Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
Institutt for industriell økonomi og teknologiledelse

Fredrik Kirkebirkeland Kristiansen og Per Håvard Kolle Hustvedt

Cyber Awareness i Små- og Mellomstore Bedrifter

Masteroppgave i Industriell innovasjon og digital sikkerhet
Veileder: Halvor Holtskog
Medveileder: Christina Marie Mitcheltree
Juni 2023

NTNU
Kunnskap for en bedre verden

Fredrik Kirkebirkeland Kristiansen og Per Håvard Kolle Hustvedt

Cyber Awareness i Små- og Mellomstore Bedrifter

Masteroppgave i Industriell innovasjon og digital sikkerhet
Veileder: Halvor Holtskog
Medveileder: Christina Marie Mitcheltree
Juni 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
Institutt for industriell økonomi og teknologiledelse

NTNU
Kunnskap for en bedre verden

Sammendrag

Små- og mellomstore bedrifter (SMB) står for en betydelig andel av Europas økonomi og mange virksomheter ser på SMB-er som viktige samarbeidspartnere. Det er fordi flere organisasjoner er avhengig av SMB-ene sine tjenester og produkter, og uten tilgang på kritiske ressurser kan mange bedrifter stoppe opp. Virksomheter er dermed bekymret for SMB-er sin informasjonssikkerhet ettersom et dataangrep mot en SMB kan påvirke forsyningskjeder, partnernettverk og økosystemer. Dette er en realitet flere bedrifter har opplevd, enten gjennom et dataangrep mot dem eller mot samarbeidende bedrifter. Den manglende kunnskapen om informasjonssikkerhet i SMB-er må dermed øke.

Dette forskningsprosjektet retter søkelyset mot bevisstgjøring i SMB-er for å oppnå en dypere forståelse for hvordan de bygger bevisstgjøring (cyber awareness). Forskningsprosjektet gjennomføres som en casestudie i samarbeid med en teknologisk avansert bedrift og deres IT-leverandør. Bevisstgjøring er subjektivt, men kan skape verdifulle resultater for SMB-markedet og bransjeeksperter. Verdien i forskningsprosjektet kan være av høy relevans for bedrifter som ønsker å lære om effekten av sosiale sikkerhetstiltak.

9. januar 2021 ble Østre Toten kommune utsatt for et dataangrep og førte til at flere bedrifter investerte i tjenester og produkter for å forbedre sikkerheten. Den samarbeidende bedriften i forskningsprosjektet var blant dem som investerte i produkter og tjenester for å forbedre virksomheten sin sikkerhet. De leide inn en IT-ekspert for å styrke sikkerheten, men resultatet av investeringen viste seg å bli et ubrukt dokument uten nytteverdi. Kort tid senere ble bedriften utsatt for et dataangrep. Konsekvensene av sikkerhetshendelsen føre til utilgjengelige ressurser, redusert produksjonsevne og økonomisk tap.

En effekt av sikkerhetshendelsen var at de investerte i ytterligere sikkerhetstiltak. Investeringen innebar teknologiske sikkerhetstiltak som tilsvarer grunnleggende sikkerhetshygiene og kan sikre bedrifter mot 98 prosent av alle dataangrep. Åpenbart er et slikt teknologisk sikkerhetstiltak effektivt, men selv med slike løsninger er ikke bedriften gardert mot menneskelige faktorer. Feil som blir begått av mennesker er årsaken til en stor andel av sikkerhetshendelser og dette er noe SMB-er sliter med å takle. Det tyder på manglende forståelse for viktigheten organisatoriske og menneskelige sikkerhetstiltak.

Abstract

Small and medium-sized enterprises (SMEs) account for a significant portion of Europe's economy, and many businesses consider SMEs to be important partners. This is because several organizations rely on the services and products provided by SMEs, and without access to critical resources, many businesses can come to a halt. Consequently, businesses are concerned about the information security of SMEs, as a data breach against an SME can impact supply chains, partner networks, and ecosystems. This is a reality that several companies have experienced, either through a data breach against them or against collaborating companies. The lack of knowledge about information security in SMEs needs to be addressed.

This research project focuses on raising awareness in SMEs to achieve a deeper understanding of how they build cyber awareness. The research project is conducted as a case study in collaboration with a technologically advanced company and their IT provider. Awareness is subjective but can yield valuable results for the SME market and industry experts. The value in the research project may be highly relevant for companies seeking to learn about the impact of social security measures.

On January 9, 2021, Østre Toten municipality was subjected to a data breach, leading several local businesses to invest in services and products to enhance their security. The collaborating company in the research project was among those who invested in products and services to improve their business's security. They hired an IT expert to strengthen their security, but the result of the investment turned out to be an unused document without any value. Shortly thereafter, the company experienced a data breach. The consequences of the security incident led to unavailable resources, reduced production capacity, and financial loss.

An effect of the security incident was that they invested in additional security measures. The investment involved technological security measures equivalent to basic security hygiene, which can protect businesses against 98 percent of all data breaches. Obviously, such technological security measures are effective, but even with such solutions, the company is not immune to human factors. Mistakes made by people are the cause of a significant portion of security incidents, and this is something that SMEs struggle to address. It indicates a lack of understanding of the importance of organizational and human security measures.

Forord

Som en del av masterprogrammet i industriell innovasjon og digital sikkerhet ved NTNU skal studenter skrive en masteroppgave. Masteroppgaven skrives i det fjerde semesteret og står for 30 studiepoeng, og skal leveres 12. juni. Oppgaven bygger videre på en obligatorisk prosjektoppgave som ble levert i slutten av det tredje semesteret.

Masteroppgaven er skrevet av Fredrik Kirkebirkeland Kristiansen og Per Håvard Kolle Hustvedt ved det toårige masterprogrammet i industriell innovasjon og digital sikkerhet ved institutt for industriell økonomi og teknologiledelse, NTNU.

Masteroppgaven er et forskningsprosjekt og er basert på teori og kunnskap knyttet til sosio-tekniske systemer og informasjonssikkerhet. Forskningsprosjektet har vært avhengig av to bedrifter. Den ene bedriften er en teknologisk avansert produksjonsbedrift, og blir i oppgaven referert til som FPH AS. Den andre bedriften er FPH AS sin IT-leverandør, og blir i oppgaven referert til som HKK AS.

Forskningsprosjektet sitt formål var å belyse hvordan små- og mellomstore bedrifter kan bygge bevissthet (cyber awareness). Videre har forskningsprosjektet basert seg på en sikkerhetshendelse i FPH AS for å undersøke hvordan bevisstgjøring kan påvirke bedriften sin informasjonssikkerhet. Å få innblikk i FPH AS og HKK AS sin tilnærming til informasjonssikkerhet og bevisstgjøring har vært viktig for forskningsprosjektet.

Problembeskrivelsen er formulert av studentene i samarbeid med nåværende veileder Halvor Holtskog og tidligere veileder Christina Marie Mitcheltree. Forskningsprosjektets overordnede tema er bevisstgjøring, der sosio-tekniske systemer fungerer som et bakteppe for oppgaven.

Halvor Holtskog og Christina Marie Mitcheltree har vært veldig hjelpsomme gjennom hele prosjektet. De har bidratt med veiledning i form av akademisk skriving, innhold i oppgaven, og oppgaven sin struktur.

FPH AS har vært åpen og hjelpsomme gjennom hele forskningsprosjektet. Bedriften stilte med syv personer som kunne delta i intervjuprosessen, og inviterte oss til to konferanser.

HKK AS deltok på et gruppeintervju med tre personer og kunne dele mye informasjon om hvilket forhold SMB-er har til informasjonssikkerhet.

Vi vil takke Halvor Holtskog, Christina Marie Mitcheltree, FPH AS, og HKK AS for all hjelp med oppgaven. Vi vil også takke medstudenter på campus som har bidratt til to fantastiske år på NTNU.

Innhold

Figurer

1 Innledning

1.1 Problembeskrivelse

Nasjonal sikkerhetsmyndighet (NSM, 2023) fremhever at det er et sterkt behov i dagens digitale risikobilde for å heve kompetansen på informasjonssikkerhet i virksomheter. Små- og mellomstore bedrifter (SMB-er) er ryggraden av europas økonomi, SMB-er representerer 99% av alle virksomheter i EU med over 100 millioner ansatte (Enisa, u.å.). Ifølge Enisa (u.å.) møter SMB-er flere utfordringer innen informasjonssikkerhet på grunn av begrensede ressurser, mangel på kompetanse, og økning i dataangrep rettet mot SMB-er. På grunnlag av dette tar forskningsprosjektet utgangspunkt i én SMB som opplevde én sikkerhetshendelse i august 2021. Forskningsprosjektet tar dermed for seg bevisstgjøring[1] (cyber awareness) i denne bedriften og har sosio-teknisk systemteori[2] (STS) som bakteppe. Videre blir samarbeidende bedrifter presentert, etterfulgt av sikkerhetshendelsen. Bedriftene i forskningsprosjektet er anonyme hvorav produksjonsbedriften blir kalt FPH AS, og IT-leverandøren blir kalt for HKK AS.

FPH AS er en SMB som er en helnorsk innovasjonsbedrift som ble opprettet i 1995. Grunnleggeren av FPH AS har siden opprettelsen i 1995 produsert aluminiumsprofiler og bygget automasjonslinjer for fabrikker. Bedriften holder til på to lokasjoner. Lokasjon 1 er fabrikken til bedriften, her produserer de alle sine varer og lokasjon 2 er hvor administrasjonen til bedriften befinner seg. Disse lokasjonene ligger ca. 10-15 minutter med bilkjøring fra hverandre. Selskapet har fra start av vist en sterk omstillingsevne og har utvidet driftshorisonten hvor de nå leverer produkter i et bredt spekter og spesialiserer seg innen alt fra elektro til utvikling. FPH AS er et selskap i vekst og som setter forskning høyt på deres agenda, og er blant annet great place to work sertifisert. Dette er en bedrift som er teknologisk avansert, de bruker maskiner og teknologi som gjør at de kan levere gode og innovative varer. Dette gjør de ved å ha høy kompetanse blant sine ansatte og ved å hele tiden være opptatt av å finne nye løsninger og å utforske nye markeder. De har vært en del av mange forskningsprosjekter og er i stadig utvikling. Dette har også resultert i at deres produkter har nådd ett verdensklassenivå som er svært ettertraktet.

HKK AS har drevet forretningsvirksomhet i over 100 år, med røtter helt tilbake til begynnelsen av 1900-tallet. Selskapet ble etablert i 1908 der fokuset den gang var kjøp og salg av fisk. Med tiden har selskapet utvidet sin horisont og leverer tjenester innen alt fra interiør til IT-løsninger. HKK AS har som mål å være Norges ledende innen bærekraftig utvikling i sin bransje. Det innebærer at selskapet arbeider tett med sine kunder og leverandører for å skape tillit til HKK AS. Selskapet kan vise til solide nøkkeltall med god lønnsomhet og meget god soliditet.

[1] Bevisstgjøring blir definert som en læringsprosess som legger grunnlaget for opplæring ved å endre individuelle og organisatoriske holdninger for å forstå viktigheten av sikkerhet og de negative konsekvensene av dens svikt (nist, u.å).

[2] Sosio-tekniske systemer innebærer at sosiale og tekniske elementer og de må bli betraktet i sammenheng. Det betyr at forbedring av et element krever at det andre elementet også blir forbedret, slik vil hele systemet oppnå optimal ytelse.

FPH AS ble i august 2021 utsatt for et dataangrep, og det ble antatt at det var en ukjent tredjepart som fikk tilgang til bedriftens nettverk og systemer. Ifølge informasjon fra FPH AS inkluderte dette antagelig bruk av phishing-, passord, og bruteforce[3]-angrep. Dataangrepet medbrakte konsekvenser for FPH sin daglige drift og resulterte i økonomiske konsekvenser samt at flere av systemene og applikasjonene ikke lenger var tilgjengelige. Systemene dataangrepet forstyrret var som følger: kundehåndtering, fakturering, konstruksjon, utvikling, regnskap, interne kommunikasjonsverktøy og lageroversikt. Før dataangrepet ble en realitet for FPH AS, ble Østre Toten angrepet i 2020, og var en oppvekker for FPH AS da de leide inn en IT-ekspert for å sikre systemene deres ytterligere.

SMB-er er for mange organisasjoner en kritisk samarbeidspartner da de kan være en trussel mot forsyningskjeder, partnernettverk og økosystemer. Ifølge World Economic Forum (WEF) (2022) var 88% av deres respondenter bekymret for de involverte SMB-er sin informasjonssikkerhet. Årsaken til bekymringen for SMB-er sin sikkerhet kan forankres i tilgjengelige ressurser og mindre fokus på informasjonssikkerhet i forhold til større og mer ressurssterke organisasjoner (WEF, 2022). Ifølge Downey (2020) tenker flere SMB-er at de ikke er like utsatt for dataangrep som store selskaper, de facto er SMB-er attraktive mål for trusselaktører. Det fremkommer at halvparten av respondentene i Downey (2020) rapport har vært utsatt for et dataangrep. I 2020 ble SMB-er utsatt for over 700.000 angrep med totale kostnader tilnærmet 2.8 milliarder (Getastra, 2023). Statistikk fra Getastra (2023) viser til at 43% av alle dataangrep er rettet mot SMB-er, hvorav bare 14% av SMB-ene er rustet for å støte på et dataangrep.

Det er blitt utført en rekke studier som påpeker at ansattes bevissthet og kunnskap innen informasjonssikkerhet ikke er god nok (Europakommisjonen, 2021; Center for Internet Security, 2022; NSM, 2023; Bueermann & Doyle, 2023; Nabe, u.å.). Teknologi kan ikke alene tilby tilstrekkelig med sikkerhet da mennesker er en sentral del av sikkerheten (Trček et al., 2007). Dette understøttes blant annet av Europakommisjonen da de i 2021 formidlet i sin rapport at menneskers kunnskap og bevissthet om informasjonssikkerhet er mangelfull (Europakommisjonen, 2021; Mark et al., 2019).

1.2 Problemstilling

Forskningsprosjektets problemstilling har blitt utviklet med tanke på utfordringene SMB-er imøtekommer og situasjonen til FPH AS. På bakgrunn av dette har følgende problemstilling blitt utarbeidet:

Hvordan bygger en SMB bevissthet (cyber awareness)?

1.3 Avgrensninger

Forskingsprosjektet tar hovedsakelig for seg bevisstgjøring i SMB-er, og går ikke noe nærmere inn på bevisstgjøring i større selskaper. STS fungerer som et bakteppe for forskningsprosjektet der det forklarer kort om sosiale- og tekniske elementer, men går ikke inn på miljøet rundt. Hensikten med STS er at teknologiske sikkerhetsløsninger

[3] Tredjepart sender inn kombinasjoner av brukernavn og passord for å gjette innloggingsinformasjon og krypteringsnøkler (Crowdstrike, 2022).

omfatter grunnleggende sikkerhetshygiene[4], og sosiale elementer omfatter organisatoriske og menneskelige sikkerhetstiltak. Det går likevel ikke i dybden på sosio-tekniske systemer, men det redegjøres for hva det er og blir brukt i deler av analysen.

Teorikapittelet informasjonssikkerhet definerer kort hva informasjonssikkerhet faktisk er, etterfulgt av sekundærkilder som beskriver relevante bransjeutfordringer og karakteristikker sett i lys av bevisstgjøring. Grunnet prosjektet sitt fokus tar det ikke utgangspunkt i hvordan sikkerhetstrusler, sårbarheter og atferd påvirker konfidensialitet, integritet og tilgjengelighet.

Sikkerhetskultur blir nevnt i teoridelen under informasjonssikkerhet, men er ikke noe som blir vektlagt eller gjort rede for. Karakteristikker som blir nevnt er en del av sikkerhetskultur, men kan også bli betraktet som relevante for bevisstgjøring og trening, og dermed er begrepene sin betydning forklart.

1.4 Prosjektets utforming

Kapittel 1 presenterer samarbeidende bedrifter, skaper kontekst for forskningsprosjektet og beskriver forskningsspørsmål.

Kapittel 2 Presenterer relevant litteratur og teori som blir brukt som grunnlag og til analyse av data.

Kapittel 3 beskriver forskningsprosjektets metodiske tilnærming, intervjuprosessen og forskningens troverdighet.

Kapittel 4 presenterer resultatene fra forskningsprosjektet.

Kapittel 5 analyserer resultater, med bruk av teori for å besvare forskningsprosjektets problem og måloppnåelse.

Kapittel 6 presenterer konklusjon.

Kapittel 7 beskriver forslag til videre forskning.

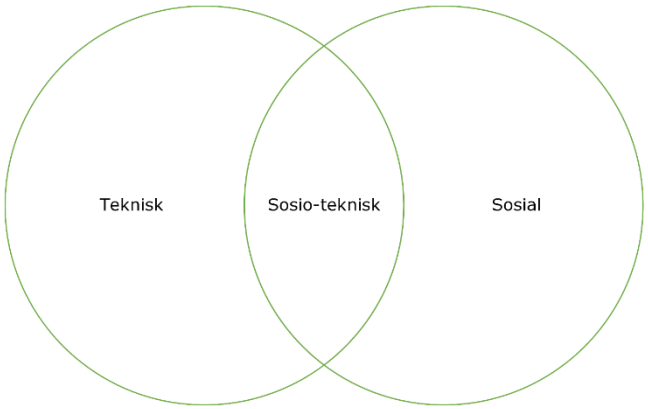
[4] Grunnleggende sikkerhetshygiene består av 5 elementer: Zero trust prinsipper, multifaktorautentisering, moderne anti-malware, holde software og hardware oppdatert, og beskytte data (Microsoft, 2022).

2 Teori

I dette kapittelet blir teori presentert for å skape forståelse for forskningsprosjektet. Teorien blir presentert i følgende rekkefølge: sosio-tekniske systemer, bevisstgjøring, og informasjonssikkerhet. Til slutt blir teorikapittelet oppsummert.

2.1 Sosio-tekniske systemer

Den sosio-tekniske teorien ble først utviklet på 1950-tallet av forskerne Eric Trist og Ken Bamforth gjennom Tavistock instituttet i London på den britiske kullindustrien. Bakgrunnen for studiet var at kull var en viktig kilde til kraft/energi på denne tiden, men produktiviteten var dalende og holdt ikke den økende takten til mekaniseringen/automatiseringen i industrien (Trist, 1981). Sosio-tekniske systemer ble etter hvert introdusert, og innebærer en kombinasjon av de sosiale og tekniske elementer som også er påvirkelige fra miljøet rundt (Appelbaum, 1997). Organisasjoner kan betraktes som komplekse systemer (Davis et al., 2014) og begrepet sosio-tekniske systemer beskriver systemer som innebærer kompleks interaksjon mellom mennesker, maskiner og miljø (Baxter & Sommerville, 2011).



Figur 1: Sammenhengen mellom det tekniske og det sosiale systemet.

Bostrom og Heinen (1977) beskriver det tekniske systemet som de prosesser, oppgaver, og teknologier som kreves for å konvertere input til output. Det sosiale innebærer menneskelige attributter som (f.eks. holdninger, ferdigheter og verdier), relasjonene mellom mennesker, belønningssystemer, og autoritetsstruktur. Applebaum (1997) trekker inn imøtekommelse av de psykologiske behovene som målet til det sosiale systemet. Det skal skape en følelse av tilhørighet, meningsfullhet og ansvar og skapes gjennom organisasjonens kultur, normer, kommunikasjon, relasjoner og atferdsmønster. Videre resulterer dette i at det skapes en relasjon mellom menneskene og organisasjonens teknologi. Det teknologiske systemet omfatter her utstyr og metoder som benyttes i omformingen av råmateriale til produkter eller tjenester.

Trist (1981) forklarer at i seg selv kan disse to elementene betraktes som uavhengige av hverandre i form av at de tilhører to forskjellige vitenskapelige retninger (sosialvitenskap

og naturvitenskap). Likevel er de fortsatt avhengig av hverandre fordi den ene har påvirkning på den andre i transformasjonen mellom input og output (Trist, 1981), dette fører til ønsket om felles optimalisering.

Felles optimalisering er hjørnestenen og grunnlaget til sosio-teknisk systemteori (Malatji et al., 2019). Det innebærer at dersom man skal få et velfungerende sosio-teknisk system med optimal ytelse må alle delsystemer bli forbedret, ikke bare et (Davis et al., 2014; Malatji et al., 2019; Trist, 1981). Man må ta hensyn til hvordan designet til et delsystem kan påvirke andre deler av hele systemet og hvordan dette kan begrense effektivitet (Davis et al., 2014). Optimaliseringen av et sosio-teknisk systems enkelte delsystem kan skape uforutsigbare forhold til andre delsystemer, og dermed en negativ ytelse på hele systemet. En slik skjevfordeling ser ut til å være tilfellet i måten informasjonssikkerhet har blitt håndtert, den har blitt for teknologisk fokusert (Davis et al., 2014; Malatji et al., 2019).

Arbeidet til Evans et al. (2019) viser at den største andelen av rapporterte sikkerhetshendelser er et resultat av menneskelige feil. Budzak (2016) sier den største trusselen til informasjonssikkerhet er mennesker og det estimerte antallet sikkerhetsbrudd på bakgrunn av menneskelige feil er mellom 50% og 90%. I den sosio-tekniske analysen av 19 ulike sikkerhetsrammeverk gjort av Malatji et al. (2019) finner de at rammeverkene oppfyller sikkerhetskravene på den tekniske siden, men finner kun at bare syv av dem delvis oppfyller det sosiale.

Gapet mellom det sosiale- og tekniske elementet sett i lys av informasjonssikkerhet kan være utfordrende for å forbedre bedrifters informasjonssikkerhet. Enhver organisasjon vil ha forskjellige behov og står ovenfor ulike utfordringer. For å kunne oppnå felles optimalisering gjennom teknologiske sikkerhetsløsninger kan det tenkes at teknologien må være tilrettelagt for organisatoriske forhold og menneskelige behov. For å adressere denne neglisjeringen foreslår Europakommisjonen (2022) at virksomheter må øke sin kompetanse og forståelse for informasjonssikkert. Dette kan komme gjennom bevisstgjøring.

2.2 Bevisstgjøring (Cyber awareness)

I dette delkapittelet blir definisjon av bevisstgjøring beskrevet, etterfulgt av noen bransjeutfordringer SMB-er imøtekommer. Til slutt blir effekten av sosiale sikkerhetstiltak presentert.

Bevisstgjøring innen informasjonssikkerhet har en sentral rolle for å øke det forebyggende sikkerhetsarbeidet i virksomheter (Forbes, 2022), og kan ha flere betydninger avhengig hvem man spør. Ifølge Toth og Klein (2014) handler bevisstgjøring om å rette oppmerksomheten mot sikkerhet, der enkeltpersoner skal kunne gjenkjenne sikkerhetsproblemer relatert til IT og deretter agere. Bevisstgjøring er formidling av informasjon til et bredere publikum tilpasset organisasjonen (Toth & Klein, 2014). Tsohou et al. (2015) definerer bevisstgjøring som en prosess der formålet er å endre individers oppfatninger, verdier, holdninger, atferd, normer, arbeidsvaner og organisasjonskultur og strukturer med hensyn til sikker informasjonspraksis. Denne definisjonen resonerer godt med at bevisstgjøring er en læringsprosess som legger grunnlaget for opplæring ved å endre individuelle og organisatoriske holdninger for å forstå viktigheten av sikkerhet og de negative konsekvensene av dens svikt (NIST, u.å.). Forbes (2022) fremhever at bevisstgjøring handler om å rette oppmerksomheten mot daglige

situasjoner. Dette innebærer å være observant over farene ved bruk av nettlesere, e-post, og digital interaksjon (Forbes, 2022).

I en systematisk litteraturgjennomgang gjort av Sony og Naik (2020) understreker de at ansatte blir svært viktige fordi de må tilpasse seg det nye digitale landskapet og bedrifter må tilrettelegge for kompetanseheving for de nåværende ansatte. Kompetanseheving handler om å øke kompetansen til arbeidere i deres nåværende roller (Europakommisjonen, 2021). Europakommisjonen (2021) formidler at det er viktig å sikre et grunnleggende kunnskapsnivå og en forståelse for det digitale ved å øke de digitale ferdighetene til ansatte.

Europakommisjonen (2021) viser til cybersikkerhet som en av de viktigste digitale ferdighetene som kommer til å være nødvendig i fremtidens fabrikker. Dette setter blant annet krav til arbeiderne sine ferdigheter, og da spesielt de digitale ferdighetene (Europakommisjonen, 2021). Digitale teknologier spiller en kritisk rolle i dagens og fremtidens industri da det er en økt avhengighet av diverse teknologier. Dette på tross av at det kan utsette industrien for tekniske forstyrrelser gjennom funksjonsfeil og cyberangrep (Kumar & Mallipeddi, 2022). Disse forstyrrelsene kan oppstå på ulike måter, men et eksempel kan være trusselaktører som utnytter menneskelige sårbarheter. De menneskelige sårbarhetene kan være manglende bevissthet og kunnskap eller feil bruk av teknologi (Mark et al., 2019).

Informasjonssikkerhets-trening er et hvert tiltak som gjøres for å forsikre seg om at alle ansatte er utstyrt med informasjonssikkerhets-ferdigheter og -kunnskap spesifikt knyttet til deres roller og ansvarsområde ved å bruke instruksjonsmetoder som seminarer og workshops (Amankwa et al., 2014). Trening handler om at de ansatte eller deltakerne er aktive i prosessen som innebærer å skaffe innsikt, kunnskap og ferdigheter (Hansche, 2001). Sikkerhetstrening gir mer detaljert kunnskap enn det bevisstgjøring kan tilby. Bevisstgjøring gir de ansatte grunnleggende informasjon, mens treningen gjør at de kan oppdage trusler og reagere på dem effektivt (Whitman og Mattord, 2019). Ferdighetene som oppnås gjennom trening bygger på grunnlaget som skapes gjennom bevisstgjøring, men aktivitetene innenfor trening forekommer ikke like ofte som bevisstgjøringstiltak. (ENISA, 2010).

Hos SMB-er viser rapporter at det er lavt nivå av bevissthet og utilstrekkelige implementering av sikkerhetstiltak (Renaud, 2016). SMB-er sliter med å takle det eksisterende trusselbildet i forbindelse med informasjonssikkerhet (Heidt et al., 2019; van Haastrecht et al., 2021). Sikkerhetsindustrien ser en økning i cyberkriminalitet og indikatorene peker mot at angrepene i økende grad er rettet mot SMB-er (Renaud, 2016).

Europakommisjonen (2020) anser cybersikkerhet som et område hvor SMB-er kan være godt tjent med en økning i ferdighetsnivået. Dersom det mangler ferdigheter hos de ansatte, vil de kunne bli en form for innside trusler som utfører utilsiktede handlinger. Williams (2008) skriver i sin artikkel at innside trusler kan være tilsiktet eller utilsiktet, begge kan ha like skadelig effekt, og det blir gjort av ansatte med legitim og autorisert tilgang til informasjonssystemer. Ofte er de interne angrepene de mest suksessfulle og de kommer gjerne som følge av mangel på teknologiske ferdigheter hos ansatte. Dette er viktige ferdigheter Europakommisjonen (2021) trekker frem i sin rapport.

En av misoppfatningene man ser i SMB-er er at cyberkriminelle foretrekker store organisasjoner fremfor SMB-ene og at de dermed kan ignorere sikkerhet (Chaudhary et al., 2023). Denne oppfatningen er skummel fordi SMB-er er faktisk ganske attraktive mål

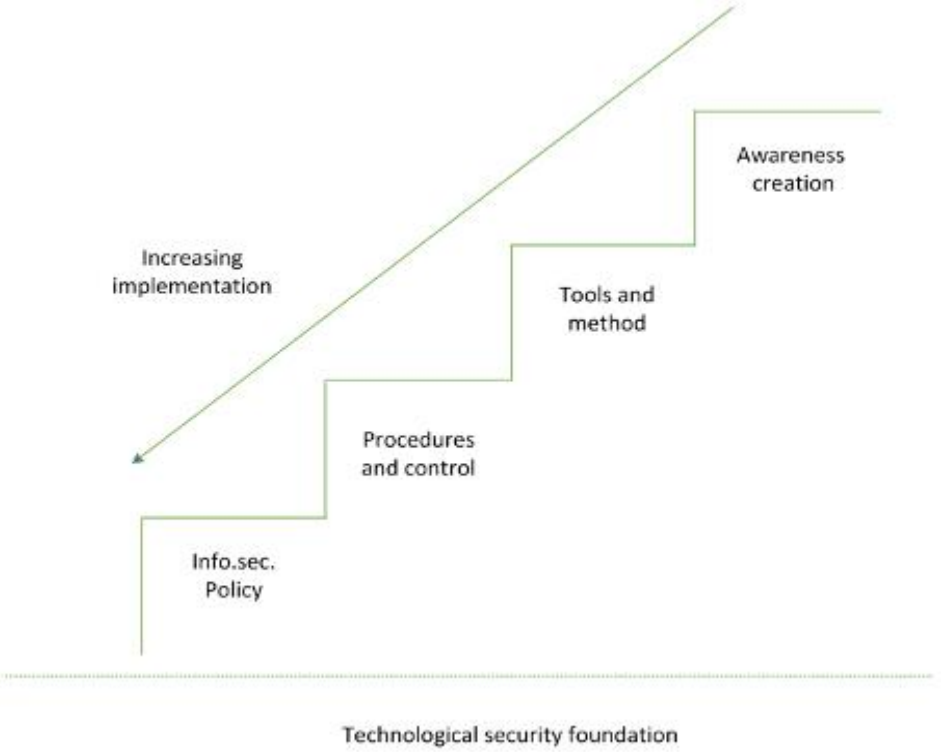
av to grunner, (1) det krever mindre innsats av de kriminelle og (2) mange SMB-er samarbeider med større organisasjoner og kan dermed være et springbrett for de kriminelle inn i de større organisasjonene (Europakommisjonen 2020; Chaudhary et al., 2023).

Mange SMB-er har lavt nivå av intern ekspertise på informasjonssikkerhetsfeltet og tyr dermed til eksterne eksperter (Cragg et al., 2011). Årsakene til dette kan variere, men noen karakteristikker er tydelige. Det er mangel på finansielle ressurser, ekspertise, skrevne formelle sikkerhets retningslinjer, og dårlig holdninger til sikkerhet og risiko (Shojaifar et al., 2020). SMB-er feiler i å investere i informasjonssikkerhet og bevisstgjøring. Det er knyttet til begrensede budsjetter, lite tid til læring, dårlige risikovurderinger, og generelt dårlig overholdelse av regler (Goucher, 2011). I forbindelse med bevisstgjøring er en av grunnene til at dette blir nedprioritert av SMB-er at de gjerne velger dyre teknologiske sikkerhetsløsninger og anser mennesker som et problem, og ikke en løsning (Chaudhary et al., 2023). Teknologi kan ikke alene håndtere sikkerhetsrisikoene man møter (Eminağaoğlu et al., 2009).

Det fremkommer fra flere kilder at ansattes bevissthet og kunnskap innen informasjonssikkerhet ikke er god nok (Europakommisjonen, 2021; CIS, 2022; NSM, 2023; Bueermann & Doyle, 2023; Nabe, u.å.). Eminağaoğlu et al. (2009) utførte en casestudie som varte i et år, der forskerne undersøkte utfallet av bevisstgjøring og trening i en bedrift på 2900 ansatte. Forskningsprosjektet til Eminağaoğlu et al. (2009) kan vise til forbedring av passord og forsiktighet ved bruk av passord, deltakelse og engasjement rundt sikkerhetskontroller og mekanismer som skal være med i kampanjer, samt høyere grad av etterlevelse på selskapets policy for informasjonssikkerhet. Av den grunn konkluderte de med at bevisstgjøring og trening er blant de mest effektive og kraftige verktøyene for å minimere informasjonssikkerhetsrisiko.

Hagen et al (2008) vurderer også bevisstgjøring som et av de mest effektive tiltakene for informasjonssikkerhet. Gjennom deres undersøkelse finner de at respondentene deres har svart at det minst implementerte tiltaket, bevissthetsskapelse (awareness creation), er det mest effektive av de organisatoriske tiltakene (retningslinjer for sikkerhet, prosedyrer og kontroller, verktøy og metoder, bevisstgjøring). De mer formelle formene for tiltak vurderes gjerne som mindre ressurskrevende å utvikle sammenlignet med bevisthetsskapende aktiviteter. Dermed er disse vanligere, og vurderes ofte som et tilstrekkelig nivå med sikkerhet. Men, selv med gode retningslinjer for sikkerhet vil de være mindre effektive når bedriften mangler bevissthet og trening (Soomro et al., 2016) For å bli bedre må man ta for seg den menneskelige delen av sikkerhet.

I figuren til Hagen et al. (2008) nedenfor er det illustrert en trapp bygget på grunnleggende teknologiske sikkerhetsløsninger som alltid må være til stede. Uten teknologiske tiltak vil det ikke være noe poeng med administrative tiltak (Hagen et al, 2008). På bunn av trappen er de mest grunnleggende og utbredte administrative tiltakene i informasjonssikkerhet, og desto høyere man kommer i trappene, desto mindre utbredt er tiltaket. Pilen i figuren beskriver den økende graden av implementering, altså høy grad av implementering desto nærmere et grunnleggende nivå. Det innebærer at f.eks. policy for informasjonssikkerhet, trinn 1, blir oftere implementert enn de øvrige trinnene. Paradokset med figuren er at tiltakene i de øverste trappetrinnene er de mest effektive, men man trenger de foregående for at det øverste trinnet skal være nyttig.



Figur 2: Trappetrinn-modell utarbeidet av Hagen et al. (2008)

Policy for informasjonssikkerhet (Information security policy)

Policy for informasjonssikkerhet spesifiserer standarder, grenser og ansvar for brukere av informasjons- og teknologiressurser som skal lette forebygging, oppdagelse, og respons på sikkerhetshendelser (Cram et al., 2017). Policyen inneholder skrevne instruksjoner fra ledelsen til ansatte og andre på arbeidsplassen om hva som er riktig atferd med hensyn til bruk av informasjon og informasjonsressurser (Whitman & Mattord, 2019). Policy for informasjonssikkerhet hevdes å være grunnlinjen i alle administrative sikkerhetsregimer, og studiet til Hagen et al. (2008) finner at retningslinjer brukes i stor grad. Dette tiltaket utgjør det nederste trinnet i figur 2 og det mest implementerte etter teknologiske sikkerhetsløsninger.

Prosedyrer og kontroll (Procedures and control)

Prosedyrer og kontroll er direkte avledet fra sikkerhetsretningslinjen og inneholder dokumenter som skal lede individuell og organisatorisk atferd (Hagen et al). Det kan gjerne være steg for steg instruksjoner som er designet for å assistere ansatte til å følge sikkerhetsretningslinjene (Whitman & Mattord, 2019). I en sikkerhetsretningslinje kan det for eksempel stå at ansatte må bruke sterke passord. I steg for steg instruksjonen vil leseren da finne prosedyren for å endre passordet og kanskje informasjon om hva et sterkt passord innebærer "Bruk små og store bokstaver, bruk spesialtegn, osv.". Hagen et al., (2008) finner også at dokumenter og kontrollaktiviteter, i likhet med sikkerhetsretningslinje, blir mye brukt.

Verktøy og metoder (Tools and methods)

Administrative verktøy og metoder er både proaktive og reaktive tiltak (Hagen et al., 2008). I følge Hagen et al innebærer dette seks elementer; (1) Hendelseshåndtering

(incident handling), som inkluderer kontinuitetsplaner, krisehåndteringsplaner, hendelsesresponsplaner; (2) Risikoanalyser, som innebærer å avgjøre i hvilken grad en bedrifts informasjonsressurser er eksponert for risiko (Whitman & Mattord, 2019); (3) rapportering, som handler om å rapportere avvik og lignende; (4) ressursklassifisering (asset classification), eksempelvis offentlig, internt, konfidensiell, eller strengt konfidensiell; (5) revisjoner fra tilsynsmyndigheter, en ekstern enhet/organisasjon vurderer sikkerhetstiltak; (6) Intern revisjon, som innebærer at bedriften ser til at tilstrekkelige kontroller, retningslinjer og prosedyrer er på plass.

Bevisstgjøring (Awareness creation)[5]

Dette øverste trinnet regnes som det mest effektive og består av tiltak som skal sørge for at de ansatte blir mer bevisste på informasjonssikkerhet (Hagen et al., 2018). De aktivitetene som inngår i dette er både individuelle og kollektive. Bevisstgjørende aktiviteter kan for eksempel være e-poster med informasjon/påminnelser, plakater, presentasjoner, gruppediskusjoner og trening. Et av de viktigere tiltakene for å øke bevisstheten og ferdighetene til de ansatte er det sistnevnte.

2.3 Informasjonssikkerhet

Informasjonssikkerhet handler om å bevare konfidensialitet[6], integritet[7] og tilgjengelighet[8] av informasjon (KIT) (ISO 27001:2022). Med et økt fokus på informasjonssikkerhet i dagens samfunn har informasjonssikkerhet gått fra å gjelde en spesifikk faggruppe til å gjelde samtlige medlemmer i virksomheten da det tar for seg sikkerheten på tvers av organisasjonen (Whitman & Mattord, 2019). NSM (2023) fremhever en økning i antall dataangrep i sin risikorapport hvorav organisatoriske og menneskelige sårbarheter ofte blir utnyttet i den sammenheng. Til tross for at virksomheter med grunnleggende sikkerhetshygiene er beskyttet mot 98% av alle dataangrep (Microsoft, 2022), så fremhever Blom et al., (2022) at mennesker er involvert i 9 av 10 hendelser.

Phishing-angrep er det enkleste og hyppigste verktøyet for å få tilgang til informasjon om et menneske eller en organisasjoner (Enisa, 2022; PST, 2023). Majoriteten av dataangrep starter som oftest med phishing som en angrepsmetode der den cyberkriminelle oppnår sitt første fotfeste i organisasjoners systemer (Global Cybersecurity Outlook 2022). Menneskelig feil er ifølge Nabe (u.å.) en stor utfordring uavhengig av sektor. Dette blir understøttet av både Bueermann & Doyle (2023) og Center for Internet Security (CIS) (2022) hvor de formidler hvor enkelt det kan være å manipulere ubevisste ansatte. Det er fordi at det er menneskelig å gjøre feil, og mange er ikke oppmerksomme på hva de gjør og hvilke konsekvenser dette kan medføre.

Fra NSMs digitale risikobilde i 2022 ble det identifisert flere sårbarheter gjennom penetrasjonstesting[9] i forskjellige virksomheter. Blant sårbarhetene er svake passord som er lette å knekke, og mange brukere lagrer passordene sine i åpne og lett tilgjengelige filer. Volumet på passordangrep har økt betraktelig de siste årene. Ifølge

[5] Begrepet bevisstgjøring brukes istedenfor awareness creation med samme betydning som cyber awareness.
[6] Konfidensialitet innebærer at informasjon ikke er tilgjengelig eller avsløres til uautoriserte personer, enheter eller prosesser.
[7] Integritet innebærer at informasjon er nøyaktig og fullstendig.
[8] Tilgjengelighet tar for seg at informasjon har egenskapen til å være tilgjengelig og brukbar på forespørsel av en autorisert enhet.
[9] Penetrasjonstest eller inntrengningstest har som mål å avdekke fysiske, logiske, tekniske, menneskelige og administrative sårbarheter i et informasjonssystem eller ved en virksomhets fysiske lokasjon (NSM, 2022).

Microsoft (2022) er det ca. 921 passordangrep i sekundet og en økning på hele 74% i antall passordangrep fra år 2021 til 2022. I rapporten til Bueermann & Doyle (2023) rapporterer de at 81% av alle dataangrep stammer fra enten phishing- eller passord-angrep. Informasjonssikkerhet kan dermed virke å være et utfordrende område for mange SMB-er, ettersom majoriteten av SMB-ene har en begrenset tilnærming til informasjonssikkerhet.

Flere av utfordringene nevnt ovenfor går direkte på organisasjonsmedlemmenes bevissthet og kompetanse. Dr. Gregor Petric og Kai Roer (2018) (tar for seg 7 dimensjoner som kan relateres til hvordan man kan bygge cyber awareness i virksomheter. De 7 dimensjonene tar utgangspunkt i hvordan man kan måle sikkerhetskultur, men Tsohou et al. (2015) sin definisjon på bevisstgjøring inneholder flere av de samme begrepene. Følgende begreper defineres slik:

Holdninger (Attitudes): Organisasjonsmedlemmenes følelser og meninger om aktiviteter som inngår informasjonssikkerhet i organisasjonen. Holdninger tar for seg følelser av frykt eller mangel på frykt, og risiko for seg selv, kollegaer, organisasjonen og eksterne.

Atferd (Behavior): Organisasjonsmedlemmenes faktiske eller tiltenkte aktiviteter og holdninger til risiko som kan påvirke organisasjonens informasjonssikkerhet direkte eller indirekte. Dette inkluderer personlig integritet, normer og regler.

Kognisjon (Cognition): Organisasjonsmedlemmenes bevissthet, kunnskap og oppfatning om praksis, aktiviteter og mestring tilknyttet informasjonssikkerhet. Det kan være forståelse av det digitale trusselbildet, sensitiv informasjon og sikkerhetspolicy.

Kommunikasjon (Communication): Organisasjonsmedlemmenes metoder for å kommunisere, tilhørighetsoppfatning, varsling og rapportering av hendelser.

Overholdelse (Compliance): Organisasjonsmedlemmenes respekt for organisasjonens sikkerhetspolicyer, bevissthet om eksistensen av og kunnskap om innholdet i sikkerhetspolicy.

Normer (Norms): Hvordan organisasjonsmedlemmer oppfatter organisatorisk oppførsel og praksis relatert til informasjonssikkerhet som uformelt kan anses å være normal eller avvikende av ansatte eller andre som er i kontakt med organisasjonen. Dette kan inkludere bevisste og eller ubevisste forventninger om sikkerhetsatferd, uskrevne regler gjeldende bruk av IKT, og holdninger til brudd på sikkerhetspolicyer.

Ansvar (Responsibility): Organisasjonsmedlemmenes forståelse av deres roller og ansvar for å opprettholde sikker informasjonsutveksling i organisasjonen, og hvordan informasjonsverdier kan komme på avveie ved brudd på KIT og sikkerhetspolicy. Dette kan inkludere ansvar for håndtering av passord, autentikatorer og organisasjonens IT-utstyr.

2.4 Oppsumering

Til nå har forskningsprosjektet presentert samarbeidende bedrifter der sikkerhetshendelsen er beskrevet i korte trekk, og det er blitt gjort rede for noen utfordringer SMB-er møter innen informasjonssikkerhet.

Teorikapittelet har tatt for seg sosio-tekniske systemer, bevisstgjøring og informasjonssikkerhet. STS er beskrevet som et bakteppe for forskningsprosjektet og er derfor en kort teoridel for å skape forståelse for sosiale- og tekniske elementer av STS.

STS handler om hvordan man må se sosiale og tekniske elementer i sammenheng og at målet er felles optimalisering.

Bevisstgjøringskapittelet fremhever et behov der ansatte på tvers av organisasjonen trenger et grunnleggende kompetansenivå og forståelse for det digitale trusselbildet. Videre presenterer kapittelet figur 2 utarbeidet av Hagen et al (2008) som illustrerer effektiviteten til ulike sosiale tiltak innen informasjonssikkerhet. Figur 2 omfatter fire trappetrinn og blir nevnt i stigende trappetrinn: (1) Policy for informasjonssikkerhet, (2) prosedyrer og kontroll, (3) verktøy og metoder, og (4) bevisstgjøring.

Informasjonssikkerhetskapittelet tar for seg hva det som begrep innebærer. Angrepsmetodikkene phishing og passordgjetting er presentert på bakgrunn av sikkerhetshendelsen FPH ble utsatt for, samt fakta om hvor kritisk disse to angrepsmetodene kan være. Avslutningsvis ble noen begreper som er relevante i både sikkerhetskultur og innenfor bevisstgjøring introdusert. I neste kapittel blir metoden for forskningsprosjektet gjennomgått.

3 Metode

I dette kapittelet redegjøres det for metodiske valg som ble tatt på forhånd av prosjektet. Kapittelet beskriver forskningsprosjektet sin metodiske tilnærming, datainnsamling, og beskrivelse av intervjuprosessen. Videre blir forskningsprosjektet sin troverdighet presentert. Til slutt blir etiske hensyn presentert for å sikre at forskningen blir utført på en god måte.

3.1 Metodisk tilnærming

Prosjektets problemstilling undersøker hvordan SMB-er tilnærmer seg informasjonssikkerhet, hvordan de samhandler med tredjeparter og hvordan de i ettertid av en hendelse har håndtert sikkerhet. Ifølge Leedy et al. (2021) så er det hovedsakelig to metodiske tilnærminger for forskningsmetode. De to tilnærmingene omhandler kvalitative- og kvantitative prosesser. Disse benyttes for å fremheve forskningsspørsmål, finne relevant litteratur, og samle inn og analysere data.

Valget av metode avhenger av forskningsspørsmålet og hva som er formålet med forskningen (Halvorsen, 2008). Kvantitative metoder involverer en nærmere studie av mengder og kvanta, her genererer studiene gjerne data som er kvantifiserbare og kan måles på ulike variabler på en numerisk måte. Kvalitative metoder har som hensikt å studere et fenomen som oppstår eller har oppstått i naturlige settinger, og metoden involverer å fange opp og studere kompleksiteten i et slikt fenomen. I en kvalitativ studie er det karakteristikker som blir studert og det kan ikke helt reduseres til numeriske verdier (Leedy et al., 2021).

Prosjektet er basert på en kvalitativ tilnærming fordi det er best egnet til å undersøke menneskelige erfaringer, holdninger og erkjennelser, samt at en kvalitativ tilnærming kan skape god forståelse av avanserte situasjoner. En kvantitativ metode kunne også blitt benyttet for forskningsprosjektet, men på grunn av unøyaktige tall, utilstrekkelig mengde statistiske analyser som er av relevans, kunne det redusert reliabiliteten og validiteten av prosjektet.

På bakgrunn av dette har forskerne diskutert hvilken type studie som passer forskningsprosjektet sitt formål. I neste delkapittel beskrives valg og begrunnelse for forskningsstudiet.

Casestudie

Som forskningsmetode har casestudier blitt brukt i mange ulike sammenhenger for å bidra til kunnskap om individuelle, gruppe, organisatoriske, sosiale, politiske, og relaterte fenomener (Yin, 2014). Yin (2014) skriver at det er tre vilkår man må tenke på ved valg av metode; (1) typen forskningsspørsmål er det; (2) graden av kontroll forskeren har på atferdshendelser; (3) graden av fokus på samtiden i motsetning til helt historiske hendelser. For at casestudie skal være relevant er det mest sannsynlig at forskningsspørsmålet er et «hvordan» eller «hvorfor» spørsmål. De to siste vilkårene for at det er et casestudie er at det er en samtidshendelse man studerer og at relevant atferd ikke kan bli kontrollert.

På bakgrunn av dette er casestudie av høy relevans til prosjektet da det undersøker hvordan en SMB opplevde og håndterte en sikkerhetshendelse, samt hvordan tillitt og tro på teknologi og påvirker kompetansen til ansatte i bedriften. I tillegg til å bare fokusere på den ene siden av bedriftens informasjonssikkerhet blir også IT-leverandøren involvert i prosjektet for å skape et helhetlig bilde av utfordringer for SMB-er sin informasjonssikkerhet, da bedriftens IT-leverandør tilbyr tjenester til flere SMB-er og kan trekke paralleller til SMB-enes informasjonssikkerhet.

3.2 Datainnsamling

Det er flere former for data man kan benytte seg av i et forskningsprosjekt for å besvare forskningsspørsmålet, det kan blant annet være observasjoner, intervjuer og dokumenter (Leedy et al., 2021), men den viktigste kilden til casestudie-data er intervjuer (Yin, 2014). Forskningsprosjektet har tatt for seg en-til-en intervjuer, og observasjonsrunder på lokasjon 1 og 2. I intervjuet med IT-leverandøren ble det utført et gruppeintervju med tre personer hvor den ene var mindre til stede på grunn av jobbmessige årsaker.

En-til-en intervjuer er mye brukt innen kvalitativ forskning og i casestudier. De har potensial til å føre til meningsfulle samtaler som kan resultere i bedre innsikt og ny kunnskap. Intervjuene i et casestudie ligner typisk på en guidet samtale fremfor et strukturert oppsatt spørreskjema (Yin, 2014). Intervjuene følger et semistrukturert oppsett der det ifølge Leedy et al. (2021) kan føre til tilpassede oppfølgingsspørsmål basert på situasjonen og gir muligheter for en dypere forståelse av intervjuobjektet resonnement og tanker.

Intervjuobjektene har friheten til å svare som de vil og er ikke avhengige av å vite hva andre svarer. Det er kun individets egne meninger, oppfatninger, erfaringer som ligger til grunn. En utfordring med dybdeintervjuer kan være å stille de rette spørsmålene og unngå at intervjuobjektet går utenfor hva forskningen tar for seg. Ved å stille åpne spørsmål fremfor ledende spørsmål kan det stimulere til en informativ samtale uten at intervjuobjektets svar påvirkes av hva som antas å være «rett» svar. Spørsmålene som blir stilt må være enkelt formulert slik at deltaker har mulighet til å forstå og reflektere (Leedy et al., 2021). Basert på forskningsdesignet kan det være hensiktsmessig å benytte seg av en-til-en intervjuer. Bakgrunnen for dette er at det kan supplere casestudier fordi man kan få ytterligere forståelse av FPH AS sin informasjonssikkerhet.

Observasjonsrunder tar for seg å undersøke menneskelig atferd, aktiviteter eller fenomener (Leedy et al., 2021). Siden et casestudie finner sted i den virkelige verden gir det mulighet for direkte observasjoner, og disse kan være enda en kilde til bevis. Observasjoner gir ofte nyttig tilleggsinformasjon om temaet som blir studert (Yin, 2014).

På den ene siden av forskningsprosjektet kan det tenkes at observasjonsrundene skaper nytte ved å undersøke ulike variabler som kan føre til hypoteser om hva som for eksempel kan påvirke atferd eller handlinger. På den andre siden kan observasjon som datainnsamling ha sine utfordringer og begrensninger ettersom forskerne ikke har like god innsikt i hva som er mest relevant og prioritert (Leedy et al., 2021).

Utvalg av intervjuobjekter

Den kvalitative tilnærmingen tar for seg å velge informanter som er av relevans for forskningsproblemet som studeres. Elementer som understøtter en kvalitativ tilnærming iht. utvalget av intervjuobjektene, kan forankres i behovet for å undersøke forskjellige ledd i organisasjonen for å fremme ulike perspektiver og erfaringer (Leedy et al., 2021).

På grunnlag av forskningsprosjektet sin problembeskrivelse og problemstilling kan det være avgjørende å skaffe et mangfoldig utvalg av intervjuobjekter på tvers av organisasjonen, ettersom sikkerheten ikke er bedre enn det svakeste ledd.

Forskningsprosjektets utvalgsstørrelse kan være avhengig av kvaliteten på intervjuene som gjennomføres. Det er ingen fasit på hva som er en god utvalgsstørrelse og fra et hvert forskningsprosjekt kan utvalgsstørrelsen variere basert på tre elementer; forskningsspørsmål, populasjon, og tilgjengelige ressurser (Leedy et al., 2021). Basert på de tre elementene er det i dette forskningsprosjektet viktig å oppnå et mangfoldig utvalg for å undersøke hvilke holdninger de ansatte har til informasjonssikkerhet, fremfor å ha et stort utvalg som kan representere en populasjon. Et mangfoldig utvalg vil bidra til et ulike syn og perspektiver på informasjonssikkerhet. Tilgjengelige ressurser er begrenset da det er to forskere uten økonomisk støtte. Det har på dette grunnlaget ført til et utvalg på 10 intervjuobjekter.

Forskningsprosjektets utvalgsstrategi er avhengig av et mangfoldig og anonymt utvalg ettersom det kan føre til ulike syn på informasjonssikkerhet på alle nivåer. Dersom forskere ønsker å undersøke en populasjon eller objekt, er det anbefalt å bruke en utvalgsstrategi som gir et representativt utvalg for populasjonen og/eller objektet. Videre fremhever Leedy et al. (2021) at sannsynlighetsutvalg inkludert tilfeldig utvalg, kan være gunstig i noen tilfeller. Det fremkommer at en slik strategi ikke alltid er anbefalt siden det kan være utfordrende eller umulig å gjennomføre eller i det heletatt er en ønsket strategi (Leedy et al., 2021).

På grunnlag av forskningsprosjektets bakgrunn og problembeskrivelse er utvalgsstrategien en kombinasjon av tilfeldig utvalg i bedriften og snøballeffekt for å nå frem til IT-leverandør. Ved et tilfeldig utvalg kan forskeren(e) anta at utvalget representerer hele populasjonen siden alle har lik sannsynlighet til å bli en del av utvalget. Snøballeffekten er en utvalgsstrategi som handler om at forskerne spør intervjuobjekter om hvem som anbefales til intervju (Leedy et al., 2021). Snøballeffekten var en strategi som i forkant av forskningsprosjektet ikke var diskutert, men ble fort en viktig strategi da flere av intervjuobjektene nevnte IT-leverandøren deres som potensielle intervju objekter. Samtidig som IT-leverandøren ble tatt opp gjentatte ganger viste majoriteten av det tilfeldige utvalget at de hadde mye tillit til IT-leverandøren.

Intervjuguide

I midten av Januar ble kontaktpersonen for selskapet kontaktet av forskningsprosjektets medlemmer i forbindelse med planlegging og bekreftelse av anonymiserte intervjuer. Involverte parter i selskapet fikk tilsendt et sammendrag over mail av forskningsprosjektets omfang for å skape forståelse av prosjektet og om det var av relevans for selskapet. I forkant av intervjuprosessen ble kontaktpersonen oppdatert på forskningsprosjektets omfang og endringer som hadde skjedd i mellomtiden. Intervjuobjektene fikk kort informasjon fra kontaktpersonen om hva intervjuet innebar, men verken deltakere eller kontaktperson fikk ytterligere informasjon om spesifikke spørsmål og delemner som skulle gjennomgås.

Intervjuobjektene fikk ikke tilsendt informasjonsskriv i forkant, men fikk all informasjon i starten av intervjuet. Intervjuene startet med er godt håndtrykk før involverte parter introduserte seg for hver andre, etterfulgt av informasjon om forskningsprosjektet. Deltakerne ble informert om fullstendig anonymisering, ingen lydopptak og alt som blir sagt kan på ingen måte spores tilbake til dem. Videre ble deltakerne informert om at

dersom noe er uklart kan spørsmål omformuleres, og dersom deltakerne ikke vil svare på spørsmålene som blir stilt kan de velge å la være å svare.

Under selve intervjuet hadde den ene forskeren ansvaret for å stille spørsmål, mens den andre skrev ned hva som ble sagt og deltok sporadisk med oppfølgingsspørsmål. Det var satt av 30 minutter med +- 10 minutters slingringsrom da noen intervjuobjekter kan dele mer informasjon enn andre.

Intervjuene med selskapet fulgte en intervjuguide som baseres på semistrukturerte intervjuer med utgangspunkt i ISO 27001:2022. ISO 27002:2022 ble brukt dersom det var behov for ytterligere informasjon om kontroller oppgitt i ISO 27001. Spørsmålene var delt inn i forskjellige kategorier hvor det først ble redegjort for intervjuobjektenes kunnskap om informasjonssikkerhet, etterfulgt av hvordan de opplevde dataangrepet både under og i etterkant. Resterende av intervjuet tok utgangspunkt i bevisstgjøring, kompetanseheving og trening. Spørsmålene var skrevet og formidlet på den måten at alle intervjuobjekter kunne svare uavhengig av erfaring og kunnskap om informasjonssikkerhet.

Intervjuguiden til gruppeintervjuet med IT-leverandøren var tilnærmet lik den som ble brukt med selskapet, men var tilpasset IT-eksperter for å svare på spørsmål rettet mot SMB-er. Spørsmålene fulgte de samme kapitlene og kontrollene i ISO 27001:2022 og ISO 27002:2022 som de gjorde i intervjuene med selskapet. Det ble gjennomført et semistrukturert intervju med gode og tunge faglige samtaler. Intervjuobjektene malte det samme bildet som selskapet gjorde, men fra hvert sitt perspektiv. Gruppeintervjuet fungerte utmerket siden deltakerne diskuterte god mellom seg fra ulike synspunkter og erfaringer.

Etter samtlige intervjuer var gjennomført reflekterte prosjektmedlemmene svarene fra deltakerne først sammen også hver for seg. De individuelle refleksjonene ble notert og delt med hverandre for så å diskutere og evaluere forskningsmetodikken. Her kan det være noe påfyll for fordeler og ulemper med valg av metode.

Analyseprosessen

Det er mange forskjellige prosesser for å analysere data og utvikle dyp forståelse for det som forskes på. Leedy et al. (2021) foreslår to sentrale metoder for å analysere data fra casestudier. (1) Data må kategoriseres og tolkes i like temaer. Dette innebærer at forskerne må identifiserer mønstre og sammenhenger i datainnsamlingen som kan være forklarende ovenfor årsaker og virkninger. (2) Syntese av data for å få helhetlig inntrykk av caset. Dette innebærer å sette sammen og integrere temaene og kodene for å beskrive caset, der målet er å sammenligne og analysere likheter og forskjeller av fenomenet som studeres (Leedy et al., 2021).

En generell strategi som ble brukt for å organisere og analysere data var «organisering av data i en innledende og overfladisk måte som gjør det lett å lokalisere dem senere i analyseprosessen» kombinert med «å fasilitere databaser for å organisere og analysere data» (Leedy et al., 2021). På bakgrunn av intervjuguiden ble det utarbeidet et excel-ark for å organisere data på en systematisk måte. Dette gjorde det lettere å se sammenhenger, koblinger og motsigelser i svarene til de ulike intervjuobjektene.

Under hvert intervju noterte den ene forskeren alt som ble sagt, hvorav ustrukturerte setninger og ord som «Ømm», «eeh», etc. ble omformulert. Utfordringer knyttet til notering underveis i intervjuet var hastigheten på samtalene, i de fleste samtaler kunne skribenten holde følge med intervjuobjektets samtalehastighet, mens det i andre

intervjuer var mer utfordrende å holde følge. I de samtalene som gikk hurtigst kan noe av det noterte komme ut av kontekst. Forskerne har derfor konkludert med å stryke dette for videre analyse dersom det ikke gir mening i etterkant av intervjuet. På den andre siden reflekterte og noterte begge forskerne umiddelbart deres oppfatninger og meninger om intervjuet, dermed kan noe av kontekstbruddene være relevante da intervjuene fremdeles ligger ferskt i minnet.

3.3 Forskningens troverdighet

Innen kvalitativ forskning kan det være avgjørende å fremme et troverdig forskningsprosjekt, hvorav troverdighet kan være av stor betydning av prosjektets forskning. Det innebærer hvor pålitelig og tillitsvekkende forskningen er, samt i hvilken grad man kan stole på forskningsresultatene og konklusjonene som fremheves i forskningsprosjektet. Den kvalitative metoden som benyttes i prosjektet handler om å skape forståelse og kontekst basert på intervjuobjektenes perspektiv. For å skape troverdighet benyttes semistrukturerte intervjuer med ti intervjuobjekter, hvorav 7 er fra FPH AS og 3 fra HKK AS, samt observasjon på begge lokasjonene til FPH AS.

Det er en triangulering av datakilder der det brukes flere ulike kilder som understøtter den kvalitative metoden. Gjennom intervjuer, observasjoner, og dokumenter, kan forskerne reflektere fra flere ulike synspunkt. Et viktig element for å fremme et troverdig forskningsprosjekt kan innebære å være bevisst på forskernes påvirkning og forståelse for deres rolle i prosjektet.

I neste delkapittel beskrives forskningsprosjektets reliabilitet og validitet, etterfulgt av generaliserbarhet.

Reliabilitet og validitet

Et grunnleggende spørsmål mål i all forskning er dataens pålitelighet. På forskningsspråket betegnes dette som reliabilitet, fra det engelske ordet reliability, som betyr pålitelighet (Johannessen et al., 2016). Reliabilitet knytter seg til nøyaktigheten av undersøkelsens data, hvilke data som brukes, den måten de samles inn på, og hvordan de bearbeiders (Johannessen et al., 2016). Reliabilitet referer til hvorvidt man kan stole på forskningen og at fremgangsmåten kan repeteres på et senere tidspunkt av andre forskere (Yin, 2014)

Uten dokumentasjon på hvilke steg som har blitt tatt i forskningen blir det til og med vanskelig for de nåværende forskerne å gjennomføre studiet nytt. Forhåpentligvis vil man med denne dokumentasjon treffe de samme resultatene. Uten at dette punktet er oppfylt kan ikke forskningen anses som reliabel og man risikerer at feilinformasjon blir spredt. Validitet er relevansen til dataene som er samlet inn og hvordan de samsvarer med virkeligheten som undersøkes (Johannessen et al., 2016).

For å sikre god kvalitet på studiet ble det lagt ned mye tid i utformingen av intervjuguiden. Dette skulle sikre at vi fikk gjennomført intervjuene på best mulig måte. Dette i form av at alle ønskede temaer blir dekt og svarene som fremkommer fra intervjuobjektene er relevante for problemet som skal belyses. Underveis i intervjuprosessen ble også små justeringer på spørsmål fra intervjuguiden gjennomført. Dette sikret unødvendige spørsmål som ble oppdaget underveis ble luket bort. Intervjuspørsmålene ble nøye planlagt og utarbeidet gjennom ISO 27000-serien, som er beste praksis innen informasjonssikkerhet. Siden spørsmålene har sin opprinnelse fra

ISO 27000-serien er det rimelig å anta at intervjuspørsmålene er av god kvalitet med riktig fokus. På den andre siden er det ingen retningslinjer eller prosedyrer i ISO 27000-serien som bidrar til å stille gode intervjuspørsmål. Det er dermed opp til forskerne selv å utarbeide gode spørsmål som er basert på beste praksis.

Fokuset rundt spørsmålene var at de ikke under noen omstendigheter skulle være ledende. Forskerne hadde som mål å fremstå som åpne og tillitsfulle gjennom intervjuprosessen. I starten av intervjuprosessen ble intervjuobjektene informert om at intervjuet skal være åpent for å skape et trygt miljø. Dersom spørsmålene var dårlig formulert eller vanskelig å forstå, ble intervjuobjektene informert om at det er bra å si at man ikke helt skjønte spørsmålet.

Siden forskningsprosjektet bygger på sikkerhetshendelsen i FPH AS kan det være vanskelig å reprodusere lignende resultater, fordi individer kan oppleve kriser annerledes. Case-studiet begrenses til 10 intervjuobjekter, der forskerne vektlegger hvorvidt funnene og forståelsen fra studien kan sammenlignes med andre lignende kontekster. Forskerne beskriver detaljene i forskningsprosjektet og skaper kontekst tidlig i forskningsprosjektet. Konteksten referer til rammen for forskningsprosjektet der utfordringen blant SMB-er sin informasjonssikkerhet belyses.

Beslutninger knyttet til forskernes kontekstgrunnlag og tilnærming av prosjektet bringer frem flere utfordringer SMB-er står ovenfor innen informasjonssikkerhet. Til tross for at forskningsprosjektet har benyttet semistrukturerte intervjuer, et gruppeintervju, og to observasjonsrunder kan det være vanskelig å bevise nøyaktigheten av studiets reliabilitet. Årsaken til at det kan være utfordrende er fordi forskerne er avhengig av en samtaleprosess, samt observasjoner, som kan være vanskelig å reprodusere.

Når data for studiet gjennomgås er det viktig at det blir tatt stilling til om informasjonen er korrekt. Potensielle fallgruver vil være at man snakker med intervjuobjekter som oppgir feilinformasjon enten bevisst eller ubevisst. Gjennom intervjuene kan det være at intervjuobjektene ikke føler seg trygge nok og ikke tørr å utgi "hele sannheten". Dette kan enten være en ubevisst aksjon eller en aksjon gjort i frykt for at intervjuet skal få konsekvenser for intervjuobjektene. For å adressere dette problemet forsikret vi intervjuobjektene om at dette var helt anonymt. Andre årsaker til deling av feilinformasjon kan komme fra intervjuobjekter som ikke er fornøyde med situasjonen, og dermed snakker ned bedriften. En annen side av dette kan være et intervjuobjekt som er godt tjent med at bedriften stilles i et godt lys. En slik person vil da gi et bedre inntrykk av tilstandene enn hva som er det faktiske tilfellet. Dette problemet adresseres ved at det er en utvalgsstørrelse på 10 intervjuobjekter.

En annen kilde til feilinformasjon er å ikke være kritisk til kildene som har blitt benyttet gjennom forskningsprosjektet. Dette vil kunne lede til feiltolkninger av teori og empiri som leder til feilslutninger på studiet. Måten dette har blitt håndtert på er at kilder har blitt vurdert før bruk og vi som forskere har analysert dataene. Da blir påstander og utsagn diskutert mellom forskerne og dette minsker sjansen for forskjellige tolkninger, og øker validiteten på det som blir skrevet.

Svakheter, sett i lys av forskningsprosjektet sin reliabilitet og validitet, bunner ut i prosjektets tidshorisont, mindre erfarne forskere og evnen til å notere alt som ble sagt under intervjuene. Noe som kunne styrket forskningsprosjektets reliabilitet var dersom flere forskere med ulike bakgrunner hadde deltatt. Fordelen ved en mangfoldig forskningsgruppe er at den kunne økt forskningsprosjektet sin kvalitet. Det er fordi

informasjonssikkerhet er et tverrfaglig emne og med flere forskere med ulike bakgrunner kan det føre til dypere forståelse av hvordan man kan bygge bevisstgjøring

Generaliserbarhet

Generaliserbarhet handler om i hvilken grad funnene og resultatene i en studie kan gi mening for andre populasjoner, kontekster eller situasjoner. En utfordring med generaliserbarhet innen kvalitativ forskning er at det er komplisert og kontroversielt. Det er fordi kvalitative forskere har hensikt å gi en rik og kontekstualisert forståelse av menneskelig erfaring gjennom studier i spesielle tilfeller. Dette kan skape konflikter om viktigheten av generaliserbarhet ettersom generalisering kan tenkes å være kunstig eller begrenset på grunn av det unike og kontekstuelle ved tilfellene som studeres (Polit & Beck, 2010).

HKK AS har mange kunder som hører til i SMB markedet, og blant deres kunder finner vi FPH AS, som dette studiet har tatt for seg. Bedriften som har blitt undersøkt er en innovativ og teknologisk avansert bedrift, som betyr at det bra kompetanse blant ansatte på teknologi. Av denne grunn bør bedriften ha større sjanse for å forstå dette problemet enn andre SMB-er. Derfor vil vi si at de funnene som presenteres i denne studien gjelder for flere SMB-er og ikke bare for FPH AS.

Etiske hensyn

Prosessen med intervjuer startet med å forhøre oss med veileder og NSD angående hvilke krav vi måtte forholde oss til ved innsamling av data. Vi forklarte dem hvordan og hva vi skulle innhente og fikk til svar at det ikke var nødvendig å melde inn prosjektet da ingen personopplysninger blir håndtert.

Intervjuspørsmålene innebar ikke personlige spørsmål og inneholder dermed ikke identifiserbare detaljer om intervjuobjektene. Spørsmålene samlet dermed kun inn anonymisert data. I tillegg har både bedriften og IT-leverandøren blitt anonymisert gjennom teksten og har kun blitt beskrevet for å gi en forståelse for bakgrunnen deres.

Navnene som blir brukt i forskningsprosjektet for å referere til intervjuobjektene fra HKK AS har ingen sammenheng med personene og er kun for å gi en bedre forståelse for gruppeintervjuet og leseopplevelse. Prosjektmedlemmene som har utført dette prosjektet har ingen tilknytning til bedriftene fra før av og er på denne måten objektive i fremstillingen av bedriften.

4 Resultat

I dette kapittelet presenteres intervjuobjektenes refleksjon på spørsmålene de ble stilt i intervjuprosessen og to observasjonsrunder. Intervjuobjektene fra FPH AS blir referert som intervjuobjekt 1 til intervjuobjekt 7. I HKK AS har intervjuobjektene fått følgende navn: Ole, Dole og Doffen.

4.1 Sikkerhetshendelsen

I dette delkapittelet fremheves svarene fra intervjuobjektene om hvordan de opplevde sikkerhetshendelsen under og etter angrepet.

Intervjuobjektene fikk spørsmål om hvordan de opplevde hendelsen og svarte umiddelbart med treghet i arbeidshverdagen på grunn av utilgjengelige ressurser, men produksjonen gikk som normalt. Intervjuobjekt 3 informerer om hvilke konsekvenser det hadde for andre aktiviteter utenom produksjonen som gikk som normalt og trekker blant annet frem et eksempel der selskapet var midt i en søknadsprosess med forskningsrådet om skattefunn. På grunnlag av dataangrepet klarte ikke selskapet å nå søknadsfristen siden de ikke hadde tilgang på rett informasjon til rett tid, resultatet var tapt inntekt på bunnlinjen. I etterkant av dataangrepet var det ingen intervjuobjekter som opplevde noe uvanlig og alt gikk tilbake som normalt. På grunnlag av dette fikk intervjuobjektene spørsmål om hva som kan ha vært årsaken til hendelsen. Samtlige intervjuobjekter svarer tilnærmet likt og det kan refereres som følger: Jeg vet ikke hva som var årsaken og fikk lite eller ingen informasjon.

Intervjuobjekt 4 var skrekkslagen og mener at de aldri kommer til å finne ut årsaken til hendelsen. Intervjuobjekt 3 starter å fortelle at Østre Toten ble utsatt for et dataangrep noen måneder før dem, og hadde det ikke vært for det angrepet kunne det fort blitt verre enn hva de opplevde. De tok umiddelbart aksjon og hyret inn en IT-ekspert for å granske systemene deres for å finne forbedringspunkter. Intervjuobjekt 3 mener dette har vært til god hjelp selv om det kan være vanskelig å tenke seg hvordan hendelsen ville vært dersom IT-eksperten ikke hadde vært hyret inn, men vet ikke hva årsaken til dataangrepet var. Intervjuobjekt 1 tror midlertidig at det kan ha vært et passordangrep der «trusselaktøren» har ligget i systemet en stund, men det er vanskelig å si hvor lenge dersom det er tilfellet. Intervjuobjekt 3 mener det var hell i uhell at det gikk slik som det gjorde og sier at man ikke kan sikre seg mot alt, men man må gjøre en vurdering på hvilke risikoer som kan aksepteres og hvilke som ikke kan aksepteres.

Samtlige intervjuobjekter får spørsmål om hva de lærte av hendelsen og svarer følgende:

Intervjuobjekt 1:

«Glemt mye, men vi har lært at sånt skjer og man må se det positive i dette».

Intervjuobjekt 2:

«Lærte ingenting. Det har ikke vært noen gjennomgang av hva som har skjedd eller hva vi kan lære av hendelsen».

Intervjuobjekt 3:

«Det blir på en måte IT-leverandøren som tar for seg dette, men vi følger med på deres løsninger og håper at de er god og trygg nok. Pris kan nok være en faktor for noen løsninger, men vi har ingen tradisjon om å ta det billigste. Vi ønsker så gode løsninger som mulig».

Intervjuobjekt 4:

Intervjuobjekt 4 starter med å fortelle om en nylig hendelse, men med lite skade på selskapet. Dataangrepet hindret tilgjengeligheten på selskapets nettside. Intervjuobjektet får igjen spørsmål om hva de lærte av hendelsen og hvordan de kan ha blitt angrepet på nytt etter at IT-eksperter har vært involvert og med en solid IT-leverandør i ryggen. Intervjuobjekt 4 svarer som følgende:

«Vi bruker Wordpress for nettsiden, og her har jeg fortalt gjentatte ganger at den er kjent for å ikke være særlig sikker. Jeg lærte at enkelte ganger må vi lære den harde veien».

Intervjuobjekt 5:

«Lærte at man ikke må klikke på lenker og at det er lurt å endre passord».

Intervjuobjekt 6:

«Jeg lærte at logistikken blir mye bedre av det digitale, og at det ikke har vært noen endringer siden hendelsen».

Intervjuobjekt 7:

«Å være forsiktig med hva man trykker på med tanke på skadevare».

Intervjuobjekt 3 fortalte at de fikk informasjon om hendelsen og at det ble videreformidlet i selskapet. På den andre siden nevner intervjuobjekt 1, 2, 4, 5, 6, og 7 at de ikke fikk noe informasjon.

Intervjuobjektene vet egentlig ikke hva som kan gjøres annerledes for å unngå lignende sikkerhetsbrudd, utenom «normal» bruk av pc, som vil si å logge av pc og ha et godt passord, kan forhindre sikkerhetsbrudd.

4.2 Intervjuobjektene sin kompetanse

Dette delkapittelet handler i hovedsak om intervjuobjektenes generelle kompetanse innen informasjonssikkerhet og deres holdninger til informasjonssikkerhet.

Intervjuobjektene får følgende spørsmål:

«Hva tenker du informasjonssikkerhet innebærer?»

Intervjuobjekt 1:

«At brukere har tilgang til det de skal ha tilgang til, og at det er minst mulig administratorer. To-faktor for innlogging så man føler seg trygg mot dataangrep».

Intervjuobjekt 2:

«Tenker mest på personinformasjon og hvordan dette deles, phishing og endre passord ofte, ca. hver måned».

Intervjuobjekt 3:

«Innebærer at vi sikrer data vi har i skyen, men rundt passord, innlogging, og multifaktor autentikator (MFA). Tenker det er mange enheter som må avhendes. Alt må slettes på en forsvarlig måte så data ikke kommer på avveie. Det er nok mange angrepsvinduer som kan bli utnyttet og man er nok egentlig veldig åpen for å bli utnyttet dersom sikkerhet og bevissthet er dårlig».

Intervjuobjekt 4:

«Sikre data, kontoinformasjon, personinformasjon, og vår egen informasjon».

Intervjuobjekt 5:

«Sikre informasjon».

Intervjuobjekt 6:

«Taushetsplikt og nettsikkerhet».

Intervjuobjekt 7:

«Jeg har ikke kjennskap til dette, men antar at det er sikkerhet for pc. At man ikke skal trykke på lenker, og f.eks. fysisk sikkerhet».

Svarene er forskjellige, hvorav intervjuobjektene fremhever ulike elementer som inngår i informasjonssikkerhet. Intervjuobjekt 6 og 7 har viser tidlig i intervjuet at dette er et begrep de ikke har kjennskap til. Intervjuobjekt 1, 2, 3 og 4 får frem viktigheten av innlogging og viser grunnleggende forståelse for hvordan data kan sikres ved å ha et godt passord, hvorav intervjuobjekt 1 og 3 påpeker bruk av MFA kombinert med et sterkt passord. Intervjuobjektene blir videre stilt spørsmål om hvordan de forholder seg til informasjonssikkerhet i deres hverdag. Intervjuobjektene 5, 6 og 7 er tydelige på at de er forsiktige når det kommer til phishing. Intervjuobjektene 1 og 3 nevner fornuftig bruk av datamaskiner, som for dem innebærer låsing av maskin når den blir forlatt eller å slå den av, samt holde seg unna ukjente nettverk.

For å få oversikt over hva intervjuobjektene kan bidra med for å unngå dataangrep i fremtiden blir de spurt om hva de tror kan føre til sikkerhetsbrudd og dataangrep. Intervjuobjektene trekker frem phishing og hacking som alternative årsaker til dataangrep og sikkerhetsbrudd. Intervjuobjekt 4 peker også mot uerfarenhet og uobservante brukere. Til tross for noe kunnskap om innlogging, phishing og hvordan man kan sikre informasjon, kommer det tydelig frem at majoriteten av intervjuobjektene ikke har særlig forståelse for hvordan man forholder seg til informasjonssikkerhet i sin arbeidshverdag.

Intervjuobjektene får spørsmål om deres kjennskap til retningslinjer/policy og interne regler innen informasjonssikkerhet, Intervjuobjekt 1, 2, 4, 5, og 7 svarer som at de ikke kjennskap til dette. Intervjuobjekt 5 informerer om at de kun har fått noe informasjon muntlig som de har måttet forholde seg til. Intervjuobjekt 7 trekker frem noen e-poster som forteller dem hva det skal og ikke skal gjøre i forbindelse med passord. Intervjuobjekt 1 og 4 begynner på eget initiativ å undersøke om de finner informasjonssikkerhets policyen i appen, men fant ingenting i appen som omhandlet informasjonssikkerhet. Intervjuobjekt 4 mener informasjonssikkerhet policy burde vært i appen og lett tilgjengelig, og om den en gang kommer i appen tror intervjuobjektet at den i så fall bør løftes opp på et høyere nivå. Intervjuobjekt 3 og 6 svarer alt sammen står i appen.

Intervjuobjektene blir spurt om hva de ville gjort dersom de fikk vite at noen brøt selskapets retningslinjer/policy. Intervjuobjekt 2 og 7 sier de hadde gitt beskjed til nærmeste leder om hendelsen. Intervjuobjekt 1 svarer følgende:

«Jeg ville rapportert til daglig leder. Vi har også et avvikssystem. Her kan alle føre avvik, men jeg vet ikke om folk er flink til å bruke det. Vi har et mål om å rapportere 1500 forbedringspunkter, så det er lav takhøyde for å rapportere avvik».

Intervjuobjekt 3 forteller at dersom det er brudd på noe i personalhåndboken agerer vi ut ifra dette. Det kan vurderes som en personalsak uansett om hendelsen var bevisst eller ubevisst. Intervjuobjekt 3 sier så følgende:

«Uansett hendelse kan det gå under kategorien: alle kan gjøre feil. Selv om man taper mye penger på hendelsen kan man fremdeles ta lærdom av det og dra nytte av en uheldig hendelse».

Intervjuobjekt 4 ville brukt avvikssystemet for å sende bekymringsmelding. Intervjuobjekt 5 og 6 ville pratet med vedkommende og sett an alvorlighetsgraden, men at det ikke er noen rutiner for hva man gjør i slike situasjoner. Intervjuobjektene blir spurt om hva de ville gjort i samme situasjon dersom det var dem selv eller andre, men med mulighet for å miste jobben. Intervjuobjekt 1 forteller om en lignende hendelse, da var det en annen person som hadde vært uheldig med en enhet og påført skader til 200.000kr. Vedkommende kom opp med en historie som endret seg over tid. Det endte med at personen til slutt meldte fra om hva som egentlig skjedde og var veldig lei seg over hendelsen og at det ble gjort på denne måten. Intervjuobjektet forteller at dette er en veldig skummel hendelse og klart at man er redd for å rapportere det og sier følgende:

«Jeg er veldig selvkritisk og kunne gått langt i kjelleren, men selv om det hadde kostet meg jobben ville jeg gitt beskjed. Det er viktig å tenke på at det er stor forskjell på mentaliteten til mennesker, viktigst er det kanskje å ta lærdom av hendelsen og ikke bare fokusere på det negative».

Intervjuobjekt 2, 4, 6 og 7 forteller at det hadde skapt noen konflikter og kommer helt an på hvilke brudd det er, men ville fremdeles gitt beskjed til nærmeste leder. Intervjuobjekt 3 forteller at man må stå for det som er gjort uansett om det er dumme ting eller en tabbe, men at det ikke må personaliseres for mye. Intervjuobjekt 5 forteller at det ville vært vanskelig å melde fra om det, men vi er flinke til å håndtere vanskelige hendelser og tar konsekvensene for det. Intervjuobjektene blir til slutt spurt om det er noen rutiner eller prosedyrer på å rapportere om avvik. Intervjuobjekt 1, 2, 5, 6 og 7 sier det ikke er noen rutiner eller prosedyrer. Intervjuobjekt 3 og 4 forteller at rutinen er å melde i avvikssystemet og/eller gå til nærmeste leder.

4.3 Intervjuobjektene sin bevissthet

I dette delkapittelet blir intervjuobjektene sin bevissthet kartlagt og presentert.

I resultatene frem til nå har appen blitt nevnt av flere intervjuobjekter. På spørsmålet angående kjennskap til retningslinjer og policy svarte intervjuobjekt 3 at alt står i appen. Intervjuobjekt 3 trekker frem appen som et eksempel på hvor viktig den er for å

kommunisere med de ansatte når det gjelder policyer, nyheter og informasjon om selskapet. Alt er lett tilgjengelig i appen: forbedringspunkter, avvik, personalhåndboken, kommunikasjon, sikkerhet, alt er i appen. På spørsmål om de har noe ansvar i forbindelse med informasjonssikkerhet svarer samtlige at ikke har noe ansvar. Det eneste som skiller seg ut av disse svarene er intervjuobjekt 5, som til å begynne med svarer at det ikke er noe ansvar, men legger til:

«Men alle har vel et eget ansvar for dette».

Intervjuobjektene blir videre stilt to spørsmål for å kartlegge bedriften sin innsats på bevisstgjøring: (1) Hvordan det arbeides i selskapet for å bevisstgjøre ansatte og hva som er deres ansvar for å ivareta sikkerheten. (2) Hvor ofte det utføres aktiviteter, kampanjer som fremmer bevisstgjøring av informasjonssikkerhet. Intervjuobjekt 1 sier at det ikke er noen rutine på dette, men det har vært to tester der de har sendt phishing e-post til ansatte i selskapet for å teste dem. Bare en person har trykket på phishing-lenken og fikk konstruktiv kritikk. Intervjuobjektet mener det bare er sunn fornuft som ligger til rette for informasjonssikkerhet enn så lenge. Utenom informasjonssikkerhet er vi veldig flink til å tilrettelegge for kompetanseheving dersom ansatte viser interesse.

Intervjuobjekt 2, 4, 5, 6, og 7 sier det aldri har vært noen aktiviteter eller kampanjer for å bevisstgjøre eller tilegne seg kunnskap om informasjonssikkerhet. Intervjuobjekt 3 sier det av og til sendes ut orienteringsbrev for å bevisstgjøre ansatte. Intervjuobjektet får oppfølgingsspørsmål om hva slike brev inneholder og svarer at det er helt vanlig informasjon som folk må forstå og tenke selv. Videre forteller intervjuobjektet at når de ble angrepet samlet de alle i plenum for å informere om hendelsen og bevisstgjøre dem om hva som hadde skjedd. Ellers er det egentlig ingenting som blir gjort for å fremme bevisstgjøring, men påpeker at de kan bli mye flinkere. Intervjuobjekt 4 sier selv at det er rom til forbedring og at det er gode muligheter for å tilrettelegge for dette, og påpeker at de ellers blir bevisst når de er under angrepet.

Videre blir intervjuobjektene stilt spørsmål om de har noen tanker om hvilke sårbarheter og trusler selskapet deres kan være utsatt for, og hva de tror kan være årsaken til at sikkerhetsbrudd forekommer. Majoriteten av intervjuobjektene svarer phishing og hacking. Intervjuobjekt 4 nevner blant annet phishing, skadevare, løsepengevirus, men at det kun er teknologiske sårbarheter og trusler som kan påvirke selskapets informasjonssikkerhet

Intervjuobjektene blir spurt om det har fått noe trening for å unngå sikkerhetsbrudd. Svarene vi får fra intervjuobjektene varierer, men bunner ut i det samme: De har ikke fått noe trening for å unngå sikkerhetsbrudd. Intervjuobjekt 7 informerer oss om at det har blitt gitt noe informasjon, intervjuobjekt 6 sier det er ingenting. Det blir også av noen intervjuobjekter sagt at det de kan er selvlært fordi de har egne maskiner hjemme hvor de passer på. Et par intervjuobjekter trekker frem læring i forbindelse med kurs dersom det er av relevans, men ikke trening.

For å følge opp det intervjuobjektene sier om kurs og læring spør vi også om hva som er vanlig å gjøre etter de har vært på kurs eller aktiviteter for kompetanseheving, som f.eks. å dele hva de har lært med hverandre. Intervjuobjekt 1 og 3 sier dette går veldig mye på interesse til ansatte i selskapet og at de interesserte derfor selv ta initiativ for å få informasjon fra personen som deltok i aktiviteten. Intervjuobjekt 3 forteller videre at

man ikke kan tvinge kunnskap på ansatte, men informasjon og kunnskap må formidles på en god måte for å motivere til læring. Intervjuobjekt 4 sier at det er helt klart at man må fortelle andre hva man lærer og er flink til å dele kunnskap. Intervjuobjekt 2 har aldri deltatt på noe slikt, men sier at det sjeldent blir snakket om hva man lærer på f.eks. kurs. Selv om det sjeldent blir snakket om påpeker intervjuobjektet at de ansatte som er interessert i å lære av deltakeren er flink til å snakke om det, men det blir internt og mellom dem. Intervjuobjekt 5, 6 og 7 sier det er veldig lite som blir delt blant dem etter slike aktiviteter. Intervjuobjektene sier det ikke er noen rutine for å dele hva de har lært med hverandre, men forteller gjerne hva de har lært dersom noen spør.

Intervjuobjektene blir stilt spørsmålet om de har noen tanker om å trene på informasjonssikkerhet. Intervjuobjekt 2, 3, 4 og 7 fremhever at det er fort gjort å gjøre mindre gode beslutninger ved uerfarenhet eller når man er stresset, trøtt, sliten etc., og trekker frem phishing som et eksempel på hva som kan påvirke selskapets informasjonssikkerhet i slike situasjoner. Intervjuobjekt 5, 6 og 7 forteller at bevisstgjøring ville vært et godt tiltak for å bli informert om hva de må være observant på, som f.eks. phishing. Intervjuobjekt 7 trekker også frem et poeng og svarer som følger:

«Jeg antar at teknologien er like god for de som driver med hacking som den er for oss. Jeg tror bevisstgjøring og trening ville vært til hjelp».

4.4 IT-leverandør

I dette delkapittelet blir svarene fra HKK AS presentert, og inneholder både generelle utsagn om SMB-er og mer spesifikt FPH AS. Intervjuobjektene i dette delkapittelet blir referert til som Ole, Dole og Doffen.

På spørsmål om hyppigheten av angrep gjort mot SMB-er kan de ikke vise til noen spesifikk statistikk. Men intervjuobjektene opplever at de ofte må bistå bedrifter på grunn av hendelser. Årsakene til disse hendelsene har intervjuobjektene heller ingen statistikk på, men basert på deres erfaring er det ofte to-faktor, teknologi og mennesker. SMB-er investerer ikke i den nødvendige i teknologien, passord kommer på avveie, phishing, og hull i brannmurer. Mange har ikke minimumskravene[10] på plass. De opplever at mange SMB-er har lite forståelse for informasjonssikkerhet.

Intervjuobjektene ble stilt spørsmål hvilke tjenester de tilbyr for at SMB-er kan oppnå et høyere nivå på informasjonssikkerhet. Ole starter å fortelle om hendelsen med selskapet slik at forskerne skulle få en forståelse av hvordan teknologien de tilbyr kunne hindret et slikt dataangrep. Det fremkommer at selskapet leide inn en IT-ekspert i etterkant av dataangrepet mot Østre Toten i 2021. Som et resultat fikk selskapet et dokument som inneholdt en 10-punktsliste der selskapet skulle følge de foreslåtte forbedringene. Ole forteller at selskapet ikke hadde gjort noe med informasjonssikkerheten annet enn at det var gjennomført en workshop.

HKK AS informerer om at 10-punktlisten ikke var godt nok implementert og egentlig ikke hadde noen effekt for sikkerhetshendelsen som inntraff. Listen og implementeringen av punktene ble ikke fulgt opp av IT-eksperten. HKK AS opplever at mange SMB-er har en

[10] Minimumskrav tilsvarer grunnleggende sikkerhetshygiene.

stor tillit til sine IT-leverandører og bruker Microsoft Office-pakken som eksempel for å demonstrere SMB-er sin holdning til, og forståelse for informasjonssikkerhet:

«Veldig mange stoler på at Microsoft har kontroll på dokumentene deres, og det er ikke behov for back-up eller lignende fordi Microsoft tar vare på dataene»

Dole supplerer med mer informasjon i samtalen og forteller at FPH AS fikk en grundig rapport som var bygget på 10-punktslisten fra IT-eksperten som ble leid inn. Rapporten tok spesifikt for seg IT-miljøet og foreslo blant annet å implementere kontroller som tar utgangspunkt i grunnleggende sikkerhetshygiene. Ole forteller at selskapets IT-miljø ikke var tilstrekkelig sikret og informerte at selskapet bare benyttet brukernavn og passord som sikkerhetsmekanismer, hvorav to-faktor var valgfritt for samtlige. Dole forteller at dette ikke er uvanlig blant SMB-er og sier at det kan være mange årsaker til dette, men kanskje hovedårsaken er at de fleste tenker:

«Vi blir ikke angrepet, det skjer ikke oss».

Dole påpeker at utfordringen de som IT-leverandør ofte støter på er kunder som oftest SMB-er som ikke helt forstår eller vil forstå viktigheten av informasjonssikkerhet. Ole legger til at økonomi også spiller en viktig rolle for hva de kan ta seg råd til å betale for, selv om SMB-er kan være vanskelig å overbevise kunder til tider om hva som er rett løsning for dem. Dole drar frem et eksempel på en kunde som kan ansees som vanskelig:

«Vi foreslo en sikkerhetsløsning til et selskap en gang og dette innebar blant annet tilgangsstyring og zero trust prinsipper. Kunden sa at dette ikke var viktig og siden han/hun kunne selv kunne styre tilganger og zero trust prinsipper fra egen datamaskin etter behov».

Dole forteller videre at dette ikke skjer ofte, men det gjentar seg til tider. Det som er skummelt med det er at kundene kunne skru dette av og på selv i når som helst etter behov med sikkerhetsløsninger de har nå eller har hatt. Ole sier informerer om at slike sikkerhetsløsninger ikke er å foretrekke da det er ønskelig å automatisere dette og til enhver tid opprettholde slike sikkerhetsmekanismer.

Intervjuobjektene blir stilt spørsmålet om hvem som har ansvar for å ivareta informasjonssikkerheten. Ole starter å svare og forteller om hvor utfordrende det kan være å tilby SMB-er rett sikkerhetsløsning tilpasset dem på grunn av kunnskap og at kundene ikke alltid ser nytteverdien. Dole forteller om nok et eksempel:

«Jeg tror enkelte bedrifter har møtt veggen for nye løsninger, det må liksom en hendelse til for at de skal forstå».

Dole sier videre at veldig mange har skjønt at det er et økende behov for å sikre bedriften digitalt, men på den andre siden så er det veldig få som faktisk gjør noe med det. Under salgsprosessen forteller Ole at de ikke kjenner på så mye tillit, men når først salget går gjennom viser kundene at de har mye tillit til IT-leverandøren og de teknologiske sikkerhetsløsningene. Dole forteller at en del SMB-er kan ansees som en umoden kundemasse i forhold til informasjonssikkerhet, ettersom de fleste kunder for det meste har passord som sikkerhetsmekanisme.

På spørsmålet om hva slags forventinger kundene deres har til dem som IT-leverandør og informasjonssikkerheten svarer Ole:

«Dersom de velger oss som leverandør har vi gjort et godt forarbeid».

Ole forklarer at informasjonssikkerhet er et stort fokusområde for dem og at de ved anledninger har sett seg nødt til å avslå bedrifter fordi de ikke har det rette fokuset. Det er altså slik at det er en forventing fra begge parter om hvordan den andre parten skal opptre. Det er ikke bare kundene i denne sammenhengen som har krav.

Intervjuobjektene blir videre spurt om hva som ble gjort i etterkant av angrepet. Ole svarer at de isolerte miljøet umiddelbart, verifiserte back-up, og startet med oppbygging av nytt miljø og satt opp alt fra start av. Ole fikk oppfølgingsspørsmål om hvordan prosessen var og svarte med at det kunne være litt utfordrende å informere om årsaken bak hendelsen og hvordan det kan arbeides videre for å forhindre slike dataangrep. Ole sier følgende:

«Vi har som policy å alltid presentere rapporten for våre kunder. Det er fordi det tekniske kan være vanskelig for mange å forstå. Da vi skulle presentere rapporten for selskapet ble resultatet at de fikk tilsendt et dokument og det stoppet der».

Ole legger til at det er dumt at man ikke får gjennomslag når det kommer til presentasjon av rapporten, og det er nok mange årsaker til at det ikke gikk denne gangen. Dole forteller at dette også er en av utfordringene for det kan oppfattes som gresk for veldig mange.

Intervjuobjektene blir spurt om hva de tenker at SMB-er må være ekstra oppmerksom på når det kommer til informasjonssikkerhet. Dole trekker frem grunnleggende sikkerhetshygiene, bevisstgjøring og trening. Dole får oppfølgingsspørsmål og tar oss videre til bevisstgjøring, kompetanseheving og trening. På oppfølgingsspørsmål om de tilbyr tjenester for å gjøre de ansatte mer observant på informasjonssikkerhet og det digitale trusselbildet svarer Ole at selskaper har mulighet til å betale for dette, men det er veldig få som benytter seg av det. Dole forteller at dersom noen kjøper disse tjenestene får de statistikk på det de blir trent på, og da kan man tallfeste resultatene og levere forbedringspunkter for å bevisstgjøre organisasjonen på den måten. Ole supplerer svaret til Dole og forteller at sikkerhetskultur kan være noe å fokusere på siden det kan bidra til at organisasjoner kan forså trusler og sårbarheter. Ole kommer inn på tjenestene de tilbyr og sier følgende:

«Kommer vi der hvor grunnleggende sikring på teknologi og mennesker er implementert, så har vi på en måte lykkes med SMB-er vi leverer tjenester til. Teknologien er lettest å selge, men er veldig budsjettavhengig. Når det kommer til å selge menneskelig trening, opplæring etc., så skjønner de hva det er, men de tror de er flink nok på dette og trenger derfor ikke kurs».

Intervjuobjektene blir spurt om hvem som har ansvaret for å utarbeide policyer, retningslinjer etc. for kundene. Ole svarer at her er dere noen steg i forveien etter salgsprosessen, og ofte kommer vi ikke så langt med majoriteten av SMB-ene. Ole sier følgende:

«Hvis jeg snakker om retningslinjer og ISO er det veldig tungt å få gjennom».

Dette er også tjenester vi kan selge, men det er ikke alltid til hjelp at selskaper har slike dokumenter tilgjengelig når de ikke handler ut ifra dokumentet. Dole og Ole diskuterer litt mellom dem og kommer med et dårlig men sammenlignbart eksempel som de kalte det. Eksempelet er 10-punktslisten selskapet dere skriver med fikk tilsendt, men selv om de hadde dokumentet så virket det som at det ikke ble prioritert. Intervjuobjektene får oppfølgingsspørsmål på hvor kritisk 10-punktlisten var i forhold til å unngå dataangrepet de ble utsatt for. Ole og Dole sier at det er vanskelig å svare konkret på, men som sagt, hvis man har et dokument å ta utgangspunkt i for å forbedre informasjonssikkerheten, men ikke gjør noe med det, så er det ikke til hjelp.

Når gjelder deling av erfaringer kan intervjuobjektene informere oss om at det ikke er noe spesielt fokus på dette, men de er med i noen forum som gjelder informasjonssikkerhet. Utover dette er det bare generell deling dersom de møter på noen kjente i miljøet, og de har som regel de samme erfaringene.

Risikoanalyser er et sentralt punkt i trappetrinn 3 av Hagen (2008), intervjuobjektene i HKK AS ble dermed spurt om de utfører risikovurderinger for SMB-er, eller om dette noe de må utføre på egenhånd. Ole svarer følgende:

«Dette er på et overordnet nivå, så ikke alltid, men vi utfører bare på de største selskapene».

4.5 Observasjon

Som en del av undersøkelsen benyttet vi oss av muligheten til å observere hvordan den fysiske sikkerheten til bedriften var, hvorav fabrikken er lokasjon 1, og hovedkontoret er lokasjon 2. Det første som utpeker seg er at vi som fremmede har mulighet til å gå rett inn døren på lokalet. Det er ingen som møter oss i døren, det er ikke låst dør, og vi ser heller ingen tegn til at det er noe annet en vanlig nøkkel som benyttes på døren. Vi gikk dermed inn på området uten at det ble stilt spørsmål ved. Videre innover i lokalet var det ganske folketomt, men vi møtte på en person. Vi hilste kort på vedkommende og beveget oss videre inn for å lete etter intervjuobjektet vi hadde avtalt møte med. Ingen spørsmål angående vår tilstedeværelse eller vårt ærend på lokasjonen ble stilt. På den tiden vi hadde til rådighet her uten at noen fulgte med oss ville det vært nok av tid til å

ta bilder, studere maskiner, eller lignende. Maskiner og rom med pc-er sto ut ifra hva vi kunne observere ulåste og ubevoktet. Av det vi kunne observere var det ingen på lokasjonen som gikk med dette synlig på seg. Intervjuobjekt 1 påpeker også dette under intervjuet og forteller oss følgende:

«Folk kan gå rett inn og det er ikke noe problem for at uvedkommende egentlig kan komme inn å begå innbrudd pga. ingen stiller spørsmål om adgangskort eller autorisasjon for å komme inn på fabrikken. Vi har også opplevd at noen fikk med seg to kontainere selv om det var vakt til stede på lokasjon nr. 2, det sier kanskje litt om hvor naie vi nordmenn kan være. Den fysiske sikkerheten er noe begrenset pga. tillit. Fysisk sikkerhet kunne vært et tiltak for slike hendelser».

I tillegg til at dette blir nevnt, kommer det også frem at det har vært tyveri ved en annen anledning. I den situasjonen var det noen datamaskiner som ble stjålet. Etter denne hendelse ble det strengere rutiner på låsing av dører. En annen intervjuobjekt nevner også den fysiske sikkerheten, men fra hans ståsted er ikke denne et problem. Vedkommende har følgende utsagn:

«Den fysiske sikkerheten er god, uansett om det kommer uvedkommende er ikke de en trussel».

Til tross for dette erkjenner vedkommende at det ikke er gjort store endringer for å sikre fysisk tilgang eller verdier ytterligere.

5 Analyse

Dette kapittelet presenterer en analyse basert på de foregående kapitlene. Analysen retter søkelyset mot sosiale sikkerhetstiltak og sikkerhetshendelsen, der det undersøkes hvordan en SMB bygger bevissthet (cyber awareness). Kapittelet analyserer først sosiale sikkerhetstiltak strukturert i henhold til figur 2 av Hagen et al. (2008). Deretter blir det diskutert hvilke konsekvenser som medfølger ved begrenset forståelse for sosiale sikkerhetstiltak og høy tillit til IT-leverandør sett i lys av sikkerhetshendelsen. På bakgrunn av sikkerhetshendelsen og FPH AS sine sikkerhetstiltak, blir det diskutert jevnt i kapittelet om investering i teknologisk sikkerhetsløsning kan skape en ubalanse i det sosio-tekniske systemet.

5.1 Sosiale sikkerhetstiltak

I dette delkapittelet blir sosiale sikkerhetstiltak fra figur 2 av Hagen et al. (2008) analysert for å fremheve effekten av bevisstgjøring.

Den tradisjonelle tilnærmingen til informasjonssikkerhet fokuserer på teknologiske elementer og ikke på sosiale (Maltaji et al., 2019). Dette fører til et tydelig gap mellom det teknologiske og sosiale, hvor det ikke bringer frem felles optimalisering av deres løsninger. Teknologisk input til organisasjonen gir ikke nødvendigvis tiltenkt effekt, fordi sikkerheten er ikke bedre enn det svakeste leddet. Forskning og rapporter sier at mennesker er involvert i opptil 9 av 10 av sikkerhetshendelser og det danner dermed grunnlag for å si at mennesker er det svakeste leddet, samt en skjevfordeling mellom det teknologiske og sosiale. Dette kan være forstyrrende i den forstand at SMB-er ikke forstår effekten av teknologien på lang sikt, men ser på teknologi som en løsning på et midlertidig problem. Det er likevel ikke sikkert teknologi er løsningen da teknologi behandles av mennesker og det er menneskelig å gjøre feil.

HKK AS implementerte grunnleggende sikkerhetshygiene i FPH AS som ifølge Microsoft (2022) kan hindre 98% av alle dataangrep. Grunnleggende sikkerhetshygiene kan være en god løsning for mange bedrifter og er en forutsetning for å de øvrige trinnene i figuren til Hagen et al. (2008). På den andre siden kan effekten av den teknologiske sikkerhetsløsningen diskuteres da det tydelig fremkommer gjennom intervjuene at det er en manglende kompetanse på informasjonssikkerhet og tillit til teknologi og IT-leverandør blir for stor. Det blir dermed en utfordring i næringslivet at SMB-er stopper på det grunnleggende sikkerhetsnivået, noe som kan resultere i alvorlige sikkerhetsbrudd og datalekkasjer.

Det erkjennes gjennom studier og rapporter hvor kritisk SMB-er er for mange virksomheter, og kan i noen tilfeller være helt avhengig av en spesifikk leverandør. Flere organisasjoner uttrykker bekymring for SMB-er sin informasjonssikkerhet på grunnlag av at flere SMB-er føler seg mindre utsatt enn større organisasjoner. Det er en generell oppfatning at SMB-er ikke ser gevinsten av investering i informasjonssikkerhet og som følger av dette belyses ikke viktigheten av bevisstgjøring. HKK AS fremhever at dersom grunnleggende sikring på teknologi og mennesker er implementert så er det utrolig bra, og sier følgende:

«Kommer vi der hvor grunnleggende sikring på teknologi og mennesker er implementert, så har vi på en måte lykkes med SMB-er vi leverer tjenester til. Teknologien er lettest å selge, men er veldig budsjettavhengig. Når det kommer til å selge menneskelig trening, opplæring etc., så skjønner de hva det er, men de tror de er flink nok på dette og trenger derfor ikke kurs».

Ettersom HKK AS har en stor kundeportefølje innen teknologiske sikkerhetsløsninger, og siden FPH AS er en teknologisk avansert bedrift, settes der spørsmålstegn ved hvorvidt alle involverte parter forstår viktigheten av hvordan sosiale elementer kan påvirke informasjonssikkerheten. Det kommer frem gjennom intervjuene at IT eksperten fra tidligere ikke etterlot FPH AS i den ønskede tilstanden. Etter ny IT leverandør ankom ble det tydelig at det foregående arbeidet var for dårlig. Altså fremstår det som at figur 2. sine trinn ikke var viktige for vedkommende. Så er spørsmålet om de nye IT-leverandøren forstår viktigheten av trinnene. HKK AS har implementert grunnleggende sikkerhetshygiene for FPH AS, men dette betyr ikke at bedriften er sikret. Ifølge Hagen et al. (2008) er det mest effektive tiltakene de som følger etter de teknologiske. I de kommende delkapitlene blir FPH AS analysert ut ifra hvert enkelt trappetrinn fra figur 2. sett i lys av hvordan sosiale elementer kan påvirke informasjonssikkerheten.

Policy for informasjonssikkerhet

Hagen et al. (2008) presenterer i figur 2. effektiviteten av ulike tiltak for informasjonssikkerhet og i hvor stor grad de er implementert. Denne figuren samsvarer med det Ole og Dole forteller, da de sier at det teknologiske er ofte det enkleste å selge inn, men det blir vanskelig når man skal bevege seg videre utover de teknologiske tiltakene. Det viser seg også gjennom intervjuene med FPH AS at de ansatte kjenner til at de har en IT-leverandør som passer på, men svært få er kjent med at bedriften har en egen policy eller hvor den er. Dette tyder på to ting; at det ikke er noe spesifikk policy for informasjonssikkerhet eller at det er lite kjennskap til temaet. Som vil si at det er lav grad av bevissthet i forbindelse med informasjonssikkerhet i bedriften. Dette understøtter at implementeringen er lavere etter hvert som man beveger seg oppover fra det teknologiske grunnlaget.

Slik FPH AS fremstår gjennom intervjuene og etter samtalen med HKK AS er det ikke lagt noe vekt på de øvrige trinnene. Hagen et al. (2008) argumenterer for at trinnene i figuren må følge en logisk rekkefølge hvor et trinn må ligge til grunn før man kommer opp på neste trinn. Med andre ord så kan ikke FPH AS begynne med det sosiale elementet av informasjonssikkerhet før de formelle tiltakene er på plass. Dette kan stemme til en viss grad, men det ikke nødvendigvis slik at ansatte ikke kan tenke på sikkerhet selv om de ikke er kjent med policy. Det er tenkelig at det krever en grad av bevissthet for å starte og implementere de rette tiltakene.

Majoriteten av intervjuobjektene var ikke kjent med policy for informasjonssikkerhet, og av de intervjuobjektene som hadde mobilen lett tilgjengelig, klarte ikke å finne policyen i appen, hvor alt skal være lett tilgjengelig. Dersom ansatte ikke har tilstrekkelig kunnskap om informasjonssikkerhet samtidig som de er ukjent med policy for informasjonssikkerhet kan dette skyldes organisatorisk svikt. Det er god praksis ifølge ISO 27001:2022 å formidle informasjon om informasjonssikkerhet på tvers av organisasjonen og tilrettelegge for hver avdeling om hva som bør fokuseres på.

Baserte på intervjuobjektene sine svar er de lite bevisste på hva bedriften sin policy for informasjonssikkerhet er og om de i det hele tatt har en policy. Det blir blant annet svart at de ikke har dette, en mener de har fått e-post med litt informasjon, en annen sier det har blitt gitt muntlige beskjed, og andre forklarer at det ligger i håndboken deres eller i appen. Uavhengig om denne bedriften har god policy eller ikke så er det i liten grad kjent for de ansatte. Dersom tilfellet er at de har en policy for informasjonssikkerhet vil ikke dette ha god effekt når de ansatte ikke er bevisste på den (Soomro et al., 2016). Dersom bedriften ønsker å oppnå bedre sikkerhet og bli mer motstandsdyktige er det dermed klart at disse retningslinjene bør løftes frem og synliggjøres. Ved spørsmål rettet til IT-leverandør om de tilbyr policyer til kundene sine så svarer Ole følgende:

«Hvis jeg snakker om retningslinjer og ISO er det veldig tungt å få gjennom».

Dette gjenspeiler seg i det de ansatte sier, og dette har ikke vært prioritert i FPH AS. Som det fremkommer i litteraturen knyttes gjerne en del av problemet vedrørende policy hos SMB-er til de kostnadene som følger av en økt innsats utover de teknologiske sikkerhetsløsningene (Goucher, 2011; Shojaifar et al, 2020). Intervjuobjekt 3 sier i intervjuet at bedriften ikke er kjent for å være sparsom og velger ikke de billigste alternativene, men i dette tilfellet virker det slik. Her virker det som om de har valgt å gå for en teknologisk løsning, som kan vurderes som det fundamentale kravet hos bedrifter (Hagen et al., 2008). Dette er også det IT-leverandøren vurderer som grunnleggende sikkerhetshygiene, og den er ofte enklest for dem å selge. Etter dette kravet er tilfredsstilt opplever IT-leverandørene at kundene er tilfreds med det som har blitt gjort og tenker at dette er nok. Dette er en av fallgruvene litteraturen viser oss, nemlig at man nedprioriterer de menneskelige faktorene (Eminağaoğlu et al., 2009; Khando et al., 2021). På den ene siden kan det tenkes at mye av ansvaret ligger på FPH AS i forbindelse med investering, men det er også tenkelig den grunnleggende sikkerhetshygienen som HKK AS tilbyr bør inkludere sosiale elementer. I og med at dette er tiltak som øker effektiviteten til tidligere implementerte tiltak vil det være gunstig for både leverandør og bedrift. Dette vil kunne skape mer tillitt til HKK AS, samt forbedre omdømmet deres. På den andre siden kan det medføre dyrere sikkerhetsløsninger og potensielt dårligere salg for HKK AS.

Policy for informasjonssikkerhet kan være viktig av flere grunner. Når det ikke er definert roller og ansvar for informasjonssikkerhet kan skape uklarhet i virksomhetens forventninger til ansattes sikkerhetspraksis. Dette kan slå direkte ut på informasjonssikkerheten. Dersom det skulle vise seg å faktisk eksistere en policy for informasjonssikkerhet i FPH AS er det helt klart at den ikke er synlig. Det kan føre til ineffektive retningslinjer og kan slå negativt ut på organisasjonsmedlemmenes atferd, holdninger og plikt til overholdelse. Konsekvensene ved å ikke synliggjøre policy eller å ikke ha en policy, er at det kan resultere i manglende kunnskap og opplæring av ansatte. Dette kan føre til misforståelser blant ansatte som videre kan føre til utilsiktede hendelser. En annen konsekvens kan være at ansatte ikke har noe eierskap til hva som er god og hva som er dårlig atferd.

Policy er et styrende dokument og har til hensikt å informere leserne om strategi. Den skal skape et grunnlag for en helhetlig og strukturert tilnærming til informasjonssikkerhet på tvers av organisasjonen. Konsekvenser av å ikke ha en policy er at det ikke er en strategi for informasjonssikkerhet som står i stil med virksomhetens strategi. Samlet sett

er policy viktig for å beskytte virksomhetens informasjon, ettersom dokumentet tar for seg retningslinjer som er gjeldende for hele virksomheten. Det kan innebære å spesifisere standarder og setter grenser og ansvar for brukere av informasjons- og teknologiressurser.

Policy for informasjonssikkerhet kan bidra til å øke bevisstheten blant de ansatte og skape et miljø hvor alle ansatte på tvers av organisasjonen har en tilnærming til informasjonssikkerhet. Det kan bidra til å forebygge, oppdage, og gi informasjon om hvordan man kan respondere på sikkerhetshendelser. Den gir også grunnlag for å lage prosedyrer og kontroller, som er det neste trinnet i figur 2.

Prosedyrer og kontroll

Prosedyrer og kontroller innen informasjonssikkerhet tar for seg retningslinjer som har til hensikt å lede individuell og organisatorisk atferd. Retningslinjene blir utledet fra bedriftens policy for informasjonssikkerhet. Basert på figur 2 har prosedyrer og kontroll en høyere vurdert effektivitet på informasjonssikkerheten enn policy. Dette er fordi de er med på å sikre korrekt oppfølging av det som står i policyen.

Det er en forutsetning at styrende dokumenter blir synliggjort og faktisk blir brukt, ettersom risikoen ved ubrukte dokumenter kan redusere effekten av retningslinjer og veiledning. Som det fremkommer gjennom intervjuene fremstår det som at ingen ansatte egentlig vet hva som er akseptabel praksis og hvordan informasjon kan bli håndtert på en sikker måte. Dette kan være svakheter med styrende dokumenter fordi sosiale sikkerhetstiltak ikke blir synliggjort og fremhevet i virksomheter, og kan potensielt resultere i sikkerhetsbrudd og datalekkasjer. Dette kan skje når brukere ikke lagrer informasjon sikkert. Eksempelvis ved at de lagrer dem lett tilgjengelig for eget bruk i åpne mapper, på skrivebordet, i ulåste skuffer, eller på telefon. Da vil dokumenter som forklarer hvordan man foretar seg sikker lagring være nyttig.

Gjennom intervjuene fremkommer det at sikkerhetshendelsen oppsto ved at en tredjepart klarte å gjette seg frem til rett passord. Dette kan tyde på at noen av de ansatte (1) ikke er kjent med policy for passord, (2) policy for passord eksisterer ikke, eller (3) lav kompetanse på hva som er et sterkt passord. Sistnevnte tyder på mangel av prosedyrer og kontroll. I en policy vil det kanskje stå ansatte skal ikke klikke på ukjente lenker eller alle ansatte skal benytte sterke passord. Denne informasjonen har blitt utgitt til de ansatte på ulike måter, men ikke gjennom en policy. Dermed er det lite trolig at FPH AS har innført eller utledet prosedyrer og kontroller basert på en policy som skal sikre at ansatte gjør ting riktig i forbindelse med ukjente lenker eller gode passord.

Det er ulike forutsetninger blant ansatte for hvordan de håndterer teknologi og om de gjør det på en sikker måte. Dette kan være grunnet alder, interesse eller arbeidsoppgaver. En som ikke håndterer teknologi i sin arbeidshverdag vil ikke måtte ta like store hensyn til dette i det daglige, men det er dog viktig at vedkommende er klar over informasjonssikkerhetspraksis. Dersom det kommer en dag hvor vedkommende må bruke teknologi som f.eks. en pc, så er vedkommende en innside trussel for utilsiktede hendelser. I FPH AS er det ansatte som ikke bruker like mye teknologi i sin hverdag. Prosedyrer og instruksjoner vil kunne veilede dem til hvordan en oppgave skal løses på korrekt vis. Dersom det er ansatte med gode teknologiske ferdigheter vil det i det minste fungere som en påminnelse om god praksis og atferd.

Prosedyrer og kontroller kan være avgjørende for informasjonssikkerhet. Det kan tenkes at de sosiale elementene som inngår i informasjonssikkerheten må bli evaluert

kontinuerlig. Det er fordi retningslinjene som er dokumentert gjerne beskriver prinsipper, krav og forventninger for hvordan man kan bevare informasjonsverdier trygt. Prosedyrer og kontroller er direkte avledet fra retningslinjene og kan bidra til å skape god organisatorisk og individuell atferd. I FPH AS sin situasjon virker det som det er dårlig atferd for informasjonssikkerhet. Argumentet for den dårlige atferden blir forankret i at intervjuobjektene i FPH AS ikke hadde noen spesifikke holdninger til risiko som kan dermed påvirke organisasjonens informasjonssikkerhet.

Ved uklar policy for informasjonssikkerhet kan det resultere i dårlige prosedyrer og kontroller som kan skape usikkerhet blant de ansatte. Ettersom det ikke er noen definerte retningslinjer som informerer brukere av hva som for eksempel er et sterkt passord, kan det føre til at ansatte lager et passord på egenhånd. Ansatte kan dermed stå i fare for å lage passord som de tror er sterke, men egentlig er de bare kompliserte, svake og upraktiske. Selv om intervjuobjektene er klar over hvor viktig det er med et sterkt passord, er det ingen prosedyrer som forteller dem hva som faktisk er et sterkt passord.

Uten prosedyrer og kontroller kan det bli utfordrende for de ansatte å håndtere informasjonsverdier sikkert ettersom det tyder på at det ikke er noen norm eller følelse av ansvar. Det kan også tenkes at handlinger ikke blir utført korrekt på grunn av dårlige rutiner. Et eksempel er sikkerhetshendelsen som skjedde i august 2021, som kan tyde på manglende eller uklare retningslinjer i forbindelse med passord.

Det fremkommer under intervjuene at alt er tilgjengelig i appen, men av de intervjuobjektene som prøvde å søke på 'informasjonssikkerhet' fant ingenting som omhandlet informasjonssikkerhet. Prosedyrer og kontroller har til hensikt å informere brukerne om hvordan man kan samhandle sikkert mellom mennesker og teknologi. Effekten av å ha tydelige og presise prosedyrer kan påvirke organisasjonen i den grad at informasjonssikkerheten forbedres ved rett bruk av de sosiale elementene.

Samlet sett kan prosedyrer og kontroller være svært sentrale elementer for å øke nivået på informasjonssikkerhet. På den ene siden bidrar prosedyrer og kontroller til å operasjonalisere retningslinjer og tilrettelegger for god organisatorisk og individuell atferd. På den andre siden kan det være vanskelig for SMB-er å bruke prosedyrer og kontroller på grunn av begrensede ressurser og kunnskap, både økonomisk og menneskelig, og mangler ofte et dedikert informasjonssikkerhetsteam.

Verktøy og metoder

Verktøy og metoder er et sentralt trinn og en forutsetning for å skape bevissthet i organisasjonen, men det krever at de tidligere trinnene er implementert. Som det fremkommer av hagen et al. (2008) omfatter det både proaktive og reaktive tiltak for å ivareta organisasjonens informasjonssikkerhet.

Det en generell oppfatning om at SMB-er har begrenset forståelse for viktigheten av informasjonssikkerhet. Dette kan dermed skape utfordringer for proaktive og reaktive tiltak for å ivareta sikkerheten. Blant dem er hendelseshåndtering, og gjennom intervjuene fremstår det som at dette ikke er noe ansatte i FPH er kjent med. Basert på manglene i de foregående trappetrinnene i figur 2 er det ingenting som tyder på at ansatte vet hva de skal gjøre dersom en hendelse inntreffer. Intervjuobjekt 3 har et utsagn som tyder på dette:

«Foreslår dataangrep øvelser som på samme måte som brannøvelser. Kanskje beredskapsplaner burde kommet inn».

For forskerne fremsto det som at dette var en åpenbaring for vedkommende. Det kan indikere at FPH AS ikke har noe nedskrevet plan for hvordan de skal håndtere en eventuell ny hendelse.

I forbindelse med metoder og verktøy blir det i intervjuet snakket om avvik og rapportering. Intervjuobjektene blir spurt om de har et system for å rapportere feil eller mangler. Intervjuobjekt 1 forteller at FPH AS har satt seg som mål at de ansatte skal rapportere inn 1500 forbedringspunkter i løpet av året. Takhøyden for å rapportere er lav og hver minste feil kan bli meldt inn. Intervjuobjekt 3 informerer om at det er en bonusordning dersom de klarer målsetningen. Dette fremstår som en god løsning og noe som bør gjøre det lettere å rapportere feil vedrørende sikkerhet. Utfordringen med løsningen er at det ikke er noen klare prosedyrer for rapportering.

FPH AS har et rapporteringssystem i appen sin, og intervjuobjekt 3 mener den fungerer utmerket og er brukervennlig. Et problem vedørende rapportering og hendelseshåndtering er hvorvidt de ansatte er klar over at en hendelse faktisk er en hendelse. Eller om de klarer å identifisere et sikkerhetsproblem dersom det skulle oppstå. Dette kan bli eksemplifisert gjennom phishingtesten som FPH AS gjennomførte. Resultatet av denne var at det bare var en person som klikket på lenken i e-posten. Dette fikk de ansatte skryt for, men det som ikke kommer frem er hvor mange som rapporterte e-posten. Dette ble ikke vektlagt, og det viser at kanskje ikke så mange egentlig visste at det var phishing eller at det var noe som måtte bli rapportert. Det er bra at systemet er på plass for å melde fra, men dersom de ansatte ikke vet når og hva de skal melde har det liten hensikt.

Intervjuobjektene ble spurt om hva de ville gjort dersom de fikk vite at noe brøt retningslinjer. Noen av intervjuobjektene svarer at de ville meldt fra til nærmeste leder, andre svarer at de ville konfrontert personen, en intervjuobjekt ville sendt bekymringsmelding. Ingen av disse svarene er feil, men det illustrerer utydeligheten. Ut i fra figur 2 så må policy og prosedyrer for informasjonssikkerhet være på plass før rapportering. Dersom disse ikke er på plass vil det være utfordrende for de ansatte å gjenkjenne og rapportere sikkerhetsbrudd. Dersom ingen eller bare et fåtall rapporterer hendelser svekker dette datagrunnlaget og man mister dermed verdifull data for å få innsikt i trusselbildet. Det tyder på at det er begrenset kommunikasjon, og dårlige holdninger til informasjonssikkerhet innad virksomheten. Dette begrenser FPH AS sin evne til å identifisere og evaluere mulige trusler og sårbarheter internt.

Intervjuobjektene ble spurt om de visste hvilke trusler og sårbarheter virksomheten deres kunne være utsatt for. Flere av intervjuobjektene svarte hacking og phishing, men det virker ikke som det kjenner til noe utover dette. Basert på spørsmål angående sikkerhetshendelsen er det samme tendensene tydelige. Det er ingen som vet hva som har skjedd og det tyder på dårlig informasjonsflyt i FPH AS innen informasjonssikkerhet. Det er ikke blitt kommunisert nåværende trusler, ei heller hva som forårsaket sikkerhetshendelsen.

Risikoanalyse er et av elementene som går under verktøy og metoder, og kan være avgjørende for å bevisstgjøre de ansatte for hvilke sårbarheter og trusler de er utsatt for. Som et proaktivt tiltak skaper risikoanalyse et godt bilde av hva man bør være observant

på, samtidig må analysen formidles på tvers av organisasjonen på en forståelig måte. Sett i lys av FPH AS sin nåværende situasjon virker det ikke som det er gjort noen form for risikoanalyse, sårbarhet- eller trusselvurdering. Det forankres i at ingen av intervjuobjektene hadde noen spesifikke svar på hva de var utsatt for eller hvordan man kunne forårsake brudd på sikkerheten. På den andre siden kan det hende FPH AS faktisk har utført risikoanalyse eller kjøpt tilsvarende tjeneste av deres IT-leverandør. Dersom det har blitt gjort har det ikke kommet godt frem, og effekten av analysen kan tenkes å være minimal. Dette kan tyde på svak eller ingen norm for informasjonssikkerhet i FPH AS.

Det fremkommer at SMB-er er svært attraktive mål for trusselaktører. Implementering av verktøy og metoder som f.eks. risikohåndtering og rapportering kan være sentrale elementer som gjør at de sosiale sikkerhetstiltakene imøtekommer teknologiske sikkerhetsløsninger, og det endrende digitale trusselbildet. Disse tiltakene kan bidra til å forbedre informasjonssikkerheten og balansere de sosiale og tekniske elementene. I neste delkapittel blir oppmerksomheten rettet mot å skape en dypere forståelse for det siste trinnet, bevisstgjøring.

Bevisstgjøring

Det fjerde og siste trinnet, bevisstgjøring, ansees som det mest effektive trinnet og kan være av høy relevans for alle organisasjoner. Dette trinnet retter søkelyset mot hvordan økt bevissthet kan bidra til å balansere ujevnheten som kan ha oppstått da FPH AS investerte i den teknologiske sikkerhetsløsningen. Bevisstgjøring bygger på de foregående trinnene og omfatter en rekke tiltak som bidrar til å gjøre ansatte bevisst på deres handlinger som kan påvirke virksomhetens informasjonssikkerhet.

Bevisstgjøring og god informasjonspraksis innebærer at det skjer en endring i holdninger og vaner hos individer (Tsohou, 2015). En viktig endring hos de ansatte kan være å sørge for at alle har holdningen om at de hver for seg har et ansvar for at sikkerheten til FPH AS blir ivaretatt. Det kan være individuelt hvor stor grad av ansvar hver enkelt ansatt skal ha. I forbindelse med ansvar ble samtlige intervjuobjekter spurt om de hadde noe ansvar i med tanke på informasjonssikkerhet. Majoriteten svarte at de ikke har noe ansvar. Dette gjelder også intervjuobjekt 5, men vedkommende la også til følgende:

«Men alle har vel et eget ansvar for dette».

Det som er interessant med dette utsagnet er at alle faktisk har et ansvar for informasjonssikkerhet i sin arbeidshverdag. Gjennom intervjuene blir det tydelig at intervjuobjektene har begrenset forståelse for sine egne roller og ansvar for informasjonssikkerhet. Slik statusen er i dag, basert på resultatene i studiet, er det ikke et stort fokus på aktiviteter for å bevisstgjøre de ansatte om informasjonssikkerhet.

Majoriteten av intervjuobjektene var ikke bevisst over hvordan de kan bidra til å forbedre informasjonssikkerheten. Fra intervjuene fremkommer det at majoriteten av de ansatte ønsker en form for trening og kompetanseheving for å kunne bidra til å forbedre informasjonssikkerheten. Dette er et ukjent område for mange og det krever dermed et kompetanseløft hos de ansatte i FPH AS. Gjennom intervjuer med ansatte i FPH AS kommer det frem at kompetansen og kjennskapen til dette temaet er relativt begrenset.

Dette kan skyldes manglende bevisstgjøring og trening. Ingen av intervjuobjektene sier de har fått trening i forbindelse med sikkerhet. Intervjuobjekt 3 har følgende utsagn:

«Man får trening til det som er relevant for jobben».

Dette åpner for spørsmål om hva som er relevant for jobben. Ansatte i FPH AS bør ha grunnleggende ferdigheter innen sikkerhet. Det er fordi det er sannsynlig at de ansatte vil havne i situasjoner som krever en grunnleggende kompetanse. Et eksempel er når forskerne kom inn på lokasjon 1, da var det ingen som spurte hvem de var og hvorfor de var der. Dermed krever det at de ansatte har kompetanse og er bevisst på både fysisk og digital sikkerhet.

En utfordring for SMB-er er den økonomiske prioritering som må til for at trening og kompetanseheving skal vektlegges. I likhet med bevisstgjøring opplever de at det er godt nok med den teknologien de har brukt penger på. Intervjuobjekt 3 mener dette bør vektlegges i større grad og være en del av budsjettet til FPH AS.

Flere av intervjuobjektene forteller at det er gode muligheter for kompetanseheving i FPH AS, og at de får tilrettelagt for dette om de selv ønsker. Dette tyder på at bedriften er interesserte i at ansatte skal få øke sin kompetanse, men hovedsakelig på andre områder enn informasjonssikkerhet. SMB-er har ofte begrensede ressurser og det kan derfor være utfordrende å allokere ressurser for å bidra til ansattes kompetanseheving og bevisstgjøring. Alternativt, fremfor å allokere ressurser direkte i ansatte, så kan det bli investert i de foregående trinnene. Det er fordi effekten av bevisstgjøring utgjør større nytte ved at de foregående trinnene er implementert. Dette vil gjøre at de ansatte i større grad vil være kapable til å se trusler og sårbarheter og reagere på dem.

På et generelt grunnlag er det ikke noen rutiner i FPH AS for å dele kompetanse man har tilegnet seg gjennom trening og andre aktiviteter som fremmer kompetanseheving eller bevisstgjøring. Det er noe ulike svar hos intervjuobjektene på dette temaet, men essensen av svarene er at kompetanse blir delt dersom kolleger spør om det, og sjeldent på eget initiativ. Ofte må det være en interesse fra ansatte og kolleger for at kunnskap skal bli delt. Dette gjelder ikke bare i forbindelse med endt aktivitet eller kurs, men også dele erfaringer som kommer av ulike hendelser. Det blir nevnt av intervjuobjekt 5 at angrepet var siste runde hvor FPH AS ansatte ble bevisstgjort på informasjonssikkerhet og Dole fra IT-leverandørene har følgende utsagn:

«Jeg tror enkelte bedrifter har møtt veggen for nye løsninger, det må liksom en hendelse til for at de skal forstå».

Det kan tyde på at dette er tilfellet for FPH også. Det virker som sikkerhet er utrolig viktig på tidspunktet hvor man står midt i en hendelse, hvilket det er, men at viktigheten avtar gradvis etterhvert som tiden går. Truslene avtar derimot ikke. En trusselaktør tenker ikke at denne bedriften må få hvile litt nå siden de akkurat har blitt angrepet. I mange tilfeller er det tilfeldig hvem som blir angrepet, eksempelvis gjennom phishing e-poster. Da er det viktig at man alltid har gode rutiner som minimerer sjansen for at slikt skjer på nytt.

Uten bevisstgjøring om informasjonssikkerhet kan det antas at flere av de ansatte i FPH AS har lik eller mindre forståelse for hvilke sårbarheter og trusler de kan være utsatt for. Ettersom de foregående sosiale tiltakene er hoppet over i FPH AS er det ikke usannsynlig at det kan skape uklarhet blant ansatte om hva som er forventet og god sikkerhetspraksis, samt hvordan sårbarheter kan håndteres.

De ansatte ikke blir informert om det digitale trusselbildet og kan føre til uaktsomhet. Det innebærer at ansatte tar beslutninger som strider mot god informasjonssikkerhetspraksis. Den manglende kunnskapen blant de ansatte kan føre til at de ikke tar nødvendige forholdsregler, som kan være å sikkerhetskopiere informasjon, og ikke skrive inn kontoinformasjon på lenker i e-poster. Det kan tyde på at det er manglende oppmerksomhet som kan slå ut på ansattes ansvarlighet ettersom fåtallet har noen tilnærming til god praksis for informasjonssikkerhet.

5.2 Sikkerhetshendelsen

I dette delkapittelet blir sikkerhetshendelsen og lærdommen fra den diskutert.

Hendelsen som oppsto på i august 2021 virker å være noe alle kan erindre. Likevel virker det som om det er begrenset med erfaring og kunnskap de tar med seg fra dataangrepet. På spørsmål om de husker eller vet hva som var årsaken til hendelsen svarer alle utenom to intervjuobjekter at de ikke vet hva som var årsaken til dataangrepet. Intervjuobjektene som tror de vet årsaken til hendelsen peker på phishing-, passord-, og bruteforce-angrep.

Intervjuobjektene sier at det ble gitt lite eller ingen informasjon om dataangrepet. Ole fra HKK AS forteller at det var vanskelig å få kontakt med FPH AS da de skulle presentere rapporten som var utarbeidet i forbindelse med sikkerhetshendelsen. HKK AS har som policy å formidle slike rapporter til alle selskaper det gjelder. Når de skulle presentere rapporten for FPH AS ble de ignorert. Ole poengterer at det kan være utfordrende å forstå tekniske rapporter, for ikke-tekniske personer.

HKK AS forteller at det i starten var veldig lett å få gjennomslag for de forslagene og løsningene de kom med, men etter hvert ble det vanskeligere. Det virker dermed som at FPH AS så et virkelig behov for hjelp under hendelsen, men etter hvert som hendelsen ble fikset og systemene var oppe igjen, så var ikke sikkerhet et like viktig tema lenger. Dermed ble det aldri gjort noen skikkelig gjennomgang av hendelsen.

På bakgrunn av dette kan det tyde på at, (1) lederne ikke har konkret informasjon om hendelsen, (2) ledelsen ser ikke behovet for dypere forståelse for hendelsen, eller (3) ledelsen ser ingen poeng i å dele informasjonen med ansatte fordi de ikke ser effekten av det. Dette skaper en oppfatning om at FPH AS har begrenset forståelse for informasjonssikkerhet. Siden FPH AS er en innovativ og lærende bedrift, kan det antas at dette gjelder flere SMB-er og ikke bare FPH AS.

På den ene siden kan det hende at FPH AS ikke ser gevinsten i å investere ytterligere i informasjonssikkerhet ettersom de har implementert grunnleggende sikkerhetshygiene. På den andre siden kan det tenkes at ledelsens oppfatning av informasjonssikkerhet er så begrenset at de ikke forstår eller ikke vil forstå konsekvensene av kortsiktige løsninger på et utbredt problem. Den generelle oppfatningen om at SMB-er har begrenset forståelse for viktigheten av informasjonssikkerhet kan tenkes å gjelde FPH AS.

Selv om selskapet ikke led store økonomiske tap, og bare gikk glipp av et skattefunn på en million kroner, virker det ikke som at informasjonssikkerhet er av betydning for dem. Likevel er det lite som har blitt gjort i ettertid av sikkerhetshendelsen i form av deling av erfaringer og refleksjon rundt det som skjedde.

Ved en gjennomgang av en slik hendelse vil de kunne reflektere over mulige årsaker, hva de kan bli bedre på og hva ansatte kan bidra med for å forbedre sikkerheten. På spørsmål om hva de lærte av hendelsen svarer intervjuobjekt 1:

«Lært at sånt skjer».

Det er ikke feil å si at sånt skjer, for det gjør det, men det handler om hva man kan gjøre for å forhindre at slike hendelser ikke skal inntreffe på nytt. Av hendelsen er det tenkelig at mange opplevde hendelsen ulikt, mange så konsekvensene av et brudd, og ble i ulik grad påvirket.

FPH AS har ikke gått gjennom hendelsen i plenum eller reflektert rundt den i ettertid. En grunn til at dette burde blitt gjort er at det kunne vært et godt utgangspunkt til å finne rotårsaker, og samtidig skape bevissthet. Øvelser med gjennomgang og refleksjon av hendelsen kunne gitt FPH AS en mulighet til å høre ansatte sine opplevelser og erfaringer. De kunne dermed kartlagt holdninger og tanker ansatte har rundt informasjonssikkerhet. En slik øvelse kunne i seg selv vært bevisstgjørende, samt at de ville fått luket ut feil og tatt lærdom. Dette ville potensielt ha redusert sjansen for en lignende sikkerhetshendelse eller konsekvensene av den.

Det er merkverdig at ingen har fått informasjon om hva som kan gjøres annerledes, eller forbedres. Ingen av intervjuobjektene vet hva som var årsaken til hendelsen, og dette sier noe om interessen til å forbedre seg på området. Siden FPH AS er et høyteknologisk selskap og deltar i flere forskningsprosjekter, er det rart at de ikke har bedre forståelse for informasjonssikkerhet. På tiden etter hendelsen har de ikke foretatt seg noen ytterligere tiltak, og eneste de har lært er at sånt skjer.

I intervjuet med HKK AS forteller Dole at det ikke er uvanlig at SMB-er har en tankegang som får dem til å tro at ingen vil rette et dataangrep mot dem, og sier følgende:

«Vi blir ikke angrepet, det skjer ikke oss».

Denne holdningen viser FPH AS også. Forskjellen på dem og mange andre SMB-er er at FPH AS har gjennomgått en sikkerhetshendelse, og burde vite bedre basert på erfaring. Dette kan også tyde på en stor tillit IT-leverandøren og usikkerhet vedrørende sitt eget ansvar.

Det kan være utfordrende for SMB-er med begrenset forståelse for informasjonssikkerhet å vite hva som er gode sikkerhetsløsninger. I forkant av dataangrepet i august 2021 mottok FPH AS en 10-punktliste fra IT-eksperten, der hensikten var å styrke sikkerheten deres. Uten nok kompetanse og forståelse på område kan det være lett å gå god for rådene man får, og det kan skape en uberettiget tillit til eksperter.

Tillitten FPH AS utviste til eksperten og 10-punktslisten som ble leid inn virker å ha vært veldig stor. Basert på intervjuene med FPH AS var 10-punktslisten implementert, noe som ifølge dem gjorde at sikkerhetsbruddet ble mindre alvorlig enn det kunne blitt. Dette gjorde at de handlet i god tro om at listen ble implementert korrekt, men det virker ikke å være tilfellet i det hele tatt. HKK AS forteller i motsetning til FPH AS at listen var av liten betydning, og dermed fremstår ikke tilliten til eksperten som berettiget.

FPH AS, med sin lave kompetanse på området, fikk umiddelbart ansvaret for implementering av punktene lagt over på seg. Med lav kompetanse er det ikke gode forutsetninger for at dette blir gjort korrekt eller etter beste praksis. Som IT-ekspert er vedkommende mest sannsynlig kjent med SMB-er sitt forhold til informasjonssikkerhet, og derav også den manglende kompetansen og forståelsen. Ved å etterlate dem til seg selv med kun en 10-punktsliste å ta stilling til tyder det på at eksperten heller ikke har forstått informasjonssikkerhet og jobber ikke etter beste praksis).

Det er tenkelig at IT-eksperten mest sannsynlig er kjent med SMB-er sitt forhold til informasjonssikkerhet, og derav også den manglende kompetansen og forståelsen. Med lav kompetanse er det ikke gode forutsetninger for at dette blir gjort korrekt eller etter beste praksis. FPH AS, med sin lave kompetanse på området, fikk umiddelbart ansvaret for implementering av punktene lagt over på seg. Ved å etterlate dem til seg selv med kun en 10-punktsliste å ta stilling til tyder det på at eksperten heller ikke har forstått informasjonssikkerhet og jobber ikke etter beste praksis. På en annen side, kan det være at FPH AS har undervurdert viktigheten å investere.

Basert på det FPH AS sier var 10-punktslisten implementert og tatt hensyn til, men ifølge HKK AS var den ikke det. HKK AS forklarer at 10-punktlisten ikke var nyttig i forhold til angrepet, fordi ingen av punktene verken så ut til å være implementert eller evaluert. Dette viser at det er liten kompetanse på området internt i FPH AS, men det kan også tyde ansvarsfraskrivelse fra tidligere IT-ekspert.

Konklusjon

Forskningsprosjektet har rettet søkelyset på hvordan SMB-er kan bygge cyber awareness gjennom et case studie med FPH AS og HKK AS for å undersøke SMB-er sin tilnærming til informasjonssikkerhet. Bevisstgjøring er en subjektiv oppfatning og kan oppfattes forskjellig fra organisasjon til organisasjon. Basert på litteratur og bransjeerfaringer som beskriver bevisstgjøring, utviklet forskerne spørsmål som kunne identifisere ansatte sin bevissthet og kompetanse sett i lys av informasjonssikkerhet i FPH AS. Gjennom forskningsprosjektet ble det funnet at majoriteten av intervjuobjektene i FPH AS hadde ingen eller liten forståelse for viktigheten av sikkerhet. De var heller ikke klar over konsekvensene dårlig sikkerhet medfører.

På en annen side var det en forventning at intervjuobjektene i FPH AS hadde bedre tilnærming til informasjonssikkerhet i forhold til hva de faktisk hadde. Det er fordi FPH AS er en teknologisk avansert bedrift der det var en oppfatning om at de hadde bedre forutsetninger til å lykkes med informasjonssikkerhet enn andre SMB-er, men feiler likevel. Spørsmålene rettet søkelyset mot intervjuobjektene sin kompetanse, bevissthet, kjennskap til policy og prosedyrer, og hvordan de opplevde sikkerhetshendelsen da den inntraff og i etterkant.

Det viste seg at majoriteten at av intervjuobjektene ikke hadde kjennskap til policy for informasjonssikkerhet, og en uenighet blant dem om det faktisk eksisterer en policy. Uten policy er det sannsynlig at prosedyrer og kontroll, samt verktøy og metoder ikke eksisterer sett i lys av informasjonssikkerhet. Hensikten med de sosiale sikkerhetstiltakene er at de skal utvikle ansatte sine holdninger, kompetanse og atferd for å fremme god sikkerhet – noe som ikke prioriteres.

De har siden sikkerhetshendelsen bevart tilliten til teknologi og leverandør, uten å innføre tiltak utover dette. Dette er en bedrift som har deltatt i flere forskningsprosjekter og er opptatt av læring og utvikling, men sikkerhetshendelsen har ikke blitt brukt til læring. Utenom investering og implementering av teknologiske sikkerhetsløsninger, sitter ikke bedriften og de ansatte igjen med noe spesifikk lærdom. De har det teknologiske på plass, men det holder ikke for en så kompetent bedrift som FPH AS å si at dette er nok. Dette viser at denne SMB-en ikke har skjønt informasjonssikkerhet.

Resultatet i forskningsprosjektet betyr ikke nødvendigvis at de ansatte i FPH AS har manglende kompetanse og bevissthet, men i forhold til hvordan intervjuobjektene svarte på spørsmålene viser det til lav kompetanse og bevissthet. Det kan være vanskelig å få frem intervjuobjektene sin tilnærming til sikkerhet gjennom et casestudie over 4 måneder og intervjusesjoner på 30 minutter. Det kan også være at intervjuobjektene kan mer enn de fikk vist på en kort sesjon, eller at forskerne ikke har klart å spille dem gode under intervjuet.

Sett fra et sosio-teknisk-perspektiv skaper de manglende sosiale tiltakene en klar skjevfordeling og felles optimalisering blir ikke oppnådd. Det teknologiske systemet er i FPH AS sitt tilfelle forbedret, men kan ha skapt en negativ effekt som manifesterer seg i form av tillit til teknologi og tredjeparter.

Videre forskning

Gjennom arbeidet i dette forskningsprosjektet har det dukket opp nye spørsmål som kan tilføre og belyse temaet ytterligere. Det første er om funnene i forskningsprosjektet representativt for SMB-er. I denne undersøkelsen har det bare blitt sett på en bedrift, men det kan være fruktbart for videre studier å undersøke et bredere grunnlag med flere SMB-er. Det andre spørsmålet som oppstår er om trappen illustrert i figur 2 gir god mening eller om det bare er en tankemodell. Det vil det være nyttig å gå inn i bedrifter og implementere tiltak som mangler, se om bedrifter må følge den logiske rekkefølgen for full effekt, om det er unntak, og å sammenligne bedrifter med ulik tilnærming.

Til slutt er det ett funn som ikke blir diskutert i analysen, men som fremkom av våre observasjoner. På lokasjonene ble det observert tegn til dårlig fysisk sikkerhet, og da spesielt på lokasjon 1. Fysisk sikkerhet er et viktig aspekt av informasjonssikkerhet ettersom uautoriserte personer kan gjøre skade på fysiske enheter og mennesker, og kan fungere som et første fotfeste for å utføre et dataangrep på et senere tidspunkt. Denne delen av informasjonssikkerhet vektlegger ikke dette forskningsprosjektene. For videre forskning vil det dermed være interessant å studere i hvilken grad fysisk sikkerhet blir prioritert av SMB-er.

Referanser

Amankwa, E., Loock, M., & Kritzinger, E. (2014, December). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 248-252). IEEE.

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management Decision*, 35(6), 452–463. https://doi.org/10.1108/00251749710173823

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Blom, I. A., Rørvik, J., Titlestad, K. (2022, 6. mars). *Menneskelige sårbarheter fører til økt trusselbilde*. Digi.no. https://www.digi.no/artikler/debatt-cybertruslene-mot-internettilkoblede-biler-vil-vokse-kraftig-i-arene-fremover/532236

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory. *MIS Quarterly*, 1(4), 11–28. https://doi.org/10.2307/249019

Budzak, D. (2016). Information security – The people issue. *Business Information Review*, 33(2), 85–89. https://doi.org/10.1177/0266382116650792

Center for Internet Security. (2022, september). *Hack the human: End-User Training and Tips to Combat Social Engineering*. Hentet 3.april 2023 fra https://www.cisecurity.org/insights/newsletter/hack-the-human-end-user-training-and-tips-to-combat-social-engineering

Chaudhary, S., Gkioulos, V. & Goodman, D. (2023). Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources. I (s. 97-115) (Lecture Notes in Computer Science). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-25460-4_6

Cragg, P., Caldeira, M., & Ward, J. (2011). Organizational information systems competences in small and medium-sized enterprises. *Information & Management*, 48(8), 353–363. https://doi.org/10.1016/j.im.2011.08.003

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Crowdstrike. (2022, 1. juni). *What is a brute force attack?* Hentet fra What is a Brute Force Attack? Definition & Examples – CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/brute-force-attacks/

Davis, M. C., Challenger, R., Jayewardene, D. N. W. & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Appl Ergon*, *45*(2), 171-180. https://doi.org/10.1016/j.apergo.2013.02.009

Downey, B. (2020, 12. desember). *Why SMBs are high risk for cybersecurity threats in 2021*. Connectwise.com. https://www.connectwise.com/blog/cybersecurity/why-smbs-are-high-risk-for-cybersecurity-threats-in-2021

Dr. Petric, G., & Roer, K. (2018). *To measure security culture*. CLTRe North America. Hentet fra WP-to-measure-security-culture-a-scientific-approach.pdf (knowbe4.com).

Eminağaoğlu, M., Uçar, E. & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information security technical report*, *14*(4), 223-229. https://doi.org/10.1016/j.istr.2010.05.002.

Europakommisjonen (2022). Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersercurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022) 454 final)). Europa-Kommisjonen. Hentet fra EUR-Lex - 52022PC0454 - EN - EUR-Lex (europa.eu).

Europakommisjonen, Research, D.-G. f., Innovation, Breque, M., De Nul, L. & Petridis, A. (2021). *Industry 5.0: towards a sustainable, human-centric and resilient European industry*. Publications Office of the European Union. https://doi.org/doi/10.2777/308407

Europakommisjonen, Small, E. A. f. & Enterprises, M.-s. (2020). *Supporting specialised skills development: big data, Internet of things and cybersecurity for SMEs: executive summary*. Publications Office. https://doi.org/doi/10.2826/84436.

European Union Agency for Cybersecurity (Enisa), & e-Governance (EGA). (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies*. DOI 10.2824/363629.

European Union Agency for Cybersecurity (Enisa). (2010). The new users' guide: How to raise information security awareness. *European Network and Information Security Agency (ENISA).*

European Union Agency for Cybersecurity (Enisa). (2022). *Enisa threat landscape 2022*. DOI: 10.2824/764318.

European Union Agency for Cybersecurity (Enisa). (u.å). *SME Cybersecurity*. Enisa. https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

Evans, M. G., He, Y., Yevseyeva, I. & Janicke, H. (2019). Published incidents and their proportions of human error. *Information and computer security*, *27*(3), 343-357. https://doi.org/10.1108/ICS-12-2018-0147

Forbes. (2022). *Cybersecurity awareness: What it is and how to start*. Forbes. Hentet fra Cybersecurity Awareness: What It Is And How To Start – Forbes Advisor

Getastra. (April, 2023). *51 small business cyber attack statistics 2023 (and what you can do about them)*. Getastra. Hentet fra https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/

Goucher, W. (2011). Do SMEs have the right attitude to security? *Computer fraud & security*, *2011*(7), 18-20. https://doi.org/10.1016/S1361-3723(11)70075-6

Hagen, J. M., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures, *Information management & computer security*, 16(4), 377-397.

Halvorsen, K. (2008). *Å forske på samfunnet: En innføring i samfunnsvitenskapelig metode* (5. utg. ed.). Oslo: Cappelen akademisk forl.

Hansche, S. (2001). Designing a Security Awareness Program: Part 1. Information Systems Security, 9(6), 1–9. https://doi.org/10.1201/1086/43298.9.6.20010102/30985.4.

Heidt, M., Gerlach, J. P. & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information systems frontiers*, *21*(6), 1285-1305. https://doi.org/10.1007/s10796-019-09959-1

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2016). Introduksjon til samfunnsvitenskapelig metode (5. utg.). Abstrakt.

Khando, K., Gao, S., Islam, S. M. & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267.

Kumar, S., & Mallipeddi, R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, 31(12), 4488-4500.

Leedy, P. D., Ormrod, J. E. & Leedy, P. D. (2021). *Practical research: planning and design* (Twelfth edition, global edition. utg.). Pearson Education.

Malatji, M., Von Solms, S. & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and computer security*, *27*(2), 233-272. https://doi.org/10.1108/ICS-03-2018-0031

Mark, M. S., Tømte, C. E., Næss, T., & Røsdal, T. (2019). Leaving the windows open – økt mangel på IKT-sikkerhetskompetanse i Norge. Norsk sosiologisk tidsskrift, 3(3), 173–190. https://doi.org/10.18261/issn.2535-2512-2019-03-02.

Microsoft. (2022). *Microsoft Digital Defense Report 2022*. Microsoft. Hentet fra Microsoft Digital Defense Report 2022.

Nabe, C. (u.å) *Impact of Covid-19 on Cybersecurity*. Hentet 19.april 2023 fra https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Nasjonal sikkerhetsmyndighet. (2022). *Nasjonalt digitalt risikobilde 2022*. Rapporter Nasjonal sikkerhetsmyndighet (nsm.no).

Nasjonal sikkerhetsmyndighet. (2023). *Risiko 2023: Økt uforutsigbarhet krever høyere beredskap*. Rapporter - Nasjonal sikkerhetsmyndighet (nsm.no).

National institute of standards and technology. (u.å.). *Awareness*. Hentet 3.april fra Awareness - Glossary | CSRC (nist.gov).

Toth, P., & Klein, P. (2013). A role-based model for federal information technology/ cyber security training. NIST Special Publication 800-16 Revision 1 (2nd Draft, Version 2).

Polit, D. F. & Beck, C. T. (2010). Generalization in quantitative and qualitative research: Myths and strategies. Int J Nurs Stud, 47(11), 1451-1458. https://doi.org/10.1016/j.ijnurstu.2010.06.004.

Politiets sikkerhetstjeneste. (2023). *Nasjonal trusselvurdering*. Politiets sikkerhetstjeneste (pst.no).

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer fraud & security*, *2016*(8), 10-18. https://doi.org/10.1016/S1361-3723(16)30062-8.

Shojaifar, A., Fricker, S. A. & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-case Study. I L. Drevin, S. Von Solms & M. Theocharidou, *Information Security Education. Information Security in Action* Cham.

Sony, M. & Naik, S. (2020). Critical factors for the successful implementation of Industry 4.0: a review and future research direction. *Production planning & control*, *31*(10), 799-815. https://doi.org/10.1080/09537287.2019.1691278.

Soomro, Z. A., Shah, M. H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Standard Norge (2023). Informasjonssikkerhet, cybersikkerhet og personvern Ledelsessystemer for informasjonssikkerhet Krav (NS-ISO/IEC 27001:2022). International Organization for Standardization ISO.

Standard Norge. (2022). Informasjonssikkerhet, cybersikkerhet og personvern Informasjonssikkerhetstiltak (NS-EN ISO/IEC 27002:2022). International Organization for Standardization ISO.

Trček, D., Trobec, R., Pavešić, N. & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour & information technology*, *26*(2), 113-118. https://doi.org/10.1080/01449290500330299.

Trist, E. L. (1981). *The evolution of socio-technical systems* (Bd. 2). Ontario Quality of Working Life Centre Toronto.

Troyer, L. (2017). Expanding Sociotechnical Systems Theory Through the Trans-disciplinary Lens of Complexity Theory. I F.-J. Kahlen, S. Flumerfelt & A. Alves (Red.), *Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches* (s. 177-192). Springer International Publishing. https://doi.org/10.1007/978-3-319-38756-7_7.

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European journal of information systems*, *24*(1), 38-58. https://doi.org/10.1057/ejis.2013.27.

Van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M. & Spruit, M. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied sciences*, *11*(15), 6909. https://doi.org/10.3390/app11156909.

Whitman, M. E. & Mattord, H. J. (2019). *Management of information security* (Sixth edition. utg.). Cengage Learning.

Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report, 13(4), 207–215. https://doi.org/10.1016/j.istr.2008.10.009 World Economic Forum. (April, 2023). *How can reskilling and upskilling talent can help shrink the cybersecurity gap*. World Economic Forum. Hentet fra Reskilling and upskilling talent help shrink cybersecurity skills gap | World Economic Forum (weforum.org).

Bueermann, G., & Doyle, S. (2023). Global Cybersecurity Outlook 2023 (weforum.org)

World Economic Forum. (2022, juli). *How organisations can use vulnerabilities to create cyber resilience*. World Economic Forum. Hentet fra Cyber trust issues: How vulnerability creates cyber resilience | World Economic Forum (weforum.org)

Yin, R.K. (2014) Case study research: Design and methods (5. utg.). Sage Publications.

Vedlegg

Vedlegg 1, intervjuguide FPH AS:

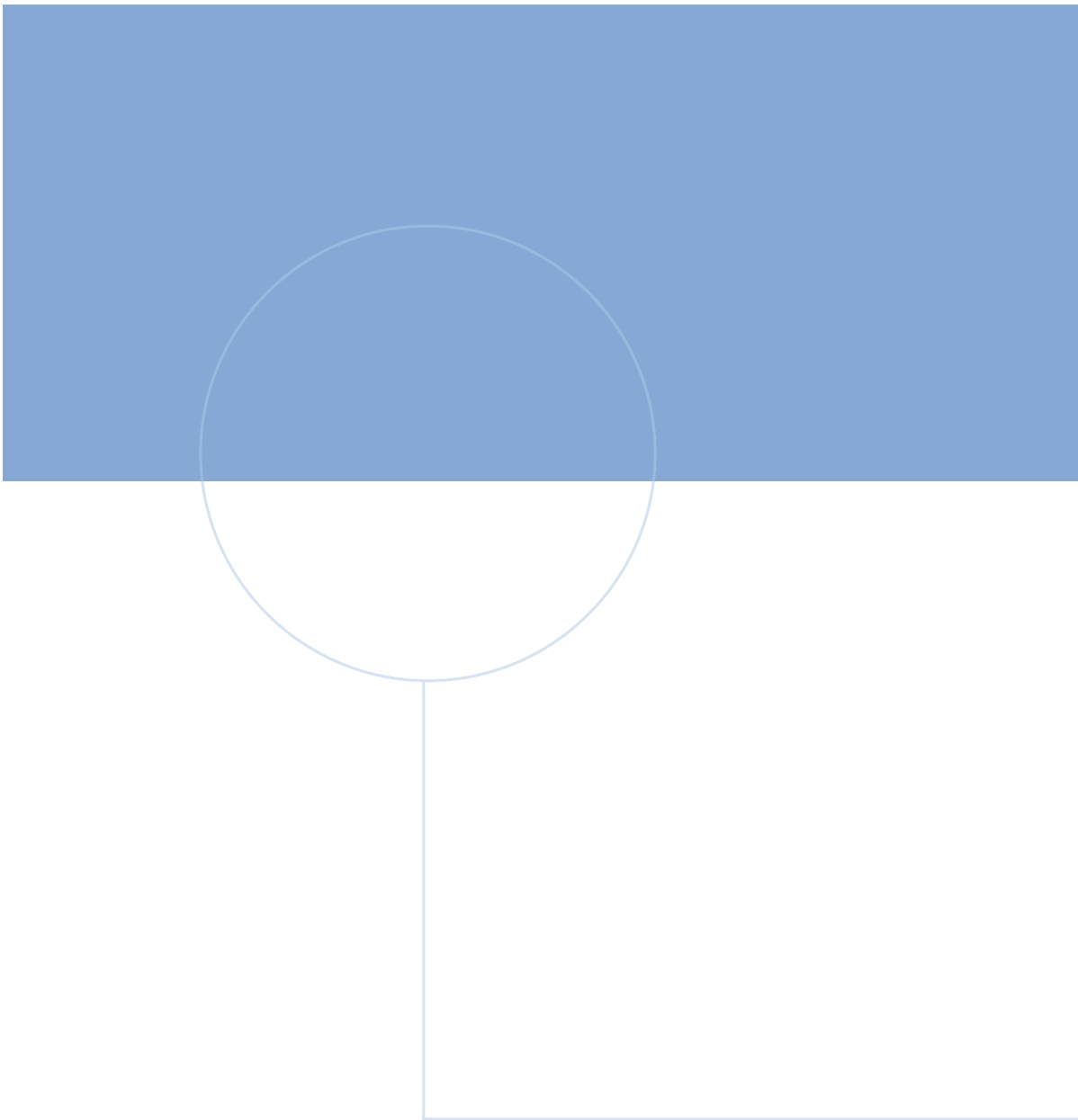
Intervjuguide FPH AS	
Hensikt	**Spørsmål**
Kartlegge intervjuobjektene sitt forhold til informasjonssikkerhet. Svarer på hva de faktisk vet.	Hva tenker du informasjonssikkerhet innebærer?
	Hvilke tanker har du rundt informasjonssikkerhet i arbeidshverdagen din?
	Har du noen tanker om hvordan du kan bidra til å unngå sikkerhetsbrudd?
	Hva tror du er årsaken til de fleste sikkerhetsbrudd/dataangrep?
Få innsikt i sikkerhetshendelsen Ansatte sitt perspektiv og opplevelse Svar på hva slags kunnskap de sitter de igjen med og hvordan ting ble håndtert	Hvordan opplevde du sikkerhetshendelsen?
	Vet du hva som var årsaken til hendelsen?
	Hvordan påvirket sikkerhetsbruddet arbeidet ditt?
	Hva lærte du av hendelsen?
	Hvordan kan du bidra til at det ikke skjer igjen?
	Har du opplevd noen endringer siden hendelsen?
Få inntrykk av hva bedriften gjør i forbindelse med bevisstgjøring. Spørsmålene svarer på om de ansatte er bevisste på informasjonssikkerhet og om FPH AS har implementert tiltak.	Har du kjennskap til retningslinjer/policy og interne regler innen informasjonssikkerhet?
	Har du noe ansvar i forbindelse med sikkerhet? Hva slags/hvorfor/hvorfor ikke?
	Har du noen tanker om hvilke trusler og sårbarheter FPH AS kan være utsatt for?
	Hvor ofte har dere aktiviteter eller kampanjer som fremmer bevisstgjøring av informasjonssikkerhet?
	Hvordan tilrettelegger AS for at du skal lære om informasjonssikkerhet?
Avdekker den treningen og opplæring som er blitt gjort på informasjonssikkerhet Hvordan opplever ansatte at de får tilrettelagt for kompetanseheving. Avdekke rutiner for å dele erfaringer med hverandre	Hva slags trening har du fått for å unngå sikkerhetsbrudd?
	Hvor ofte får du opplæring og trening innen informasjonssikkerhet? Eventuelt oppfølgingsspørsmål: Hvordan ble aktivitetene utført?
	Har du noen tanker om å trene på informasjonssikkerhet
	Hvordan tror du trening og bevisstgjøring kan påvirke virksomhetens sikkerhet?

	Når du lærer noe nytt, eller har vært på seminar, forteller du til kollegaene dine hva du har lært og hva som ble snakket om?
	Etter endt aktivitet, hva er vanlig prosedyre? F.eks. Test, gruppereflekSjon, repetisjon, oppfølgning av aktivitet osv.
Kartlegge ansatte sin kjennskap til rapportering. Vet de hvordan de gjør dette, og hva hadde de gjort? Svarer på om det er interne rutiner/regler/retningslinjer og om de ansatte er kjent med dette.	Hva hadde du gjort dersom du fikk vite at noen brøt selskapets regler?
	Hva tenker du om å rapportere hendelser som går utover deg selv eller andre?
	Er det noen prosedyre for å rapportere en hendelse?

Vedlegg 2, intervjuguide HKK AS

Intervjueguide HKK AS	
Hensikt	**Spørsmål**
Få en generell oppfatning av IT-leverandøren sitt syn på informasjonssikkerhet i SMB-markedet. De jobber med mange og har antakelig god oversikt.	Er det mange SMB-er som opplever sikkerhetsbrudd?
	Hvor ofte blir SMB-er utsatt for dataangrep?
	Hvor ofte må dere bistå bedrifter som opplever sikkerhetsbrudd?
	Hva er som regel årsaken til dataangrep?
	Hva tenker dere SMB-er må være ekstra oppmerksom på når det kommer til informasjonssikkerhet?
	Har dere statistikk aller analyser av de vanligste årsakene til sikkerhetsbrudd hos deres klienter?
	Deler dere erfaringer med andre IT-leverandører?
FPH AS sin hendelse. Spørsmålene belyser hendelsen i et annet perspektiv enn det FPH AS selv kan gi. Det gir svar og en forståelse av hendelsen som kan bli vurdert opp mot svarene fra ansatte i FPH AS	Vet dere hva årsaken til sikkerhetsbruddet var hos FPH AS?
	Hvordan opplevde dere sikkerhetsbruddet, og hvordan håndterte dere det?
	Er det noe dere FPH AS kunne gjort annerledes for å hindre dataangrepet?
	I etterkant av dataangrepet ble/blir FPH AS (og SMB-er generelt) informert om årsaken til hendelsen? Hvis ja, oppfølgingsspørsmål: Hva som kan forbedres? Og eventuelt: Hvordan følger dere opp forbedringspunktene?
	Hvordan bidrar dere til at FPH AS ikke blir utsatt for slike angrep igjen?
Få innsikt i hva de som leverandører tilbyr til sine kunder Svarer på hvordan de som IT-leverandører operer.	Hvilke tjenester tilbyr dere SMB-er for at de skal oppnå et høyere nivå på informasjonssikkerhet?
	Er dere ofte ute hos klientene deres og gjør vurderinger?
	Hvordan bidrar dere til å bevisstgjøre SMB-er innen informasjonssikkerhet og deres trusselbilde?

	Hvilke kampanjer eller aktiviteter tilbyr dere for å bevisstgjøre kjøpere av deres IT-løsninger på informasjonssikkerhet?
	Tilbyr dere informasjonssikkerhets policyer til SMB-er eller er dette noe de lager selv?
	Utfører dere risikovurderinger for SMB-er, eller er dette noe selskaper generelt må utføre på egenhånd?
Belyse forholdet HKK AS og kundene deres har til hverandre med tanke på forventninger og tillit.	Har dere mye tillit fra klientene deres?
	Dersom et selskap velger dere som IT-leverandør, hvilke forventninger har de til informasjonssikkerheten?
	Tror dere selskaper føler seg trygge med IT-løsninger som dere selger og hjelper dem med?
	Tror dere selskaper føler seg trygge med IT-løsninger som dere selger og hjelper dem med?
	Er alt ansvaret på dere eller er det delt ansvar på å ivareta informasjonssikkerheten? Eventuelt oppfølgingsspørsmål: Hva er deres ansvar og hva er SMB-ene sitt ansvar?
	Hva er viktig for dere I en prosess der en SMB vil outsource IT eller flytte data til skytjenester?



NTNU

Kunnskap for en bedre verden