Masteroppgave

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

Erik Fredriksen Dulin og Jørgen Kjekk Alfredsen

Hvordan få en økt bevissthet rundt cybersikkerhet i små- og mellomstore bedrifter?

Masteroppgave i Industriell innovasjon og digital sikkerhet
Veileder: Halvor Holtskog

Desember 2023

NTNU
Kunnskap for en bedre verden

Erik Fredriksen Dulin og Jørgen Kjekk Alfredsen

Hvordan få en økt bevissthet rundt cybersikkerhet i små- og mellomstore bedrifter?

Masteroppgave i Industriell innovasjon og digital sikkerhet
Veileder: Halvor Holtskog
Desember 2023

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

NTNU
Kunnskap for en bedre verden

Sammendrag

I dagens samfunn er cyberangrep i stor vekst, spesielt mot små og mellomstore bedrifter (SMB). Dette er også grunnen til at disse bedriftene har blitt mer opptatt av cybersikkerhet de siste årene. Europas økonomi består i store deler av SMB og mange av de store virksomhetene er avhengige av SMB sine produkter og tjenester. Uten tilgang på ressursene SMB leverer vil det påvirke store deler av næringskjeder, forsyninger og økonomi. De fleste virksomheter er derfor bekymret for utviklingen av cyberangrep i SMB, spesielt da det hevdes at 1 av 5 virksomheter har blitt utsatt for en eller annen form for cyberangrep. Derfor er vi nødt til å gjøre noe med den manglende kunnskapen og bevisstheten om cybersikkerhet i bedrifter.

I løpet av denne oppgaven vil vi se nærmere på hvordan man kan bygge bevissthet i SMB for å oppnå en bedre cybersikkerhet. Oppgaven blir gjennomført i samarbeid med en ganske normal mellomstor virksomhet i form av en casestudie. Oppgaven kan ha stor relevans for virksomheter som ønsker å lære om hvordan man kan bygge bevissthet og hvordan en økt bevissthet påvirker cybersikkerhet i virksomheten.

Virksomheten vi samarbeider med er i en digitaliseringsprosess der de skal gjøre om store deler av lagringen av og deling av informasjon. Når prosessen er ferdig vil man ha behov for et høyere kunnskapsnivå om cybersikkerhet blant de ansatte, da virksomheten i stor grad er avhengig av teknologi. Vi ønsker å avdekke hvordan man kan bygge kunnskap om temaet og hvordan økt kunnskap kan gi en bedre bevissthet. Virksomheten er bekymret for at et cyberangrep kan føre til at de ikke får utført arbeidet sitt.

I løpet av oppgaven vil vi se nærmere på hvordan ulike teorier kan brukes sammen for å bygge bevissthet. Dette vil være relevant for bruk i virksomheten som er i en digitaliseringsprosess der det trengs nye tiltak knyttet til sikker databruk og cybersikkerhet. Vi ønsker å finne ut hvordan teoriene fungerer hver for seg og om det kan fungere bedre når vi bruker de sammen. Ved å bruke teoriene sammen vil man kunne dekke hullene som de har hver for seg og oppnå en bedre kunnskapsarena som kan være med å øke bevisstheten.

Teoriene vi har tatt for oss er Trappetrinnsmodellen av Hagen et al. (2008) og soft-systems metoden av Checkland (1981). Modellene fokuserer hver for seg på det organisatoriske og det menneskelige. Trappetrinnsmodellen fungerer veldig top-down der policyer, prosedyrer og kontroller kommer fra ledelsen ned til de ansatte. Problemet med dette er at man ikke vet om de ansatte vil handle rasjonelt på problemer der de har lite kunnskap. Checkland fokuserer på en systematisk gjennomgang av problemet for å finne rotårsak, der man danner konseptuelle modeller for å visualisere problemet ovenfor de ansatte. Dette kan føre til en bedre bevissthet og gi mer rasjonelle beslutninger i samarbeid med trappetrinnsmodellen.

Abstract

Cyberattacks are in massive growth, especially towards small- and medium-sized enterprises (SMEs). This is also the reason that these enterprises has focused more on cybersecurity over the last few years. Europe's economy largely consists of SMEs and a many of the large enterprises rely on SMEs providing their products and services. The supply chain will suffer massively without access to the resources that SMEs provide, and it would impact economies, supplies and supply chains. That is why most enterprises are concerned for the growing trend of cyberattacks towards SME, considering there are claims that $1/5^{th}$ of enterprises have been attacked in some sort of way. This is why we wanted to focus on the knowledge and awareness that is missing in a lot of enterprises.

We wanted to take a closer look at how we can build awareness in SMEs to achieve a higher level of cybersecurity. This project has been a collaboration between a normal medium-sized enterprise and us students in the form of a case study. The project can be relevant for other enterprises that wants to learn about building awareness and how increased awareness can impact cybersecurity within the enterprise.

The enterprise we are working with is in the middle of a digitalization process, where they are converting a lot of data and information sharing from analog to digital. When this process is done, the enterprise will have a need for a higher level of knowledge of cybersecurity between the employees because of the increased use of technology. We want to see how an enterprise can build knowledge about cybersecurity and how increased knowledge can lead to improved awareness. The enterprise is worried that a cyberattack might lead to them not being able to complete everyday tasks.

Throughout the project we want to look closer at how different theories can be used collaboratively to build awareness. This is relevant as the enterprise is in the middle of a digitalization process, where new measures and procedures are needed to fulfill secure use of data and cybersecurity. We want to find out how each theory work individually and if using them collaboratively will make them more efficient. By using the theories collaboratively, it will be possible to fill the gaps between them and achieve a better arena for creating knowledge and increasing awareness.

The theories we have focused on is the Staircase-method (SCM) by Hagen et al. (2008) and Soft-systems methodology by Checkland (1981). The models focuses on the organizational and human parts separately. The SCM works in a top-down way, where policies, procedures and control is coming from the leaders. The issue with this is that we cannot expect the employees to act rationally in situations where they lack knowledge. Checkland focuses on a systematic approach by analyzing the problem and finding its root cause, you will then make conceptual models to visualize the problem at hand to the employees. This might lead to increased awareness and more rational choices in collaboration with SCM.

Forord

Etter 2 fine år ved masterprogrammet Industriell innovasjon og digital sikkerhet ved NTNU er det tid for å skrive masteroppgave. Oppgaven skrives i det fjerde semester og bygger videre på en obligatorisk prosjektoppgave som ble levert i tredje semester. Denne masteroppgaven er utarbeidet av Erik Fredriksen Dulin og Jørgen Kjekk Alfredsen.

Masteroppgaven er et forskningsprosjekt basert på kunnskap og teori knyttet til hvordan SSM kan øke bevisstheten. Dette forskningsprosjektet har vært avhengig av empiri fra Anlegg AS, et fiktivt navn vi har valgt å bruke for å beskytte bedriftens egentlige identitet.

Formålet med forskningsprosjektet har vært å belyse hvordan mellomstore bedrifter kan øke cyber bevisstheten. Videre har vi sett på hvordan ulike modeller og metodikk kan tilpasses for å skape kunnskap og økning av bevissthet. Ved hjelp av empiri fra Anlegg AS har vi kunne dannet et grunnlag for hvordan dagens bevissthet ser ut. Å få innblikk i denne informasjonen har vært viktig for forskningsprosjektet.

Problembeskrivelsen er formulert av studentene i tett samarbeid med veileder Halvor Holtskog. Forskningsprosjektets overordnede tema er bevissthet rundt cybersikkerhet og hvordan kunnskap kan påvirke bevisstheten. Underveis i prosjektet har veileder vært svært hjelpsom og har bidratt med veiledninger i form av innhold, akademisk skriving og struktur i masteroppgaven.

Anlegg AS har vært behjelpelige og åpne underveis i forskningsprosjektet. Bedriften ga oss fri tilgang til intervjuobjekter og mulighet for å sende ut spørreundersøkelse til hele bedriften.

Vi ønsker å rette en stor takk til Halvor Holtskog og Anlegg AS for all hjelp og bidrag til forskningsprosjektet. Vi ønsker også å rette en takk til medstudenter på campus som har bidratt til to flotte og lærerike år på NTNU.

Innhold

Figurer

Innledning

Problembeskrivelse

Ifølge Canalys's siste cybersikkerhets-prognoser vil verdens forbruk på cybersikkerhet øke med 13.2% i 2023, med et forventet forbruk på US$ 223.8 milliarder (Canalys, 2023). Likevel øker antallet cyberangrep og de blir stadig mer utfordrende. Ifølge World Economic Forum sin rapport Global risk report, økte malware (skadevare) med 358% og løsepengeangrep med 435% i 2020 (WEF, 2022). Det er forventet at skadeverdien av cyberkriminalitet vil øke med 15% hvert år frem til år 2025 og vil dermed nå US$ 10.5 trillioner, opp fra US$ 3 trillioner fra 2015 (Morgan, S. 2022). Det ser ut til at selv med smarte systemer, prosesser og teknologi, så er ikke dette nok til å stoppe cyberangrep. Dette vil si at bedrifter og organisasjoner bør investere mer i opplæring rundt cybersikkerhet og bevisstgjøring.

I løpet av COVID-19 så vi en økning i bruken av hjemmekontor, dette har ført til en økende avhengighet av digitale systemer. De siste årene har vist at cybersikkerhet virkelig er i vinden. Det har blitt synligere i media at cyberangrep har funnet sted både hos den norske stat og i norske bedrifter. I tillegg er det som nevnt over, store økninger i antall angrep fra år til år.

Gjennom denne oppgaven kommer vi til å bruke fiktive navn på både bedrift og ansatte. Derfor vil bedriften sitt navn være Anlegg AS gjennom dette prosjektet. Dette for å hindre identifisering av bedriften og personer.

Bakgrunnen for dette prosjektet er at Anlegg AS skal digitalisere systemene innad i bedriften. Anlegg AS ønsker å bedre bedriftens systemer og rutiner gjennom å avdekke styrker og risikoer knyttet til cybersikkerhet. For Anlegg AS er det viktig å skape en god bevissthet hos de ansatte rundt cybersikkerhet. De er ikke bekymret for at andre bedrifter kopierer slik de jobber grunnet utfordringene knyttet til arbeidsprosessen sin. På den andre siden så er de bekymret for at de blir utsatt for et cyberangrep slik at de ikke får utført arbeidet sitt, og det er denne oppgaven som skal hjelpe Anlegg AS med å øke bevisstheten innad i bedriften. Det er også viktig å si at ene gruppemedlemmet har fått seg jobb i firmaet og jobber 50% under masteroppgaven hos bedriften.

Formålet

Formålet med prosjektet er å belyse kunnskapen og bevisstheten rundt cybersikkerhet hos mellomstore bedrifter gjennom ett case studie. Hovedfokuset i oppgaven er altså øke bevisstheten på cybersikkerhet hos de ansatte. Studien frembringer ulike perspektiver på problemstillingen gjennom analyse av spørreundersøkelse og intervjuer. Spørreundersøkelsen har blitt besvart av de ansatte i bedriften Anlegg AS.

Problemstilling:

"Hvordan få en økt bevissthet rundt cybersikkerhet i små- og mellomstore bedrifter?"

Avgrensning av studie

Gjennom dette prosjektet har vi kun tatt utgangspunkt i å studere Anlegg AS som er en mellomstor bedrift i Norge. Dette vil si at dette studie ikke kan rette seg mot alle bedrifter, men denne oppgaven kan bidra med å øke innsikten i problemstillingen. Måten singel case studien kan bidra med til økt innsikt i denne problemstillingen er fordi casen er av en helt ordinær bedrift. Dette kan føre til at andre bedrifter på lik størrelse kan bruke casen og tilpasse til sin egen bedrift. Kritikk av studiet vårt er at den ene studenten i dette prosjektet jobber hos Anlegg AS. Dette kan bli med på farge inntrykk av situasjoner som vi har kommet med igjennom denne perioden.

Definisjoner/Begreper

Mellomstor bedrift

Europa kommisjonen definerer små og mellomstore bedrifter, SMB, som en bedrift der årsomsetningen ikke overstiger 50 millioner euro, antall ansatte er under 250 og årsbalansen overskrider ikke 43 millioner euro (European Commission, u.å.).

I Norge er det vanlig å definere små og mellomstore bedrifter som bedrifter med under 100 ansatte. Næringslivets Hovedorganisasjon, heretter NHO, definerer bedrifter med 1-20 ansatte som små, bedrifter med 21-100 ansatte som mellomstore og over 100 ansatte som store. NHO spesifiser at 99% av norske bedrifter blir betegnet som SMB, der 47% av antallet ansatte i næringslivet er ansatt i SMB. De sier også at 44% av verdiskapningen fra norske bedrifter stammer fra SMB, noe som tilsvarer 700 milliarder NOK (NHO, u.å.).

Grunnet disse uenighetene om definisjonen av mellomstore bedrifter, har vi valgt å definere Anlegg AS som en mellomstor bedrift. Dette er fordi bedriften har mellom 100 og 250 ansatte, har under 50 millioner euro i årsomsetning og under 43 millioner euro i årsbalansen.

Cybersikkerhet

En vanlig feil å gjøre er å bruke begrepene data- og cybersikkerhet om hverandre, selv om de har ulik definisjon. Datasikkerhet er beskyttelsen av informasjonssystemer, prosesser og dataene i digitale systemer (Whitman & Mattord, 2017). Cybersikkerhet sikrer også enhetene og den digitale infrastrukturen som ikke er relatert til selve informasjonen på en datamaskin. Dette kan være eksempelvis digitalt produksjonsmaskineri, skylagring eller nettverk.

Cybersikkerhet er praksisen om å beskytte enheter, systemer, nettverk, data og applikasjoner fra cyberangrep. Det overordnede målet er å avverge interne og eksterne angrep som forsøker å få tilgang til eller ødelegge data, forstyrre normal forretningsdrift eller utpressing for penger. (SAP, u.å.).

Digitalisering

Digitalisering betegner en transformativ prosess der noe blir digitalt – en digital prosess, en digital organisasjon eller et digitalt samfunn (Andersen & Sannes, 2018). I en organisasjonsmessig sammenheng blir digitalisering definert som transformasjonen fra at IT er et støtteverktøy i virksomheten til at det er en del av dens DNA. Det betyr at forretningsmodell og -praksis samt organisasjon og prosesser er designet for å utnytte dagens og morgendagens teknologi (Andersen & Sannes, 2016). Med andre ord er det endring til en digital organisasjon.

Regjeringen definerer digitalisering som; Å bruke teknologi til å fornye, forenkle og forbedre. Det handler om å tilby nye og bedre tjenester, som er enkle, effektive og pålitelige. Digitalisering legger til rette for økt verdiskapning og innovasjon, og kan bidra til å øke produktiviteten i både privat og offentlig sektor (Regjeringen, 2014).

Teori

I dette kapittelet tar vi for oss ulike teorier knyttet til opparbeidelse av kunnskap, innføring av policyer og prosedyrer og bruk av SSM i organisasjoner. Vi har valgt å se nærmere på trappetrinnsmodellen fra Hagen et al. (2008), SSM av Checkland (1981) og individ mot organisasjonslæring. I tillegg til disse teoriene ser vi nærmere på hvordan de påvirker cyber awareness i organisasjon og hvordan økt læring og kunnskap kan føre til en høyere bevissthet.

Bevissthet

Bevisstgjøring knyttet til cybersikkerhet er et relativt nytt tema og det er derfor vanskelig å finne en konkret definisjon eller betydning på begrepet. Cyber awareness er nivået på en persons tekniske bevissthet og ferdigheter, og sikrer de mest grunnleggende prinsippene innen vanlige teknologiske aktiviteter, inkludert sikker bruk og normalt vedlikehold (Okereafor, 2008).

Toth og Klein (2014) peker på oppmerksomheten til sikkerhet, der brukerne blir informert om trusler og sårbarheter knyttet til cybersikkerhet. Bevisstgjøring informerer brukerne om trusler og sårbarheter som kan påvirke organisasjonen og deres personlige arbeidsmiljø ved å forklare «hva», men ikke «hvorfor» innen sikkerhet, samt kommunisering om hva som er lov og ikke. (Toth & Klein, 2014)

National Institute of Standards and Technology (NIST) viser til at bevisstgjøring ikke er trening, men en læringsprosess. Poenget med bevisstgjøring er kun for å rette oppmerksomheten mot sikkerhet. Presentasjoner om bevisstgjøring gir brukeren muligheten til å gjenkjenne cybertrusler og reagere korrekt. Ved bruk av bevisstgjøringsaktiviteter har ofte den som lærer en aktiv rolle i situasjonen, mens den eller vil ha større fokus på å ta imot informasjon (NIST, u.å.).

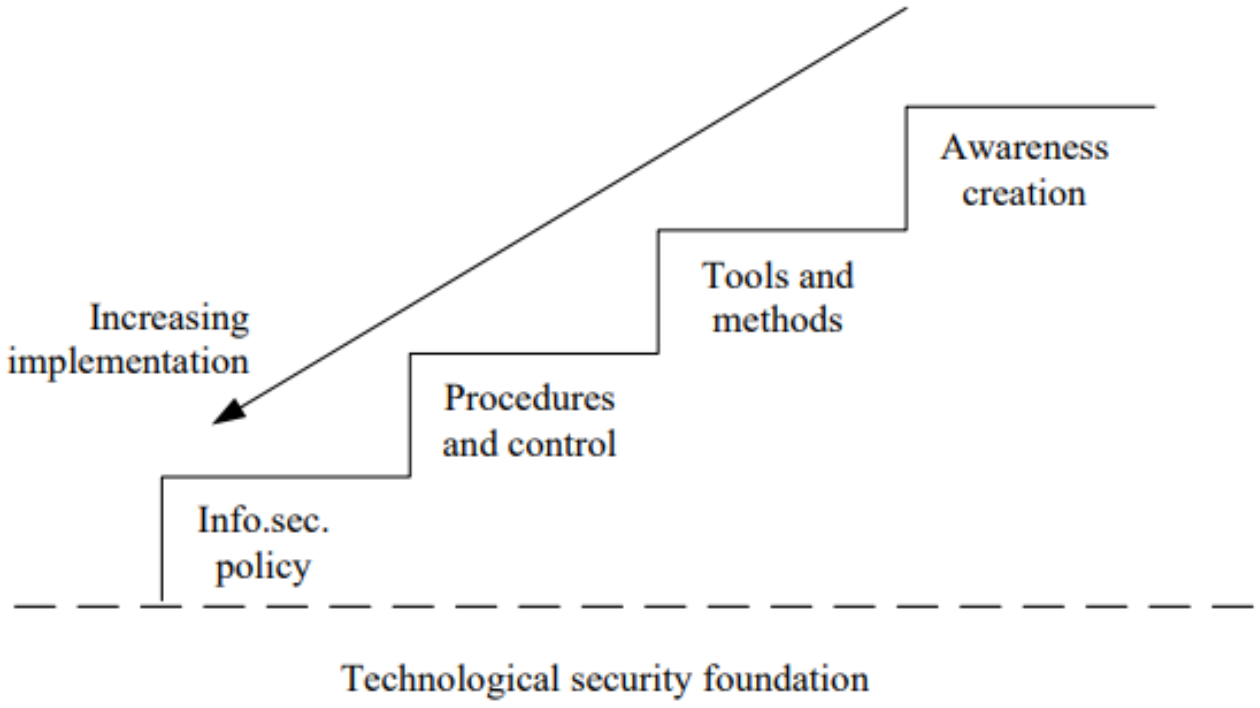
Cybersikkerhet vil være en av de viktigste digitale ferdighetene, og vil være en nødvendighet i fremtidens fabrikker ifølge Europakommisjonen (2020). Ifølge en litteraturgjennomgang av Europakommisjonen (2020) har de satt opp en skala for å måle viktigheten av Big Data, Internet of Things (IoT) og cybersikkerhet for små og mellomstore bedrifter. På denne skalaen scorer cybersikkerhet 5,76 av mulige 7, der 7 kategoriseres som ekstremt viktig. Dette er betydelig høyere enn både Big Data (5,02) og IoT (4,72). De peker også på kompleksiteten av nye teknologier, som Business in Cloud som en av hovedgrunnene til at bevisstheten rundt digital teknologi er for lav. Små og mellomstore bedrifter er ofte mindre bevisst rundt potensiale og aktivitetene som behøves før å optimalisere bruken av data (Europakommisjonen, 2020). Europakommisjonen peker på at fullføringen av Digital Single Market (DSM) kan gi en økning til EU's økonomi på hele 415€ milliarder. Fullføringen av DSM krever en bevisstgjøring rundt optimalisering av teknologi, cybersikkerhet og kunnskap innad i bedriften.

Trappetrinnsmodellen

Hagen et al. (2008) har gjort en undersøkelse hvor det kommer frem at bevisstgjørelse er blant de mest effektive tiltakene for å øke cyber- og informasjonssikkerhet. Likevel har de gjort funn som tilsier at dette er det minst implementerte tiltaket av eksemplene som ble gitt under undersøkelsen; informasjonssikkerhetspolicy, prosedyrer og kontroll, verktøy og metoder og bevisstgjøring. Det nevnes at noe av grunnen til dette kan være at de mer formelle tiltakene, eksempelvis informasjonspolicyer er enklere og mindre ressurskrevende å implementere enn aktiviteter for å øke bevisstheten til de ansatte.

Hagen et al. (2008) viser til figuren nedenfor. Figuren er illustrert som en trapp, som er bygget på de grunnleggende teknologiske sikkerhetsløsningene som alltid må være på plass. Uten teknologiske sikkerhetsløsninger trenger vi heller ikke administrative tiltak, siden det er de teknologiske løsningene som forhindrer, oppdager og reagerer på uønskede hendelser der teknologi brukes (Hagen et al, 2008).

På det nederste trinnet finner vi de mest grunnleggende og vanlige tiltakene innen informasjonssikkerhet. Jo høyere man går i trappen, jo mindre vanlig er implementering av tiltaket. Pilen viser den økende implementeringen, det vil si høyere grad av implementering jo nærmere det grunnleggende nivået vi kommer. Figuren sier at eksempelvis informasjonssikkerhetspolicy oftere blir implementert enn de øvrige trappetrinnene. Det interessante med figuren er at de øverste trappetrinnene viser det mest effektive tiltaket, men man er nødt til å ha de nedre trinnene for at det øverste skal være effektivt.



Figur 1 Trappetrinnsmodell fra Hagen et al. (2008)

Informasjonssikkerhetspolicy

Policy for informasjonssikkerhet hevdes å være grunnlaget i et hvert administrativt sikkerhetsregime (Hagen et al, 2008). Funnene fra Hagen et al (2008) viser at policyer brukes i stor grad, der dokumenter og kontrollaktiviteter ofte bygges på disse policyene. En policy spesifiserer grenser, ansvar og standarder for brukere av informasjons- og teknologisystemer som skal forenkle oppdagelse, respons og forebygging (Cram et al., 2017). Dette trinnet utgjør grunntrinnet i trappetrinnsmodellen og er vesentlig for videre utvikling.

Informasjon som ressurs er uvurderlig for enhver organisasjon og beskyttelse og hemmelighold av denne informasjon er kritisk. Informasjonssikkerhetspolicyer etableres for å sikre integritet, autentisitet, tilgjengelighet og konfidensialitet av all informasjon som håndteres av organisasjonen. Disse policyene ble utformet for å legge opp til en kultur av bevissthet og ansvarlighet. En policy er organisasjonens offisielle retningslinjer og prinsipper for hvordan arbeid skal gjøres (Dahl, 2021).

Disse policyene skal summere, på en oversiktlig måte, hva som er viktig for å sikre mål og verdier i egen organisasjon. Policyene er et oversiktsdokument over områder en må tenke på, mens det en skal gjøre i praksis vil være beskrevet mer i detalj i egne operasjonelle retningslinjer (Nettvett, 2021).

En informasjonssikkerhetspolicy gir en felles plattform som gjør det mulig å handle konsekvent når det gjelder informasjonssikkerhet. Klare policyer minsker risikoen for at ansatte spør seg:

Hvilke regler er det som gjelder?

Hvem har ansvar for hva, hvem kan jeg spørre?

En klart uttalt informasjonssikkerhetspolicy synliggjør for mellomledere og andre ansatte hvordan informasjonssikkerheten skal prioriteres. Det vil også være enklere å velge riktige sikringstiltak når langsiktige føringer for sikkerhetsarbeidet er gitt (Nettvett, 2021)

Målsettinger for informasjonssikkerhetspolicyer er å sikre;

1. Konfidensialitet: Beskytte organisasjonens informasjon fra uautorisert tilgang og sørger for at kun autoriserte personer kan få tilgang til filer og kontoer (Microsoft, u.å.).
2. Integritet: Passer på at informasjonen din er det den skal være, og at ingen har lagt inn, endret eller slettet uten din tillatelse. Du kan for eksempel endre et tall i et regneark med onde hensikter (Microsoft, u.å.).
3. Tilgang: Sørger for at tilgang til informasjon og systemer er kontrollert. Et eksempel på et tilgangsproblem kan være et tjenesteangrep der angripere overfyller systemet med nettverkstrafikk for å gjøre det nærmest umulig å få tilgang til (Microsoft, u.å.).
4. Autentisitet: Verifiserer identiteten til brukere, systemer og enheter for å hindre uautorisert tilgang.
5. Overholdelse: Opprettholder samsvar med gjeldende lover, standarder og forskrifter relatert til informasjonssikkerhet.

I forkant av arbeidet med å lage en informasjonssikkerhetspolicy er det viktig å kjenne hvilke verdier, langsiktige forretningsmål og hvilken risiko virksomheten er utsatt for. Ut ifra dette kan man beskrive hvilken beskyttelse som er nødvendig og hvilken prioritet sikkerhetsarbeidet skal ha. En enkel risikovurdering vil gi dette grunnlaget (Nettvett, 2021).

Prosedyrer og kontroll

Prosedyrer og kontroll er direkte utviklet ut ifra informasjonssikkerhetspolicyen. Denne gruppen tiltak består av dokumenter som guider individuell og organisatoriske handlemåter, slik som brukerinstruksjoner, sikkerhetsplaner, konfidensialitetsavtaler og disiplinærprosesser (Hagen et al, 2008). Whitman & Mattord (2019) peker på at det kan være steg for steg-guider som er laget for å hjelpe og forenkle sikkerhetsretningslinjene for de ansatte.

Prosedyrer og kontroll knyttet til cybersikkerhet inneholder flere elementer som er kritisk for å beskytte konfidensialitet og tilgang til informasjon opp mot organisasjonen.

Sentralt i arbeidet innen cybersikkerhet ligger sikkerhetstiltak. Når man er kjent med en risiko kan man iverksette sikkerhetstiltak for å håndtere denne. Noen risikoer kan unngås ved å endre oppgaver som utgjør en risiko eller ved å endre på fremgangsmåten, mens andre risikoer kan gjøre at man er nødt til å la være å gjøre enkelte oppgaver grunnet risikoens opphav. Et sikkerhetstiltak er noe som etableres og forvaltes. Det kan dokumenteres og stå på en liste eller inngå i en oversikt over en virksomhets etablerte sikkerhetstiltak, og man bør kunne peke på en navngitt person eller funksjon som har ansvaret for forvaltning (Digdir, u.å.).

Mange bedrifter sitter på store verdier i form av bedriftshemmeligheter. Dette kan være informasjon som din organisasjon har tilgang til, men ikke konkurrenten din er klar over noe som gir deg et konkurransefortrinn. Derfor er det viktig å ha et bevisst forhold til hvilken informasjon man kan dele og begrense delingen i størst mulig grad. En konfidensialitetsavtale, populært kalt NDA, er en avtale som beskytter informasjon de ansatte kan ha tilgang til. Dersom taushetsplikten kun går ene veien, kalles det en taushetserklæring. Ofte finner man disse som en del av ansettelsesavtaler, hvor de er en del av en større avtale mellom to parter (Aarflot, u.å.)

I direkte tilknytning til policyene er det kritisk at de ansatte får implementert opplæringsprogrammer for å øke bevisstheten og redusere risikoen for menneskelige feil. Ifølge AIGs rapport fra 2019 økte andelen forsikringskrav som skyldes menneskelige feil fra 7% til 14% i løpet av året. Mange ledere for små og mellomstore bedrifter har en tendens til å tro at cyberangrep ikke vil skje i deres organisasjon ettersom de er for små. Sannheten er at mange små og mellomstore bedrifter med særlig sensitiv informasjon tilhører en stor risikogruppe innen datakriminalitet, uten å være klar over det. Deres rapport viser også en økende trend hvor ansattes uaktsomhet fører til tap av sensitiv informasjon (AIG, 2019.)

Tapet av sensitiv informasjon kan føre til tap av eksempelvis konkurransefortrinn, nedetid eller tap av kundedata. For å forhindre dette innfører man ofte strenge retningslinjer for tilgangskontroll for å sikre at kun autoriserte personer får tilgang til spesifikke typer data. Tilgangskontroll hindrer konfidensiell informasjon fra å bli stjålet av tvilsomme aktører eller andre uautoriserte brukere. Det reduserer også risikoen for dataeksfiltrasjon – uthenting av sensitiv informasjon – utført av ansatt, og det holder nettbaserte trusler i sjakk (Microsoft, u.å.).

Dersom tap av sensitiv informasjon har skjedd, er det viktig å være forberedt i forkant. Mange bedrifter tar derfor i bruk sikkerhetskopiering eller skylagring som et tiltak for å forhindre nedetid eller tap av data. Ved bruk av sikkerhetskopiering har man mulighet til å gjenopprette systemet til et tidligere tidspunkt, noe som gjør at dataen som har forsvunnet nå vil være der. Et eksempel kan være en ansatt som ved et uhell sletter et Excel-ark, der mange timers arbeid går tapt. Det er anbefalt å lagre sikkerhetskopien eksternt, da sjansen er stor for at det samme skjer med all data som er lagret på et sted. Derfor er det viktig å oppbevare sikkerhetskopien på en måte som gjør den bedre beskyttet enn originaldataene, slik at ikke alt går tapt dersom man skulle bli utsatt for et cyberangrep (Estil, 2023).

Et siste tiltak mange bedrifter tar i bruk er kryptering. Når man krypterer en fil vil informasjonen låses ned med en matematisk nøkkel, noe som gjør at man trenger riktig nøkkel for å få tilgang til filen igjen. Man har symmetrisk og asymmetrisk kryptering, der symmetrisk kryptering bruker samme nøkkel til å låse ned og opp informasjon. Asymmetrisk kryptering, også kalt offentlig kryptering benytter et nøkkelpar; en privat og en offentlig nøkkel, der den offentlige kan gjøres tilgjengelig for hvem som helst mens den private kun er kjent av nøkkelens eier (Datatilsynet, 2017).

Verktøy og metoder

Hagen et al. (2008) mener administrative metoder kan være både reaktive og proaktive tiltak. Ifølge Hagen et al (2008) inneholder dette trinnet seks elementer; Hendelseshåndtering, rapportering, risikoanalyse, klassifisering av ressurser, revisjoner av regulatoriske myndigheter og interne revisjoner.

Hendelseshåndtering innebærer krisehåndteringsplaner, kontinuitetsplaner eller hendelsesresponsplaner. Rapportering handler om å rapportere avvik, klager og lignende. Risikoanalyse innebærer en analyse av hvilke risikoer bedriftens informasjonsressurser står ovenfor, og hvor eksponert de er for hver risiko. Klassifisering av ressurser handler om å klassifisere ressursene etter eksempelvis strengt hemmelig, hemmelig, intern eller offentlig. Revisjoner av regulatoriske myndigheter innebærer revisjon av eksterne myndigheter uten tilknytning til organisasjonen. Intern revisjon innebærer kontroll av prosedyrer og retningslinjer av gjennomført internt i organisasjonen.

Nært knyttet til policy finner man også hendelseshåndtering. Dette prinsippet handler om å være forberedt på at innsideaktivitet og andre uønskede hendelser kan komme til å skje. Virksomheten bør ha en plan for hvordan den skal håndtere det menneskelige aspektet ved en potensiell hendelse (NSM, 2020). Dette er spesielt viktig da man vil være bedre rustet til å håndtere uønskede og truende hendelser og dermed vil kunne ivareta sikkerhetstilstanden i organisasjonen. Tydelig rollefordeling, kontinuitetsplaner og nødvendig opplæring er alle anbefalte tiltak å ha med i hendelseshåndteringen.

For å danne en plan for hendelseshåndtering tar organisasjoner ofte i bruk risikovurderinger. En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for risiko og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå tilfredsstillende cybersikkerhet (Datatilsynet, 2019). Når man har gjennomført risikovurderingen kan man begynne med utviklingen av klare informasjonssikkerhetspolicyer som beskriver retningslinjer for de ansatte knyttet til bruk av digitale systemer.

Rapportering innen cybersikkerhet er kritisk for å gi organisasjonens ledelse og andre interessenter innsikt i organisasjonens status, trusselbilde og effektivitet av cybersikkerhetstiltakene. Aspekter som hendelses-, risiko- og sikkerhets-rapporter er verktøy for å dokumentere hendelser og tiltak, men også for å informere interessenter og å hjelpe med å forme strategier og handlingsplaner for cybersikkerhet. En omfattende og tydelig hendelsesrapport er en viktig referanse for sikkerhetsteam og administrasjon av sikkerhetstjenester. En hendelsesrapport konsoliderer hendelsesinformasjon fra ulike datakilder som er tilgjengelige (Microsoft, 2023).

En risikorapport bygger på risikovurderingen som nevnt over. En slik rapport tar for seg de ulike truslene organisasjonen står ovenfor, og er viktig for å bygge kunnskap og bevissthet om truslene man står ovenfor. Ved å danne en systematisk gjennomgang av trusselbildet og risikoen var at trusselen kan inntreffe kan være med å danne et klarere bilde om hvilke tiltak som må gjøres.

For mange organisasjoner er data, informasjon og kompetanse en vesentlig del av verdiene. Derfor er cybersikkerhet ikke bare en øvelse i å tette hull når de oppdages, det bør være en strategi for å sørge for at hullene ikke oppstår. Blant disse strategiene er sikkerhetsrapporter. En sikkerhetsrapport vil oppsummere bedriftens IT-infrastruktur. (Lindbak, u.å.). Bakgrunnen for en slik rapport vil være at man har behov for en gjennomgang av hvilke tiltak organisasjonen aktivt tar i bruk, samt også simulering av angrep for å teste de ansattes rutiner og den tekniske sikkerheten.

Som en dataforvalter er også Anlegg AS ansvarlig for at dataene brukes og deles i samsvar med lover og regler. Det forutsetter at de har oversikt over hva slags hvilke data som må beskyttes, hvilke som kan gis tilgang til under visse vilkår og hvilke som kan brukes fritt. En vanlig metode for dette kalles trafikklyssystemet, dette systemet samsvarer med EUs klassifikasjon for tilgangsstyring og er forholdvis enkelt å benytte. Allmenn tilgang er grønn, betinget tilgang er gul og ikke-allmenn tilgang er rød. (Digdir, u.å.).

Bevisstgjøring

Dette er trinnet som regnes for å være det mest effektive ifølge Hagen et al (2008). Bevisstgjøringstrinnet består av tiltak som skal legge til rette for at de ansatte blir mer bevisst når det kommer til cybersikkerhet. Tiltakene på dette trinnet er både kollektive og individuelle og kan innebære; trening/opplæring i form av workshops og lignende, presentasjoner, diskusjoner i grupper eller e-poster med informasjon til de ansatte. Hagen et al (2008) peker også på å få med toppledelsen og involvere alle parter i organisasjon for å oppnå høyest mulig læring.

Store Norske Leksikon definerer bevisstgjøring som det å komme til en erkjennelse av noe; å oppnå større psykologisk innsikt (SNL, 2020).

Når det kommer til cybersikkerhet innebærer begrepet å være oppmerksom på cybersikkerhet i daglige situasjoner. Cyberbevissthet handler om forståelsen og kunnskapen om digitale risikoer, trusler og beste praksis for å unngå disse og beskytte organisasjonen. Det å ha innsikt om risikoene man står ovenfor gir den ansatte mulighet til å unngå de. Dersom de ansatte ikke har blitt gjort bevisst på hvilke risikoer man står ovenfor, kan man heller ikke forvente at de skal klare å unngå de. Å være bevisst om cybersikkerhet handler om å være proaktiv og at den ansatte selv tar ansvar for den digitale sikkerheten.

Kritisk for å skape bevissthet i en organisasjon ligger opplæring. Det anslås at ca. 90% av alle cyberangrep er forårsaket av menneskelig feil eller oppførsel (Wilhelmsen, 2021). Derfor er det spesielt viktig at organisasjonen tar i bruk opplæring også innen datasystemer og arbeidsoppgaver som foregår digitalt. Formålet med opplæring er å gjøre den ansatte i stand til å utføre arbeidet på en måte som reduserer risiko og belastninger i arbeidet. Opplæringen skal sørge for at den ansatte mestrer arbeidet sitt, at arbeidet er meningsfylt og skal bidra til å forhindre arbeidsulykker samt fremme produktivitet (Arbeidstilsynet, u.å.). Det er organisasjonens ansvar å sørge for at den ansatte har mottatt tilstrekkelig opplæring for å kunne utføre arbeidet, samt mestre arbeidsoppgavene sine. Underveis i opplæringen vil også den ansatte underbevisst skape en bevissthet om hvilke konsekvenser arbeidet kan ha, eksempelvis endring av et tall i Excel som kan føre til at flere ark inneholder feil informasjon.

Et tiltak som mange organisasjoner har implementert og som også ble nevnt under vår intervju runde, er å sende ut eposter med informasjon. Dette kan være informasjon om trusselbildet, slik at de ansatte får med seg hvilke trusler de står ovenfor. For å opprettholde en god cybersikkerhet er de ansatte nødt til å vite hvilke risikoer de tar i arbeidet sitt, og hvilke risikoer man enkelt kan unngå. God informasjonsflyt kan være nøkkel til å øke bevisstheten til de ansatte, slik at man eksempelvis ikke åpner en mistenkelig epost fordi man tror den kan være ekte.

Hagen et al. nevner også at diskusjoner i grupper kan være en god måte å skape bevissthet innad i organisasjon. En felles diskusjon skaper muligheter for refleksjon om konkrete punkter man ikke har tenkt på tidligere. Ofte i løpet av skolegangen blir man satt i grupper for å diskutere en oppgave eller et resultat. Resultatet av dette er ofte at man ser nye perspektiver man ikke så tidligere, samt at man får flere sider av samme sak noe som belyser nye utfordringer eller løsninger. Dette kan man ta med seg direkte inn i organisasjonens verden, ved å legge til rette for gode diskusjoner som belyser nye sider og skaper bevissthet blant de ansatte.

Utfordringen med Hagen et al. (2008) sin modell er at den forutsetter at de ansatte tar rasjonelle beslutninger i henhold til policyer og prosedyrer for å komme seg videre til neste trinn. I en organisasjon der informasjonen ikke når alle, vil ikke de ansatte ha den nødvendige kunnskapen eller informasjonen for å ta rasjonelle beslutninger i ethvert scenario. Modellen fokuserer i stor grad på at et trinn følger et annet, og sett fra et teknologisk perspektiv fungerer modellen utmerket alene.

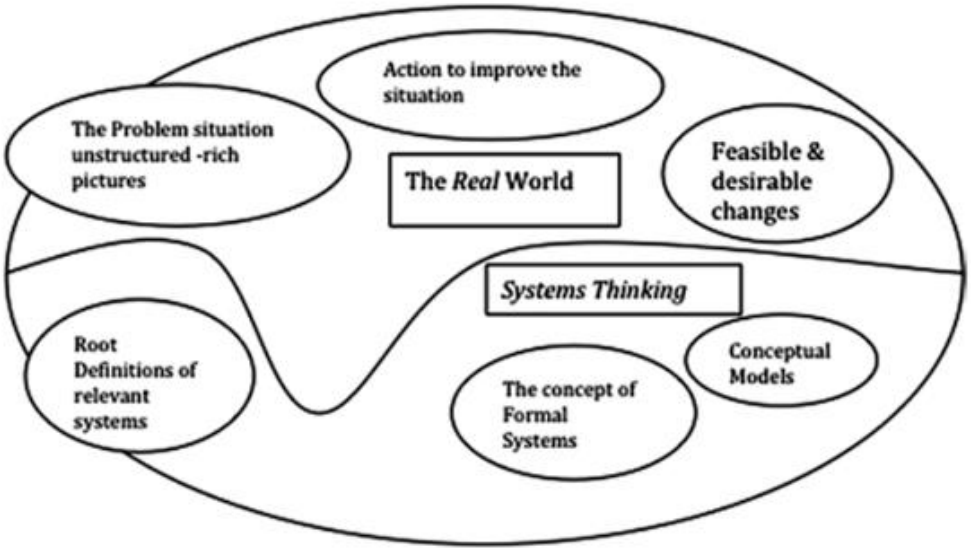
Dette er fordi man forutsetter at de ansatte tar «riktig» og rasjonelle valg i enhver situasjon og at ingen gjør feil. I virkeligheten vil de ansatte gjøre feil, bevisst eller ubevisst. Ofte vil en ubevisst feil være manglende kunnskap og kontekst rundt problemsituasjonen. Om man ser på hvert trinn for seg selv, så finnes det mye litteratur som støtter oppunder antakelsene som blir gjort underveis i modellen. Likevel vil trinnene være vanskelig å oppnå steg for steg, dersom man ikke implementerer de ansatte underveis. Det er heller ikke sikkert at modellen passer godt inn i hvordan organisasjon blir drevet på. Prosedyrer og organisatoriske endringer kan ha direkte innvirkning på hvordan arbeidsoppgaver blir gjennomført og kan føre til misnøye blant de ansatte.

Soft-systems metode

Soft systems metode eller SSM kom først fra Peter Checkland i 1981. Det er en tilnærming som tar for seg den sosio-tekniske delen av teknologien. Soft systems er systemer som har mennesker involvert i seg (Andriessen et al. 2023). SSM legger vekt på forståelsen av de ulike perspektivene hos interessentenes syn på et komplekst problem eller en situasjon. Et eksempel på soft system kan være et flyselskap. Et flyselskap kombinerer flymaskiner, datamaskiner, kommunikasjonsutstyr som disse tre vil gå under teknologi, også involverer flyselskapet mennesker gjennom piloter, bakkemannskap og flyvertinner (Andriessen et al. 2023).

Meningen med soft-systems metode er å sammenligne hva man kan observere i den virkelige verden og hva som kan bli tatt inn i system tenkning. Dette for å øke bevisstheten når det blir komplekse problemer. Om vi ser på Checkland sin modell av SSM sine kjernepunkter i figur 2, vil vi se på hva som foregår i den virkelige verden og hvordan en tilnærming til system tenkning av problemet er. Den virkelige verden tar for seg endringer som både er gjennomførbare og ønskelige, handlinger til å gjøre endringene og forstå det Checkland kaller Rich picture.

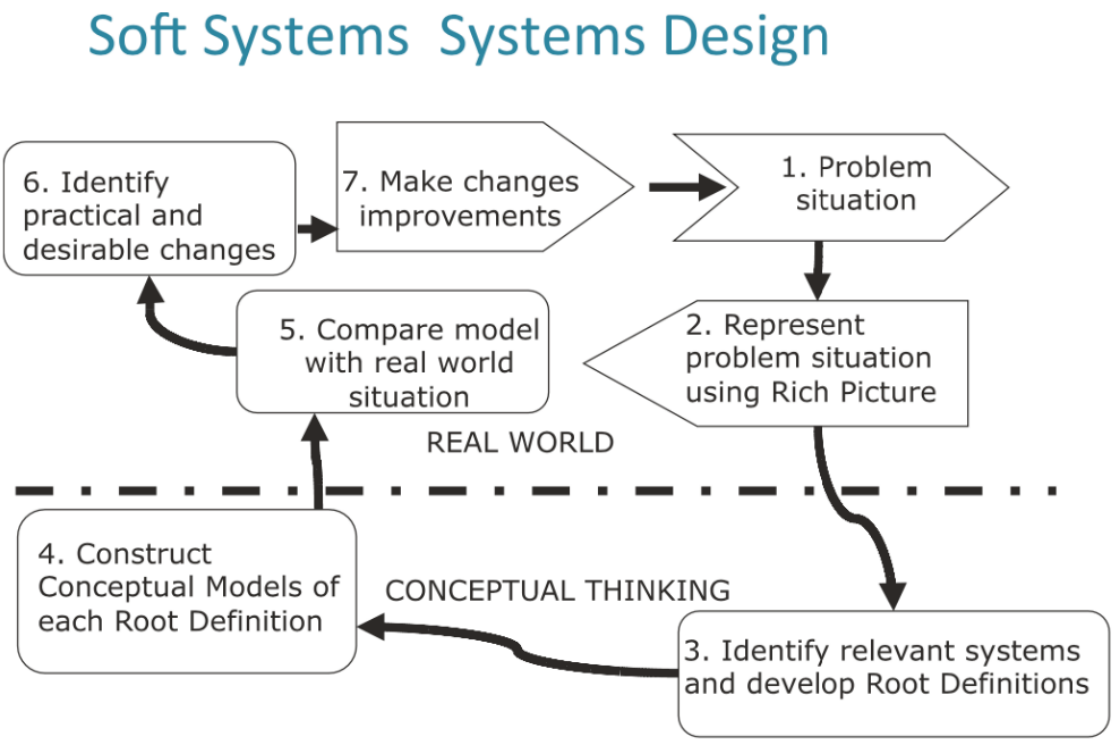
Rich picture eller dyp innsikt som vi har valgt å bruke i denne oppgaven, er et verktøy i SSM som kan vise om det er et system eller ikke (Checkland, 1981). Det fører også til at man får et godt overblikk over en kompleks situasjon eller et problem som kan løses. For å utføre en dyp innsikt må man bruke Checkland sine 7 steg. Dette blir gjort med interessenter for problemet. I systemtenkningsbiten av SSM til Checkland kommer det holistiske blikket på hvordan man skal løse problemet som har oppstått i den virkelige verden, samt hvordan konseptet fungerer i forhold til organisasjonens problem (Checkland, 1981).



Figur 2 SSM sine kjernepunkter (Andriessen et al. 2022)

Det er viktig å ha med seg et holistisk bilde av komplekse systemer. Dette fordi mange systemer er meget gode og oppfyller de ønskelige og gjennomførbare endringene, men systemene kan likevel feile grunnet at det ikke er kompatibelt med den virkelige verden og menneskene som skal operere i systemet (Baxter & Sommerville, 2011).

Figur 3 viser de 7 stegene til Checkland sin modell. Denne modellen kan bli brukt til å øke bevisstheten i en organisasjon på et problem område. SSM til Checkland er en prosess som kontinuerlig kan brukes for å øke bevisstheten i bedriften. Måten dette blir gjort på er å identifisere et problem eller situasjon som det er et ønske om å undersøke nærmere. Videre kommer forståelsen av situasjonen, dyp innsikt, som nevnt tidligere. Steg nummer 3 tar for seg identifisering av de underliggende rotårsakene til problemet. Det fjerde steget blir det utarbeidet en konseptuell modell. I neste steg blir den konseptuelle modellen vurdert inn mot interessentene om modellen er bærekraftig i den virkelige verden. Videre blir det vurdert endringer som er gjennomførbare inn mot problemsituasjonen. Siste steget handler om å gjennomføre endringene fra steg 6 (Checkland, 1981).



Figur 3 Checkland sin 7-stegsmodell (Andriessen et al. 2022).

Problemsituasjon

Problemsituasjonen er det som referer til problemet i bedriften. Det er i det første steget problemsituasjonen kommer inn, det er steget som belyser et problem eller en situasjon som en bedrift eller organisasjon ønsker å forbedre (Andriessen et al. 2022). Her blir en gruppe interessenter satt sammen for å arbeide med problemsituasjonen. Det er viktig i steg 1 å forstå hva problemstillingen hos bedriften er, dermed innhenter interessentene informasjon om problemstillingen for å få en oversikt over situasjonen. Det er flere forskjellige måter for interessentene å innhente informasjon på. Eksempler på typer informasjonsinnhenting som kan bli brukt er spørreundersøkelser eller observasjoner for å kartlegge bredest mulig.

Representere problemsituasjonen ved bruk av dyp innsikt
Dyp innsikt er et holistisk bilde av problem situasjonen som kommer frem i steg 1. At interessentene tar med seg flere detaljer og analyserer resultatene som kom fra kartleggingen i steg 1. Dyp innsikt vil si et bilde av problemsituasjonen som ser på det store og hele bildet i bedriften eller organisasjonen på et detaljnivå (Andriessen et al. 2022). Det er viktig å lage et bilde som ikke blir avgrenset til et for lite området, når man skal lage et bilde med dyp innsikt. Det er bedre med for mye enn for lite. Grunnen til dette er fordi det er viktig å ta i betraktning, alle de forskjellige aspektene rundt problemsituasjonen. Dermed er det ikke så viktig med å strukturere eller analysere den dype innsikten prosessen, men det er viktig å inkludere så mye informasjon som mulig for å få en riktig nok dyp innsikt.

Definere rotårsakene som er relevant for problemsituasjonen
Dette steget er det første steget i konsept tenkningsfasen. Her blir det utarbeidet rotårsaker til de forskjellige problemsituasjonene. Rotårsakene er mer presise beskrivelser på hva problemsituasjonene skal oppnå i de ulike systemene (Andriessen et al. 2022). Konsept tenkningsfasen er en refleksjonsfase av tidligere input fra steg 1 og 2 og vil få en output som setter lys og kommer frem til ulike løsninger på problemsituasjonene. Dette steget kan bli gjort flere ganger for å få et mer presist utfall av steget.

Utvikle konseptuelle modeller knyttet til rotårsakene
I dette steget blir det utviklet konseptuelle modeller på hvordan problemsituasjonen ideelt sett skulle fungert i bedriften. Konseptuelle modeller representer et system og brukes for å hjelpe personer å forstå eller simulere et emne som modellen presenterer (Andriessen et al. 2022). Modellene hjelper med å analysere og de er viktigere for senere steg i modellen til Checkland.

Sammenligne modellene og den virkelige verden
I dette stadiet blir modellen som ble skapt i den tidligere fasen ytterligere utviklet når modellen blir sett opp imot den virkelige verden (Andriessen et al. 2022). Det vil si å sette teorien av den konseptuelle modellen ut i praksis. Grunnen til dette steget er fordi det kan være forskjell på hvordan en modell fungerer i teorien og hvordan den fungerer i praksis.

Definere endringer mot problemsituasjonen
Dette steget handler om å gjøre bestemmelser om endringer i henhold til de konseptuelle modellene som er gjennomførbare og definere dem slik at problemsituasjonen nærmer seg den ideelle tilstanden som kom frem i steg 4 (Andriessen et al. 2022).Dette stadiet vil kunne føre til store endringer hos bedriften eller organisasjonen. Endringer kan være i strukturen, prosesser eller menneskelige adferd.

Implementering og forbedring av endringene
Det siste steget i Checkland er implementeringen av de definerte endringene i forrige steg og hvordan man tar det ut i bedriften (Andriessen et al. 2022). Det er viktig at implementeringen overvåkes og tilpasses etter behov som tiden går. Når dette skjer vil det oppstå nye problemsituasjoner som igjen starter Checkland sin 7 stegs modell, og bedriften vil kontinuerlig bli forbedret. Grunnen til at det vil oppstå nye problemsituasjoner er fordi det er en kontinuerlig utvikling og vil da føre til behov for forbedringer og endringer.

Det som Checkland tar med i sine modeller er det menneskelige aspektet. Checkland prøver å få frem med sin modell de underliggende faktorene og prosessene i en organisasjon, som ikke alltid er lett å se uten en analyse.

SSM er en god metode som gjør det mulig å forstå komplekse problemsituasjoner i bedrifter bedre, men det er også noen utfordringer knyttet til Checklands fremgangsmåte. Denne prosessen kan bli tidkrevende og komplisert, dette fordi slike komplekse problemer gjerne er svært omfattende. Er bedriften i tidsnød, kan denne metoden vise seg å være utfordrende å jobbe med, nettopp fordi den i stor grad er omfattende og tidkrevende. SSM krever interessenter, og noe som vil resultere i at ressurskapital blir bundet opp under prosessen. Dermed må bedriften være villig til å investere tid og menneskelig kapital for å få gjennomført metoden. En annen utfordring i SSM er interessentene som deltar i prosessen. Disse er som regel ikke objektive. SSM har også behov for en eller flere personer som kan fungere som fasilitator. Uten denne kan gruppedynamikken og prosessen bli uryddig. Det siste som er knyttet til utfordringene relatert til SSM er organisasjonens endringsvilje. Hvis organisasjonen møter mye motstand rundt endringer, kan det føre til at Soft system-metoden ikke er en egnet prosess for å forbedre problemsituasjonen i en bedrift.

Individ vs organisasjonslæring

Individuell læring refererer til læringsprosessen til enkeltpersoner, og hvordan de tilegner seg kunnskap og ferdigheter på egen hånd. Dette kan skje gjennom selvstudier, opplevelser, kurs, forelesninger eller interaksjoner med andre. Individuell læring kan være en effektiv måte å utvikle kunnskap eller ferdigheter innen spesifikke områder. Individuell læring er begrenset som virkemiddel i det planmessige arbeidet med å produsere og reprodusere organisasjonskompetanse, selv om individet og individets kunnskap er byggesteinene i organisasjonen. Organisert arbeid er også kollektiv samhandling. Derfor vil også forståelsen av hva som skal gjøres, måtte skapes i det samme kollektivet. Individuell kunnskap har et potensial som først utnyttes fullt i samhandling med andre. (Klev & Levin, 2009, s.92-93)

Organisasjonslæring handler derimot om hvordan organisasjonen tilegner seg kunnskap og ferdigheter som kan hjelpe dem med å forbedre ytelsen og nå sine mål. Dette kan være utvikling av retningslinjer og prosedyrer, implementering av ny teknologi samt opplæring av ansatte. Organisasjonslæring er ofte et fokusområde for bedrifter og organisasjoner som ønsker å forbedre effektiviteten og produktiviteten sin. Organisasjonslæring forutsetter at organisasjonens medlemmer på en eller annen måte deltar i læringsprosessen og kan ikke settes bort til noen få på av vegne av fellesskapet. (Klev & Levin, 2009, s.92)

Et lærende individ er nødvendig, men ikke en tilstrekkelig forutsetning for at organisasjonen lærer. Det er en nødvendig forutsetning siden organisasjonens oppgaver til syvende og sist utføres av individer i organisasjonen. Dersom individene verken har endret sine oppfatninger av arbeidet som skal utføres eller i realiteten gjør noe på en annen måte, vil heller ikke organisasjonen gjøre noe nytt. Derfor kan det heller ikke hevdes at organisasjonen har evnet å lære. (Klev & Levin, 2009, s.91)

En mulighet vi har til å øke bevisstheten rundt cybersikkerhet gjennom individuell læring kan være et eksternt kurs der det individuelle medlemmet høster erfaringer, refleksjoner og ideer som skaper grunnlag for en ny praksis. Faren her er at dette medlemmet ofte får den gamle organisasjonsmessige hverdagen midt i fleisen når de kommer tilbake, og vi kan derfor ikke si at læring på individnivå automatisk skaper endringer på organisasjonsnivå.

Endringer i organisasjoner kan ikke bare rettes mot å bygge opp nye individuelle kunnskaper og ferdigheter, men må også ta høyde for utvikling av samhandlingen mellom medlemmene. Den bruksteorien som styrer samspillet mellom organisasjonens enheter, er et sosialt produkt som er skapt over lang tid. Endringer i bruksteorien kan heller ikke skje på en annen måte gjennom sosialt samspill og praktisk trening. (Klev & Levin, 2009, s.93)

Oppsummering av teorikapittelet

Som nevnt i forklaringen av trappetrinnsmodellen trenger man en bedre forståelse av problemsituasjonen, samt menneskelig involvering for å kunne utnytte modellen på en effektiv måte. Ved å forvente rasjonelle beslutninger av de ansatte vil modellen virke mer effektiv enn den er, og man ender med at de som styrer metodikken tror at man er trinn over det man er.

Ved å ta med SMM som metode med trappetrinnsmodellen vil man kunne opparbeide en bedre forståelse av problemsituasjonen og man vil kunne utarbeide mer hensiktsmessige policyer og prosedyrer. I tillegg kan man ta med de ansatte i SSM metoden, slik at de ansatte kan føle eierskap til løsningen man ender med. SSM er ikke en cyber awareness metode, men hvis man bruker trappetrinnsmodellen og de grunnleggende teknologiske sikkerhetsløsningene ifølge Hagen et.al., så kan dette hjelpe SSM til å komme frem til en løsning på cyber awareness. SSM kan også være en god fasilitator for organisasjonslæring og deling av kunnskap og informasjon innad i organisasjonen. Dette bidrar til økt detaljkunnskap og informasjonsflyt, som kan gi de ansatte bedre grunnlag for å ta rasjonelle beslutninger ved å gjøre de mer bevisst på konsekvensene av beslutningene som må tas.

Ved å få en høyere bevissthet blant de ansatte vil organisasjonen i større grad dra nytte av policyene og bestemmelsene som blir gitt. Dette er fordi at det er mer sannsynlig at ansatte tar rasjonelle beslutninger og ikke utsetter organisasjonen for risiko. Dette kan for eksempel være å sende personsensitiv data via Messenger eller lignende tjenester fordi man sparer tid i forhold til normale prosedyrer.

Når ansatte er involvert i prosessen, og hensikten er å oppnå organisasjonens mål, kan dette bli sett på som organisasjonslæring. Ved en SSM er det en kontinuerlig forbedringsprosess som tar med seg ansatte inn mot forbedringene. Disse ansatte tar høyde for å forbedre hele læringen i organisasjon, og ikke bare seg selv.

Metode

Formålet med prosjektoppgaven er å øke bevisstheten på cybersikkerhet hos en mellomstorbedrift. For å gjøre dette har vi brukt ulike forskningsmetode verktøy for å komme frem til svar på forskningsspørsmålet til oppgaven.

Forskningsstrategi

Valg av prosjektoppgavens metode er først og fremst avhengig av oppgavens problemstilling, men også oppgavens formål og omfang. Valget mellom en kvalitativ og kvantitativ forskningsstrategi kan sees på som et pragmatisk valg eller et valg av vitenskapsfilosofisk standpunkt (Ringdal, 2018). For å kunne besvare prosjektoppgavens problemstilling best mulig, er det essensielt med innhenting av data gjennom bestemte metoder. En kvalitativ forskningsstrategi fokuserer på innhenting av mengder informasjon, samt dypere forståelse av sammenhenger og komplekse situasjoner (Leedy & Ormrod 2021). Dette vil i prosjektoppgavens tilfelle fremstå som hensiktsmessig grunnet behov for stor grad av detalj ved utforskning av forskjellige konsepter og erfaringer.

Prosjektoppgavens problemstilling tillater en viss nærhet til det som studeres, samt behandling av tekstdata og uformelle analyseteknikker. Behovet for dypere forståelse kommer frem blant annet av verdien som kommer av å studere hvordan prosesser og daglig drift gjennomføres i Anlegg AS. White og Cooper (2022) beskriver hvordan et rent objektivt syn ikke er intensjonen ved kvalitativ forskning, men heller et syn på hvordan virkeligheten er konseptualisert og vårt/casebedriftens bilde av verden.

Det er i tillegg til den kvalitative forskningsstrategien blitt gjennomført kvantitative metoder for innhenting av data. Dette er sett på som hensiktsmessig ettersom det innenfor det kvantitative paradigme oppstår et ønske om en "bredere" forståelse og kartlegging av dagens situasjon i Anlegg AS. Ifølge Ringdal (2018) går kvantitative metoder i bredden ved at de registrerer sammenlignbar og strukturert informasjon i et stort utvalg, som gjerne analyseres gjennom statistiske analysemetoder.

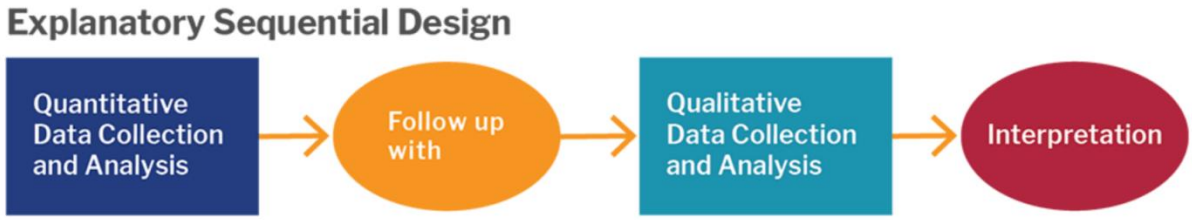
Oppgavens forskningsstrategi kan bli sett på som en kombinasjon mellom kvalitative og kvantitative forskningsmetoder, ofte kalt "mixed methods", eller blandede forskningsmetoder. Ifølge Heale og Forbes (2013) kan bruk av kombinasjonen kvalitative og kvantitative forskningsmetoder for å besvare et spesifikt forskningsspørsmål resultere i tre forskjellige utfall. Første utfall er konvergering av resultater og dermed føre til like konklusjoner. Resultatene kan også relatere seg til forskjellige objekter og fenomener, men kan være komplementære til hverandre og dermed brukes til å supplere individuelle resultater.

Til slutt kan resultatene være divergerende eller motstridende. Bruk av "mixed methods" er sett på som hensiktsmessig i denne prosjektoppgaven ettersom konvergerende resultater kan føre til økt validitet gjennom verifisering, mens komplementære resultater fremhever ulike aspekter ved et fenomen. Divergerende, eller motstridende resultater kan føre til nye og bedre forklaringer på fenomenet som undersøkes.

Forskningsdesign

Innenfor både det kvalitative og kvantitative forskningsdesign er det sett på som hensiktsmessig å gjennomføre en case-studie, hvor Anlegg AS er tilfellet. Dette passer fint med Yin (2018) sin beskrivelse om case-studiens evner til å la forskeren fokusere i dybden på et tilfelle, samt beholde et helhetlig og virkelighetsbasert perspektiv. Bevissthet rundt cybersikkerhet i en mellomstor bedrift er i høy grad sentrert rundt menneskets atferd og organisatoriske og ledelsesmessige prosesser, som legger grunnlaget for valg av forskningsdesign. Ettersom det gjennom prosjektoppgaven er benyttet både kvalitative og kvantitative forskningsmetoder, vil forskningsdesignet bevege seg i retning "mixed methods case study design". Dette er en type studie innen "mixed methods" der den kvantitative og kvalitative datainnsamlingen, resultatene og integrasjonen brukes til å gi en dyptgående forståelse av en sak eller utvikling av materiale for sammenlignbare analyser (Creswell & Clark, 2017).

Prosjektoppgavens "mixed methods" case-studie har en forklarende sekvensiell tilnærming til innhenting av data og analyse, se figur 4. Dette er en tilnærming innen "mixed methods" der forskningen består av to distinkte faser; kvantitativ etterfulgt av kvalitativ forskningsmetode (Ivankova et al., 2006). Det er gjennom prosjektoppgaven først blitt samlet inn og analysert kvantitative data (spørreundersøkelse). Kvalitative data som dybdeintervjuer og observasjoner er samlet inn som nummer to i sekvensen, og bidrar med å forklare, eller utdype de kvantitative resultatene oppnådd i første fase. Den kvalitative fasen bygger på den første, kvantitative fasen og begge fasene kobles sammen underveis i studien. For prosjektoppgaven gir kvantitative data og påfølgende analyse en generell forståelse rundt forskningsspørsmålet, mens kvalitative data og dets analyse foredler og forklarer funn fra første sekvens i dybden.



Figur 4 "Forklarende sekvensielt forskningsdesign" (Harvard Catalyst, 2023)

Datainnsamling

Det er gjennom prosjektoppgaven blitt innhentet data ved bruk av spørreundersøkelse, observasjoner og dybdeintervjuer. Informasjonen vi har hentet inn handler i stor grad om hvordan dagens systemer fungerer, hvordan de ansatte ser på endringen rundt digitaliseringen, hvordan dagens situasjon er i forhold til cybersikkerhet og hvor kunnskapsnivået rundt cybersikkerhet ligger.

Vi begynte datainnsamlingen med en spørreundersøkelse for å få en bedre forståelse av hvilke spørsmål vi trengte videre svar på. Etter spørreundersøkelsen gikk vi gjennom svarene og analyserte de hver for oss. Deretter sammenlignet vi analysene, slik at man får to perspektiver og kan danne et bedre grunnlag for forståelse av svarene. Etter å ha analysert svarene kom vi frem til noen punkter vi så mangler på. Blant annet manglende fokus på policyer fra de ansattes side, et veldig høyt fokus på cybersikkerhet sammenlignet med kunnskapsnivået blant de ansatte og uregelmessigheter knyttet til passordpolicy.

Derfor var vi nødt til å lage en intervjuguide for å kunne danne et bedre bilde av spørsmålene vi trenger. Ved å lage en intervjuguide på forhånd får vi en bedre mulighet til å forberede intervjuene, samt at det er enklere å lage et informasjonsskriv om hva man ønsker å gå gjennom med intervjuobjektene. Vi følte det var viktig at de ansatte vi intervjuet fikk et informasjonsskriv i forkant, slik at de hadde mulighet til å forberede seg og ikke følte at de ble tatt på sengen underveis i intervjuene.

Intervjuene ble gjennomført ved at en av forskerne tok ansvar for samtalen, mens den andre var skribent og skrev ned alt. Som regel gikk dette veldig bra og objektene snakket i en fart der det er mulig å holde følge for skribent. I enkelte scenarioer kunne det gå for fort, og dersom vi følte at noen av svarene falt ut av kontekst i notatene så ble disse fjernet etter at vi hadde analysert de.

Rett etter intervjuene gikk vi gjennom svarene og gikk gjennom vår opplevelse og oppfatning av svarene som ble gitt. Dette var for å ha muligheten til å huske kontekst rundt svarene, slik at vi ikke måtte fjerne svar der kontekst uteble i notater. Senere ble det igjen analyserte vi igjen hver for oss, før vi sammenlignet svar og perspektiver. Denne metoden fungerte godt med å gi oss forståelse for svarene som ble gitt.

Det ble også gjennomført observasjoner underveis i prosjektet, da prosjektet har mulig for on-site observasjon ved at en forsker er ansatt i Anlegg AS.

Spørreundersøkelse

Spørreundersøkelse er en forskningsmetode som belager seg på å sende ut spørsmål til et større utvalg, hvor svarene blir kodifisert for å finne ut om det eksisterer trender eller mønstre innen utvalget (Leedy & Ormrod, 2021).

Spørreundersøkelse er i prosjektoppgavens tilfelle først og fremst brukt for å kartlegge dagens situasjon, med hensikt om å belyse ansattes tanker om nye rutiner. Kartlegging av dagens situasjon kommer av et behov for å finne et gjennomsnittlig ståsted for ansatte i forbindelse med IT og cybersikkerhet. Behovet for innhenting av ansattes tanker om nye rutiner kommer blant annet av en potensiell sammenheng mellom cybersikkerhetskunnskap og hvor positivt innstilt man er til endring av rutiner.

Det er gjennom prosjektoppgaven blitt brukt en webbasert spørreundersøkelse, men utsendelse av et spørreskjema til 39 respondenter i Anlegg AS. Spørreundersøkelsen inneholdt totalt 39 spørsmål. Respondenter er hentet inn gjennom en "purposive sampling", som vil si at respondenter er rekruttert gjennom bestemte kriterier (Leedy & Ormrod, 2021). Kriterier brukt ved rekruttering var at respondentene jobbet i Anlegg AS og hadde en e-post tilknyttet Anlegg AS og var koblet opp mot serveren. Dette resulterte i at enkelte ansatte i Anlegg AS ble utelukket.

Kriteriene kommer blant annet av ledelsens oppfattede begrensede verdi av data fra ansatte som verken var på serveren eller hadde intern e-post. Selve rekrutteringen av respondenter ble gjort gjennom en felles e-post sendt til ansatte i Anlegg AS. For å sørge for høy svarprosent ble det sendt ut påminnelser etter en viss tid var gått.

Spørreundersøkelsen har i dette forskningsprosjektet blitt brukt som en deskriptiv undersøkelse for å samle inn informasjon om prosentvise andeler og ulike nivåer på eksempelvis kunnskap og implementering av cybersikkerhet i virksomheten. Dette ga oss et bedre grunnlag for å lage spørsmål til intervjuguiden og finne relevant informasjon underveis i intervjuene.

Spørsmål stilt i spørreskjemaet er utarbeidet i samarbeid med daglig leder i Anlegg AS og prosjektoppgavens veileder. Det er tatt utgangspunkt i at spørsmålene danner et godt grunnlag for belysning av prosjektoppgavens problemstilling, samt videre analyse gjennom intervjuer og observasjoner. Respondentenes besvarelser er anonyme og dermed ikke sporbare.

Dybdeintervju

Dybdeintervjuer er ofte brukt innen kvalitativ forskning og i case-studier, og er prosjektoppgavens tilfelle. Denne formen for intervjuer har muligheten til å føre meningsfulle samtaler som kan resultere i bedre innsikt, samt ny kunnskap. Intervjuer i en case-studie vil ofte bære preg av en guidet samtale fremfor et strukturert oppsatt spørreskjema (Yin, 2014). Gjennomførte intervjuer har fulgt et semistrukturert oppsett der det ifølge Leedy et al. (2021) kan fremkomme tilpassede oppfølgingsspørsmål basert på situasjon, og dermed åpne opp for en dypere forståelse av intervjuobjektets resonnement og tanker.

Prosjektoppgavens intervjuobjekter er gitt friheten til å svare som de vil, og er ikke avhengig av å vite hva andre intervjuobjekter har svart. Det er kun individets egne meninger, oppfatninger og erfaringer som ligger til grunn. En utfordring ved dybdeintervjuer kan være å stille de rette spørsmålene, samt unngå at intervjuobjektet beveger seg utenfor hva forskningen tar for seg.

Ved å stille åpne, fremfor ledende, spørsmål kan det stimulere til en informativ samtale uten at intervjuobjektets svar påvirkes av hva som antas å være "riktig" eller "korrekt". Spørsmålene som er stilt har hatt et behov for å være enkelt formulert for å gi deltaker mulighet til forståelse og refleksjon (Leedy et al., 2021). Basert på forskningsdesignet har det vært hensiktsmessig å benytte seg av dybdeintervjuer med ett intervjuobjekt av gangen.

Dersom det etter gjennomførte intervjuer oppstår store gap i hvordan standard og praksis i bedriften er, vil det bli tatt i bruk en gap-analyse som et verktøy for å analysere og åpne opp for innsikt i avvikets opprinnelse. Det er grunnleggende med lik standard og praksis, hvor en betydelig forskjell vil kunne føre til stagnering innen teknologisk utvikling ved dagens digitalisering. Arbeidet vil gå som planlagt dersom gap mellom ansatte og ledelse ikke kommer frem.

Potensielle feilkilder ved bruk av intervju som forskningsmetode kan oppstå, som kan påvirke slik at datainnsamlingen får andre svar enn den ville gjort ved andre forhold. Slike feilkilder kan være noe så lite som intervjuobjektets dagsform, men kan ha stor betydning på prosjektoppgavens utfall. Denne "usikkerheten" er forsøkt eliminert ved å sende ut intervjuguide i forkant av intervjuene, som gir intervjuobjektene tid til å forberede seg og gi et best mulig svar fra deres side.

Utvalg av intervjuobjekter

Den kvalitative tilnærmingen tar for seg å velge informanter som er av relevans til problemsituasjonen som skal studeres. Elementer som støtter en kvalitativ tilnærming i henhold til intervjuobjektene, kan forankres i behovet om å undersøke ulike ledd i organisasjonen (Leedy & Ormrod, 2021).

Måten vi valgte intervjuobjekter var å finne interessenter som kunne gi oss en dyp innsikt. Dette var personer som var i forskjellige stillinger i forskjellige avdelinger av bedriften, men samtidig kunne gi oss et godt bilde på situasjonen. De intervjuobjektene vi valgte var blanding av toppledelsen, mellomledere og medarbeidere. Vi valgte kun å bruke intervjuobjekter som satt på kontor. Grunnen til dette er fordi bedriften ikke ville at intervjuene skulle ta av driften på ansatte ute, og at det i stor grad er de ansatte på kontordelen som blir påvirket av digitaliseringsprosessen i prosjektperioden.

Utvalgsstørrelse på intervjurunder kan være avhengig av kvaliteten på intervjuene som blir gjennomført. Leedy & Ormrod (2021) sier at ikke finnes noen fasit for en god utvalgsstørrelse og at det fra enhver intervjurunde kan variere basert på tre elementer; tilgjengelige ressurser, populasjon og forskningsspørsmål.

Det er totalt blitt gjennomført dybdeintervju av 7 intervjuobjekter. Intervjuobjekter er valgt gjennom et behov for interessenter som bidrar til bred nok forståelse av dagens situasjon. Dette er ansatte med forskjellige stillinger tilhørende forskjellige avdelinger i Anlegg AS. Intervjuobjekter bestod av en blanding av toppledelse, ledere og medarbeidere, og er avgrenset til ansatte på kontor ettersom intervjuene ikke skulle bruke tiden til ansatte ute. Intervjuobjekter er fra forskjellige deler av landet, og det ble opprettet kontakt for å planlegge dato og arena for gjennomførelse i forkant av intervjuene.

Intervjuguide

Intervjuobjektene fikk tilsendt informasjon og temaer i forkant av intervjuet, slik at de hadde mulighet til å forberede seg. På denne måten sitter vi ikke i intervjuet med et objekt som er usikker på hva de skal bli intervjuet om, og de får en mulighet til å forberede seg. Intervjuguiden ble utarbeidet av studentene etter spørreundersøkelsen, med innspill fra veileder. Guiden hjelper også oss studenter med å huske spørsmål.

Vi tok i bruk en semi-strukturert guide der alle temaer er satt på forhånd, men rekkefølgen blir bestemt underveis i intervjuet. Dette gir oss mulighet til å bygge videre på det intervjuobjektet forteller, uten å måtte hoppe til et nytt tema. Denne fleksibiliteten hjalp oss med å gi rom for å snakke om temaer når objektet ønsket det selv, slik at intervjuet blir mer spontant og vi får svar som ikke er uttenkt på forhånd.

Noen fordeler ved bruk av semi-strukturert intervju er at de samme spørsmålene gir likt grunnlag for alle objektene, men at intervjuet til en viss grad formes ut ifra svarene. Dette kan føre til at objektet føler at intervjuet oppleves mer som en samtale enn et avhør. Noen ulemper er at intervjuerne må ha kontroll på hvilke erfaringer og opplevelser det blir snakket om, å ta valg ut ifra dette. Det kan også gjøre det enklere å spore av fra intervjuguiden, noe som kan føre til utfordringer når man skal sammenligne svarene fra de andre objektene

Intervjuene ble gjennomført digitalt og deltakerne ble informert om fullstendig anonymisering, der ingen svar kunne lede tilbake til dem. Dette var for å skape en trygghet i intervjuet, slik at objektet kunne snakke fritt. Videre ble objektene også informert om at de kunne la vær å svare på spørsmål, dersom de følte på det.

Intervjuet ble ledet an av den ene studenten, mens den andre hadde ansvar for å skrive referat og deltok sporadisk med oppfølgingsspørsmål. Dette var for å sikre at vi fikk med oss svarene, slik at de ikke gikk tapt underveis i intervjuet. Dersom vi i analyseprosessen fant svar som ikke ga mening gitt kontekst, ble disse slettet.

Observasjoner

I tillegg til datainnsamling gjennom intervju og spørreundersøkelse er det også blitt gjennomført observasjoner gjennom en fullstendig observerende rolle. Prosjektoppgavens observasjoner kommer først og fremst av en unik on-site observasjonsevne ettersom én forsker er ansatt i Anlegg AS.

Observasjoner har bidratt til en videre forståelse etter gjennomført spørreundersøkelse og dybdeintervjuer, og sørger for en økt kredibilitet. Ettersom observerende forsker er ansatt i Anlegg AS, har det vært svært viktig å ta høyde for inhabilitet. Observerende forsker har dermed observert på avstand under observasjoner slik at utfallet fremkommer upåvirket.

Rekruttering av informanter

Måten vi har rekruttert informanter til spørreundersøkelsene våre er å sende ut felles e-post til alle som har tilgang til serveren til Anlegg AS og inviterte informantene til å delta på spørreundersøkelsen. Dette fungerte veldig bra. For å prøve å få så høy svarprosent som mulig sendte vi ut flere påminnelser til de inviterte slik at de ikke glemte å svare.

Rekrutteringen av intervjuobjekter gjorde vi på en annen måte, her rekrutterte vi gjennom dialog med toppledelsen i bedriften om hvem som kunne være gode intervjuobjekter slik at vi fikk mest mulig spredt utover bedriften. Dette førte til at vi valgte intervjuobjekter fra fra forskjellige avdelinger i forskjellige deler av landet. Intervjuobjektene tok vi kontakt med for å finne hvilken dato og tid det passet best for de og delta i intervjuet på.

Forskningens troverdighet

Når det kommer til kvalitativ forskning er det avgjørende å fremme et troverdig forskningsprosjekt, hvor prosjektets troverdighet kan ha mye å si. Dette innebærer i hvilken grad man kan stole på resultatene og konklusjonene som presenteres i forskningsprosjektet, samt hvor tillitsvekkende og troverdig forskningen er.

I prosjektet har vi benyttet kvalitativ metode, med innspill fra kvantitativ forskning, som handler om å skape kontekst og forståelse, basert på de ulike perspektivene fra intervjuobjektene. For å skape troverdighet ble det benyttet semi-strukturerte intervjuer med 7 ansatte ved Anlegg AS, samt observasjon i bedriften.

Validitet og reliabilitet

Innen forskning stilles det alltid spørsmål om dataens pålitelighet. Dette beskrives om som reliabilitet, fra det engelske ordet reliability. Golafshani (2003) beskriver reliabilitet som; I hvilken grad resultatene er sammenhengende over tid, og at det gir en riktig representasjon av den totale populasjon som studeres. Reliabilitet knytter seg til nøyaktigheten av forskningens data, hvilke data som brukes, hvordan dataen samles inn og hvordan dataen håndteres og bearbeides (Johannessen et al. 2016).

Validitet sier noe om gyldigheten av prosjektet. Om prosjektet har validitet eller ikke blir bestemt gjennom hvilken grad det kan bli trukket gyldige konklusjoner til det tiltenkte formålet som skal bli undersøkt gjennom en studie (Dahlum, 2021). Prosjektet vårt er en case-studie og ene prosjektmedlemmet jobber i case-bedriften. Dette kan føre til feilaktige eller objektive konklusjoner. Dette har vi valgt å løse med at det prosjektmedlemmet som ikke jobber i Anlegg AS har holdt god avstand fra bedriften.

For å sikre en god kvalitet på dataen og forskningsprosjektet, ble det lagt ned store ressurser i utformingen av intervjuguiden. Ettersom dette er vår hovedsakelige innsamling av data, var det svært viktig for oss at denne ble utarbeidet på en god måte som sikret at intervjuene ble gjennomført på best mulig måte. En godt utarbeidet intervjuguide gjør at vi får dekket alle ønskede temaer og at svarene fra objektene er relevante til vårt forskningsspørsmål. Underveis i intervjuene ble det også endret litt på intervjuguiden, da enkelte punkter ble sett på som irrelevante i henhold til svarene som ble gitt. Enkelte spørsmål ble også omformulert, dersom objektene ikke forsto spørsmålet.

Hovedfokuset var at spørsmålene som ble stilt under ikke skulle være ledende. Ledende spørsmål kan endre svarene fra objektene og gå utover reliabiliteten og gyldigheten til svarene som blir gitt. Målet var å fremstå som pålitelige og åpne gjennom intervjuprosessen, og objektene ble informert om at det skulle være et åpent intervju for å skape et trygt miljø.

Underveis i forskningen har det vært fokusert på potensielle fallgruver knyttet til om informasjonen vi har mottatt er korrekt. Dette kan være om intervjuobjektene har gitt feil informasjon, enten bevisst eller ubevisst. Under intervjuprosessen kan det være at objektene ikke følte seg trygge og derfor ikke gir hele sannheten. Dette kan være i frykt om at svarene kan få konsekvenser for objektene eller det kan være gjort ubevisst i god tro om at det er unyttig informasjon. Intervjuobjektet kan også fremstille situasjonen som bedre enn den egentlig er. Dette kan være fordi objektet vil fremstå bedre eller det fremstå fordelaktig å stille organisasjonen i bedre lys.

For å motarbeide disse fallgruvene gjorde vi det tydelig på starten av intervjuene og i informasjonsskrivet som ble gitt ut i forkant at alle svar er anonyme, og at de ikke kan spores tilbake til objektet. Det ble også nevnt at det ikke er noen andre i organisasjonen som vet hvem som intervjues. For å motarbeide en forbedret fremstilling av situasjonen valgte vi å intervjue 7 objekter, samt markere ut svar som stikker seg ut fra mengden og analysere disse nærmere.

En annen kilde til feilinformasjon er kritisk kildebruk underveis i forskningsprosjektet. Dersom man bruker informasjonskilder ukritisk kan dette være til feiltolkninger data og empiri, noe som vil gi følgefeil videre i forskningen. Vi har håndtert dette ved å vurdere kilder før bruk og analysering av dataene. Kildens påstander og utsagn blir diskutert mellom forskerne for å forminske muligheten for forskjellige tolkninger, noe som gir en økt validitet på prosjektet.

Generalisering

Generalisering handler om i hvilken grad forskningen kan være relevant for andre organisasjoner, personer eller situasjoner. Innen kvalitativ forskning har man en hensikt om å gi en kontekstualisert og rik forståelse av menneskelige erfaringer gjennom studie. Derfor er det komplisert og kontroversielt å generalisere funnene gjort underveis i prosjektet.

Polit & Beck (2010) sier at det kan skape konflikter om viktigheten av generaliserbarhet ettersom generalisering kan være kunstig eller begrenset grunnet de kontekstuelle tilfellene som studeres.

Anlegg AS er en standard mellomstor bedrift, uten noe spesielle eller unike trekk. Det er en gjennomsnittlig kompetanse på teknologi og cybersikkerhet. Dette gjør at Anlegg AS ikke har noe lavere sjanse for å forstå problemer eller utfordringer knyttet til sentrale temaer i prosjektet. Dette til grunn, så kan funnene som er gjort underveis i studiet gjelde for flere mellomstore bedrifter og ikke bare for Anlegg AS.

Etiske hensyn og håndtering av data

Prosessen med håndtering av data startet med å ta kontakt med veileder. Før prosjektet startet søkte vi NSD og undersøkte hvilke krav som blir stilt til prosjektets innsamling av data. Underveis i prosjektet har vi ikke håndtert personopplysninger eller identifiserende informasjon.

Spørsmålene under intervjurunden inneholdt ikke personlige eller personidentifiserende spørsmål. Intervjuene samlet kun inn anonymisert data, i tillegg til at bedrift og intervjuobjekter har blitt anonymisert i teksten. Navnene som har blitt brukt i prosjektet har vært for å referere til et fast punkt underveis, eksempel Anlegg AS og er kun for å gi leseren en bedre opplevelse. Et prosjektmedlem har en stilling i Anlegg AS, men ettersom vi ikke fremstiller bedriften i annet enn form av empiri har ikke dette hatt en innvirkning på vinklingen av bedriften.

Resultat

Resultatene som kommer frem i oppgaven vår, har kommet gjennom intervjurundene og spørreundersøkelsen vi har hatt i prosjektet. Resultatene er refleksjoner fra ansatte i Anlegg AS. Det er også gjort observasjoner av det gruppemedlemmet som jobber på Anlegg AS. For å anonymisere intervjuobjektene har vi valgt å bruke fiktive navn.

Konsekvens av cyberangrep

Intervjuobjektene fikk spørsmål om de hadde nok informasjon om trusler på internett. De fikk samtidig spørsmål om hva de kunne gjort for å øke oppmerksomheten mot trusler. Gjennom intervjuene med de ansatte i Anlegg AS, ble det tydelig at det er en oppfatning blant de ansatte at konsekvensene av et cyberangrep eller andre ondsinnete angrep er underkommunisert.

Det de ansatte var mest opptatt av var den manglende informasjon om hva som kunne skje både individuelt og organisatorisk dersom bedriften ble utsatt for et cyberangrep. Noen av de ansatte uttrykte et ønske om oppdateringer og mer informasjon rundt konsekvensen av et cyberangrep og hva som er lurt å gjøre i forhold til trusler. For å få mer kontinuerlige oppdateringer ble det nevnt at oppdateringene kunne komme i form av nyhetsbrev eller ukentlige/månedlige informasjonse-poster om endinger og nye trusler i dataverden, samt regelmessige påminnelser om cybersikkerhet.

Intervjuobjekt 1 – Susann

«Kunne tenke meg å få oppdatering på mulige trusler akkurat som jeg får av nettbanken.»

Resultatene i spørreundersøkelsen avslørte at syv deltakere konsekvent valgte å låse pcen sin hver gang de forlot den. Ytterlige syv deltakere svarte det samme, men bare hvis de var over 30 sekunder borte fra pcen. I intervjurunden kom det frem at det var ingen som låste pcen sin, bortsett fra én som låste pcen sin fordi den ansatte hadde andre rettigheter på serveren enn de andre ansatte. Det som personen sa i intervjuet var at «Jeg låste ikke pcen tidligere, men gjør det nå siden jeg har skjønt at ikke alle har tilgang til samme informasjon som meg».

Det kommer også frem at det er flere som ikke låser pcen grunnet de sitter i låst bygg og de tror folk har bedre ting å gjøre enn å gå inn på deres pc. Observasjoner gjort av gruppemedlemmet som jobber på Anlegg AS er at det har vært flere personer gjennom dette året som ikke har jobbet hos Anlegg AS som har hatt tilgang til bygget grunnet andre jobber.

Intervjuobjekt 2 -Kari

«Synes det var stress å låse pcen i starten, men nå har jeg skjønt konsekvensene av å la være.»

Etter å ha lest retningslinjene om cybersikkerhet i bedriften faller det naturlig at de ansatte føler seg underkommunisert på konsekvensene som kan oppstå etter et cyberangrep. Grunnen til dette er fordi cybersikkerhet er et ganske nytt begrep hos Anlegg AS og gjennomsnitts ansienniteten hos Anlegg AS er på 12 år. Dermed har ikke alle fått lest de nye retningslinjene i personalhåndboka for cybersikkerhet som kom i 2018 hos Anlegg AS.

Personalhåndboka skal leses av alle nyansatte og skal signeres at de har lest gjennom. På den andre siden trenger ikke de ansatte som har jobbet der i lang tid å signere på at de har lest den oppdaterte versjonen av personalhåndboka. Det vi fant gjennom spørreundersøkelsen og intervjuene er at noen ansatte har lest personalhåndboka, men i praksis så opprettholder de ikke retningslinjene.

En potensiell grunn til den manglende konsekvenstenkningen når det kommer til cybersikkerhet kan være at bedriften tidligere har opplevd svært få cyberangrep. I tillegg har konsekvensen av disse angrepene vært såpass små, at det ikke har påvirket bedriften i stor grad. Et eksempel på en konsekvens var at de ansatte ikke kunne være på datamaskinen i 30 minutter. Det er naturlig å tenke at dersom konsekvensene i tidligere angrep hadde vært større, ville også bedriften i større grad fokusert på cybersikkerhet. Det kan også være at de ansatte hadde flere tanker om cyberangrep som ikke kom frem under intervjusesjonene, da disse kun var på 30 minutter.

Ansattes forhold til internett og data

Resultatene av spørreundersøkelsene og intervjuene var at det var blandet forhold til internett og data. Noen synes det var morsomt å prøve nye ting og se på hvilke muligheter internettet hadde. Andre synes var greit å gjøre det minimale på dataen og internettet.

Et av funnene våre blant ansattes forhold til internett og data er at de ansatte har en oversikt over hvilke ting de bør se etter om en e-post er godartet eller ondsinnet. Det som flere ansatte gir uttrykk for er at det har blitt vanskeligere og vanskeligere de siste årene og skille mellom gode og onde e-poster. Det de ansatte forklarte var at hvis de var usikre på en e-post så spurte de IT om hjelp. Dette vil si at samtlige er oppmerksomme på innkommende e-poster, men det som kom frem var at de ansatte ikke hadde samme forhold til nettsider som e-post. Intervjuobjektene ga også uttrykk for at de ikke hadde like god kjennskap til risikoer på nettsider, som de har på e-post.

Intervjuobjekt 3 Kent
«Føler at jeg har god kontroll på de truslene jeg møter på pcen.»

Intervjuobjekt 3 Kent mente på at han hadde god kontroll på farer som kunne komme på pcen. Kent var en av de som er blitt observert mer ivrig på nyheter på data og internett, samtidig som han uttrykket det I intervjuet.

Gjennom året har det vært observert flere ganger at ansatte har vært oppmerksomme på svindel e-poster. Det er derimot langt færre av de ansatte som vi har sett gjennom observasjoner og intervjuer som var like oppmerksomme på nettsider og nedlastninger fra nettet. De var mindre kritiske til internettet.

Ansatte som ble intervjuet ved Anlegg AS uttrykket forståelse ovenfor IT-policyen til bedriften. Denne forståelsen kom i hovedsak av at de så nødvendigheten av å ha regler for internettbruk og håndtering av data for å være mer trygg og sikker på nettet. Imidlertid bemerket vi oss at det var et betydelig mer fokus på drift enn cybersikkerhet for de ansatte.

God cybersikkerhet ifølge de ansatte

Intervjuobjektene har enstemmig uttrykt at tofaktor verifisering er et godt sikkerhetstiltak, selv om det tar litt ekstra tid. De fleste objektene var fornøyd med implementering, men to av objektene synes det var veldig tungvint å ta i bruk tofaktor selv om de ser nytteverdien. Under en observasjonsrunde ble det observert ved flere anledninger at enkelte ansatte synes det var unødvendig med sikkerhetstiltak fordi «ingen vil hacke oss».

Tofaktor vil beskytte mot både brute force attacks og phishing. Brute force attacks går ut på at angriperen prøver å gjette riktig passord ved å gjette. Denne formen for angrep foregår som oftest ved hjelp av automatikk, som gjør at det kan gjettes flere tusen ganger i løpet av kort tid. Dersom man skulle treffe riktig passord, vil tofaktor stoppe angrepet da man må verifisere innloggingen eksternt. Phishing går ut på at man mottar en lenke, ofte via epost, som ber deg oppgi brukernavn og passord. Lenken leder til en side som ligner på den vanlige nettsiden man logger inn på, eksempelvis Facebook eller Netflix.

Når man da skriver inn informasjon sitter angriperen på brukernavn og passord til dette nettstedet. Ifølge vår spørreundersøkelse svarte 87.2% at de bruke samme passord flere steder. Da sitter plutselig angriperen på innloggingen til flere nettsteder.

Dette er et ganske vanlig inntrykk blant ansatte i SMB. Likevel viser dataen at 8 av 10 vellykkede løsepengevirus-angrep er hos SMB-virksomheter (Myrvold, 2022). I 2019 svarte 40% av norske bedriftsledere i en undersøkelse at de er enig eller delvis enig i påstanden om at det trolig vil være billigere å betale løsepenger ved et eventuelt cyberangrep, enn å investere i sikkerhetssystemer for å avverge det (E24, 2019).

Problemet med dette som Lisbeth Børresen påpeker i artikkelen, er at selv om bedriften betaler løsepenger så har de ingen garanti for at de kriminelle vil holde sine lovnader om å gi tilbake dataen (E24, 2019). Resultatene fra undersøkelsen gir grunn til bekymring ettersom forekomsten av cyberangrep øker i rekordfart. Ifølge NTT Security økte antallet løsepengeangrep med 350% i 2018. I første kvartal av 2022 økte antallet vellykkede løsepengeangrep med nesten 30% sammenlignet med første kvartal 2021 (Myrvold, 2022).

Flere av de ansatte nevnte også VPN som et eksempel på god cybersikkerhet. Dette ble introdusert til de ansatte under pandemien, da mange måtte jobbe på hjemmekontor og koblet seg eksternt til serveren via VPN. NSM sier at man bør benytte et VPN til all nettverkstrafikk. VPN er et virtuelt nettverk som krypterer dataen du sender og mottar via nettet (NSM, 2020).

Flere av de ansatte svarte at de var oppmerksomme på nedlasting av filer fra internett og e-post. Dette er veldig positivt da den vanligste inngangen for et cyberangrep er via e-post. En e-post inneholder gjerne en lenke som kan låse den ansattes datamaskin eller hele bedriftens nettverk frem til løsepenger er betalt. Det kan også inneholde phishing lenker eller nedlastingslenker der man laster ned ondsinnet programvare. De fleste ansatte fra både spørreundersøkelse og intervjuer setter seg ganske høy på bevissthet når de bruker e-post. Dette er et godt tegn, men de nevner også at bevisstheten rundt sikkerbruk av nettleser kunne vært bedre.

Det siste sikkerhetstiltaket som har blitt innført og godt mottatt blant de ansatte er kvartalsmessig endring av passord. Enkelte intervjuobjekter nevnte at de slet med å huske passordene når de måtte bytte så ofte, men at nytteverdien er såpass stor at det må gjøres likevel. I mai 2019 gikk Microsoft vekk fra sin offisielle sikkerhetsanbefaling om bytting av hver 60.dag. Passordekspert Per Thorsheim sier at passord bør byttes hver 13 til 15 måned, og at man burde bruke en enkel setning som passord fordi de ofte er enklere å huske. Han nevner også at dersom man går vekk fra jevnlig passordbytte, burde alle ansatte ha passord på minimum 15 tegn. Dette er fordi en setning som «Erlend, din fjasemikkel!» har en 85-bits entropi og vil ta århundrer å knekke med dagens teknologi (Røise, 2019).

Det har blitt et sikkerhetskrav fra eierne i Anlegg AS at alle ansatte skal låse pcen når de er borte fra sin PC. Det kommer derimot frem i undersøkelsen at en stor del av de ansatte mener det er lite poeng i dette, da de ikke kan se risikoene ved å la pcen stå åpen i kort tid på kontoret. Under intervjuene nevnes hovedgrunnen til dette at de har nøkkelkort med kode på hoveddøren til kontorlokalet, så det vil ikke være mulig for fremmede å komme inn i lokalene. Kontorlandskapet hos Anlegg AS består av separerte kontorrom, med muligheter for å låse døren når man går ut av rommet, de ansatte er enige i at de alltid hadde låst pcen dersom man satt i åpent kontorlandskap. Det nevnes også at man har liten tro på at en besøkende har ondsinnete mål med å komme seg inn på et tomt kontor med en ulåst pc. Innstillingene på pc-ene i dag har automatisk låsing av maskinen etter 30 minutter med inaktivitet.

I tillegg fremstår det som vanlig praksis å legge vekk pcen når man går hjem fra jobb, slik at den ikke ligger synlig på kontorene. Dette er for å forhindre å fysisk miste datamaskiner i forbindelse med et innbrudd. Dersom man fysisk mister maskinen, kan i verste fall inntrengeren få tilgang til hele bedriftens nettverk.

7-stegs modellen

Gjennom observasjoner, spørreundersøkelse og intervjuer har vi fått data som vi har tatt inn i Checkland sin 7 stegs modell for å prøve å besvare vår problemstilling:

"Hvordan få en økt bevissthet rundt cybersikkerhet i små- og mellomstore bedrifter?"

For å få et dypt bilde hos Anlegg AS tok vi først en spørreundersøkelse for å kartlegge store deler av bedriften. Dette gjorde vi for å få en bred oversikt over hvordan problemsituasjonen egentlig var. Deretter intervjuet vi 7 ansatte som ble valgt ut ifra avdelinger og lokasjoner innad i Anlegg AS. Dette var for å få en dypere forståelse av Anlegg AS sin dype innsikt. Resultatene av intervjuene og spørreundersøkelsen har blitt tatt opp før i dette kapitelet. I disse resultatene fant vi ut at problemsituasjonen var bevisstheten rundt cybersikkerhet.

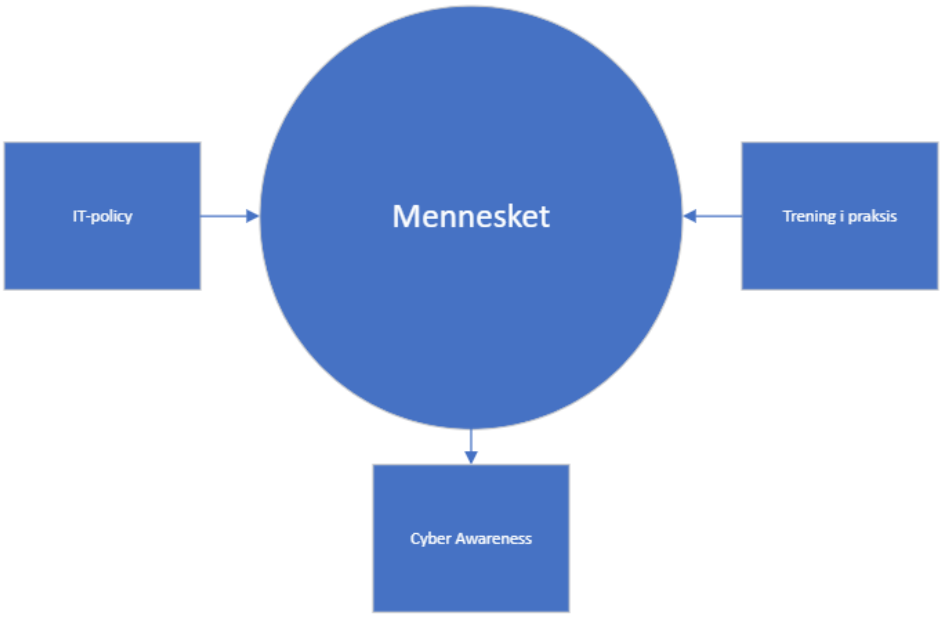
Den dype innsikten som kom frem hos Anlegg AS var at det var forskjellige forhold til internett og data hos de ansatte. Det førte til at også det var forskjellig interesser for mye av IT-policyen hos Anlegg AS som noen av ansatte synes var forståelig. Etter videre observasjoner og intervjuer fant vi ut av den dype innsikten var en uforståelig og for dårlig utarbeidet IT-policy.

Etter den dype innsikten så vi nærmere på hva det dype bilde kunne ha som rotårsaker. Rotårsakene vi kom frem til var lav kommunikasjon og lite trening i praksis for de ansatte. Det var vanskelig for de ansatte i Anlegg AS å vite hva som trengtes av dem og hvordan de skulle oppføre seg på dataen. Måten vi fant rotårsakene på var at vi analyserte intervjuene, og som nevnt tidligere var det mange som hadde lest IT-policyen, men de ansatte synes informasjonen i policyen var for komplisert og uforståelig for dem. Dermed ble IT-policyen for teoretisk og for lite vennlig i praksis ovenfor de ansatte. Dermed ble rotårsakene:

Lav kommunikasjon i IT-policy

Lite trening i praksis av IT-policyen

Neste steg var å lage konseptuell modell opp mot rotårsakene som kunne bidra til å løse problemsituasjonen. Det vi valgte med vår konseptuelle modell var løse begge rotårsakene i en modell. Med modellene ville vi at mennesket skulle være i sentrum fordi vi menter at menneskene er de viktigste i cyber awareness. Dermed lagde vi mennesket størst og sentrert for å illustrere dette best. Modellen har to inputer som er rotårsakene i den dype innsikten til Anlegg AS. IT-policyen er viktig å ha med fordi der kommer det prinsipper på hvordan bedriften skal handle på IT. Det er også viktig å ha en policy som er god og ikke for avansert for menneskene som er involvert. Den andre inputen er trening i praksis. Dette mener vi var viktig å ha med fordi det var flere ansatte i Anlegg AS som vi har observert ikke følge retningslinjene og IT-policyen i praksis. Med denne konseptuelle modellen mener vi at med inputen i mennesket, så vil outputen bli cyber awareness.



Figur 5 Egen modell - Konseptmodell fra SSM

Neste steg var å bruke vår konseptuelle modell inn i den virkelige verden hos bedriften. Først gikk vi igjennom om den konseptuelle modellen ville fungere inne hos Anlegg AS. Vi mente at denne kom til å virke, og dermed gikk vi videre med denne konsept modellen over. Steg fem og seks ble samme steg for oss, vi gjorde begge samtidig og det ble hoppet rett til steg syv. Måten vi gjorde steg syv på var å informere om endring i IT-policy og viste de ansatte ulike phishing e-poster og hva de skulle se etter av trusler, i tillegg så viste vi de ansatte om hva de skulle gjøre hvis de trykket på en lenke eller fikk virus på pcen. Gjennom observasjoner med denne modellen observerte vi at det var en økning i antall ansatte som tok kontakt med IT om mulige trusler på e-post.
Det ble også observert at det var en ansatt som trykket på en link som var svindel, men den ansatte skjønte hva han hadde gjort med en gang, og gjorde det han hadde fått beskjed om gjennom informasjonen han fikk gjennom oss.

Diskusjon

I diskusjonen skal vi gå gjennom hvordan ferdigheter, policyer og teoriene kan være med å påvirke bevisstheten i organisasjonen. Ved å gå gjennom disse punktene ønsker vi å danne et bilde på hvilke tiltak og teorier som påvirker de ansattes bevissthet i størst grad, samt se hvordan de eventuelt kan fungere bedre sammen.

Ansattes ferdigheter

Resultatene vi kom frem til gjennom oppgaven vår var at de ansatte sine ferdigheter i forhold til internett og data var veldig forskjellig. Spørsmålet som kommer opp etter dette resultatet er:

Hvordan kan Anlegg AS øke ferdighetene i forhold til internett og data?

Det kan være mange måter å øke ferdighetene til de ansatte på, men det er vanskelig og tar ofte lang tid. Grunnen til at det er vanskelig å øke ferdighetene er som nevnt tidligere, forskjellige interesse for de ansatte rundt tema. For å øke ferdighetene kan trening og opplæring av de ansatte fungere. Hvis IT-avdelingen lærer opp alle ansatte og trener de til å få de basis ferdighetene de trenger for at bedriften kan være relativt trygg med ansattes adferd på internett og dataen, så vil dette øke bevisstheten til de ansatte. Ved å øke ferdighetene til de ansatte vil det øke den organisatoriske læringen, og bidra på veien til målet om å øke bevisstheten i forhold til internett og data.

Det er også viktig at treningen og opplæringen skjer med jevne mellomrom. Dette fører til at det er en kontinuerlig økning av ferdighetene for de ansatte. Grunnen til dette er at hvis de ansatte ikke får mengdetrening på dette, så kan de fort glemme kunnskapen de har tilegnet seg hvis treningen skjer for eksempel hvert femte år. Det er dermed viktig med aktiv kommunikasjon som fører til at ansattes ferdigheter kan bli økt videre etter opplæringen.

På den andre siden så kan dette føre til at de ansatte som ikke er interessert i treningen og opplæring kan føle at de blir tvunget til noe de ikke har lyst til og kan føre til en negativ effekt med at de kan bli irriterte på ledelsen. Det andre som kan skje som er alvorlig for bedriften er at trening og fokuset på økning av ansattes ferdigheter i forhold til internett og data kan gå ut over den daglige driften.

Det kan forekomme negativitet hos de ansatte med en aktiv kommunikasjon fra IT-avdelingen og ledelsen. Det som kan forekomme er at de ansatte får en følelse på at ledelsen ikke stole på dem hvis de får aktiv kommunikasjon på for eksempel farer eller andre saker knyttet til internett og data. Det er derfor viktig at ledelsen kommuniserer godt og legger opp til at det ikke blir misforståelser hos de ansatte.

For å unngå de negative konsekvensene som kan forekomme av trening og opplæring er det viktig at ledelsen er med på forslaget og at de går foran med et godt eksempel. Det er vanskelig å få med seg alle ansatte hvis ikke ledelsen er med selv.

IT-policy

Gjennom resultatene kom det tydelig frem at Anlegg AS hadde en for dårlig og for dårlig kommunisert IT-policy til de ansatte. Disse to problemstillingene er viktig å få forbedret. For å forbedre disse to problemstillingene må vi først finne ut:

Hvordan lage en IT-policy som de ansatte kjenner seg igjen i?

Det våre intervjuobjekter har gitt uttrykk for i forhold til IT-policyen hos Anlegg AS er at den er uforståelig for dem. Den er skrevet av ledelsen med hjelp av en IT-leverandør. Det er språk i den nåværende IT-policyen som er vanskelig og overhodet ikke tilrettelagt for de ansatte. Det trengs en ny IT-policy som kan hjelpe de ansatte til å veilede dem med IT.

Måten dette kan bli gjort er å ta med noen ansatte inn i opprettelsen av en IT-policy. Det er mange forskjellige måter dette kan bli gjort på, men den vi har valgt å gå videre med er at IT-avdelingen sette opp et forslag til en IT-policy. Videre tar IT-avdelingen den videre til ledelsen og noen ansatte. Ledelsen og de ansatte kommer med tilbakemelding, og tilbakemeldingene blir tatt med videre inn i IT-policyen og forbedret med tilbakemeldingene.

Det som kan være en nedside med å involvere så mange i denne prosessen er at det er for mange som kommer med forskjellige meninger. IT-policyen skal tilfredsstille både IT, ledelsen og de ansatte. Dermed kan det skje at de ansatte ikke føler seg hørt fordi IT og ledelsen må ta noen valg som IT-policyen absolutt må inneholde. Dette kan føre til at de ansatte får mindre eierskap og føle at de ikke faktisk hadde noe med IT-policyen å gjøre.

For å svare på den andre problemstillingen tatt opp som er at IT-policyen er for dårlig kommunisert må vi finne ut:

Hvordan forbedre kommunikasjon ut til de ansatte inn mot IT-policy?

Det er lett å si at man skal bedre kommunikasjonen ut til de ansatte for å forbedre en problemsituasjon som en bedrift har. Det som derimot er desto vanskeligere er å faktisk forbedre kommunikasjonen ut til de ansatte i praksis. Når en IT-policy er ferdig utarbeidet så må endringene bli kommunisert ut til alle ansatte. Dette kan blir gjort gjennom kanaler som bedriften har, som e-post og fysiske eller digitale informasjonstavler. Det er også mulig å kommunisere dette ut på samlinger som alle ansatte er til stede på. Denne kommunikasjonen mener vi bør inneholde endringer som er gjort og forklaringer på hvordan IT-avdelingen og ledelsen tenker. Dette er viktig fordi vi mener da vil alle få samme startpunkt på hvordan de ansatte tolker kommunikasjonen som er gitt ut.
Med en forbedret kommunikasjon inn mot IT-policyen vil de ansatte få bedre oversikt over hva som IT-policyen inneholder og når den blir oppdatert. Dette kan føre til at flere ansatte får med seg informasjon som er viktig på IT i bedriften.

Det som kan være negativt for kommunikasjonen ut til de ansatte med IT-policyen er at de tar det som mas fra ledelsen. Det er mange ansatte som blir presset på tid og prestasjon i

bedriften, og hvis ledelsen sender ut noe som oppleves som mas kan dette få negativ innvirkning på de ansatte.

Det som også er en fallgruve med en IT-policy er at de ansatte får den tilsendt, men ikke leser den. Dette vil si at bedriften er like langt. En mulig løsning på dette er en blanding mellom begge problemstillingene i dette kapitelet, nemlig mer tilrettelagt IT-policy for de ansatte og bedre kommunikasjon som forklarer hvorfor det er en IT-policy og at den har blitt mer tilpasset de ansatte.

SSM inn i trappetrinnsmodellen

Trappetrinnsmodellen til Hagen et al. (2008) fokuserer på tiltak man kan gjøre i innen cyber- og informasjonssikkerhet for å øke bevisstheten til ansatte. Tiltakene vi har gått igjennom som informasjonssikkerhetspolicy, prosedyrer og kontroll, verktøy og metoder og bevisstgjøring er alle tiltak som fokuserer på en organisatorisk endring.

Modellen ser kun på disse trinnene, noe som gjør at den har glemt det menneskelige aspektet da den kun ser på resultatet av menneskelige handlinger. Ved å kun fokusere på det teknologiske sikkerhetsfundamentet tar man forgitt at de ansatte følger punktene som er skrevet ned i ulike dokumenter, rutiner osv. Dette er en utfordring da de ansatte sitter på forskjellig kunnskapsnivåer. Man kan ikke forvente at de ansatte gjør rasjonelle handlinger hvis de ikke har kunnskap og informasjon om det aktuelle temaet. Herbert Simon (1997) peker på dette som begrenset rasjonalitet.

Begrepet begrenset rasjonalitet blir brukt for å peke ut rasjonelle valg som også tar innover seg den kognitive begrensningen til beslutningstakeren – det vil si begrensinger knyttet til kunnskap og beregnings-messig kapasitet (Simon, 1997). Simon studerte beslutningsprosesser i organisasjoner, og sa at det i den forbindelse var nødvendig å modifisere forutsetningen om deltagernes rasjonalitet og nyttemaksimering. Han mente at deltagerne er «begrenset» rasjonelle og at de søker et tilfredsstillende resultat fremfor et optimalt utbytte av sin innsats (Berg, 2019).

Grunnet denne begrensede rasjonaliteten blir det vanskelig å forutsi resultatet fra forskjellige ansatte. For å forstå handlingene må man vite om den kunnskap og informasjon som den ansatte vil ha i handlingsøyeblikket. Mennesker har en enkel tendens til å følge og ta avgjørelser basert på regler, eksempelvis gå på grønn mann, stopp på rød mann ved et fotgjengerfelt. Modellen til Hagen et al. forutsetter at alle de ansatte følger de samme reglene, og at ingen hadde krysset fotgjengerfeltet på rød mann, selv om det ikke kommer noen biler.

Simon har også beskrevet hvordan organisasjoner utnytter sin struktur til å trosse sine ansattes begrensede rasjonalitet, til å fortsatt operere effektivt. Han peker på hvordan viktig informasjon stiger fra bunnen til toppen av hierarkiet, slik at toppledelsen i hver organisasjon kan ta beslutninger uten å sitte på detaljkompetansen til de ansatte lenger ned i hierarkiet har. På den måten avlaster organisasjonen lederens begrensede rasjonalitet slik at det er mulig å administrere og ta beslutninger på vegne av organisasjonen.

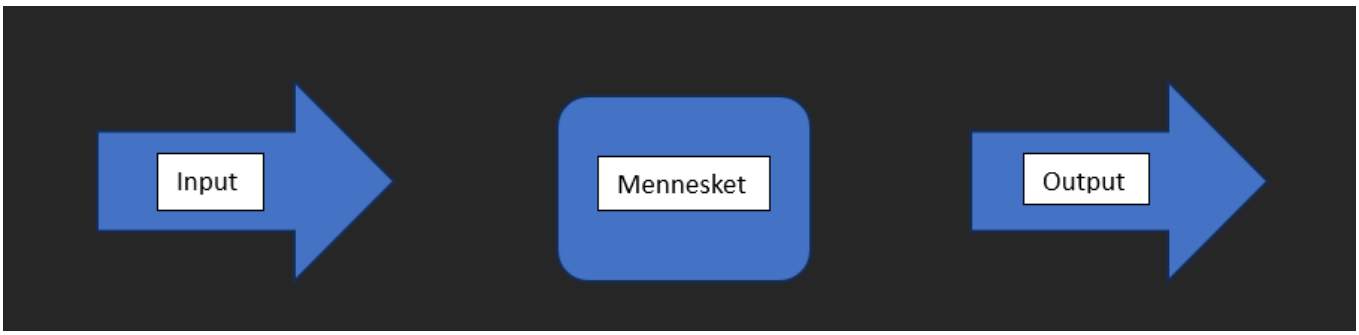
For å integrere de ansatte i organisasjonens prosedyrer og policyer er tydelig kommunikasjon kritisk. Ved å ha en tydelig kommunikasjon til de ansatte, legger man til

rette for et høyere kunnskapsnivå noe som vil føre til en mindre begrenset rasjonalitet knyttet til beslutninger som tas i løpet av arbeidsdagen.

Et problem med modellen dukker opp når informasjonsflyten blir snudd på hodet. Når informasjonen kommer fra toppen og ned i hierarkiet, vil det alltid være noe informasjon som forsvinner underveis. Dette fører til at den ene parten har mer informasjon enn den andre, og kalles informasjonsasymmetri (Lee et al. 2005).

Mange organisasjoner hevder at alle ansatte vet om alt, men dette stemmer sjeldent. Informasjon flyter aldri fritt i en organisasjon, og det er også legitimt at det er enkelte ting ikke alle ansatte har behov av å vite. Når informasjonsflyten ikke er perfekt, vil noen ansatte sitte på mer informasjon enn andre og dermed også mer kunnskap om spesifikke temaer. Denne kunnskapen spiller inn på beslutningene en tar i henhold til policyer og de andre trinnene fra modellen til Hagen et al. i motsetning til Simons beskrivelse av hvordan en toppleder tar avgjørelser uten detaljkunnskap, dette gjør at den enkelte handler mer på sin rasjonalitet enn et helhetlig bilde av situasjonen.

Modellen til Hagen et al. virker å være skrevet fra et teknologisk perspektiv, der all informasjon man gir ut blir gjort om til kunnskap og man forventer at den ansatte vil handle rasjonelt ved alle beslutninger. Med andre ord vil et teknologisk perspektiv vise til at en type input gir samme type output hver gang man setter det inn, som at mennesket er en «blackbox» som gir samme utfall hver gang som vist i modellen under.



Figur 6 Egen modell - visualisering av blackbox teorien

Utfordringen kommer når man ser det fra et organisatorisk perspektiv. Mennesket er ikke en «blackbox» der man kan forvente å få det samme resultatet hver gang. Med informasjonsasymmetri og begrenset rasjonalitet kan man ikke forvente at de ansatte tar «korrekt» beslutning hver gang, noe modellen til Hagen et al. legger opp til at de ansatte gjør. Dersom de ansatte hadde handlet slik en teknolog ønsker, ville man kunne forutsi hvilke beslutninger de ansatte tar på forhånd.

Det er her soft-systems metoden til Checkland kommer inn. Hans fokus på den sosio-tekniske delen, der systemer har mennesker involvert fra start gir et godt innblikk i hvorfor trappetrinnsmodellen, har enkelte utfordringer som gjør den vanskelig å ta i bruk. Fokuset til SSM er organisatorisk læring fra problematiske situasjoner der mennesker er involvert. Checkland peker på at en menneskelig situasjon inneholder mennesker som ønsker å handle målrettet og at det derfor bygges modeller som er relevant for å hjelpe mennesket med å handle målrettet ved læring. Metoden gir de som deltar mulighet til å lære deres vei til en felles handling som vil gjøre problemsituasjonen bedre (Checkland & Winter, 2006).

Ved å ta i bruk soft-systems metodikken får de ansatte mulighet til å sette seg inn i situasjonen ved hjelp av dyp innsikt og definerte rotårsaker. I tillegg til metodene nevnt, så skaper man visuelle modeller underveis i SSM. Ved å ta i bruk disse for diskusjon og refleksjon legger man til rette for deling av kunnskap og innsikt i situasjoner der ikke alle ansatte sitter på samme kunnskap og informasjon.

SSM legger vekt på å involvere mennesker i hele prosessen, fra problemsituasjonen oppstår, til forståelse og implementering av løsninger. Ved å gjøre dette sikrer man et mangfold av synspunkter og at systemet som utvikles er mer sannsynlig å møte de behovene til de involverte interessentene.

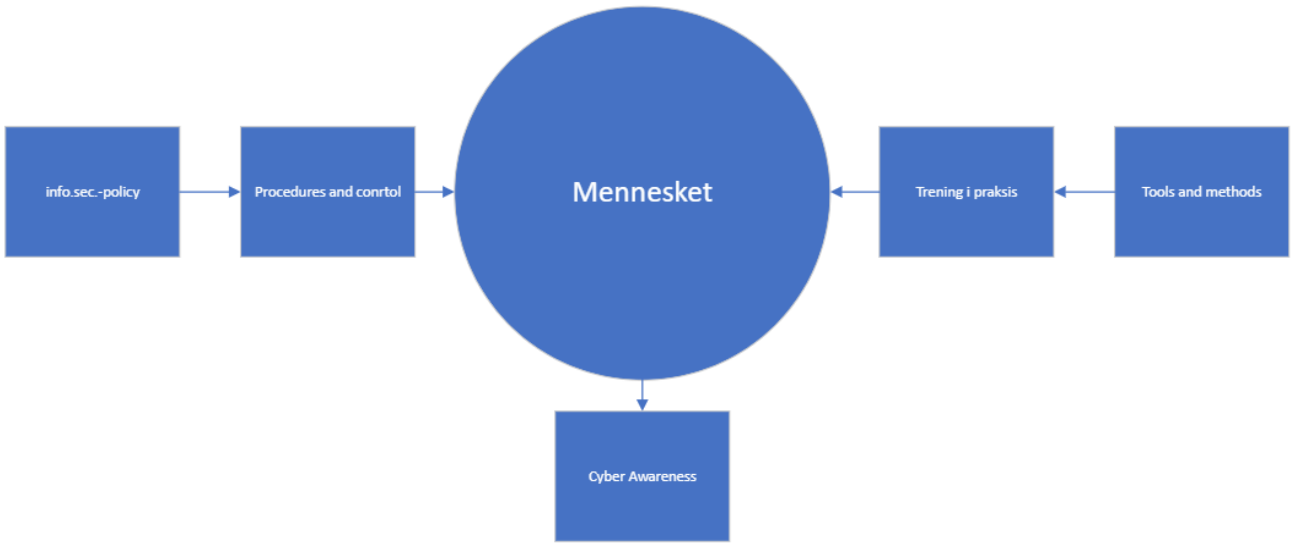
Måten soft-systems metode kan bidra med å øke cyber awareness i bedriften er gjennom dens tilnærming til å håndtere og forbedre komplekse problemsituasjoner innenfor organisatoriske og menneskelige systemer. Å øke cyber awareness er en meget kompleks problemsituasjon i noen bedrifter, og Anlegg AS er intet unntak. SSM tar med seg interessenter i prosessen, dette kan føre til mer eierskap for de som er med som interessenter, og med eierskapet kan de ta en mer aktiv rolle til å øke cyber awareness. Resten av bedriften som ikke er med i SSM prosessen, kan få økt cyber awareness ved resultatet av SSM. SSM prosessen kan føre til implementeringer av cybersikkerhetstiltak som er basert innsiktene som har kommet frem i SSM prosessen. Eksempler på implementeringer knyttet til cyber awareness som kan komme av SSM prosessen er: opplæring og endring av arbeidsprosesser.

Det er viktig å poengtere at Soft system metoden ikke er en metode som er direkte knyttet opp mot cyber awareness eller cybersikkerhet, men det kan være et hjelpemiddel til å øke cyber awareness i en bedrift.

SSM er en fleksibel metodikk som enkelt kan tilpasses andre metoder og tilnærminger. Derfor har vi studert muligheten for å tilpasse SSM til trappetrinnsmodellen, for å veie opp for mangelen på det menneskelige aspektet i modellen. SSM involverer mennesket fra første steg og har menneskelige interaksjoner gjennom hele prosessen. SSM bruker en gruppe interessenter som skal løse en problemsituasjon, og den samme gruppen kan brukes inn i Hagen et al. sin trappetrinnsmodell.

Grunnen til at interessenter kan bidra til å heve trappetrinnsmodellen er fordi ikke alle i en bedrift kan bidra på samme måte inn mot en informasjonssikkerhetspolicy, prosedyrer og kontroll, verktøy og metoder. SSM tar i bruk menneskene og videreutvikler, samt tilpasser, løsningen til å passe inn i bedriften. Ved å gjøre dette oppnår man en kontinuerlig forbedring.

For å øke bevisstgjøring i en bedrift trenger den en kontinuerlig økning av kunnskap om cybersikkerhet. Grunnen til dette er fordi trusler og risikoer som følger med internett og bruk av teknologi stadig blir videre utviklet fra onde interessenter. Som nevnt tidligere fremstiller Hagen et al. cyber bevissthet som noe man oppnår etter å ha fulgt de tidligere trinnene. På den andre siden kan man tilpasse SSM til trappetrinnsmodellen, slik at den tar med seg det menneskelige aspektet og en kontinuerlig tilnærming til bevisstgjøring. Ved å gjøre dette kan trappetrinnsmodellen bli mer korrekt.



Figur 7 Egen modell - Blanding av SSM og trappetrinnsmodell

Modellen over er en blanding av SSM og Hagen et al. trappetrinnsmodell. Måten vi har gjort det på er at mennesket er i sentrum og størst for å illustrere at det er den viktigste delen av modellen, uten mennesket er det ikke en fullverdig modell. Mennesket får input fra begge sidene. Venstre siden kommer med input om informasjonssikkerhetspolicy som kommer i første ledd fra ledelsen eller IT-avdelingen. Videre føres dette inn i prosedyrer og kontroll for å se om informasjonssikkerhetspolicyen blir opprettholdt. Høyre siden av modellen får mennesket input av verktøy og metoder som er med på å bidra til å hjelpe til med forståelse og utførelse av venstre siden av modellen. I tillegg har vi lagt inn en del på venstre siden som prosesserer verktøyene og metodene som kommer fra trappetrinnsmodellen til Hagen et al. Dette punktet er trening i praksis. Grunnen til at vi har valgt å supplere med trening i praksis er fordi vi ville ta høyde for at den begrensete rasjonaliteten ble så lav som mulig. Hvis mennesket får opplæring og trening i verktøyene og metodene vil utbyttet av inputen fra begge sider av modellen bli høyere. Til slutt kommer det en output fra mennesket eller den svarte boksen som er i trappetrinnsmodellen, og denne outputen er økt cyber bevissthet.

Konklusjon

Dette prosjektet har sett nærmere på hvordan SMB kan øke bevisstheten innad i organisasjonen, gjennom et case studie i samarbeid med Anlegg AS. Bevisstgjøring spiller en stor rolle i beslutninger som tas på daglig basis, men det er også subjektivt og viktigheten av det kan oppfattes annerledes fra organisasjon til organisasjon. Gjennom litteraturgjennomgang, observasjoner og intervjuer har vi fått et innblikk i hvordan man kan øke bevisstheten ved hjelp av teorier og modeller. Tidlig i spørreundersøkelsen kom det frem at de fleste mente at Anlegg AS hadde fokusert i stor grad på cybersikkerhet de siste årene, men få av de ansatte kunne peke på spesifikke tiltak som hadde blitt gjort. De ansatte var heller ikke klar over at SMB ofte er mål for cyberangrep og tenkte at «vi er såpass små, så det skjer ikke oss».

Vi kom inn i prosjektet, uvitende om hvilket nivå bedriften lå på når det kom til kunnskap om cybersikkerhet. Med tanke på digitaliseringsprosessen de nå står i, var nivået lavt i forhold til hva vi hadde trodd og det virket som de ansatte tok lett på cybersikkerheten. Under intervjuene nevnte de fleste at det kom en del phishing-mail, noe som er positivt målt opp mot cybersikkerhetsnivået men likevel ønsker vi at bedriften skal øke nivået for å redusere risikoen for angrep. Spørsmålene vi stilte under intervjuene rettet seg mot de ansattes kompetanse og kunnskapsnivå når det kommer til cybersikkerhet, samt kjennskap til policy og prosedyrer under et eventuelt angrep.

Her kom det frem at store deler av de ansatte ikke hadde lest policyene, hovedsakelig p grunn av lite interesse for temaet. De ansatte er enige om at det finnes en policy, men interessen for temaet har gjort at få har satt seg inn i den. Som påpekt i trappetrinnsmodellen mener Hagen et al. (2008) at en policy er første steg for å oppnå cyber awareness, og uten det første steget kan man heller ikke forvente rasjonelle beslutninger knyttet til prosedyrer og de videre trinnene hvis de eksisterer i det hele tatt.

Soft-system metoden kan hjelpe bedriften med å lage en bedre policy hvis interessentene i SSM er fra flere ledd i bedriften. Dette kan føre til at flere ansatte får mer eierskap til policyen. I tillegg kan det føre til at andre ansatte føler seg mer igjen med policyer eller andre prosedyrer hvis de blir laget komplimentert av personer som ikke er ledelsen eller IT-avdelingen.

Resultatet fra prosjektet viser at en manglende kompetanse på temaet kan ha store innvirkninger på valgene som blir tatt. Dette gjør at man er nødt til å fokusere på å tette kunnskapshull og legge til rette for at de ansatte skal lære. Ved å bruke SSM og trappetrinnsmodellen sammen, kan man involvere de ansatte i problemsituasjonene for å lage klare prosedyrer og policyer som de ansatte føler eierskap til. Dette kan også være en felles læringsarena, der de ansatte tar til seg detaljkunnskap om temaene som blir tatt opp og derav får en økt bevissthet.

Kilder:

AIG. (2019) *Menneskelige feil – en større trussel for datasikkerheten enn du kanskje tror.* Hentet 29. oktober fra: https://www.aig.no/business/nyheter/managing-objections-to-purchase-cyber-insurance2

Andersen, E. & Sannes, R. (2016) *Norske toppledere på bunn i digitalisering.* Aftenposten. Hentet 09. november 2023 fra: https://www.aftenposten.no/meninger/debatt/i/4QoxE/kronikk-norske-toppledere-paa-bunn-i-digitalisering-ragnvald-sannes-og-espen-andersen

Andersen, E. & Sannes, R. (2018) *Hva er digitalisering?* Hentet 29. april 2023 fra: https://biopen.bi.no/bi-xmlui/handle/11250/2569870

Andriessen, J., Schaberreiter, T., Papanikolaou, A., Röning, J. (2022). *Cybersecurity Awareness (Advances in Information Security, 88)*

Arbeidstilsynet. (u.å.) *Generelle krav til opplæring.* Hentet 27. oktober 2023 fra: https://www.arbeidstilsynet.no/arbeidsforhold/generelle-krav-til-opplaring/

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with computers, 23*(1), 4-17.

Berg, O.T. (2019) *Organisasjonsteori.* Hentet 25. oktober 2023 fra: https://snl.no/organisasjonsteori

Bryn Aarflot. (u.å.) *NDA: Hvordan fortelle en hemmelighet og samtidig beholde den.* Hentet 10. november 2023 fra: https://baa.no/alle-artikler/nda-hvordan-fortelle-en-hemmelighet-og-samtidig-beholde-den

Canalys. (2023) *Cybersecurity investment to grow by 13% in 2023.* Hentet 20. April 2023 fra: https://canalys.com/newsroom/cybersecurity-forecast-2023?fbclid=IwAR0M0E57zjdiQzzMMLtEB34qVWgVAorYZSYHGsdA2w4YtdoRXo6POph87rg

Checkland, P. (1981). *Systems Thinking, System Practice.* John Wiley & Sons

Checkland, P. (1999). *Systems Thinking, System Practice: Include a 30 year Retrospective.* Wiley

Checkland, P. & Winter, M. (2006) *Process and content: two ways of using SSM.* (1.utg.) Journal of the Operation Research Society.

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

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

Dahl, A. (2021) *Policy*. Hentet fra: https://snl.no/policy

Dahlum, S. (2021) *Validitet* Hentet 29. november 2023 fra https://snl.no/validitet

Datatilsynet. (2017) *Kryptering.* Hentet 8. juli 2023 fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/

Datatilsynet. (2021) *Risikovurdering* Hentet 14. november 2023 fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/

Digdir. (u.å.) *Steg 4: Vurdere tilgangsnivå.* Hentet 8. oktober 2023 fra: https://www.digdir.no/informasjonsforvaltning/steg-4-vurdere-tilgangsniva/2723

Digdir. (u.å.) *Om sikkerhetstiltak.* Hentet 8. oktober 2023 fra: https://www.digdir.no/informasjonssikkerhet/om-sikkerhetstiltak/3042

E24. (2019) *Norske bedrifter betaler heller løsepenger enn å investere i IT-sikkerhet.* Hentet 10. november fra: https://e24.no/teknologi/i/BRmJQl/norske-bedrifter-betaler-heller-loesepenger-enn-aa-investere-i-it-sikkerhet

Estil, S. (2023) *Hvorfor og hvor ofte bør bedriften din ta data backup?* Hentet 12. november 2023 fra: https://www.visma.no/blogg/data-backup-hvorfor-og-hvor-ofte-bor-bedrifter-ta-backup/

European Commission. (u.å.) *Internal Market, Industry, Enterpreneurship and SMEs.* Hentet 17. november 2023 fra: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

Europakommisjonen, Small, E. A. f. & Enterprises, M.-s. (2020). Supporting specialized skills development: big data, Internet of things and cybersecurity for SMEs: executive summary. Publications Office.

Golafshani, N. (2003) *Understanding Reliability and Validity in Qualitative Research.* University of Toronto, Toronto, Ontario, Canada. The Qualitative Report Volume 8 Number 4.

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

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. *Evidence-based nursing*, *16*(4), 98-98.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field methods*, *18*(1), 3-20.

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

Klev, R. & Levin, M. (2009). Forandring som praksis (2.utg). Fagbokforlaget.

Lee, B.C., Ang, L., & Dubelaar, C. (2005) *Lemons on the Web: A signaling approach to the problem of trust in Internet commerce.* Journal of Economic Psychology.

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

Lindbak. (u.å.) *Sikkerhetsrapporten er et viktig strategisk verktøy.* Hentet 20. november 2023 fra: https://www.lindbak.no/sikkerhetsrapporten-er-et-viktig-strategisk-verktoy

Microsoft. (u.å.) *Hva er cybersikkerhet?* Hentet 3. november 2023 fra: https://support.microsoft.com/nb-no/topic/hva-er-cybersikkerhet-8b6efd59-41ff-4743-87c8-0850a352a390

Microsoft. (u.å.) *Tilgangskontroll forklart.* Hentet 3.november 2023 fra: https://www.microsoft.com/nb-no/security/business/security-101/what-is-access-control

Microsoft. (2023) *Opprett en hendelsesrapport med Microsoft Sikkerhet Copilot i Microsoft 365 Defender.* Hentet 3. november 2023 fra: https://learn.microsoft.com/nb-no/microsoft-365/security/defender/security-copilot-m365d-create-incident-report?view=o365-worldwide

Morgan, S. (2022). *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics.* Hentet 18. november 2023 fra: https://cybersecurityventures.com/cybersecurity-almanac-2022/

Myrvold, K. (2022) *SMB-virksomheter er offeret i 8 av 10 vellykkede løsepengevirus-angrep.* Hentet 18. november 2023 fra: https://www.digi.no/artikler/debatt-smb-virksomheter-er-offeret-i-8-av-10-vellykkede-losepengevirus-angrep/520753

Nasjonal Sikkerhets Myndighet (2020). *Grunnprinsipper for IKT-sikkerhet.* Hentet 29.oktober 2023 fra: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

Nasjonal Sikkerhets Myndighet. (2020) *13 råd for bedre sikkerhet på mobile enheter.* Hentet 29. oktober fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/13-rad-for-bedre-sikkerhet-pa-mobile-enheter

National Institute of Standards and Technology. (u.å.) *Awareness.* Hentet 28. april fra: https://csrc.nist.gov/glossary/term/awareness

Nettvett. (2021). *Informasjonssikkerhetspolicy.* Hentet 5. juni 2023 fra: https://nettvett.no/informasjonssikkerhetspolicy/

NHO. (u.å.) *Fakta om små og mellomstore bedrifter (SMB).* Hentet 5. november 2023 fra: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/

Okereafor, K. (2008) *Impacts of Cyber Attacks on Corporate Business Continuity: Fostering Cyber Security Consciousness in the Citizienry.* Hentet 13. november 2023 fra: https://www.researchgate.net/publication/331936672_Impacts_Of_Cyber_Attacks_On_Corporate_Business_Continuity_Fostering_Cyber_Security_Consciousness_In_The_Citizenry

Polit, D. F. & Beck, C. T. (2010). *Generalization in quantitative and qualitative research: Myths and strategies*. Int J Nurs Stud, 47(11), 1451-1458.

Regjeringen. (2014) *Digitalisering i offentlig sektor.* Hentet 23. oktober 2023 fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Ringdal. (2018). *Enhet og Mangfold - Samfunnsvitenskapelig forskning og Kvantitativ Metode.* (4.utg.) Fagbokforlaget

Røise, M.B. (2019) *Vi har alle irritert oss over at vi må bytte passord alt for ofte. Nå er det endelig slutt på elendigheten.* Hentet 11. november 2023 fra: https://www.digi.no/artikler/vi-har-alle-irritert-oss-over-at-vi-ma-bytte-passord-alt-for-ofte-na-er-det-endelig-slutt-pa-elendigheten/466865

SAP. (u.å.) *Hva er cybersikkerhet?* Hentet 23. oktober 2023 fra: https://www.sap.com/norway/products/financial-management/what-is-cybersecurity.html

Simon, H.A. (1997) *Models of bounded rationality.* (1.utg.) Massachusetts Institute of Technology.

SNL. (u.å.) *Bevisstgjøring.* Hentet 28. april 2023 fra: https://snl.no/bevisstgj%C3%B8ring

Toth, P. & Klein, P. (2014). *A Role-Based Model for Federal Information Technology/Cybersecurity Training.* (3.utg.) NIST Special Publication 800-16 Revision 1.

Wilhelmsen, W. (2021) *Datasikkerhet – dette må bedriften vite om IT-sikkerhet.* Hentet 11. november 2023 fra: *https://www.advania.no/kunnskap/artikler/datasikkerhet*

World Economic Forum (2022). *The Global Risks Report 2022 17th Edition.* Hentet 28.april 2023 fra: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf?_gl=1*10ysxse*_up*MQ..&gclid=CjwKCAiA68ebBhB-EiwALVC-NroUadfQ-cR7JrcQPAyNV5OePteTeK2mSSy9426ppb9D1Z4sfCdS0RoCB3YQAvD_BwE

White, R. E., & Cooper, K. (2022). *Qualitative Research in the Post-Modern Era: Critical Approaches and Selected Methodologies*. Springer Nature.

Whitman, & Mattord, H. (2017). Management of information security (5th ed., pp. XXII, 650). Cengage Learning.

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

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

Yin, R. K. (2018). *Case study research and applications* (Vol. 6). Thousand Oaks, CA: Sage.

Figurer:

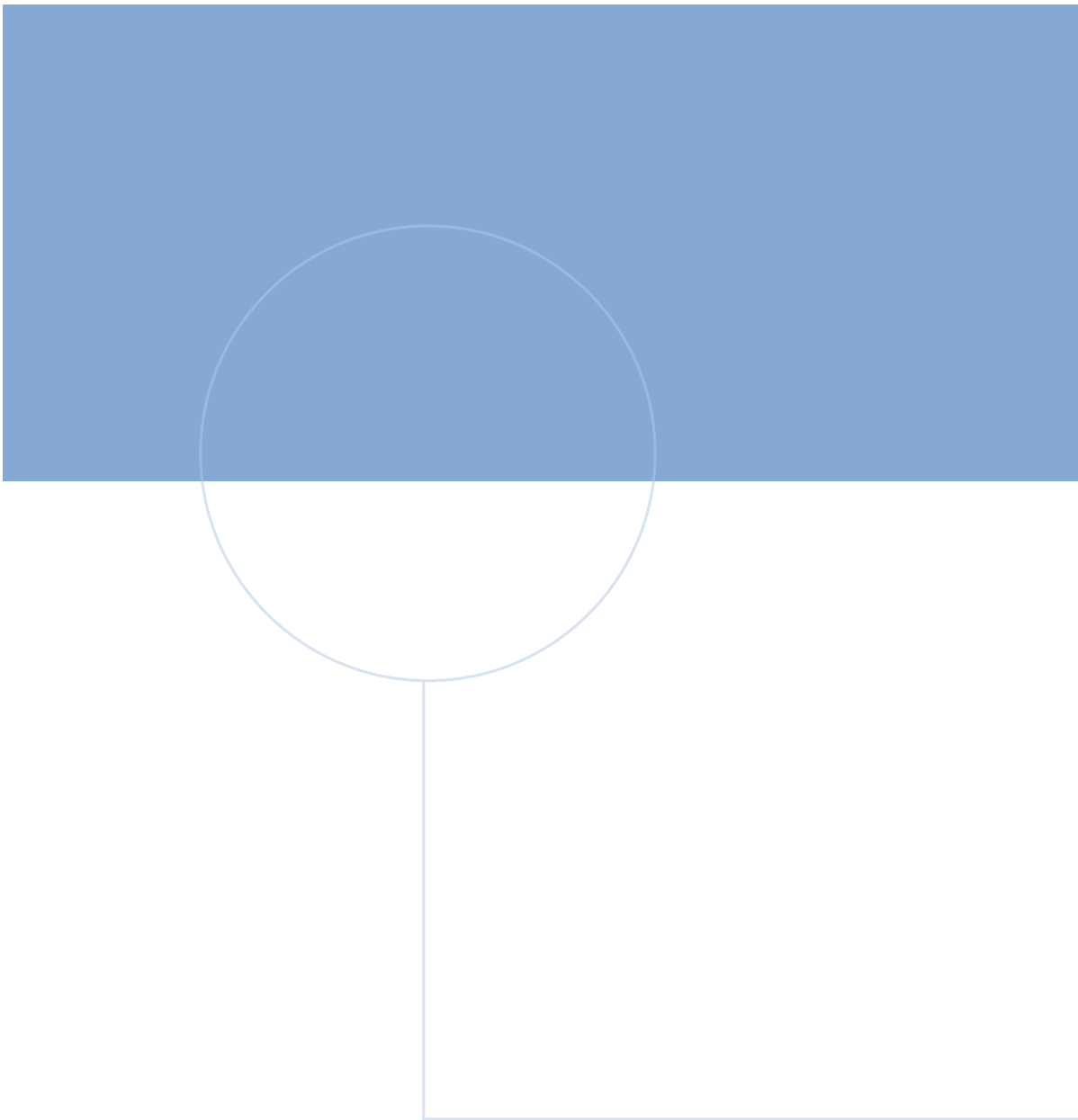
Vedlegg:

Vedlegg 1, Intervjuguide for Anlegg AS.

Intervjuguide

Intervjuguide Anlegg AS	
Hensikt	Spørsmål
Spørreundersøkelsen viser at 38,5% ikke hadde lest retningslinjene for cybersikkerhet i bedriften. Vi ønsker å finne ut hva som gjør at de lar være å lese dette.	Hvorfor tror du så mange har droppet å lese retningslinjene? Hvordan er det å finne retningslinjene? Synes du retningslinjene er forståelige? Tror du de som ikke har lest retningslinjene tar cybersikkerhet forgitt? Evt hvorfor
Spørreundersøkelsen viser en score på 4,5 av 5 på hvordan bedriften har fokuset på cybersikkerhet de siste årene. Ut ifra resten av svarene fra undersøkelsen, kan dette virke kunstig høyt. Vi ønsker å finne ut om dette faktisk stemmer.	Hvilke tiltak har bedriften gjort de siste årene for å øke fokuset? Oppfølgingsspørsmål om nevnte tiltak. Er det noen tiltak du ville innført som ikke har blitt nevnt i bedriften tidligere?
Spørreundersøkelsen viste at de ansatte ser på seg selv som en median på 3 av 5 innen datakyndighet. Vi ønsker å finne ut hva de vektlegger innen datakyndighet, og hvordan de kategoriserer begrepet.	Hva legger du i ordet datakyndig? Hva tenker du om at medianen er på 3? Ville det vært hensiktsmessig og gjort tiltak for å øke datakyndigheten i bedriften?
Vi fant ut at passordene skulle byttes kvartalsvis i etterkant av spørreundersøkelsen, og hadde ikke med dette som et alternativ i undersøkelsen. Spørreundersøkelsen viser at 64% bytter passord på jobb-brukeren månedlig. Vi ønsker å finne om de siste 36% svarte hvert	Fikk beskjed i første intervju om at alle må bytte kvartalsmessig. Derfor er spørsmålene fjernet.

halvår, fordi vi ikke hadde med kvartalsmessig i undersøkelsen.	
Spørreundersøkelsen viser at 94,9% skjuler passordet sitt når andre er til stede. Vi ønsker å se hva som blir lagt i begrepet skjule.	Hva anser du som å skjule et passord? Tror du mange av de ansatte lar være å skrive inn et passord når det er andre til stede? Tror du evt de gjemmer skjerm dersom det er på mobil, eller prøver å hindre sikt til tastatur?
Ut ifra svarene i undersøkelsen ønsker vi å finne ut om de ansatte har mottatt noe opplæring i form innen cybersikkerhet. Og eventuelt hvordan de oppfattet opplæringen.	Har dere fått noen opplæring innen cybersikkerhet? Oppfølging: Hvilke aktiviteter ble eventuelt utført? Hvor ofte får du tilbud om opplæring? Hvordan tror du økt kunnskap om cybersikkerhet kan påvirke bedriftens sikkerhet?



NTNU

Kunnskap for en bedre verden