar allt material. Respondenten nämner fler verktyg som används i följande utdrag:

> *"Och sen kan man säga att alla vägar in till oss, alla kunder som vill boka tid, bygger på någon form av identifiering via bankid eller via 1177."* (Appendix 4, rad 32)

> *"Vidare när vi sitter i telefontider, så försäkrar vi om att patienten identifierar sig och att man inte lämnar ut uppgifter via telefon."* (Appendix 4, rad 44)

R5 förklarade att de är skeptiska till mail och pdfer, därför föredrar de att få dokument i pappersformat, för att på så sätt undvika hot. Vidare kräver R5s organisation personuppgifter i viss utsträckning, vilket är en del av rutinen, ett sätt att vara kritisk och inte lita på vem som helst.

4.5 Centralisering och decentralisering

4.5.1 Möjlighet att påverka strategier

Hur mycket medarbetarna får vara med och påverka företagets cybersäkerhetspolicy skiljde sig åt i respondenternas svar. R1 förklarade att medarbetarna inte får delta i skapandet av cybersäkerhetspolicyer, istället förmedlas informationen till de anställda. Till skillnad från R1 nämnde R2 att medarbetare kan komma med input:

> "*Jo men det har vi haft. Jag har inte varit med och format vår cybersäkerhetspolicy, men till varje dokument finns det ett tilläggssystem, där man kan anmärka på saker. T.ex. den här formuleringen var inte så bra, ni kanske inte har tänkt på det här etc. Där har vi sett att flera grejer har kommit in och uppdaterats.*" (Appendix 2, rad 43)

R3 som är VD nämnde att medarbetare har väldigt lite påverkan i cybersäkerhetspolicyer och det är IT-chefens uppgift att se till att policyer fungerar. R1 svarade att information om cybersäkerhetspolicyer förmedlas och att det inte har tagits några initiativ där medarbetarna har inflytande i cybersäkerhetspolicyer. Även R4 som är delägare, menade att medarbetare inte är delaktiga i framtagandet av säkerhetspolicyer:

> "*Nej, det är nog inget vi bollar ut i organisationen, utan vi tar in lite offerter och sen diskuterar vi detta inom styrelsen, som sedan kommer fram till ett styrelsebeslut.*" (Appendix 4, rad 63)

R5 upplevde att sekreterarna kan delta och har inflytande i diskussionen om cybersäkerhetpolicyer, samtidigt som organisationen har en top-down approach. Detta förklaras i följande:

> "*Sättet det kommuniceras är egentligen uppifrån och ned. Det kanske är advokaterna som flaggar för att det finns ett behov av se över vissa rutiner och det brukar då se ut, att vi bokar ett möte tillsammans med alla.*" (Appendix 5, rad 33)

> *"Vårt sekreterararbete är ändå hyfsat självständigt, vilket jag tror att advokaterna vill, alltså att vi har stort inflytande. För i slutändan är det vi som gör det och även advokaterna lyssnar på vad vi har att säga om cybersäkerhet."*(Appendix 5, rad 35)

4.5.2 Medarbetarnas inflytande inom organisationen

I intervjun med R2 framgår det att medarbetarna driver projekten, men att de har kundens behov och krav i beaktande:

> *"Jag har alltså stor möjlighet att styra över mina arbetstider och miljö. Vidare är det hur vi arbetar, stacken är ganska satt, men vi har ju olika sätt vi bygger system på, ibland använder vi microservices och ibland gör vi på andra sätt. Kunden som jag för närvarande har, är väldigt lyhörd och öppen för input och rekommendationer från oss, men ibland är det mindre svängrum och då bygger vi på ett visst bestämt sätt.*" (Appendix 2, rad 6)

R2 upplevde också att det finns möjlighet att påverka sitt arbete och att respondentens åsikter tas i beaktande:

> "*Det tycker jag känns väldigt bra och mina chefer och projektledare är lyhörda för vad jag vill och vilka uppdrag jag vill ha och vad jag tycker är bra/dåligt, samt om jag vill byta uppdrag.*" (Appendix 2, rad 10)

Även R1 hade inflytande över sitt arbete, både i vilka uppgifter respondenten har och när respondenten kan utföra dessa arbetsuppgifter. R3 förklarade att det är de själva tillsammans med IT-avdelningen som tar fram policys. På så sätt har repspondenten har inflytande i organisationen och i rollen som VD. Vidare inkluderar R3 sina medarbetare i kommunikationen för att lösa ett problem:

> "*Oftast sitter vi tillsammans och pratar. Man pratar med medarbetare och kanske leverantörer som man har, men även med kunden om hur man kan komma fram till en lösning.*" (Appendix 3, rad 24)

Som tidigare nämnts förklarade R4 att respondentens medarbetare inte har inflytande i skapandet av cybersäkerhetsstrategier och istället tar respondenten in offerter. Offerterna, respondenten, diskuterar sedan policyer tillsammans med styrelsen. R4 har till skillnad från sina medarbetare inflytande inom organisationen. R5 upplevde att denne har inflytande och förklarar det i följande:

> *"Jag känner att jag har ganska stort inflytande. Vi är en ganska tydlig organisation. Därmed är det tydligt att jag har absolut mindre inflytande än de som jobbar som advokater, samtidigt har jag betydligt mer inflytande än de som jobbar som sekreterare. Då jag är chefssekreterare. Jag har inflytande över schemaläggning, inflytande över hur våra rutiner ser ut och våra öppettider och så."* (Appendix 5, rad 4)

5 Diskussion

Från den empiriska undersökningen framkom diverse skillnader och likheter bland respondenterna, deras organisation och dess sektor, vilket diskuteras i detta kapitel tillsammans med teorier från litteraturgenomgången. Vidare diskuteras medarbetarnas upplevelser från empirin och respondenternas svar gällande deras organisationer tillsammans med teorier från litteraturgenomgången.

5.1 Övergripande skillnader och likheter

5.1.1 Roll

Rollerna mellan respondenterna skiljer sig. Dels i vilken avdelning av organisationen respondenterna arbetar på, vilken arbetsroll de har och i vilken befattningsnivå de arbetar inom. Två av respondenterna, R3 och R4, hade högre befattningar såsom delägare och VD, vilket påverkar arbetsuppgifter och ansvarsområden. Respondenter med högre befattning kan ha ansvarsområden som inkluderar beslutsfattning gällande IT-hantering och personalhantering vilket kan påverka deras svar i intervjuerna. Vidare hade R4 flera roller inom organisationen, då respondenten fortfarande var barnmorska på 50% samt delägare. En annan skillnad mellan respondenterna i undersökningen var att R5 var studerande samtidigt som respondenten jobbade på advokatbyrån, vilket skiljer sig från övriga respondenter som arbetade heltid. Detta gör det värt att lyfta att även arbetslivserfarenhet och ålder kan vara två faktorer som kan påverka kunskap och förmåga. Kort sagt fanns det en mångfald bland respondenterna.

5.1.2 Organisation

Det fanns flertalet skillnader i organisationerna som deltog i undersökningen. Dels i antalet anställda, grad av digitalisering och organisationsstruktur. IT-företaget, Life-Science-företaget inräknas i medelstora företag. Mödravårdsföretaget och energi-företaget inräknas i ett litet företag, medan advokatbyrån räknas som ett mikroföretag, enligt EUs definition av SME i antalet anställda (se tabell 3.1). Dessa skillnader framkom i undersökningen, då till exempel advokatbyrån med 10 anställda inte hade en IT-avdelning, eller en specifik cybersäkerhetspolicy. Advokatbyrån upplevdes även vara den minst digitaliserade verksamheten i undersökningen, exempelvis genom att dokument hanterades i pappersformat och att företaget helst inte tog emot PDF-filer, i syfte att undvika cyberhot. Sådana skillnader kan bero på organisationens storlek, resurser och teknologisk infrastruktur, vilket indirekt kan påverka förmågan att hantera cyberhot.

En skillnad från advokatbyrån var IT-företaget som framstod som mest digitaliserat bland respondenternas företag eftersom de arbetade med att utveckla digitala miljöer eller system, vilket troligtvis innebär att de arbetade mer i digitala miljöer. IT-företaget kan på grund av den digitala miljön utsättas för andra typer av cyberhot än de andra organisationerna i undersökningen. Det kan således diskuteras om risken för cyberhot ökar ju mer digitaliserat ett företag är. Vidare beskriver IT-företaget att det finns en mer genomgående cybersäkerhetsmedvetande under deras projekt, vilket påverkade graden av digitalisering och

IT-beredskap. De övriga organisationerna verkar däremot arbeta allt mer i digitala miljöer och med digitala verktyg. R1 arbetade exempelvis just nu med att skapa en automatiserad anställningsprocess. R3 arbetade i en digital miljö, där kunddata lagras. R4 hade precis uppdaterat deras IT-system och arbetade i övrigt mycket med digitala verktyg som 1177. Vidare hanterade R4 deras patientdata i ett digitalt system.

5.1.3 Sektor

Hur säkra medarbetarna kände sig på att kunna hantera ett cyberhot eller en attack varierade mellan respondenterna. R1, som arbetade inom energisektorn, svarade exempelvis att respondenten inte hade kunskap och var väldigt rädd för att det skulle inträffa. Även R4, som arbetade inom mödravården, nämnde att denne saknar förmåga att hantera ett hot och hade behövt lämna över den uppgiften till någon som har kompetens. R5, som arbetade inom juridiska sektorn, svarade att förmågan finns för att kunna identifiera mail som utgör ett hot, men att respondenten utöver detta saknar kompetens och kunskap inom krishantering. Vidare förklarade respondenten att denne hade behövt lämna över uppgiften till någon annan inom verksamheten. R2, som arbetade inom IT-sektorn och R3, som arbetade inom life-science -sektorn, nämnde istället att de har en tro på sin egen förmåga att hantera ett hot. Dessa skillnader kan bero på att respondenterna arbetade inom olika sektorer. Det kan därmed diskuteras om medarbetare inom life-science och IT-sektorn har mer kunskap och en större tro på sina egna förmågor vid hot eller attacker. Tron på sina egna förmågor kan dock också bero på att IT-konsulten och projektledaren har tydligare direktiv och en tydligare krishanteringsplan vid cyberhot, vilket i sin tur kan bero på att de arbetar på större bolag. Det behöver därmed inte nödvändigtvis bero på vilken sektor medarbetaren arbetar inom utan kan även grunda sig i företagets resurser och kapacitet.

Vidare kan en skillnad tydas i respondenternas förståelse för företagets säkerhetspolicy och riktlinjer. R1 förklarade att deras policy handlar om att förstå hur medarbetaren själv kan arbeta med cybersäkerhet, men R1 uttryckte även att det kan finnas en frustration vid autentisering via Microsoft, då många inte förstår varför det behövs. R4 upplevde inte att respondenten förstod företagets cybersäkerhetspolicy fullt ut. R5 svarade att det inte fanns några oklarheter och att respondenten förstod de policyer som företaget hade. Vidare förklarade R5 att företaget dock inte hade någon direkt cybersäkerhetspolicy. Både R2 och R3 beskrev att de förstod företagets säkerhetspolicy. Även dessa skillnader kan bero på respondenternas sektorer. Det kan dock också bero på att R2 har andra förutsättningar, då företagets säkerhetschef och CISCO har gått igenom policyn och att de kontinuerligt är tillgängliga för att svara på frågor från medarbetarna. R3 är projektledare samt VD och är därmed delaktig i framtagandet av företagets cybersäkerhetspolicy, vilket kan vara en bidragande faktor till respondentens förståelse för policyn.

5.2 Medarbetare

5.2.1 Motivation

Om man ser till respondenternas uppfattning om hot och risker skiljer sig uppfattningen åt. Utifrån R2s svar verkar det som att respondenten ansåg att det är viktigt att cybersäkerhet är en del av det “vardagliga arbetet” och att det finns en “medvetenhet” och “konstant tänk”. R5

och R4 nämnde också att deras förhållningssätt till cybersäkerhet är att man som medarbetare alltid har en "kritisk inställning" eller är extra "misstänksam".

Som tidigare nämnt enligt PMT, kommer en individ att motiveras att vidta åtgärder om denne anser att hotet är allvarligt, känner sårbarhet och tror på sin egen förmåga att kunna skydda sig från hotet (Rogers, 1975). Majoriteten av respondenterna verkade se cyberhot som något allvarligt, men R5 nämnde däremot att det inte är något respondenten tänker på dagligen. R1 nämnde också att företaget kanske skulle behöva en mer formell utbildning, där syftet är att skapa mer medvetenhet och att få medarbetarna att bli mer kritiskt eftertänksamma i olika situationer. Detta kan tolkas som att R1 inte tycker att cyberhot tas på tillräckligt stort allvar inom organisationen på grund av bristande medvetenhet.

Vidare uttryckte R4 att det skulle vara väldigt skrämmande om verksamheten skulle bli utsatt för en cyberattack, vilket kan tolkas som att denne känner sig sårbar. R1 uttryckte också att respondenten känner rädsla för att en cyberattack skulle drabba företaget. Även övriga respondenter visade en viss ödmjukhet och sårbarhet i sina svar gentemot cyberattacker. Gällande kunskap och tron på sin egen förmåga uttryckte som tidigare nämnt enbart R2 att denne hade en tro på sin egen förmåga, resterande respondenter uttryckte att de saknade kunskap eller att de hade tagit hjälp av en chef, IT-avdelning eller extern IT-tjänst. R3 beskrev att respondenten trodde på sin egen förmåga, men skulle lämna över arbetet till IT-avdelningen.Vidare upplevde R3 att den största utmaningen i deras cybersäkerhetsstrategi var att hålla hela organisationen på tårna och följa med i de verktyg som finns, då hoten blir allt fler.

Om ovanstående information tas i beaktande verkar det som att okunskap och avsaknad av tron på den egna förmågan, är bristande faktorer för att en anställd ska motiveras till att vidta åtgärder vid attacker eller i det dagliga arbetet enligt Rogers (1975) teori. Däremot är människan komplex och det finns flera andra motivationsfaktorer att ta hänsyn till som kan påverka huruvida medarbetarna arbetar IT-säkert. Okunskap och tron på den egna förmågan behöver därmed inte vara de enda avgörande faktorerna.

Motivationen kan även ställas i relation till Herzbergs tvåfaktorsteori. De grundläggande hygienfaktorerna som lön, belöningssystem och interpersonella relationer kan enligt teorin påverka hur medarbetarna utför sitt arbete. Dessutom kan även motivationsfaktorer såsom prestationer, eget ansvar, uppskattning och möjlighet till utveckling bidra till att den anställde vill göra ett bra jobb och känner sig tillfredsställd (Herzberg, 2003). Trots att medarbetarna inom R4's verksamhet saknade kunskapen och förmågan att hantera ett hot eller en attack, fanns det alltså andra motivationsfaktorer som kunde väga upp. R4 som var delägare lade stor vikt vid att visa uppskattning gentemot sina anställda genom att till exempel uppmärksamma kollegor som gjort bra ifrån sig, fira födelsedagar och åka på personalresor. R4 beskrev även att de satsade mycket på att medarbetarna skulle få gå utbildningar och utvecklas inom sina roller. Att visa uppskattning och att ge medarbetarna möjlighet att utvecklas kan som tidigare nämnt enligt Herzbergs (2003) teori öka motivationen och ge tillfredsställelse och därmed även bidra till att medarbetarna arbetar mer IT-säkert.

Flera av respondenterna nämnde att de upplevde möjligheter till utveckling inom sina roller, och IT-konsulten kände att respondenten fick ta ett betydande eget ansvar. En del av respondenterna kände också att de hade kontroll över sitt arbete genom möjligheten att arbeta varifrån de önskade samt genom flexibla arbetstider. Detta kan bidra till ökad motivation bland medarbetarna att arbeta mer IT-säkert. Denna observation stöds av litteraturen där eget

ansvar och möjligheter till utveckling främjar en önskan bland medarbetare att prestera bättre (Herzberg, 2003).

5.2.2 Mänskliga faktorer

Enligt (European Parliament, 2022), orsakas 60% av alla dataläckor med komponenter av SET där exploatering av mänskliga fel görs för att få tillgång till information. I frågorna kring medarbetarnas trivsel och arbetsbörda upplevde flera av respondenterna att stress och att mängden arbetsbörda gick i perioder. R4 nämnde däremot att arbetsbördan periodvis har varit tung de senaste 14 åren och att det har varit för mycket att göra. Respondenten nämnde dock att trivseln i arbetet och trivseln med kollegor bidrog till att respondenten orkar med den höga arbetsbördan. Detta stödjer Herzberg (2003) tvåfaktorsteori om att interpersonella relationer, som är en hygienfaktor, är viktig för hur människan genomför sitt arbete. Arbetsmängden var inte problemet i R3s fall, utan snarare att respondenten blev splittrad när det inte fanns utrymme att arbeta med en och samma uppgift under en längre period. Detta kan tolkas som att R3 kände sig distraherad och splittrad då respondenten arbetade med flera uppgifter och deltog i olika möten samtidigt, vilket kan bero på den högre arbetsbefattningen som VD.

Corradini (2020) benämner distraktion och hög arbetsbelastning som två faktorer att ta hänsyn till för att undvika misstag. Respondenterna verkade i det stora hela känna sig nöjda med sina arbetsbelastningar, medan R2 och R4 upplevde att det kunde bli lite för mycket ibland. R2 hade dock lyhörda chefer och de hade tidigare tillsammans löst situationer om det har blivit för mycket. R3 upplevde snarare en splittring i arbetet, vilket eventuellt kan leda till misstag.

Stress och press är mänskliga brister som kan leda till att människan begår misstag (Kanki & Hobbes, 2023). Detta stöds i undersökningen av R4 och R3, som båda svarade att de har begått misstag på grund av stress. R3 uttryckte till och med att det är något som har hänt vid upprepade tillfällen och R3 förklarade att denne upplevde att det påverkade hur respondenten utförde sitt arbete. Vidare beskrev R3 att respondenten upplevde press om det fanns krav från olika avdelningar eller krav på att leverera det kunden förväntar sig. Press kan också eventuellt leda till misstag. R3 nämnde dock att denne ofta får tid för återhämtning, vilket är ett sätt att hantera pressen. Vidare nämnde R5 att det ibland kan vara utmanande att få ihop schemaläggningen då alla sekreterare är studenter. Detta kan i sin tur skapa både stress och press då chefssekreteraren beskriver att det kan påverka studier, då de ibland behöver skippa föreläsningar.

5.3 Svenska SME

5.3.1 Organisationskultur

Cybersäkerhet kommunicerades på olika sätt inom organisationerna vilket påverkade organisationskulturerna i denna undersökning. R2 förklarade att cybersäkerhet kontinuerligt kommunicerades/diskuterades mellan kollegor, exempelvis i deras Slack-kanaler eller genom interna konferenser som hölls av organisationen. R4 berättade att de regelbundet pratar om cybersäkerhet, exempelvis om någon råkar öppna ett misstänkt mail, vilket syftade till att öka

medvetenheten bland medarbetarna. Dessutom diskuterade R4 cybersäkerhetsfrågor under sina arbetsträffar några gånger om året. R1 och R3 nämnde att hot diskuterades så fort de upptäcktes. R5 förklarade att cybersäkerhet endast kommunicerades genom rutiner och instruktioner som tilldelades vid anställningstillfället.

Corradini (2020) förklarar att ett positivt ledarskap kan påverka organisationen i en positiv riktning. Om ledningen inte uppmärksammar cyberhot riskerar medarbetarna att ta efter samma beteende. Ett positivt ledarskap inom cybersäkerhet kan främja en medvetenhet om cybersäkerhet i organisationen. Corradini (2020) och Allport (1954) förklarar även att människans beteende påverkas av andra människors närvaro och inställning. Detta kan skapa sociala normer och en press att följa dessa vilket kan påverka beteende och agerande hos medarbetare. Vidare visar Asch konformitetsexperiment att människor tenderar att anpassa sig efter gruppens förväntningar och normer trots att det strider mot sin egen uppfattning (Asch, 1955). Milgrams lydnadsexperiment visar att människor kan utföra handlingar som strider mot deras egen moral eller åsikter om de påverkas av högre auktoritet (Milgram, 1963).

I R2:s fall sker kommunikationen om cybersäkerhet och arbetet med cybersäkerhet i ett proaktivt syfte, vilket blir tydligt när R2 diskuterar hur organisationen arbetar med IT-säkerhet. Att hålla sig uppdaterad "är en del av arbetet" vidare förklarade respondenten att cybersäkerhet kommuniceras genom deras slack-kanaler. Samt nämner respondenten att "när vi bygger något från grunden, så är det säkerhet som vi tänker på.". Detta proaktiva arbetssätt genomsyrar organisationskulturen, kollegornas samarbete och kommunikationen hos IT-företaget. Denna organisationskultur stöds av litteraturen där medarbetarna påverkas i en positiv riktning om det finns ett positivt ledarskap och att medarbetarna påverkas av varandra (Corradini, 2020). Vidare stödjer R2s organisationskultur Asch (1995) som syftar till att människors beteende påverkas av andra människors inställning.

Vidare skiljer sig kommunikationen om cybersäkerhet hos IT-företaget från t.ex. energiföretaget:

R1 förklarade att efter att hot upptäckts diskuteras detta bland kollegor. R1 poängterade att det finns en skillnad i cybersäkerhetspolicyn och hur organisationen agerar. Policyn handlar om att *"förstå hur man kan jobba med det själv, i ett förebyggande syfte. Vilket skiljer sig från idag då organisationen har ett retroaktivt förhållningssätt*". Vidare i frågan om respondenten kommunicerar med sina kollegor om de upptäcker hot, svarade R1 att när respondenten fått phishing mail upplevde respondenten det som ganska allvarligt, "*men jag upplever inte att det finns lika stor förståelse för det internt eller hos vår IT-avdelning".* R1 förklarade även att en brist i organisationen är att: "*jag saknar riktlinjer gällande vad man inte får göra*. *T.ex. att man inte kollar sin mail på sin jobbdator. Det hade jag inte gjort personligen, men jag vet att det förekommer.*" Vidare önskade R1 att organisationen skulle*"skapa interna kanaler för att kommunicera och uppmärksamma avvikelser som kan leda till större hot"*. Att R1 upplevde att IT-avdelningen inte hade förståelse för phishingmail, kan bero på att ledningen inte har en proaktiv eller kontinuerlig diskussion gällande organisationens cybersäkerhetsarbete. Det kan därmed skapa en social norm, att inte fokusera på att förbättra cybersäkerheten på energiföretaget. Medarbetarna i R1s organisation arbetade inte särskilt IT-säkert, trots att detta möjligtvis skulle kunna vara något de vill prioritera. Om detta är fallet, stöds situationen av Milgrams lydnadsexperiment, som syftar till att människor kan utför handlingar som bryter mot deras inre moral om de influeras av en högre auktoritet (Milgram, 1963). Situationen kan även stödjas i litteraturen där medarbetare vill delta i utformandet av cybersäkerhetspolicyer, då detta ligger i medarbetarnas intresse (Pham et al., 2017).

Vidare komunicerades cybersäkerhet inom mödravården företaget på följande sätt:

R4 förklarade att respondenten saknar kunskap och förmåga att hantera cyberhot eller attack. Vidare i frågan, “har dina anställda denna kunskap?" svarade respondenten: “*Nej verkligen inte. Det är ju mitt uppdrag, och har jag själv ingen kunskap, så det har inte mina anställda heller.”* R4 beskrev alltså att den egna förmågan tas efter av de andra anställda. Detta stödjer Milgrams experiment som menar medarbetarnas handlingar kan påverkas av en högre auktoritet (Milgram, 1963). Det kan därmed diskuteras om ett ledarskap där ledningen har mer kunskap och uppmuntrar till ett mer IT-säkert arbete, kommer att ha en effekt av mer IT-säkert arbete bland medarbetarna?

5.3.2 Tekniska ramverk

Zero Trust

Gällande de tekniska ramverken användes delar av Zero Trust hos flera av sektorerna. Zero Trust kan beskrivas enligt Madsen (2024) med talesättet "Tillit är bra, men kontroll är bättre". Med Zero Trust ges åtkomst efter noggrann verifiering, och all kommunikation måste vara krypterad (Madsen, 2024). Vidare finns konceptet Just-in-time access (JITA) och Just-enough access (JEA), där JITA ger åtkomst i realtid och vid behov, medan JEA ger rättigheter som är nödvändiga för att genomföra en uppgift (Shore et al. 2021).

Zero Trust hade flera av respondenterna inte hört talas om. För R4 förklarades innebörden av Zero Trust och därefter höll R4 med om att delar av Zero Trust användes i organisationen. Detta gick även att avläsa när R4 poängterade “*identifiering via bankid eller 1177*”. Vidare tolkar vi det som att R1 använde Zero Trust genom förklaringen “*att autentisering flera gånger per dag via Microsoft*”, då Microsoft använder just Zero Trust i stora delar av sin lösning. Just autentisering kan förklaras genom koncepten JITA och JEA, se figur 2.1. Även R3 tolkar vi använde Zero Trust, “*Allting som går via Office 365 är deras säkerhets authenticator osv*”. Däremot verkar det som att Zero Trust i form av autentisering är så pass välanvänt idag att det inte ses som ett tekniskt ramverk eller en strategi att implementera. Flertalet organisationer som använder Microsoft använder indirekt delar Zero Trust.

NIST CSF

Gällande NIST CSF uttryckte ingen av respondenterna att det tekniska ramverk användes. Däremot fanns delar av respondenternas svar som hade principer likt NIST CSF. Exempelvis NIST CSF Core. CFS Core beskriver de önskade resultaten av riskhantering av cyberhot, som ska förstås av medarbetare oberoende cybersäkerhetskunskaper. Core består av 5 funktioner: granskning, identifiering, skydda, svara och återhämtning från potentiella cyberattacker. Vidare innefattar CORE riskhantering, genom strategier, översikt av tillgångar såsom mjukvaror, hårdvara, tjänster, analyser av avvikelser för möjliga intrång och rapportering (National Institute Security Technologies, 2024).

Riskhantering gjordes på ett eller annat sätt av samtliga respondenter. Vidare hade respondenterna olika roller och varierande kunskap om cybersäkerhet. R1 rapporterade phishing-mail som ärenden till IT-avdelningen. Denna rapportering är ett svar eller en återhämtning av en cyberattack. R2 utförde hotmodellering och riskanalys av angreppsytor när konsulten utvecklade system. R2s handling är en del av att granska, identifiera och skydda mot cyberhot. R3 identifierade behörighet av information genom månadsrapporter över vem

som hade tillgång till servar, ytor och verktyg. Detta skapar översikt över tillgångar och hårdvaror för att upptäcka möjliga intrång. R4 förklarade att de regelbundet byter lösenord, de hade även en funktion som rensade mail och att de undvek att arbeta i mail. R4:as hantering är en del av skyddande och granskning av potentiella cyberattacker. R5 och advokatfirman tog inte emot pdfer i mail och istället tog de emot dokument i pappersformat. Detta är en del av en skyddande funktion i deras skydd mot cyberhot. Genom dessa handlingar utförde samtliga respondenter en del av NIST CSF CORE.

Vidare finns CFS organizational profiles och CFS tiers. CFS organizational profiles används som en utvärdering av organisationens säkerhetsläge, samt hur det önskade säkerhetsläget skulle se ut. CFS tiers innebär en identifiering för efterlevnad av cybersäkerhetshantering och cybersäkerhetsgranskning. CFS tiers bedöms med ett betyg i ett spann av 4 nivåer (National Institute Security Technologies, 2024).

Eftersom ingen av organisationerna använde sig av NIST CFS, användes inte organizational profiles eller tiers i sin helhet. De flesta av respondenterna profilerade inte sina organisationers säkerhetsläge eller betygsatte organisationens cybersäkerhetsgranskning eller cybersäkerhetshantering. Däremot fanns koncept i organizational profiles och tiers som liknade hur respondenterna beskrev sina organisationer. R5 förklarade "*Vi är en väldigt liten organisation, som kanske inte gör så mycket för att hantera cybersäkerheten*", vilket talar för att respondenten gör en utvärdering av organisationens säkerhetsläge och en indikation på hur cybersäkerhet efterlevs. R5 förklarade även *"Jag tror att för en sådan här liten organisation är det svårt att hantera det på ett annat sätt"*, vilket förklarar att organisationen inte har ett större mål för cybersäkerhetsarbetet. Dock är betygssättning inget som görs i R5s organisation, då ramverket inte används.

NIST och Zero Trust anpassning till Svenska SME

Vidare var hoten som organisationerna upplevde i dagsläget phishing mail (SET), eller bluffakturor. Hantering av dessa hot kan hanteras genom t.ex. NIST Core, "granska, identifiera, skydda" (National Institute Security Technologies, 2024). Vidare kan Zero Trust sjunde princip användas för att hantera hot: "företaget samlar så mycket information som möjligt om det aktuella tillståndet av tillgångar, nätverksinfrastruktur och kommunikationer och använder det för att förbättra sin säkerhetsställning" Rose et al. (2020). Trots att bluffakturor och phishingmail var hoten i dagsläget, kände flera av respondenterna rädsla inför framtida hot. R1 förklarade att respondenten kände rädsla för att inte lyckas identifiera phishing mail, medan R3 påpekade att hoten blir fler. Vidare uppgav R4 en rädsla för att bli attackerad som Vellinge kommun blev, dvs en rädsla för ransomware attacker. R2 blev nyligen utbildad inom attacker som hardware attacker och supply chain attacker i en intern konferens. Av denna anledning kan de tekniska ramverken vara fördelaktiga, då de kan stödja företag att hantera hot, samt användas inom samtliga sektorer/storlekar på företag. De tekniska ramverk bidrar till en djup analys av organisationers cybersäkerhetsarbete.

Vad som talar emot att använda dessa ramverk i sin helhet är t.ex. att NIST CSF är resurskrävande, komplext (vilket gör det svårt att förstå för medarbetare), saknar specifika rekommendationer och betygskriterier (Benz & Chatterjee, 2020). Zero Trust kan vara ineffektivt att implementera och medarbetarna kan upplevas vara ett hinder p.g.a brist på teknisk kompetens (Nordgren et al. 2023), (Shore et al. 2021) & (Teerakanok et al. 2021). Dessa faktorer kan påverka SME både långsiktigt och kortsiktigt.

Konsekvenser av NIST

Den långsiktiga konsekvens av NIST CSF är dess kostnad. Det kan därmed diskuteras om SMEer kan uppfylla Return On Investment eller Break Even, efter att ha implementerat ramverket i verksamheten. Vidare hade tre av organisationerna en outsourcad IT-avdelning, därmed skulle möjligtvis dessa behöva använda sig av ytterligare outsourcing för att implementera NIST, vilket ökar kostnaden för omställningen. R5 hade inte en IT-avdelning eller en IT-policy, vilket innebär att organisationen skulle behöva ytterligare resurser för att implementera NIST. En kortsiktig konsekvens av NIST CSF är att ramverket är komplext och kan vara svårt att förstå, där medarbetarna ska lära sig ett nytt vokabulär. Därmed kan det utvecklas en motstånd att ta sig an ett nytt ramverk bland medarbetarna. Missnöje upplevdes redan bland annat av R1, som förklarade att IT-policy inte efterlevdes och att medarbetarna inte hade inflytande över beslutsfattning om cybersäkerhetspolicy. En implementering av ett nytt ramverk kräver att medarbetarna har en inverkan och en vilja att förstå policyer, vilket i sin tur kan vara tidskrävande och resurskrävande från verksamhetens dagliga arbete.

Konsekvenser av Zero Trust

Den långsiktiga konsekvensen av Zero Trust är även dess kostnad att implementera. En annan konsekvens är om medarbetarna på organisationen har brist på teknisk kompetens, är det ett påvisat hinder vid Zero Trust (Nordgren et al. 2023). Brist på teknisk kompetens förklarade flera av respondenterna att deras organisationer hade, dels R5s organisation och dels R4s organisation. Om medarbetarna inte har teknisk kompetens skulle implementering och användning av ramverket ta lång tid att införa i den dagliga verksamheten. Den kortsiktiga effekten av Zero Trust blir dess ineffektivitet att implementera framförallt gällande policy och behörighetsreglering (Shore et al., 2021). Zero Trust kan kräva att en hel arkitektur ska byggas om (Nordgren et al. 2023) I sin tur kan en arkitektonisk omstrukturering generera fler hinder för det företag som implementerar ramverket. Vidare kan ineffektiviteten resultera i användaravbrott, vilket påverkar verksamhetens dagliga arbete (Shore et al., 2021).

Andra ramverk som används bland organisationerna är: NIS som används av R1s organisation, samt ISO 27001 som användes av R2s organisation.

Kontinuerlig utbildning

Då tre av fem respondenter svarade att de inte hade kunskap för att hantera ett cyberhot eller en attack, kan det argumenteras för att det finns ett behov av mer kontinuerlig utbildning. Däremot kan det också vara en fråga om resurser. Som tidigare nämnts arbetar respondenterna som upplevde att de hade kunskap på större bolag än de andra. R5 som arbetade på ett mindre företag uttrycker att de största utmaningarna är brist på kompetens och resurser.

R2 nämnde att de inte har några regelrätta utbildningar, men att de hade ett mer kontinuerligt arbete där de håller sig uppdaterade samt, har en diskussion i deras slack-kanaler. Respondenten berättade också att säkerhetschefen och CISO har varit nere på deras kontor och gått igenom riktlinjer och regler, samt att de har interna konferenser där de lyfter viktiga punkter. Detta kontinuerliga arbetssätt kan bero på att bolaget är större. Detsamma gäller R3 som också arbetar på ett större bolag. De hade därmed även en IT-chef, en IT-avdelning och micro-utbildningar med jämna mellanrum. R3 nämnde även att de hade behörighetshantering där de får en månadsrapport från IT-avdelningen, som visar vem som har access till vissa servrar, ytor och verktyg osv. Detta sågs över minst en gång i månaden.

Detta kan kopplas till Kanki och Hobbes (2023) som menar att för lite resurser och brist på kunskap är två bidragande faktorer till att mänskliga misstag kan ske.

5.3.3 Centralisering och Decentralisering

Gällande att låta medarbetarna vara med och påverka företagets cybersäkerhetspolicyer skiljde sig svaren åt. De flesta respondenter svarade att det inte lämnas utrymme för medarbetare input, förutom R2 och R5 som får delta i ändringar av policyer. Som tidigare nämnts i Bakos och Dumitrașcu (2021), bör riskhantering ske genom ett decentraliserat arbetssätt, anpassningsbara metoder och samarbetet mellan olika nivåer. Pham (2017) poängterar att en klyfta mellan IT-experter eller chefers åsikter och medarbetarnas åsikter kan uppstå gällande cybersäkerhet. Medarbetare vill delta i utformandet av cybersäkerhetspolicyer, då medarbetarna har ett intresse och ett nöje inom IT-säkerhet. Chefer vill istället att medarbetarna passivt ska följa policyer. Marquet (2013) poängterar att när medarbetare är följeslagare utan kontroll resulterar det i låg moral och att stora misstag görs.

Teorierna bekräftas av R1 som förklarade scenariot på sin arbetsplats och hur det resulterade i att cybersäkerhetspolicyn inte följs. Vidare förklarade respondenten att medarbetarna inte hade inflytande över cybersäkerhetsbeslut. R1 uttryckte brister i cybersäkerhetsarbetet och hade själv egna förslag på hur man kunde hantera cybersäkerheten, såsom att skapa interna kanaler för att kommunicera och uppmärksamma avvikelser som kan leda till hot. Vidare uttryckte R1 att de cybersäkerhetspolicyer som organisationen har förklarade hur man kan jobba med cybersäkerhet i ett förebyggande syfte. Dessa policyer följdes inte av organisationen, istället hade organisationen ett retroaktivt förhållningssätt till cybersäkerhetsarbetet. Bakos och Dumitrașcu (2021), uttrycker att det finns brister med ett centraliserat arbetssätt i riskhantering. Att stärka samarbetet mellan olika nivåer gällande beslutsfattaning skulle vara fördelaktigt och det skulle skapa en mer flexibel riskhanteringsstrategi (Bakos & Dumitrașcu, 2021).

Till skillnad från R1 hade R2 möjlighet att göra anmärkningar på företagets cybersäkerhetspolicy. R2 berättade att policyer är enkla att följa, är lättillgängliga och om det finns frågor uppmuntras man att ställa dessa. Vidare förklarade R2 att det är en del av arbetet att hålla sig uppdaterad om cybersäkerhet. Därmed visar detta att när medarbetare får delta i beslutsfattning bidrar det till att policyn efterföljs.

Därmed kan en centraliserad beslutsfattning inom cyberäskerhetpolicy få negativa konsekvenser i en organisation genom att policyer inte efterlevs. En decentraliserad beslutsfattning inom cybersäkerhet kan leda till en större efterlevand av cybersäkerhetspolicyn.

6 Slutsats

Huvudsyftet med uppsatsen har varit att svara på forskningsfrågorna:

1. *Hur kan cybersäkerhetsbeteenden främjas hos medarbetare inom olika sektorer som inte har IT-säkerhetsrelaterade roller?*
2. *Hur ser svenska SMEs förmågor ut att arbeta med erkända tekniska ramverk?*

Undersökningen visade att cyberhot uppfattas som allvarligt, men att det finns en variation i respondenternas medvetenhet och uppmärksamhet av cybersäkerhet i det dagliga arbetet. Okunskap och bristande självförtroende i hantering av cyberhot är faktorer som majoriteten av respondenterna upplevde och dessa faktorer kan ses som ett hinder för att vidta åtgärder. När kunskapen inte fanns tog medarbetarna hjälp av deras IT-avdelning, IT-ansvarig eller närmsta chef, medan när kunskapen fanns använde sig medarbetare av olika verktyg för att rapportera hot.

Vidare upplevde samtliga respondenter möjligheter att utvecklas i arbetet och respondenterna beskrev att de trivdes på sina arbetsplatser. Studien visade även att beröm för prestationer prioriterades. Möjligheter till utveckling, uppskattning och eget ansvar kan öka motivationen och därmed förbättra engagemanget i cybersäkerhetsarbetet. Goda interpersonella relationer, som trivsel och bra relationer med kollegor, var också viktiga faktorer för arbetsprestationer. Respondenterna upplevde sina arbetssituationer som hållbara, däremot hade vissa begått misstag på grund av stress. En respondent hade känt sig splittrad i arbetet på grund av att denne hade för många arbetsuppgifter igång samtidigt, vilket kan påverka förmågan att arbeta säkert.

Därefter visade undersökningen att det fanns en varierande kommunikation kring cybersäkerhet inom de olika sektorerna. Verksamheter med en proaktiv ledning som arbetade för att öka medvetenheten om cybersäkerhet, tenderade också att ha en integrerad säkerhetskultur. Ledningens kunskap inom cybersäkerhet kunde korrelera med medarbetarnas kunskapsnivå. Respondenter med större ansvarsområden som VD och delägare, visade en större oro för cyberattacker, vilket kan främja ett kritiskt tänkande inom organisationen. Dessutom verkade respondenterna vara medvetna om verksamheternas brister såsom kunskapsbrist hos personalen, att det saknades riktlinjer och en krishanteringsplan. Detta kan tala för en slags konformitet inom organisationskulturen eller att auktoriteten hade en inverkan.

Vidare visade studien att få av organisationerna hade formella utbildningar, men att majoriteten hade en fastställd säkerhetspolicy. Faktorer som sektor och storlek på organisationerna kan påverka cybersäkerhetarbetet, varav graden av digitalisering och resurser också har en inverkan. Företag som undvek att arbeta digitalt, indikerade att det manuella arbetet var en strategi för att undvika cyberhot. Brist på resurser och kunskap kan vara en bidragande faktor till mänskliga misstag. Respondenterna kände inte till erkända tekniska ramverk som Zero Trust och NIST, men använder delar av ramverken trots att dessa inte var uttalade strategier inom organisationerna. Att implementera dessa ramverk i sin helhet kan vara resurskrävande och komplext, särskilt med hänsyn till behovet av teknisk kompetens och utbildning för medarbetarna. Ramverket bör därmed skräddarsys efter svenska SME behov och resurser.

Det fanns även ett samarbete på samtliga företag, vilket talar för en viss decentraliserad kultur där medarbetare inkluderades i problemlösning. Däremot framkom det att medarbetare inte får vara med och påverka företagets säkerhetspolicy, vilket kan skapa klyftor mellan ledningen och medarbetarna, vilket i sin tur kan påverka förhållningssättet gentemot cybersäkerheten. Empirin stärkte teorin om att medarbetare som får delta i beslutsfattning bidrar till att cybersäkerhetspolicyer efterföljs mer noggrant.

Avslutningsvis, med tanke på att SME har begränsade resurser jämfört med större bolag, är det av hög relevans att arbeta mer med motivation, socialpsykologiska och mänskliga faktorer för att främja cybersäkerheten. Idag fattas beslut uppifrån och ner, vilket kan skapa ett motstånd bland medarbetarna, om de inte förstår varför strategier och policyer implementeras. Det bör därmed läggas stor vikt i att SME inkluderar sina medarbetare i cybersäkerhetsarbetet, att det finns en ledning med IT-kompetens och att man ser till att mänskliga behov såsom återhämtning och trivsel tillgodoses. Detta bör göras då mänskliga fel uppkommer på grund av följande faktorer: hög arbetsbelastning, distraktion, okunskap eller bristande medvetenhet, samt organisatoriska problem. Dessa faktorer anses vara de främsta anledningarna till varför cyberattacker sker (Corradini, 2020). Organisationer behöver bli mer medvetna om hur möjlighet till utveckling, självständighet och beröm påverkar medarbetarnas motivation. Vid behov behöver organisationerna även utveckla kompetensstrategier som ökar medarbetarnas kunskap och självförtroende. Slustasen blir att SME:er som tar hänsyn till organisationskultur, IT-kompetens och mänskliga faktorer samt inkluderar medarbetare i sin cybersäkerhetsstrategi kan utveckla en mer hållbar cybersäkerhetspraxis.

6.1 Förslag till vidare forskning

Då det sker allt fler cyberattacker mot verksamheter är det viktigt att fortsätta forska inom området. Det sker kontinuerligt supply chain attacker, dataintrång, ransomware attacker och phishing attacker. Medarbetare som inte arbetar med IT-säkerhet kan av misstag orsaka att en angripare kommer åt verksamhetens data. Vidare kan organisationer brista i sitt arbete genom att inte hantera/lagra data på ett säkert sätt. Därmed är ett förslag till vidare forskning att genomföra fler fallstudier som testar de erkända ramverkens applicerbarhet på SME, eller upprepa denna undersökning och inkludera fler företag eller fler respondenter per företag för att ge ett säkrare resultat. Ett annat förslag på vidare forskning är att undersöka vilka verksamheter som är mest sårbara i dagens cybersäkerhetsläge och på så sätt kartlägga i vilka sektorer cybersäkerhetsarbete ska prioriteras. Med denna bakgrund kan man vidare undersöka hur medarbetare bäst bör arbeta på ett cyber-säkert sätt, antingen om det är att utbilda sig mer tekniskt, eller om företagen behöver jobba mer aktivt med att hantera cyberhot genom exempelvis olika strategier. Vidare, när det gäller medarbetarnas arbete kan ett förslag på framtida forskning vara att genomföra socialpsykologiska experiment relaterade till cybersäkerhet. Det kan även vara viktigt att utföra experiment hur cybersäkerhet skulle påverkas av genom en decentraliserad beslutsfattning av cybersäkerhetspolicyer. Med andra ord finns det flera aspekter att undersöka i området och det är även viktigt att undersöka samtliga aspekter, då cybersäkerhet är ett komplext arbete som innefattar människor, teknik, strategier, ledarskap och dess samspel.

7 Bilagor

Bilaga 1 Användning Av AI-verktyg (max 400 ord)

1. Verktyg:
    - Chat GPT
2. Grad av användning

   Chat GPT version 3.5 och 4 har använts för att få idéer gällande ramverk som används inom cybersäkerhet hos företag. Svar som gavs av Chat GPT innefattade NIST CFS och Zero Trust. Vidare blev dessa svar stärkta genom LUB-Search, Google Scholar och annan litteratur, som vi använde för djupare och analyserande information. Chat GPT användes även för att få idéer om motivationsfaktorer. Även svar som gavs av ChatGPT såsom PMT, Herzberg tvåfaktorsteori, GDMS blev stärkt av LUB-Search, Google Scholar och annan litteratur. Chat GPT har även använts för grammatik, synonymer, referering av Harvard referencing 3 och stavningskontroll. ChatGPT har använts i en liten utsträckning till att hitta kopplingar mellan litteraturgenomgång och det empiriska resultatet. Utöver detta, har inte Chat GPT använts.

   Chat GPT har använts i följande kapitel:

   - Litteraturgenomgång
   - Källförteckning och referering
   - Diskussion

Bilaga 2 Information & Samtyckesblankett

Studien kommer att följa Vetenskapsrådets 4 krav för forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.

Information

Enligt samtyckeskravet gäller följande för studien: "*De som medverkar i en undersökning skall ha rätt att självständigt bestämma om, hur länge och på vilka villkor de skall delta. Om en deltagare vill avbryta sin medverkan t.ex. mitt i en intervju står det honom/henne fritt att göra detta. De skall kunna avbryta sin medverkan utan att detta medför negativa följder för dem. I sitt beslut att delta eller avbryta sin medverkan får inte undersökningsdeltagarna utsättas för otillbörlig påtryckning eller påverkan*"

Deltagaren har rätt att vara anonym och även organisationen som denne tillhör. Däremot kommer organisationen att beskrivas genom sektor och antalet anställda för att uppnå kravet som SME. Intervjun kommer att spelas in för att förenkla sammanställning av data.

Enligt nyttjandekravet kommer deltagarnas svar och uppgifter endast användas i forskningsändamål för denna studie. "*Uppgifter om enskilda, insamlade för forskningsändamål, får inte användas eller utlämnas för kommersiellt bruk eller andra icke-vetenskapliga syften*".

"Vidare enligt konfidentialitetskravet kommer: "*Alla uppgifter om identifierbara personer antecknas, lagras och avrapporteras på ett sådant sätt att enskilda människor ej kan identifieras av utomstående. Detta innebär att det skall vara praktiskt omöjligt för utomstående att komma åt uppgifterna".*

Samtycke till deltagande i studien om Cybersäkerhet vid institutionen för Informatik, Lunds Universitet

Jag bekräftar härmed att jag har tagit del av skriftlig och muntlig information om studien och accepterar att delta. Jag har fått möjlighet att ställa frågor om studien.
Jag har fått information om att de uppgifter som samlas in om mig kommer att behandlas konfidentiellt, på ett sådant sätt att min identitet inte kommer att avslöjas för obehöriga.
Jag är medveten om att min medverkan är helt frivillig och att jag när som helst och utan närmare förklaring kan avbryta mitt deltagande.

Ort och
datum_____
Förnamn och
efternamn_____
Adress_____
Telefonnummer_____
Underskrift_____

Tystnadsplikt

Härmed undertecknar vi en förbindelse om tystnadsplikt gällande all information som deltagaren framför under intervjun.

Underskrifter_____

Kontaktuppgifter till skribenterna och kursansvarig lärare

Maja Vigh
e-post: Maja.hvk@gmail.com
tel: +46 72 588 5330

Hanna Laremark
e-post: Hanna.laremark@gmail.com
tel: +46 70 173 5667

Osama Mansour (Ansvarig lärare för examensarbetet)
e-post: osama.mansour@ics.lu.se

Bilaga 3 Intervjuguide

1. Berätta om din roll i företaget och vilka arbetsuppgifter du har?

2. Hur mycket inflytande känner du att du har över ditt arbete i nuläget? Hade du velat ha mer eller mindre?

3. Känner du att du har möjlighet att utvecklas inom ditt arbete och att du får beröm för dina prestationer? Alt. (Hur ser utvecklingsmöjligheterna ut i ditt arbete och hur ser uppmuntran till prestationer ut?)

4. Hur upplever du din arbetsbörda och din arbetsmiljö?

5. Är företagets cybersäkerhetspolicy något som du behöver ha i beaktande för att genomföra ditt arbete, på vilket sätt?

6. Förstår du vad verksamhetens cybersäkerhetpolicier innebär?

7. Om du misstänker att du blir utsatt för en cyberattack på arbetet, hur hade du gått tillväga för att hantera detta? Tror du på din egen förmåga att hantera ett hot?

8. Hur hanteras cybersäkerhet inom verksamheten? Dvs har ni outsourcat denna uppgift eller hanteras den internt?

9. Hur kommuniceras cybersäkerhetspolicyer inom din organisation?

10. Berätta om en gång när du arbetade tillsammans med dina kollegor för att lösa ett problem. Hur kom ni fram till en lösning?

11. Vilka åtgärder vidtar ledningen när en attack sker?

12. Har ni regelbundna utbildningar inom cybersäkerhet och hur ser dessa ut?

13. Känner du att du har kunskap eller verktyg för att hantera ett cyberhot, på vilket sätt då?

14. Har ni några nuvarande strategier eller ramverk i hantering av cybersäkerhet? T.ex. NIST, Zero Trust eller ISO dylikt?

15. Hur fattas beslut kring cybersäkerhetsstrategier i din organisation? Upplever du att det finns utrymme för medarbetarinput?

16. Vilka upplever du är de största utmaningarna ni möter i er cybersäkerhetsstrategi idag?

8 Källförteckning

Allabolag. (n.d.). https://www.allabolag.se/ [Accessed 6 April 2024]

Allport, G, W. (1954). The Nature Of Prejudice, New York, United states: Addison-Wesley publishing company

Alvehus, J. (2019). Skriva uppsats med kvalitativ metod : en handbok, Stockholm : Liber

Asch, S, E. (1955). Opinions and social pressure. *Scientific American*, vol. 193, pp.31-35, https://www.jstor.org/stable/24943779

Bakos, L., & Dumitrașcu, D, D. (2021). Decentralized Enterprise Risk Management Issues under Rapidly Changing Environments. MPDI, *Risks* vol. 9,: 165, Advances in Sustainable Risk Management, https://doi.org/10.3390/risks9090165

Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a better understanding of SMB CEOs' Information Security Behavior:Insights from Threat or Coping appraisal. *Journal of Intelligence Studies in Business*, Vol 5, No 1 (2015) p5-17, 13p. https://doi.org/10.37380/jisib.v5i1.109

Beautement, A., Sasse, M. A., & Wonham, M. (2009).The compliance budget: managing security behavior in organisations. *In Proceedings of the 2008 New Security Paradigms Workshop*, pp. 47–58, https://doi.org/10.1145/1595676.1595684

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, vol. 63, no. 4, pp. 531-540, https://doi.org/10.1016/j.bushor.2020.03.010

Boss, S. R., Galletta, D., Lowry, P. B., & Moody, G. D. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly*, vol. 39, issue. 4, pp. 837-864, https://www.researchgate.net/publication/304459467_What_do_systems_users_have_to_fear_Using_fear_appeals_to_engender_threats_and_fear_that_motivate_protective_behaviors_in_users

Buck, C., Olenberger, C., Schweizer, A., Völter, F. & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers and Security* vol. 110, https://doi.org/10.1016/j.cose.2021.102436

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, vol. 107, pp.438-458, https://doi.org/10.1108/02635570710734316

Commission Recommendation (2003) 1422. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. The Commission of the European Communities. https://eur-lex.europa.eu/eli/reco/2003/361/oj

Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology, [e-book] Springer International Pub, https://eds.p.ebscohost.com/eds/search/basic?vid=0&sid=2ded87d3-cfcf-4885-a5bd-b6ced90e5aeb%40redis

European Parliament. (2022). Cybersecurity: main and emerging threats, European Parliament, 27 January 2022, https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats [Accessed 25 February 2024]

Fernandez, E. & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, vol. 89, https://doi.org/10.1016/j.csi.2024.103832

Herzberg, F. (2003). One More Time: How Do You Motivate Employees?. *Harvard Business Review*, January https://hbr.org/2003/01/one-more-time-how-do-you-motivate-employees [Accessed 8 maj 2024]

Jacobsen, D, I. (2002). Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen, Lund: Studentlitteratur

Kanki, G, B. & Hobbes, N, A. (2023). Chapter 18 - Maintenance human factors and flight safety. *Human Factors in Aviation and Aerospace* 2023, 3 edn, pp. 477-515, https://doi.org/10.1016/B978-0-12-420139-2.00019-8

Lella, I., Tsekmezoglou, E., R, Svetozarov, Naydenov., C, Ciobanu,. A, Malatras,. M, Theocharidou, & European Union Agency for Cybersecurity (2022). ENISA threat landscape 2022 [pdf] https://data.europa.eu/doi/10.2824/782573

Madsen, T. (2024). Zero-Trust - an Introduction, [e-book] River Publishers, Taylor & Francis Group https://eds.p.ebscohost.com/eds/detail/detail?vid=2&sid=7b3d6a5e-161d-4aac-a99b-b0179c3c0480%40redis&bdata=JkF1dGhUeXBlPWlwLHVpZCZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d#AN=atoz.ebs103087286e&db=cat02271a

Marquet, L, D. (2013). Turn the ship around! A true story of turning followers into leaders, [e-book] New York: Google Scholar, chap. 6,7, 9, 13, 14, http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/4603/Turn%20the%20Ship%20Around!%20-%20A%20True%20Story%20of%20Turning%20Followers%20into%20Leaders.pdf?sequence=1

Milgram, S. (1963). Behavioral study of obedience. *The Journal of Abnormal and Social Psychology*, vol. 67, pp.371–378, https://doi.org/10.1037/h0040525

Mutabazi, P., Ndashimye, E., & Ndibwile, J, D. (2023). Investigating the Challenges Companies in Rwanda Face when Implementing Zero-Trust Network, paper 10, 10.1109/FiCloud58648.2023.00062 [Accessed 6 Maj 2024]

Myndigheten för samhällsskydd och beredskap. (2023). När kriget kom nära: Årsrapport it-incidentrapportering 2022, https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/ [Accessed 19 March 2024]

National Institute Security Technologies. (2024). "The NIST Cybersecurity Framework (CSF) 2.0". https://doi.org/10.6028/NIST.CSWP.29 [Accessed 20 March]

National Institute Security Technologies. (n.d.). Computer Security Resource Center, https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#M [Accessed 24 March 2024]

Nordgren, A., Michel, J. & Boqvist, D. (2023). IT-världens Paradise Hotel – lita inte på någon!: En kvalitativ studie om Zero Trust inom svenska företag och myndigheter, BSc thesis, Department of IT Forensics and Information Security, Halmstad University, pp. 27-32, https://www.diva-portal.org/smash/get/diva2:1776138/FULLTEXT02.pdf [Accessed 20 March 2024]

Norton, R, J. & Fox, R, E. (1997). Organizational structure: Removing the barriers. in, The change equation: Capitalizing on diversity for effective organizational change, Washington DC : *American Psychological Association*, pp 183-241, https://doi.org/10.1037/10224-006

Osborn, E. & Simpson, A. (2018). Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study. *The Computer Journal*, vol 61, no 4, pp 472–495, https://doi.org/10.1093/comjnl/bxx093

Pham, C, H., Pham, D, D., Brennan, L., & Richardson, J., (2017), Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, vol 21, https://doi.org/10.3127/ajis.v21i0.1321

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, vol. 91, issue. 1, pp. 93-114, https://doi.org/10.1080/00223980.1975.9915803

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). NIST Special Publication 800-207: Zero Trust Architecture. U.S. Department of Commerce, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-207 [Accessed 22 March 2024]

Sakib, S., Raiaan, M., Fahad, N., Mukta, S., Mamun, A. & Chowdhury, S. (2023). A Review of the Evaluation of Ransomware: Human Error or Technical Failure? Educational and Psychological Measurement (ICICT4SD), https://ieeexplore-ieee-org.ludwig.lub.lu.se/stamp/stamp.jsp?tp=&arnumber=10303580&tag=1 [Accessed 3 May 2024]

Sarkar, S., Choudhary, G., Shishir, S., Hussain, A. & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: *Sustainability* 2022, vol 14, 11213. https://doi.org/10.3390/su141811213

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement*, vol. 55, issues. 55, https://doi.org/10.1177/0013164495055005017

Shore, M., Zeadally, S. & Keshayira, A. (2021). Zero Trust: The What, How, Why, and When. *Computer*, vol. 54, issue. 11, pp.26-35, https://ieeexplore.ieee.org/document/9585170

Statistiska central byrån. (2019). "Digitalisering och säkerhet i svenska företag" 20 November. https://www.scb.se/hitta-statistik/statistik-efter-amne/naringsverksamhet/naringslivets-struktur/it-anvandning-i-foretag/pong/statistiknyhet/it-anvandning-i-foretag-2019/ [Accessed 19 March 2024]

Svt. (2021)."It-attacken mot Coop – detta har hänt" 5 June, https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant [Accessed 19 March 2024]

Svt. (2024). "120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade", 22 January https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda [Accessed 19 March 2024]

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. *Security and Communication Networks*, vol. 2021, Article ID 9947347, pp. 1-10 https://doi.org/10.1155/2021/9947347

The White House. (2014). Launch of the Cybersecurity Framework, https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/launch-cybersecurity-framework [Accessed 24 March 2024]

Vetenskapsrådet. (2002). Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning, Sverige : Elanders Gotab

Wengraf, T. (2001). Qualitative Research Interviewing, [e-book] SAGE Publications, https://doi.org/10.4135/9781849209717

Young, H., van Vliet, T., van de Ven, J., Jol, S., & Broekman, C. (2017). Understanding Human Factors in Cyber Security as a Dynamic System. *In Proceedings of the AHFE 2017 International Conference on Applied Human Factors and Ergonomics, Advances in Intelligent Systems and Computing* (vol. 593, pp. 244-254). Springer. https://doi.org/10.1007/978-3-319-60585-2_23