Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

Tosic Selver

Informasjonssikkerhet og innovasjon i Skatteetaten

Utfordringer knyttet til høy innovasjonstakt og et trusselbilde i endring

Masteroppgave i Organisasjon og ledelse (MORG)
Veileder: Petter Grytten Almklov

Juni 2020

NTNU
Kunnskap for en bedre verden

Skatteetaten

Sammendrag

Trusselbildet til Skatteetatens IT-systemer er i konstant endring og endrer seg nå mye raskere enn det tidligere har gjort. I kombinasjon med økt digitalisering og krav til tilgjengelighet, har interessen fra kriminelle trusselaktører blitt en stor bekymring for både private og offentlige virksomheter.

For å være motstandsdyktige mot aktører med onde hensikter, må det eksistere sikkerhetsmekanismer samtidig som det må tilrettelegges for innovasjon og kreativitet blant ansatte. Skatteetaten har et høyt ambisjonsnivå og er en av de mest innovative virksomhetene i Norge, i tillegg til at de har en av samfunnsoppdragets viktigste oppgaver – å samle inn skatter og avgifter som finansierer velferdsstaten Norge.

Gjennom bruk av kvalitativ metode med dybdeintervjuer i kombinasjon med en spørreskjemaundersøkelse, ønsker jeg i denne oppgaven å kaste lys over hvilke praktiske utfordringer det er med høy innovasjonstakt og ambisjonsnivå, samtidig som vi har et komplisert trusselbilde og relativt liten risikoaksept.

Dette forskningsarbeidet diskuterer om eksisterende sikkerhetsmekanismer hemmer innovasjonsarbeidet i Skatteetaten og hvordan vi kan være mer innovative på sikkerhetssiden, slik at vi er bedre rustet mot et dynamisk trusselbilde.

Funnene i dybdeintervjuene viser at eksisterende sikkerhetsmekanismer kan hemme innovasjonsarbeidet på enkelte områder. Samtidig påpeker intervjuene at innovasjon i sikkerhetsarbeidet er viktig for at Skatteetaten skal være motstandsdyktig mot det dynamiske trusselbildet. Konkret kom det blant annet frem at:

- Dokumentene på nivå 3 i styringssystemet for informasjonssikkerhet (SFI) kan virke hemmende på innovasjonsarbeidet til Planleggingsstaben
- Det må innoveres på sikkerhetssiden gjennom safety 2 og ALARP prinsippet
- Sikkerhetsstaben må være mer oppsøkende, synlig og ha fokus på bevisstgjøring gjennom hele året slik at sikkerhet blir en naturlig del av hverdagen

Svarene fra spørreunderundersøkelsen på sin side bekrefter at Skatteetaten har et dynamisk og komplisert trusselbilde, som gjør at det må jobbes mer effektivt for å øke motstandsdyktigheten. De konkrete funnene fra spørreundersøkelsen viser at:

- Skatteetaten har et dynamisk trusselbilde med avanserte trusselaktører, som også er det største utfordringen for IRT
- Sikkerhetsstaben til enhver tid må være oppdatert på Skatteetatens trusselbilde, da IRT kvalitetssikrer sine metoder, prosesser og verktøy gjennom dem.

Abstract

The Norwegian Tax Administration's IT threat landscape is in constant change and develops faster than before. In combination with the exploding digitalization and higher demands of availability, the interest from criminal threat actors has become a big concern for both private and public sectors.

To be resilient against actors with evil purposes, security mechanisms has to exist although we have to facilitate for innovation and creativity among employees. The Norwegian Tax Administration has a high level of ambition and is one of the most innovative businesses in Norway, in addition to have one of the most important social missions – collect taxes and fees which finances the welfare in Norway.

Through the use of qualitative methods with depth interviews, in combination with a questionnaire, I hope to throw lights on practical challenges when it comes to having high speed of innovation, while we have a complicated threat landscape and relative low risk acceptance.

This paper discusses whether existing security mechanisms hampers the innovative work in the Norwegian Tax Administration and how we can be more innovative in the security field in order to be more resilient.

The findings from the depth interviews shows that securitymechanisms can hamper innovation in certain areas. In addition the interviews emphasize that innovation is important in IT-security in order to be resilient against the dynamic threat landscape. The actual findings are:

- Reconsider the ownership of the documents at level 3 in the Information Security Management System (ISMS).
- Innovation has to exist in IT-security, through the safety 2 and ALARP principle.
- The security staff needs to be more visible and focus on security awareness throughout the whole year, in order to get security a part of the everyday.

The answers from the questionnaire on the other side, confirms that the Norwegian Tax Administration has a dynamic and complex IT threat landscape, which demands more efficient processes to achieve resilience. The concrete findings shows that:

- The Norwegian Tax Administration has a dynamic IT threat landscape with advanced threat actors, which is also the IRT's biggest challenge.
- The security staff needs to continuously be updated on the threat landscape, as the IRT keeps their methods, processes and tools effective through quality assurance with them.

Innhold

Figurer

Tabeller

Begreper

Innovasjon

Betyr å lage noe nytt. Dette kan være en mindre eller større endring i noe eksisterende, eller noe helt nytt og revolusjonerende. En mindre endring kan for eksempel forekomme i et eksisterende produkt, prosess, forretningsmodell, etc. En større endring kan være et helt nytt produkt eller tjeneste, (Gjelsvik, 2007).

Styringssystem for informasjonssikkerhet (SFI)

Internt i Skatteetaten er styringssystem for informasjonssikkerhet et sett med dokumenter som beskriver regler og prosedyrer ansatte må følge for å ivareta informasjonssikkerheten til en organisasjon. Reglene og prosedyrene skal understøtte strategien til organisasjonen og er ofte delt inn i flere nivåer; et generelt overordnet nivå, et undernivå hvor reglene er delt inn i spesifikke områder/temaer, et nivå med konkrete eksempler og situasjoner.

Kunstig intelligens (AI)

Det er mange ulike definisjoner av kunstig intelligens (AI) og definisjonene endrer seg gjerne i takt med hva som er teknologisk mulig. I Norges nasjonale strategi for kunstig intelligens tar de utgangspunkt i EUs ekspertgruppes 5 definisjon for AI, og definerer det slik:

Kunstig intelligente systemer utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål. Enkelte AI-systemer kan også tilpasse seg gjennom å analysere og ta hensyn til hvordan tidligere handlinger har påvirket omgivelsene, (Kommunal- og moderniseringsdepartementet, 2020)

ISO-standarder

Er standarder definert av en internasjonal organisasjon, bestående av eksperter på sitt fagfelt. Man kan se på ISO-standarder som en formel som beskriver den beste måten å gjøre noe på. Dette kan for eksempel være når et produkt lages, en prosess skal gjennomføres eller en tjeneste skal ytes, (ISO-standards, "STANDARDS", Hentet 29. mai 2020 fra https://www.iso.org/standards.html)

Resilience

I norsk sammenheng oversettes dette ordet til *motstandsdyktighet*. En presis definisjon av resilience er: "the intrinsic ability of a system or organization to adjust its functioning prior to, during, or following changes, disturbances, and opportunities so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2010).

GDPR

General Data Protection Regulation (GDPR) er en lovgivning utgitt av EU, også gjeldende for Norge, som ble innført 25 mai 2018. Den lovgivningen ga virksomheter mer ansvar for personvern i form av strengere krav, og datasikkerhet var en sentral del av det nye regelverket, (Bergsjø & Windwik, 2018, s. 96).

Incident Response Team (IRT)

Incident Response Team er navnet på gruppen ansett som første linje forsvar ved et angrep på IT-systemene til Skatteetaten. Det kan være flere IRT innenfor en organisasjon avhengig av område. I noen organisasjoner kan for eksempel første linje forsvar ved digitale angrep hete Computer Security Incident Response Team (CSIRT) for å presisere at de har ansvaret for hendelser relatert til IT-systemene. I Skatteetaten benyttes begrepet IRT. Det er dermed de som oftest først vil oppdage eller bli varslet ved et angrep på IT-systemene og samtidig respondere og gjenopprette normalsituasjonen, (Robin Ruefle, Defining Computer Security Incident Response Teams, Hentet 29. mai 2020 fra https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams).

Sikkerhetsmekanismer

I denne oppgaven benyttes ordet sikkerhetsmekanismer som et samlebegrep for alle systemer som har som formal å forbedre sikkerheten på IT-systemene. Dette kan være regler, rutiner, praksis, antivirus, sperring av nettsider, detektering og blokkering av ondsinnede handlinger, etc. I arbeid med IT er ikke skillet mellom mennesker og teknologi alltid opplagt, mens noen av mekanismene er manuelle er andre programmert og automatiske, (Johansen, Almklov & Mohammad, 2016). Eksempler på dette kan være regler og rutiner som blir fulgt step by step av en ansatt, mens antivirus og sperring av ondsinnede nettsider reagerer ofte øyeblikkelig av et automatisert system.

1 Innledning

Teknologiutviklingen de siste årene er et bevis på hva menneskets kreativitet klarer å få til i løpet av kort tid. Selvdrevne biler, droner som leverer varer kjøpt over internett, robotstøvsugere og betaling med mobiltelefonen er bare noen få av de siste oppfinnelsene markedet har å tilby. Vi blir generelt mer digitaliserte og alt skal være tilgjengelig på alle tidspunkt fra overalt i verden, noe som åpner for nye muligheter og samtidig risikoer man tradisjonelt sett ikke har hatt.

Noen ganger går det så fort i utviklingen at man produserer og installerer teknologi som fungerer veldig godt i utgangspunktet, men hvor sikkerheten ikke er ivaretatt. Daglig dukker det opp hendelser i media om forskjellige typer sikkerhetsbrudd og det er ikke så rart. Hver person har i gjennomsnitt 90 nettbaserte kontoer, hvor vi legger igjen opplysninger verdifulle for noen med onde hensikter, (Lord, 2018). Samtidig er Norge helt i verdenstoppen hva gjelder kontantløs betaling via elektroniske tjenester og IKT, noe som gjør at vi er attraktive mål for kriminelle aktører, (Capgemini, 2019, s. 33). For å tilegne seg verdifull informasjon til sin egen vinning tar de kriminelle gjerne i bruk ulovlige metoder for å få tak i informasjon, enten det er personopplysninger, passord, bankkortinformasjon eller konkurransesensitiv informasjon.

Teknologi som benytter seg av kunstig intelligens (AI) har allerede kommet på banen, også i bruk som forsvarsmekanismer ved angrep på IT-systemer. I en CTF konkurranse (Capture The Flag) på den anerkjente konferansen Def Con i 2016, stakk superdatamaskinen Mayhem, basert på kunstig intelligens, av med seieren. Konkurransen som går ut på å finne sårbarheter i programvare og rette dem, ble utført på sekunder av Mayhem - noe som vanligvis tar måneder å gjennomføre, (Darpa, 2016). Dette sier noe om potensialet til kunstig intelligens når aktører med onde hensikter tar dem i bruk som angrepsverktøy for å utnytte sårbarheter den finner.

Trusselbildet til Skatteetaten er i konstant endring og endrer seg nå mye raskere enn det tidligere har gjort. I kombinasjon med at digitaliseringen har eksplodert og det er økt krav til tilgjengelighet, har interessen fra kriminelle trusselaktører blitt en stor bekymring for både private og offentlige virksomheter, (Borrett, Carter & Wespi, 2013, s. 164). Kriminelle aktører er veldig kreative og utspekulerte og har stor motivasjon for å gjennomføre sine angrep, ikke så rart når Skatteetaten alene samler inn over 1050 milliarder kroner årlig i skatter og avgifter. Trusselaktører tar i bruk de mest avanserte former for utstyr og teknologi i sine angrep, noe som gjør forsvarsjobben utfordrende.

Skatteetaten har definert tre verdier – *profesjonell, imøtekommende og nytenkende*, som skal støtte opp under visjonen deres er: *et samfunn der alle vil gjøre opp for seg.* Dette åpner blant annet opp for at vi også skal ta i bruk ny teknologi for å løse våre utfordringer. Vår satsing på innovasjonsområdet gjenspeiles i å ha fått tildelt Digitaliseringsprisen i 2015 og 2018. Skatteetaten har også blitt rangert som den 5. mest innovative virksomheten i Norge, i undersøkelse gjort av Norges ledende innovasjonsmagasin, (Berg, 2019).

Å møte organisasjonens behov for innovasjon og kreativitet, og samtidig være motstandsdyktige mot trusselaktørene vi står ovenfor, er en utfordring som krever stor balanse. Med dette ønsker jeg å utforske grenseflaten mellom to viktige ambisjoner for skatteetaten: å være innovativ og ha god informasjonssikkerhet. På noen måter kan disse

dra i samme retning, men de kan også være i konflikt. I dette forskningsarbeidet vil jeg derfor diskutere om sikkerhetsmekanismer hemmer innovasjonsarbeidet i Skatteetaten og hvordan vi kan være mer innovative på sikkerhetssiden, slik at vi er bedre rustet mot et dynamisk trusselbilde.

2 Bakgrunn

2.1 Om Skatteetaten

Skatteetaten er underlagt Finansdepartementet og har ansvaret for et oppdatert folkeregister og at skatter og avgifter blir fastsatt og innbetalt på riktig måte. Vi har over 6500 ansatte som jobber for å sikre finansieringen av velferdssamfunnet i Norge. Visjonen deres er et samfunn der alle vil gjøre opp for seg. Med sine 56 kontorer rundt om i landet og med over 6500 ansatte som samler inn over 1050 milliarder kroner hvert år, er det ingen tvil om at de innehar et stort ansvar med stor betydning for Norge.

Skatteetaten er avhengig av stor tillit i befolkningen og et av målene er å gjøre det enkelt for alle å følge skattereglene. Alle landets innbyggere kommer i noen form for kontakt med Skatteetaten uansett om det er familie- eller arbeidsrelaterte situasjoner. På den måten kan man si at Skatteetaten har hele Norges befolkning som kunder og brukere. Møtene med de ulike brukergruppene har mye å si for folkets tillit til oss. Derfor er det viktig at vi alltid er imøtekommende og profesjonelle, i tillegg til å være nytenkende i måten vi løser oppgaver på.

For å øke effektiviteten og fokuset på vårt samfunnsoppdrag, ble etaten den 1.1.19 omorganisert, noe som blant annet førte til at enkelte avdelinger ble omstrukturert, ansatte fikk nye oppgaver, enkelte måtte fysisk flytte, mens noen ble ikke så mye berørt av endringene. Et endelig overordnet organisasjonskart ble slik:

Figur 1: Overordnede organisasjonsstrukturen i Skatteetaten etter 1.1.19

Skatteetaten består nå av et direktorat og seks divisjoner med landsdekkende ansvar. Skattekontorene løser oppgaver på etatsnivå og for hele landet, ikke bare for egen region, som tidligere.

Skattedirektoratet

Skattedirektoratet har fire avdelinger: virksomhetsstyring, HR, kommunikasjon og juridisk avdeling. Avdelingene er etatens kontaktpunkter ovenfor Finansdepartementet på sine fagområder. Direktoratet har også en Sikkerhetsstab, en internasjonal stab og en enhet for administrative tjenester. Stabene synes ikke på dette organisasjonskartet, men er plassert rett under Skattedirektøren.

Divisjonene

Divisjonene har landsdekkende ansvar for sine fagområder. Fire av divisjonene, informasjonsforvaltning, brukerdialog, innsats og innkreving, har landsdekkende ansvar for etatens kjerneproduksjon. I tillegg skal divisjonene utvikling og IT støtte kjernevirksomheten og direktoratet.

Informasjonsforvaltning ivaretar Skatteetatens sentrale rolle som informasjonsforvalter i offentlig sektor. Divisjonen er en spesialisert enhet for innhenting, kvalitetssikring, forvaltning og tilgjengeliggjøring av opplysninger internt og eksternt.

Brukerdialog har ansvar for veiledning, kontroll og fastsetting av skatter og avgifter. Divisjonen sikrer ett kontaktpunkt for Skatteetatens brukere og sikrer etterlevelsen av skatte- og avgiftsregler.

Innsats sikrer riktig fastsetting av skatt og avgift for prioriterte risikoområder og komplekse forhold gjennom kunnskaps- og risikobasert innsats. I tillegg har divisjonen ansvar for helhetlig behandling av storbedriftskonsern m.m.

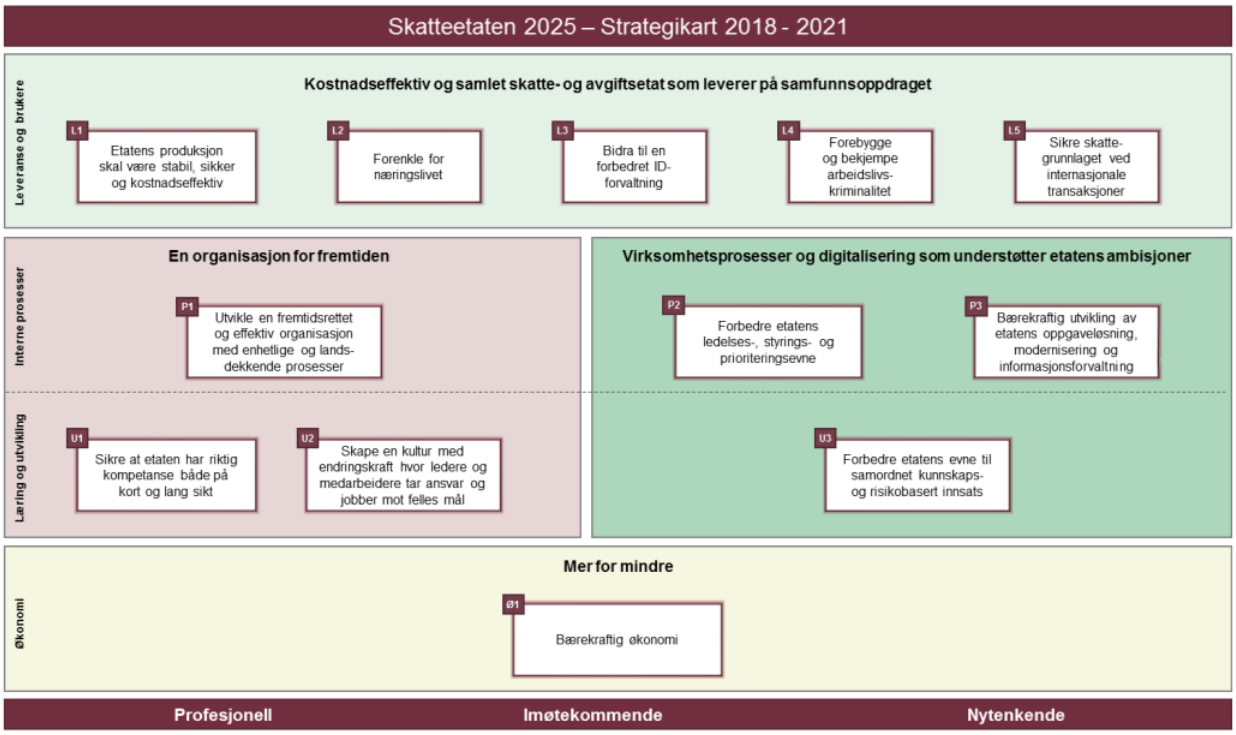
Innkreving har hovedansvaret for innkreving (regnskap og innfordring) på vegne av staten. Enheten sikrer at skatter, avgifter og andre krav betales til rett tid, og har kontakten med de kommunale skatteoppkreverne.

Utvikling støtter direktoratets og resultatenhetenes evne til helhetlig utvikling av samfunnsoppdraget ved å bygge kunnskap. De skal fremme forslag til forbedring av etatens oppgaveløsning, og bygge kunnskap om endringer og risikoer i omverden som understøtter etatens leveranseevne. Divisjonen skal på oppdrag lage beslutningsgrunnlag i tråd med etatens mål og langtidsplaner.

IT skal sikre at etaten har en velfungerende IT-portefølje som understøtter etatens leveranseevne på samfunnsoppdraget på kort og lang sikt, gjennom planlegging, utvikling og forvaltning.

2.1.1 Strategiene, målene og verdiene til Skatteetaten

Skatteetatens sentrale verdier er *profesjonell, imøtekommende og nytenkende*. Disse verdiene er grunnleggende for å løse samfunnsoppdraget og realisere ambisjonene i fremtidsbildet til etaten. For at etaten skal lykkes med å bygge et omdømme som støtter opp under disse verdiene, må de etterleves internt og det må tilrettelegges for det.



Figur 2: Skatteetatens strategikart mot 2021

I strategiperioden 2018-2021 skal etatens brukere erfare at Skatteetaten er en samordnet skatte- og avgiftsforvaltning som yter god service. Skatteetaten skal sikre at samfunnsoppdraget ivaretas ved at produksjonen er sikker og stabil, at det legges til rette for etterlevelse gjennom målrettet innsats på prioriterte risikoområder, ved at etaten leverer gode tjenester og videreutvikler en effektiv oppgaveløsning. Sentralt i samfunnsoppdraget ligger etatens evne til å sikre etterlevelse av det regelverket etaten forvalter

Det er verdt å legge merke til at strategikartet til Skatteetaten inneholder elementer som er interessante for denne oppgaven. De skal være en organisasjon for fremtiden, samtidig som hele produksjonen til Skatteetaten skal være sikker. Som måleparameter på måloppnåelse på disse områdene benyttes blant annet følgende;

- Uten brudd på konfidensialitet og integritet eller andre hendelser som kan svekke brukernes tillit til etaten.
- Vi samhandler i organisasjonen for bedre kvalitet og effektivitet i oppgaveløsningen
- Vi samarbeider med brukere og eksterne samarbeidspartnere for å sikre helhetlige og innovative leveranser

2.1.2 Endring og digitalisering i Skatteetaten

Den teknologiske utviklingen akselererer raskere enn noen gang og påvirker stadig flere områder i samfunnet. Det estimeres at en endring skjer 10 ganger raskere og har 3000 ganger større påvirkning nå sammenlignet med den industrielle revolusjonen, (Dobbs, Manyika og Woetzel, 2015, s. 1). Det er mange eksempler på endringer som skjer fort og som har veldig stor påvirkning i samfunnet.

Om få år vil selvkjørende biler være en del av trafikkbildet. Datamaskiner innebygd i våre armbåndsur, hvitevarer, kjøkkenmaskiner, varmeovner, betalingsterminaler, medisinsk utstyr og tusenvis av andre ting vil kunne kommunisere via internett.

Informasjonsmengdene øker voldsomt. Analyse av store mengder informasjon til ulike formål ved hjelp av stadig kraftigere datamaskiner og verktøy, er blitt en stor industri. Stadig flere virksomheter blir basert på forvaltning av informasjon og i mindre grad på tradisjonell produksjon.

Selvlærende datamaskiner (kunstig intelligens) som finner svar på spørsmål, løser oppgaver og utvikler ny kunnskap raskere enn et menneske kan, er allerede en realitet. Om kort tid vil det være helt vanlig med datamaskiner som både forstår menneskelig tale og hva som ble ment. Industrier og virksomheter kommer til å bli mer og mer robotbaserte. Den teknologiske utviklingen kan gjøre etaten mer effektiv og frigjøre ressurser til andre oppgaver.

Endringer i teknologiske muligheter vil i løpet av de årene som kommer få stor betydning for etatens arbeidsprosesser, kompetansebehov, teknologiske plattform og organisasjonen. Vi har gått fra papirbaserte innleveringer av selvangivelsen og bruk av pc for innlevering, til skjemainnlevering fra mobile plattformer som telefon og tableter. Det er også sannsynlig at flere av etatens oppgaver over tid, helt eller delvis, vil kunne bli erstattet av smarte IT-løsninger. Samtidig må Skatteetaten unngå å havne i en situasjon der etatens systemer, løsninger, metoder og arbeidsprosesser blir utdaterte og inkompatible med omgivelser som er i rask endring. Ikke minst må sikkerheten ivaretas da endringer ofte fører til nye risikoer.

Den høye innovasjonstakten, ambisjonene, strategimålene og moderniseringen ellers i samfunnet driver oss til å digitalisere og hele tiden utfordre våre etablerte løsninger og metoder. Skatteetaten satser derfor tungt på digitalisering, det gjenspeiles i flere priser vi har mottatt relatert til digitalisering og modernisering de siste årene, sist i 2018 da vi mottok digitaliseringsprisen.

2.2 Forretningsutvikling og innovasjon i Skatteetaten

Forretningsutvikling er en avdeling som skal støtte direktoratet og kjernevirksomhetens evne til helhetlig utvikling av samfunnsoppdraget. Med sine 19 ansatte er de er organisatorisk plassert under divisjonen Utvikling. De har ansvar for å levere ulike oppdrag og deltar i utviklingsaktiviteter slik at sammenhengen mellom regelverk, prosesser, teknologi og organisasjon ivaretas. De skal bidra til kunnskapsdeling og rådgivning som sikrer sammenhenger på tvers og som ikke dekkes av pågående utviklingsaktiviteter. Divisjonen utvikler og vedlikeholder felles metodikk for forretningsutvikling i etaten og bistår i resultatenhetenes utviklingsarbeid. De er en pådriver for innovasjon og samarbeider tett med andre avdelinger for gjennomføringen av pilotprosjekter og nye idéer som kan forbedre og forenkle direktoratets oppgaver.

2.2.1 Kjerneoppgavene til Forretningsutvikling

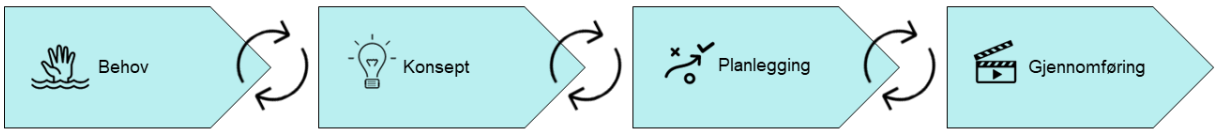
- Levere beslutningsgrunnlag for tidlige faser av utviklingen
- Utarbeide løsning-, behovs- og konseptforslag for større ordningsendringer
- Være en pådriver for dialog om tverrfaglige sammenhenger på tvers av divisjoner i forretningsutviklingen

- Utvikle og forvalte metodeverk for koordinert forretningsutvikling
- Ivareta helhetlig utvikling gjennom å forvalte og koordinere prinsipper og krav til forretningsutviklingsarbeidet
- Forretningsutvikling i prosjekter, deltakelse i aktuelle styringsgrupper og fagråd
- Prosjektstyring og prosjektgjennomføring
- Gevinstarbeid gjennom fasilitering og støtte for tiltak/initiativer i tidlig fase

De jobber og utvikler behov og konsepter basert på oppdrag fra både interne og eksterne aktører, blant annet; Finansdepartementet, Skattedirektoratet, Divisjonene og behov identifisert fra aktiv dialog med omgivelsene og samfunnet generelt. De skal blant annet sikre at utviklingstiltakene løser reelle behov og at de har effekter på tvers av divisjonene. Arbeidet deres er strømlinjeformet gjennom metodikk og prosesser beskrevet nedenfor.

2.2.2 Overordnet prosess

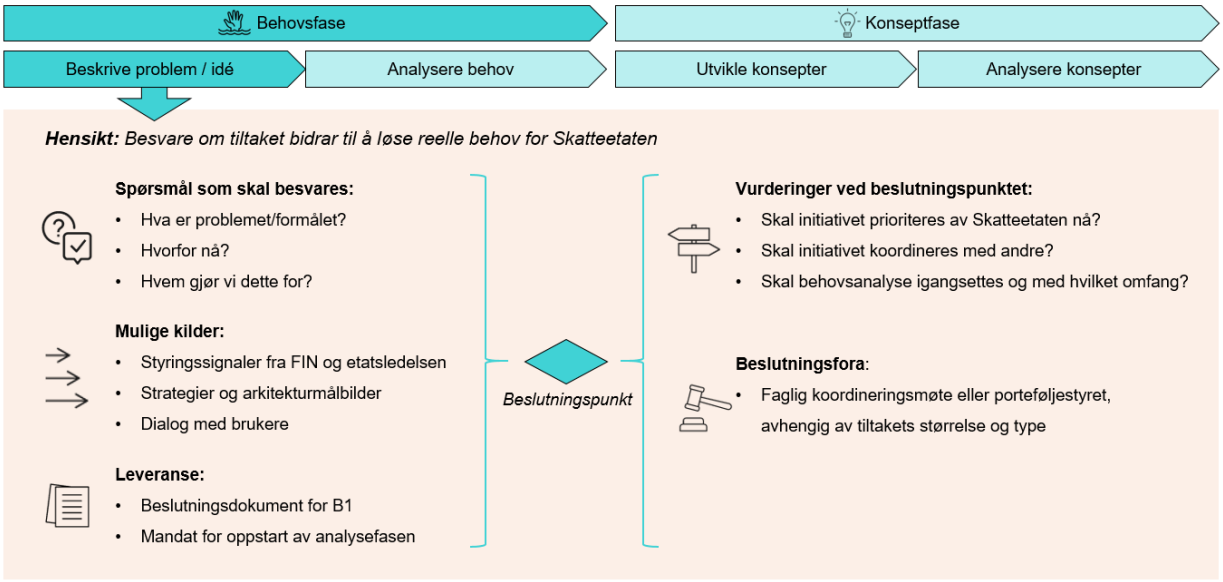
Den overordnede prosessen som avdelingen Forretningsutvikling følger i etaten er delt inn i fire faser; behov, konsept, planlegging og gjennomføring. I behovsfasen kartlegger de problemet eller idéen, samt analyserer behovet. Deretter analyserer de og utvikler konsepter, før de setter i gang planleggingen og rigger prosjektorganisasjonen. Til slutt gjennomføres dette som et prosjekt i etaten, med en anbefaling om man skal gå videre med å rulle ut dette i større sammenheng.



Figur 3: Overordnet innovasjonsprosess i Skatteetaten, (Hentet fra forretningsutviklingsplanen til Skatteetaten)

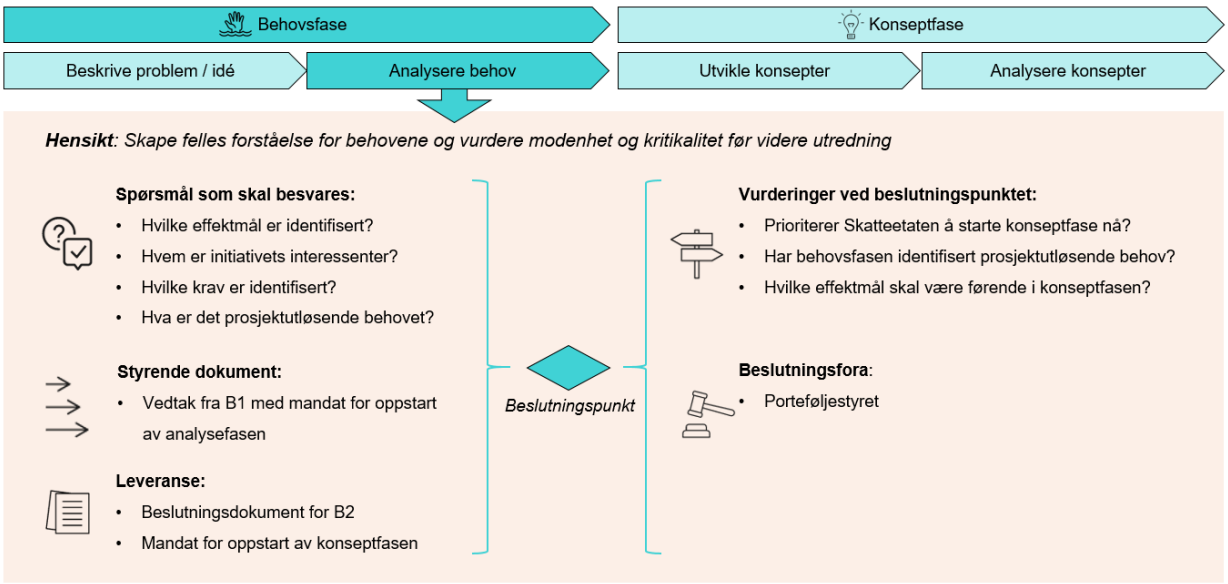
2.2.3 Detaljert prosessbeskrivelse

Hvert steg i forskjellige fasene består av flere delsteg; spørsmål som skal besvares, dokumenter/kilder som benyttes som grunnlag, hva som er leveransen for den aktuelle fasen, hva som skal besluttes i fasen og hvem som er med på å ta avgjørelsen. Under følger en detaljert beskrivelse av hver fase og steg, vist gjennom forskjellige figurer som er hentet fra forretningsutviklingsplanen til Skatteetaten. Disse fasene og stegene benyttes aktivt i arbeidet til avdelingen Forretningsutvikling, som også har gitt meg introduksjon til selve prosessen. Jeg har valgt å skrive en kort forklaring under hver fase og aktivitet, slik at også leseren ser sammenhengen mellom dem.



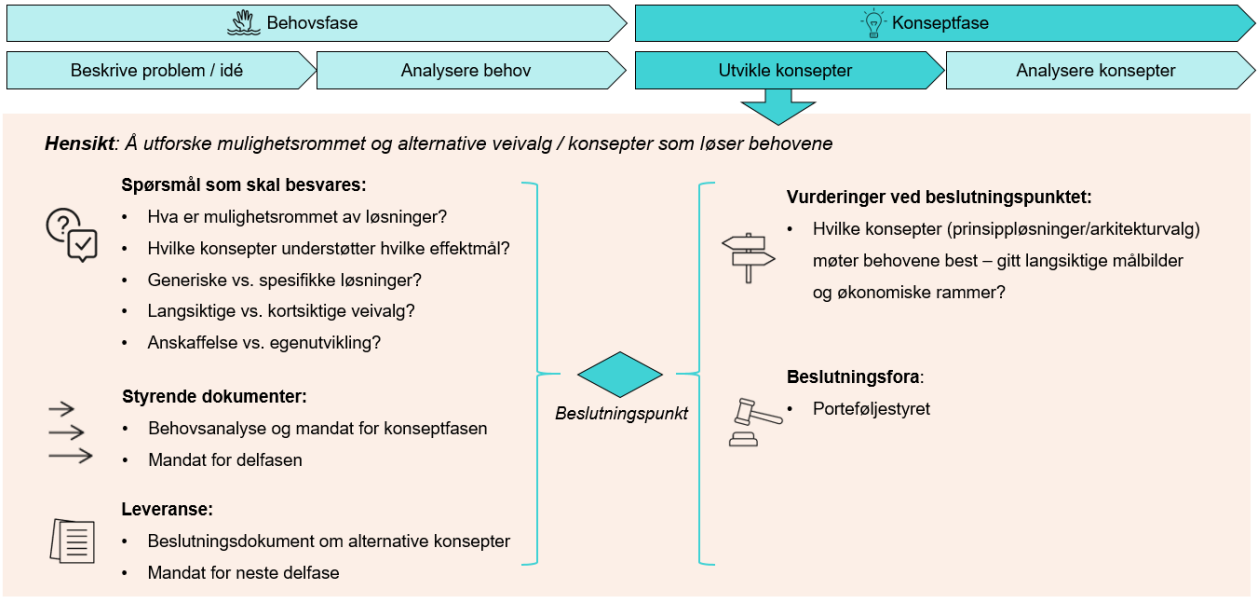
Figur 4: Viser aktiviteten der problemet eller idéen beskrives, (Hentet fra forretningsutviklingsplanen til Skatteetaten)

Under behovsfasen kartlegges først idéen eller problemet. Hensikten med denne aktiviteten er å besvare om tiltaket bidrar til å løse et behov for Skatteetaten. Det blir stilt relevante spørsmål som avdekker om behovsanalyse skal settes i gang og eventuelt hvilken prioritet og omfang dette arbeidet skal ha.



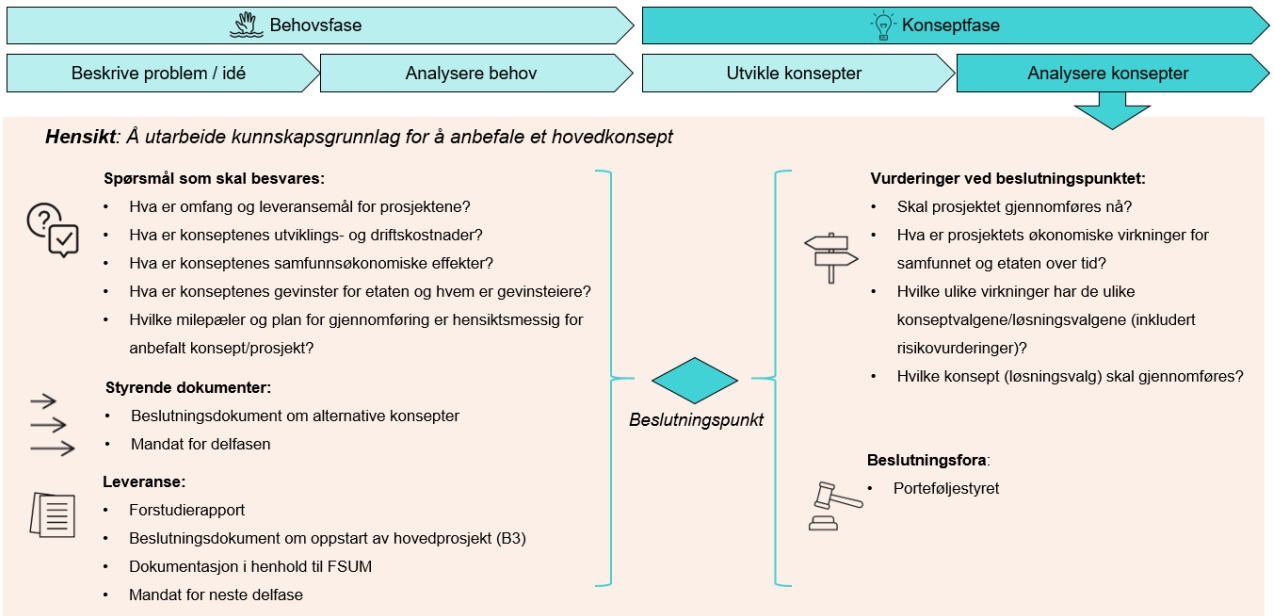
Figur 5: Viser aktiviteten der behovet analyseres, (Hentet fra forretningsutviklingsplanen til Skatteetaten)

Dersom det i forrige steg ble identifisert at man skal gå videre med idéen, analyseres selve behovet. Hensikten med denne aktiviteten er å skape felles forståelse for behovene, vurdere modenhet og kritikalitet for videre utredning. Arbeidet i denne fasen danner grunnlaget for et beslutningspunkt om det skal startes en konseptfase, som da er mer omfattende arbeid.



Figur 6: Viser aktiviteten der mulighetsrommet og veivalg blir utforsket, (Hentet fra forretningsutviklingsplanen til Skatteetaten)

Konseptfasen består av to aktiviteter, hvor den første innebærer å utforske mulighetsrommet og finne konseptene som kan løse behovene fra forrige steg. I denne fasen vurderes også de forskjellige tilnærmingene, om man skal ha mer generelle løsninger eller spesifikke og om man skal gå til en anskaffelse eller utvikle det internt i etaten.



Figur 7: Viser aktiviteten som analyserer konseptene, (Hentet fra forretningsutviklingsplanen til Skatteetaten)

Den andre aktiviteten i konseptfasen analyserer de forskjellige konseptene og foreslår til slutt et hovedkonsept for gjennomføring. Før det kommer dithen ser man på kostnader, leveransemål, effekter og gevinster ved å gjennomføre dette fullt ut.

2.2.4 Innovasjonsarbeidet

Selve innovasjonsarbeidet i etaten er ikke forbeholdt divisjonen Utvikling. Det er lagt opp til at alle divisjonene har mulighet og midler til å forbedre og innovere på sine respektive områder. Dette er blant annet sikret gjennom egne budsjettposter i den enkelte divisjonens budsjett som tildeles årlig. Mens divisjonen Utvikling har ansvaret for det konseptuelle hva gjelder innovasjon og forretningsutvikling på etatsnivå, er de andre divisjonene ansvarlig for gjennomføring og realisering av dette på sine underområder. For eksempel for IT divisjonen blir det hvert år satt av midler til å fornye, forbedre og innovere IT-systemene og resten av de underliggende oppgavene de har ansvaret for å levere til direktoratet. Investeringer for å fremme innovasjon i denne divisjonen blir dermed gjennomført gjennom en egen Planleggingsstab.

Planleggingsstaben har ansvaret for å utøve langsiktig, strategisk planlegging av IT-divisjonens behov og leveranser for utvikling av IT-applikasjoner og IT-infrastruktur. Samtidig har de ansvaret for å støtte IT-direktøren og etatsledelsen i strategiske IT-relevante spørsmål, samt være premissgiver for arkitekturstyringen av IT-applikasjoner og IT-infrastruktur. Innovasjon på IT-sikkerhetsområdet, som er sentralt i denne oppgaven, vil derfor til syvende og sist falle inn under ansvaret til IT divisjonen med input fra Planleggingsstaben.

2.3 Sikkerhet i Skatteetaten

Skatteetaten er avhengig av tilliten til skattyterne, storting og departement. Håndtering av sikkerheten i etaten er viktig for å oppnå og opprettholde denne tilliten, noe som ivaretas gjennom en Sikkerhetsstab og IT-sikkerhet.

Sikkerhetsstaben, organisert som en stab rett under Skattedirektøren, teller 10 ansatte. De har et helhetlig ansvar for sikkerhet og kriseberedskap i etaten, herunder ansvar for samfunnssikkerhet, informasjonssikkerhet, fysisk sikkerhet og personsikkerhet. Kravene til disse domenene er nedfelt i etatens styringssystem (se forklaring på side x) som er obligatoriske for alle etatens ansatte. Styringssystemet utarbeides, vedlikeholdes og følges opp av Sikkerhetsstaben og besluttes av skattedirektøren. Divisjonene på sin side har ansvaret for tilrettelegging slik at de underliggende avdelingene og deres medarbeidere kan oppfylle kravene på arbeidsplassen. I denne oppgaven vil det være fokus på informasjonssikkerhet og de øvrige ansvarsområdene til Sikkerhetsstaben, som selvsagt er viktige områder, vil ikke bli diskutert i denne oppgaven. Ansvarsområdene til Sikkerhetsstaben kan brytes ned i flere konkrete aktiviteter som:

- Dekke Skattedirektørens definerte, myndighets- og lovpålagte behov for styringssystemer, fag-kompetanse og oppfølging innen sikkerhet, krisehåndtering og beredskap
- Ha metodikk, planer og prosedyrer for samfunnssikkerhet og beredskap, samt bidra til å identifisere og påse at sikkerhetstiltak iverksettes.
- Følge opp operativ sikkerhet i IT (IT-Sikkerhet)

- Følge opp at linje og prosjekter leverer akseptabelt sikre løsninger, benytter sikkerhets- mekanismer og forholder seg til krav i styringssystemene
- Følge opp divisjonenes planer og øvelser innen krisehåndtering og beredskap
- Følge opp etterlevelse av etatens Personsikkerhet
- Sørge for at etatens styring på sikkerhetsområdene kan inkorporeres og koordineres med etatens øvrige styringsparametere
- Gjennomføre opplæring og stille krav til sikkerhetskompetanse i etaten
- Rapportere direkte til Skattedirektør ved kritiske sikkerhetshendelser eller ved observerte situasjoner som medfører høy risiko
- Gjennomføre sikkerhetsmotiverte internkontrollaktiviter (sikkerhetstester, sikkerhetsgjennomganger, sikkerhetsrevisjoner) i etatens enheter, leveranseprosesser og systemer.
- Iverksette krav om personellsikkerhet og sikkerhetsklareringer basert på Sikkerhetsloven, forskrifter og risikovurderinger

Sentralt i sikkerhetsarbeidet står også IT-sikkerhet som er organisatorisk plassert under IT-divisjonen. De har ansvaret for å følge opp dagligdagse digitale trusler mot organisasjonen og deres ansatte, i tillegg til føringene de får fra Sikkerhetsstaben. Det er også her Skatteetatens Incident Response Team (IRT) er plassert, som er å anse som førstelinje forsvar dersom en digital uønsket hendelse inntreffer mot etatens IT-systemer. De har 9 ansatte i avdelingen som inngår i en beredskapsordning i samarbeid med sentrale nasjonale aktører.

2.3.1 Informasjonssikkerhet

God informasjonssikkerhet bidrar til et godt omdømme og opprettholder tillit til norsk offentlig forvaltning. Det bidrar også til å nå etatens mål og følger etatens strategier med hensyn til akseptabel risiko. Sikkerhetsstaben har, innenfor segmentet informasjonssikkerhet, ansvaret for å tilrettelegge, bistå og gi råd til linjene i deres arbeid med informasjonssikkerhet. De har også et ansvar for at avtalepartnere og leverandører er bevisste på sikkerhetsbestemmelsene og etterlevelse av dem. Arbeidet med informasjonssikkerhet i Skatteetaten følger en del viktige styringsprinsipper:

i. Akseptabelt risikonivå

Oppbevaring og behandling av informasjon med tilhørende IT-systemer og rutiner i Skatteetaten skal basere seg på risikovurdering og holde seg innenfor akseptabelt risikonivå.

Ved kryssende sikkerhetsbehov skal behovene for sikring av konfidensialitet og integritet som hovedregel gå foran hensynet til tilgjengelighet.

ii. Sikkerhetsmessig lønnsomhet

For hendelser som etter en risikovurdering havner i området der tiltak skal vurderes, gjelder prinsippet om sikkerhetsmessig lønnsomhet. Et sikkerhetstiltak skal normalt koste mindre i anskaffelse og drift enn det koster å leve med den risiko tiltaket vil eliminere. Før etablering av prioriterte tiltak skal derfor ansvarlig ledelse vurdere hvilke kostnader tiltaket medfører,

målt opp mot den nytte og de fordeler som redusert risiko kan medføre. Hendelser med særlig høy konsekvens skal vurderes nærmere selv om sannsynligheten er lav.

iii. Minste privilegiums prinsipp

Ansatte og avtalepartnere skal bare gis tilgang til de IT-systemer og den informasjon vedkommende har behov for i sitt arbeid. Skatteetaten skal praktisere minste privilegiums prinsipp, slik at akseptabel sikkerhetsrisiko oppnås ved avveiing mellom behovet for sikkerhetstiltak, behovet for fleksibel og effektiv administrasjon og oppgaveløsning, samt behov for informasjonsutveksling som virkemiddel for samarbeid og kompetanseutvikling.

iv. Arbeidsdeling

Ansvarlige ledere skal så langt praktisk mulig innføre arbeidsdeling ved utførelse av kritiske oppgaver innen sitt ansvars- og myndighetsområde. Arbeidsdeling innebærer at forskjellige personer utfører ulike arbeidssteg for å fullføre oppgaven. På denne måten reduserer etaten muligheten for at enkeltpersoner kan utføre vinningskriminalitet eller på annen måte undergrave tillit til Skatteetaten eller skade etatens omdømme.

v. Eierskap til produkter og interne tjenester

Ansvaret for produkter og interne tjenester er plassert i linjen. Ansvarlige i linjen skal klassifisere produkter og tjenester med utgangspunkt i det aktuelle bruksområdet og den informasjon som behandles. Formålet er å indikere den kritikalitet produktet/tjenesten har for Skatteetaten. Ansvarlige i linjen har også ansvar for gjennomføring av risikovurdering av informasjonssikkerhet jevnlig og ved endringer som påvirker risikobildet.

vi. Sikkerhet i dybden

Etatens tjenester og løsninger skal utformes slik at prinsippet om sikkerhet i dybden ivaretas. Prinsippet setter krav om at det skal eksistere flere lag av uavhengige sikkerhetsmekanismer (prosedyrer, praksiser og teknologier - for en mer detaljert forklaring se i Begreper på side xi). Hensikten er å øke vanskelighetsgraden av å kunne gjennomføre en uønsket hendelse ved å måtte passere flere lag enn kun ett, samt at én feil i et lag ikke alene vil resultere i en uønsket hendelse.

vii. Sikkerhetsbetingelser for avtalepartnere

Tredjepart som skal ha tilgang til Skatteetatens informasjon eller IT-systemer, skal inngå en kontrakt som inneholder eller refererer til alle nødvendige krav for å sikre overensstemmelse med etatens styringssystem for informasjonssikkerhet.

2.3.2 Fysisk sikkerhet

Med etatens 6500 medarbeidere, hvor noen ansatte sitter på kontor, noen veileder skattytere og andre er på kontrollaksjoner, er behovet for fysisk sikkerhet uansett tilstede.

Omfanget på dette området er ganske stort ettersom det gjelder alt fra vernesko og stikksikre vester brukt på kontroller, til adgangskontrollsystemer og skuddsikre glass på kontorene.

Alle medarbeiderne har et ansvar for at den fysiske sikkerheten opprettholdes, samt å rapportere observerte feil og mangler.

2.3.3 Beredskap

Overordnet plan for beredskap er en sentral plan som beskriver hvordan en krise kan håndteres i forskjellige situasjoner. Spesifikke underliggende planer skal eksistere for IT-systemene og for vesentlige deler av sentral infrastruktur og samfunnsoppdraget forøvrig. Dette er noe som skal øves på og vedlikeholdes med jevne mellomrom.

Kontorene utarbeider lokale planer for å opprettholde kritiske funksjoner når sentrale funksjoner ikke er tilstede, eller har sterkt redusert kapasitet. Sikkerhetsstab gir råd og støtte til utarbeidelse, samt deltar på øvelser.

2.3.4 Krisehåndtering

Sikkerhetsstab har ansvar for å ha en oppdatert terrorberedskapsplan og den sentrale planen for krisehåndtering, i tillegg har de ansvar for å øve den sentrale kriseledelsen i planverket.

3 Teori

Dette kapittelet skal gi en oversikt over litteratur og teorier relatert til innovasjon og informasjonssikkerhet som skal understøtte min analyse. Jeg vil også legge frem Skatteetatens trusselbilde før jeg presenterer tidligere forskning på innovasjon og informasjonssikkerhet. Avslutningsvis i dette kapittelet går jeg også inn på hva et trusselbilde i endring innebærer, for å gi leseren en forståelse av den siden av sikkerhetsaspektet.

3.1 Innovasjon

Ordet innovasjon stammer opprinnelig fra det greske ordet "innovare" som betyr "å lage noe nytt". Vi finner en del misoppfatninger om at innovasjon og oppfinnelse er det samme, både i litteraturen og i dagligtale. Oppfinnelse, eller oppdagelse, er derimot den første fasen i en innovasjonsprosess – det vil si den første fasen når ideen til et produkt eller prosess oppstår. Begrepet innovasjon benyttes når oppfinnelsen har kommet i bruk eller blitt implementert, (Gjelsvik, 2007). Samtidig finnes det ulike former for innovasjon, Gjelsvik påpeker følgende former en entreprenør kan ta initiativ til:

- Produkt og tjenesteinnovasjon
- Prosessinnovasjon, måten produkter og tjenester utvikles og distribueres
- Nye ressurser
- Åpne og utnytte markedet
- Omstruktureringer av hele bransjer (nye forretningsmodeller)

Når det gjelder selve innovasjonsprosessen finnes det flere definisjoner på dette og de er ofte sammensatt av flere faktorer, noe som gjør det vanskelig å definere innovasjonsprosessen som én. En slik prosess skiller ut seg avhengig av hvilken økonomisk sektor det er snakk om, kunnskapsområde, type innovasjon, hvilket land det er snakk om og hvilken historisk periode som er aktuell. Den endrer seg også etter størrelsen på organisasjonen og hva forretningsstrategien til den aktuelle organisasjonen er. Økonomer strever etter å økonomisk beregne effekten av innovasjon, mens spesialister på organisering fokuserer på å innovere aktiviteter og prosesser som vil ha effekt på de sosiologiske aspektene, (Fagerberg, Mowery & Nelson, 2006).

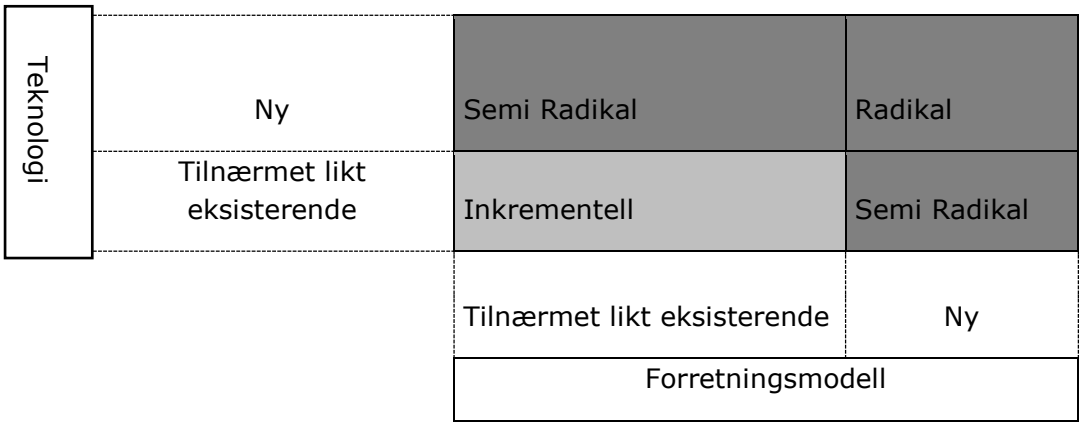
For denne oppgaven har jeg valgt å ta utgangspunkt i produkt og tjenesteinnovasjon, samt prosessinnovasjon. Dette valget gjorde jeg basert på at det allerede eksisterer både verktøy og prosesser i de miljøene jeg skal samle inn data fra. I kombinasjon med det utgangspunktet vil jeg bruke definisjonen og rammeverket som Fagerberg, Mowery og Nelson beskriver i sin bok *The Oxford handbook of innovation*. Grunnen til at jeg valgte akkurat det rammeverket for en innovasjonsprosess, er fordi den samsvarer godt sammen med problemstillingene i denne oppgaven, samt at den er generell nok til at den kan tilpasses til konkrete problemstillinger som finnes i denne oppgaven;

Innovasjonsprosessen involverer utforskningen og utnyttingen av muligheter for nye forbedrede produkter, prosesser eller tjenester, basert på en avansert teknisk praksis eller endring i markedsbehovet – eller en kombinasjon av disse to. Innovasjon er usikkert, da det er umulig å forutse eksakte kostnader, ytelse og effekt av en ny gjenstand, samt hvordan brukere vil reagere. I en innovasjonsprosess er man derfor nødt til å ha med en læringsfase, enten gjennom eksperimentering (prøv og feil) eller forbedret forståelse (teori). (Fagerberg et al., 2006, s.88 – oversatt av meg selv).

Det er også en generell misoppfatning at innovasjon betyr noe helt nytt eller revolusjonerende eller at det bare er en teknologisk endring, men det er absolutt ikke tilfellet. Innovasjon kan også være endring i forretningsmodellen; endring i rutine, prosess, et eksisterende produkt eller kombinasjon av disse, noe som jeg har tenkt å basere meg på i denne oppgaven, (Davila, Epstein & Shelton, 2007). Samtidig påpeker Davila, Epstein og Shelton i sin bok *Making innovation Work,* tre typer innovasjonsstrategier som også passer veldig godt i denne oppgaven og som er relativt enkle å forholde seg til;

- Inkrementell
- Semi-radikal
- Radikal

Inkrementell innovasjon leder til mindre forbedringer i et allerede eksisterende produkt eller forretningsprosess. Man kan se på det som en øvelse eller workshop for problemløsing hvor målet er å finne ut hvordan deres behov skal bli dekket. På den helt motsatte siden av skalaen har vi den radikale innovasjonen som resulterer i nytt produkt eller tjeneste levert på en helt ny måte – ofte kalt *"game changer".* For å finne en strategi for hvilken inndeling eller retning man velger, er det viktig å forstå innholdet i hver inndeling og når det er gunstig å benytte dem. Figuren under viser de forskjellige inndelingene og hvordan de passer inn i innovasjonsmatrisen.



Figur 8: Innovasjonsmatrisen, (Davila et al., 2007)

Inkrementell innovasjon er den mest utbredte formen for innovasjon i de fleste organisasjoner. De fleste organisasjonene innoverer gjennom prosjekter hvor målet er mindre endringer i forretningsmodellen eller teknologien. Ved inkrementell innovasjon forsøker man å bringe frem så stor nytteverdi som mulig i et eksisterende produkt eller tjeneste uten å endre for mye eller investere altfor mye i endringen. Mange organisasjoner tyr kun til inkrementell innovasjon av produktene sine som kan det være en fallgruve for

dem hvis de har for lite av denne type innovasjon. Det gjør det lettere for konkurrenter å kopiere ideene og man risikerer å miste kunder. For at en organisasjon skal ha langsiktig suksess er man derfor avhengig av å kombinere innovasjonsmetoder, slik at organisasjonen er konkurransedyktig og attraktiv.

En semi-radikal innovasjon kan bidra til en større endring enn inkrementell innovasjon. For å gjennomføre vellykket semi-radikal innovasjon må det en vesentlig endring til i enten forretningsmodellen eller teknologien, men ikke begge samtidig. Den ene siden er uansett linket til den andre og vil påvirke den og derfor kombineres de ofte ved å for eksempel ha semi-radikal innovasjon på teknologisiden og en inkrementell innovasjon på forretningsmodellen, eller omvendt. En slik link og avhengighet fører til nye muligheter på begge sider, men man må være klar over at en større innovasjon av denne typen krever at organisasjonen er godt forberedt og har kapasitet nok for å gjennomføre den fullt ut.

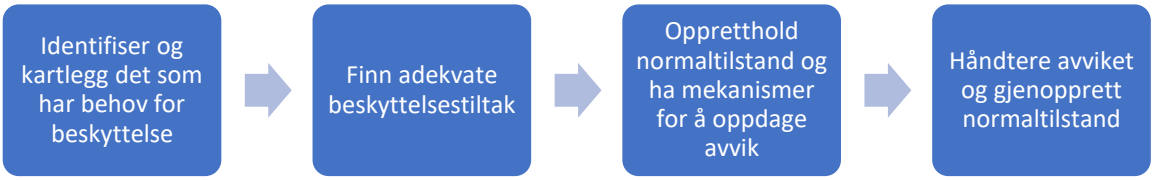
Radikal innovasjon er som ordet selv sier en betydelig endring av både forretningsmodellen og teknologien i en organisasjon. Denne type innovasjon bidrar til stor endring i konkurransebildet innenfor en bransje og dersom den er suksessfull får de ofte betegnelsen "game changer". Et eksempel på det er introduseringen av bleier på 1970-tallet, som kom på et tidspunkt da det ble benyttet bomullstøy på barnerumpene. De nye bleiene absorberte bedre, var til engangsbruk og krevde ikke vask, samtidig som de var lett tilgjengelig. Senere har bleien utviklet seg gjennom semi radikal og inkrementell innovasjon ved å tilføre endringer som bedre feste, absorbering, etc. Radikal innovasjon er samtidig risikabelt, da sannsynligheten for å lykkes er lavere enn ved mindre endringer i et suksessfullt produkt, noe som kan føre til konsekvenser for organisasjonen og investeringen.

3.2 Informasjonssikkerhet

De siste årene har det vært økende fokus på informasjonssikkerhet og økning av antall sårbarheter globalt, (Skybox Research Lab, 2019). I Norge rapporteres det også om økning av sikkerhetsrelaterte hendelser fra år til år. Nasjonal sikkerhetsmyndighet (NSM), som bidrar til å beskytte mot angrep på IT-systemene til grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv, har også vokst i antall årsverk for å håndtere slike hendelser. De påpeker også i sin årsrapport for 2019 at statlige aktører utgjør den største digitale risikoen mot viktige samfunnsfunksjoner og nasjonale interesser, (NSM, 2020). Dette gjør at informasjonssikkerhetsarbeidet aldri har vært viktigere i bade globalt og norsk sammenheng.

Arbeidet med informasjonssikkerhet handler om å sikre informasjonen og informasjonsbehandlingen i alle former og alle ledd, både fysisk og digitalt. Dette gjøres gjennom prinsippene;

- Konfidensialitet: Informasjonen avsløres ikke for uvedkommende og kun autoriserte personer og systemer får tilgang til den.
- Integritet: Informasjonen og informasjonsbehandlingen har ikke blir endret av uautoriserte
- Tilgjengelighet: Informasjonen er tilgjengelig ved behov til riktig ressurs. Spesielt viktig i en verden hvor internett kobler ting sammen og man har mulighet til å nå informasjon fra hvor som helst og til hvilken som helst tid.



Figur 9: Viser grunnleggende IKT-prinsipper, (Bergsjø & Windwik, 2018)

En generell og enkel beskrivelse av hvordan man skal ivareta konfidensialitet, integritet og tilgjengelighet av informasjon, har Bergsjø og Windwik beskrevet i sin bok *Datasikkerhet for ledere*.

Først identifiserer og kartlegger man det som har behov for beskyttelse. Dette er typisk informasjon som har høy verdi for en organisasjon, noe som kan være så mangt; for eksempel alt som kan føre til tap av liv og helse eller økonomi, samt skader på omdømmet til organisasjonen. Avhengig av informasjonen organisasjonen besitter og behandler kan det være alt fra helseopplysninger til bank- og kredittkortopplysninger.

For å finne adekvate beskyttelsestiltak må man først analysere kontekst og type medium informasjonen er på. Dersom man for eksempel har et papirdokument som er unntatt offentlighet, og som dermed ikke skal kunne leses av uautoriserte, ivaretas konfidensialiteten ved å hindre innsyn. Da vil man typisk ikke ha et slikt dokument liggende slik at andre kan få tak i det og man vil heller ikke ta det frem på offentlige plasser hvor andre kan lese det. Beskyttelsestiltaket her kan for eksempel være opplæring av ansatte, låsbare skap på kontoret eller innsynsfilter på pc skjermen.

På den andre siden har man et digitalt tekstdokument i et redigerbart format, for eksempel en rapport som ikke skal kunne endres av andre enn forfatterne selv, er det viktig å ivareta integriteten. Hvis det for eksempel er behov for å sende denne rapporten til andre forfattere med annen geografisk plassering, overføres det gjennom metoder som sikrer at rapporten ikke er endret på veien til mottaker. Dette er for eksempel spesielt viktig i saksbehandlingsløp der endring av data under en arbeidsprosess kan få konsekvenser for utfallet i en sak – noe som er viktig i for eksempel skatteprosessen.

Hvis man likevel skulle være utsatt for et brudd på konfidensialitet, integritet eller tilgjengelighet av informasjon, er det viktig å kunne oppdage det og opprettholde normaltilstand. For å kunne gjøre det må det eksistere mekanismer som trigger eller sier ifra dersom et brudd har skjedd. Slike triggere kan være alt fra fysiske innbruddsalarmer til sensorer i datanettverket som melder ifra ved unormal aktivitet.

Hvis alarmen går og det har oppstått et avvik må det også eksistere rutiner og beredskap for å håndtere denne hendelsen. Det vil da være behov for å ettergå hendelsen og finne ut hva som har skjedd og samtidig kunne gjenopprette normaltilstanden, gjennom for eksempel sikkerhetskopier.

Informasjonssikkerhet i denne oppgaven handler om sikring av digital informasjon sett opp mot uønskede hendelser i eller gjennom IT-systemer. Hvordan man faktisk sikrer digital informasjon i et IT-system er situasjonsavhengig, men dette kan være alt fra enkle tiltak som passord og tilgangsstyring til brannmurer og mer avanserte krypteringsløsninger.

3.2.1 Styringssystem for informasjonssikkerhet

Et styringssystem for informasjonssikkerhet er et sett med dokumenter som beskriver regler og prosedyrer laget for å ivareta informasjonssikkerheten til en organisasjon. Disse reglene og prosedyrene skal understøtte strategien til organisasjonen og er ofte delt inn i flere nivåer; et generelt overordnet nivå, et undernivå hvor reglene er delt inn i spesifikke områder/temaer, et nivå med konkrete eksempler og situasjoner. Viktigheten og verdien i et styringssystem ligger i at alle ansatte forstår og følger reglene som er nedfelt der.

Dokumentene som utgjør styringssystemet for informasjonssikkerhet (SFI) i Skatteetaten er delt i nivåer i henhold til beskrivelsen ovenfor. Overordnet policy er på nivå 1, spesifikke policyer på nivå 2 og tilhørende standarder, instrukser og veiledninger er på nivå 3. Denne oppbygningen er basert på ISO 27001 standarden, som stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.

Figur 10: Strukturen på styringssystemet for informasjonssikkerhet (Skatteetatens overordnede policy for informasjonssikkerhet, 2019)

Den overordnede sikkerhetspolicyen (SFI-1.1) er forankret hos etatens øverste ledelse og de spesifikke sikkerhetspolicyene (SFI-2.n) forankres på riktig nivå og i riktige organisasjonsenheter i linjen avhengig av innhold og målgruppe. Den overordnede policyen gir føringer for alle sikkerhetspolicyene for håndtering av sikkerhet, mens de spesifikke sikkerhetspolicyene setter krav til informasjonssikkerhet på underliggende sikkerhetsområder.

Eksempler på slike spesifikke sikkerhetspolicyer innenfor informasjonssikkerhet (SFI-2.n):

- Sikkerhetsansvar
- Risikostyring av sikkerhet
- Internkontroll av informasjonssikkerhet
- Personellsikkerhet
- Driftssikkerhet
- Nettverkssikkerhet
- Kontinuitet
- Fysisk sikkerhet
- Systemsikkerhet

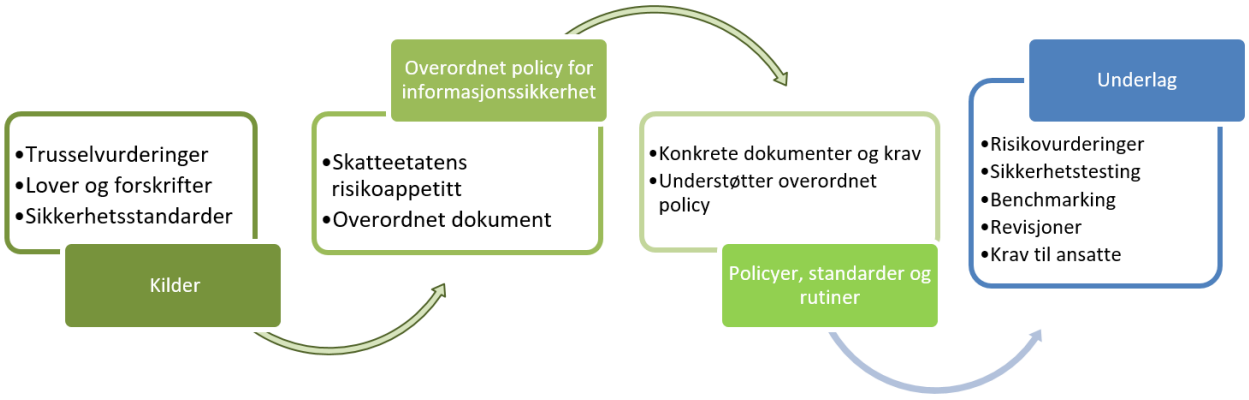
- Identitetsforvaltning
- Sikkerhetsgradert informasjon
- Sikkerhet i informasjonshåndtering
- Logging
- Kryptografi

Med basis i spesifikke policyer foreligger nødvendige sikkerhetsstandarder, sikkerhetsinstrukser og/eller sikkerhetsveiledninger på nivå 3 (SFI-3.n) i SFI:

- *Sikkerhetsstandarder* er detaljerte beskrivelser av hvordan sikkerhetskravene i en policy oppfylles. En standard kan i noen tilfeller inneholde mer detaljerte krav til hvordan sikkerhet skal løses for eksempel i ulike IT-systemer. Det kan være flere standarder som understøtter en policy.
- *Sikkerhetsinstrukser* beskriver konkret sikkerhetsansvar og oppgaver/prosesser tillagt ulike ansatte og/eller funksjoner i Skatteetaten, for eksempel brukere, ledere, driftspersonell og sikkerhetspersonell.
- *Sikkerhetsveiledninger* er gode råd, forklaringer og hjelp til implementering av informasjonssikkerhet. Dokumentene skal forankres på riktig nivå i organisasjonen avhengig av innhold og målgruppe.

3.2.2 Arbeidsprosessene relatert til styringssystemet for informasjonssikkerhet

Forvaltning av styringssystemet er en av Sikkerhetsstabens viktigste oppgaver, da det danner grunnlaget for sikkerhetsarbeid som gjøres i Sikkerhetsstaben og ellers i etaten. Styringssystemet setter føringer og krav til linjen, den enkelte ansatte samt leverandører og avtalepartnere. Det består av flere dokumenter, hvor noen krav er detaljerte, mens andre er mer overordnet. Kravene ansvarliggjør den enkelte ansatte på sikkerhetsområdet og brukes ofte som oppslagsverk, det er derfor viktig at styringssystemet er oppdatert og bidrar til å sikre etatens informasjon, ansatte og omdømme. For å holde styringssystemet oppdatert i henhold til det generelle trusselbildet er Sikkerhetsstaben avhengig av input fra relevante kilder. Blant annet benyttes gjeldende lover og forskrifter, sikkerhetsstandarder som beskriver beste praksis på området og trusselvurderinger fra sentrale internasjonale og nasjonale aktører.



Figur 11: Overordnet prosess for arbeid med styringssystemet for informasjonssikkerhet

Som kilder til SFI benyttes blant annet trusselvurderinger fra PST, NSM og NorSiS, samt nasjonale strategier og føringer gitt fra regjeringen. I tillegg til dette er også ISO-standarder i 27000-serien lagt til grunn for beste praksis, som sikrer at etaten følger internasjonale bransjestandarder på sikkerhetsområdet. Dette, sammen med lover og forskrifter, blir brukt som grunnlag for Skatteetatens overordnede policy for informasjonssikkerhet. Det er et overordnet dokument som beskriver etatens akseptable risikonivå og risikoappetitt. Deretter er det policyer og standarder som bygger opp under den overordnede policyen, som setter konkrete krav til ansatte, linjer og prosjekter slik at sikkerheten blir ivaretatt over hele organisasjonen. De kravene blir også brukt i det daglige arbeidet til Sikkerhetsstaben når det blir gjennomført risikovurderinger, revisjoner, sikkerhetstester og andre aktiviteter relatert til sjekk av etterlevelse. Frekvensen av endringer på de ulike nivåene er avhengig av kildene som benyttes som input. Dersom det kommer en ny trusselvurdering, lov, forskrift eller sikkerhetsstandard som fører til endringer i risikobildet til Skatteetaten, endres også Skatteetatens overordnede policy for informasjonssikkerhet og eventuelle dokumenter på nivåene under. Selv om figuren over, som viser prosessen for arbeid med SFI, kan se lineær ut, skal dokumentene i SFI vurderes oppdatert minst en gang i året.

3.2.2.1 Modell 1 og modell 2

Regler og prosedyrer lages ofte etter to forskjellige modeller, såkalt modell 1 og modell 2, og er på sitt beste samlende og funksjonelle, mens på det verste kan de skape kaos og meningsløshet. Meget kort handler modell 1, ofte kalt eksternalisert kunnskap, om at de som lager reglene ikke er de som utfører dem i praksis. Dette fører ofte til at reglene blir altfor teoretiske og virkelighetsfjerne og er således rasjonalistiske. Modellen behandler regler, gjerne med beskrivelse av hvordan man skal handle, og utføre en handling på – "the one best way". Etter denne modellen så bør regler følges slavisk og ikke brytes, og dersom de brytes, er det tegn på motstand og uønsket atferd. Reglene skal følges selv om praktikeren ikke opplever dem som tilpasset for den aktuelle situasjonen, og blir således en tvangstrøye for handling som ikke tar hensyn til skiftende praktiske forhold, (Heldal & Dehlin, 2017).

Modell 2 er har en motsatt og fleksibel tilnærming til forskjellige situasjoner. Denne modellen representerer et regelsett som skal være til veiledning og hjelp for operatører, og er dermed underordnet praktikeren og ikke omvendt. Den er oppstått som et handlingsmønster, som gjerne har sprunget ut fra tidligere erfaringer. Det ligger derfor i kortene at av og til vil det være nødvendig å bryte eller fravike regelen. Reglene kan ikke dekke alle mulige utfall, spesielt ikke i en dynamisk og fleksibel praktisk virkelighet. Denne modellen har derfor et sett med regler som ikke er en oppskrift som skal følges blindt, men et hjelpemiddel som alltid må tilpasses, justeres og oversettes til praktisk handling. Ekspertene og regelskriverne er i denne sammenhengen operatørene, det vil si de som utfører handlingene og ikke lederne eller forskere, (Heldal & Dehlin, 2017).

3.2.3 Trusselbildet til Skatteetatens IT-systemer

Det har gått lang tid siden siste sikkerhetshendelse med alvorlig konsekvens i Skatteetaten, og man har begynt å få større risikoappetitt. Til daglig har vi en risikobasert tilnærming hvor vi prøver å ta en kalkulert risiko basert på økonomisk grense, ressursbruk og effektivitet, samtidig som ansatte skal få utført jobbene sine. Dette er noe som tilsvarer ALARP prinsippet, *as low as reasonably practicable*, (Kongsvik, Albrechtsen, Antonsen, Herrera, Hovden & Schiefloe, 2018). Ethvert trusselbilde endrer seg med tiden, spesielt dersom man endrer på arbeidsmetoder og digitaliserer. På den ene siden er vi ikke avhengig av å ha stor risikoappetitt fordi vi ikke kan tape kundemasse, men vi er likevel pålagt å modernisere og digitalisere gjennom nasjonale og etatens egne strategimål samtidig som innovasjonstakten i etaten er generell høy.

Dette har åpnet for en del nye risikoer vi tradisjonelt sett ikke har hatt. Et eksempel på det er outsourcing og lange leverandørkjeder, noe som gir økt risiko men som samtidig kan være kostnadsreduserende og innovativt. Der tjenesteleverandører tidligere hadde tilnærmet full kontroll over verdikjeden, er bildet i dag langt mer fragmentert, (NOU 2015:13, s.43). Det vil føre til at underleverandør som har utkontraktert sentrale deler av virksomheten til et annet land, vil kunne arve sårbarheter fra de tilsvarende sektorene i vedkommende land, (NOU 2015:13, s.15). Eksempler på hvordan det kan gå fryktelig galt med lange leverandørkjeder, kan man se til Helse Sør-Øst hendelsen i 2017 hvor underleverandører satt i Asia og Øst-Europa med tilgang på sensitive pasientdata til 2,8 millioner av norske borgere, (Tomter, Remen & Helljesen, 2018). Et år før dette satt det også underleverandører i India med sikkerhetskritiske oppgaver for Statoil, (Tomter, Remen & Wernersen, 2017). I begge tilfellene har de gjort endringer i outsourcingen av disse operasjonene, slik at disse utføres i Norge med mindre risiko.

Under følger en grovanalyse jeg har utført av trusselbildet til Skatteetatens IT-systemer, som er relevant for denne oppgaven. Ettersom et trusselbilde kan bestå av utilsiktede og tilsiktede hendelser, har jeg her fokusert på tilsiktede hendelser da det er mest relevant i denne oppgaven.

Trusselaktør	Beskrivelse	Årsak/motivasjon	Enkel konsekvens/ kapasitet
Utro tjener	Utro tjener som utnytter sin posisjon og kunnskap for å ødelegge Skatteetatens omdømme eller systemer. De kan også utnytte sin posisjon for sin egen vinning.	Kan være motivert av ønske om "hevn" ved en tvist med Skatteetaten, økonomisk gevinst som motivasjon eller en utro tjener som har politiske mål. Det kan også være at vedkommende er betalt eller presset til å utføre handlinger som rammer Skatteetaten.	Disse har ofte stor kompetanse om systemene og kan ha vide tilganger som kan gjøre stor skade med høy konsekvens.

Ekstern hacker	Person som har onde hensikter og ønsker å utnytte eventuelle sårbarheter i Skatteetatens eksternt eksponerte tjenester.	Disse har som regel en klar motivasjon og mål. Det kan for eksempel være et ønske om berømmelse eller økonomisk vinning for seg selv.	Kan ha relativ stor kompetanse og mange verktøy. De vil også kunne gjøre skade med høy konsekvens dersom de lykkes.
Organisert kriminell gruppe	Gruppe av kriminelle eksterne hackere som fremstår organiserte og som har onde hensikter og utnytter sårbarheter i Skatteetatens eksternt eksponerte tjenester, samt interne tjenester.	Disse har som regel klar motivasjon og mål. Det kan for eksempel være et ønske om berømmelse eller betalingsoppdrag for seg selv eller andre.	Vil ha mye kompetanse og mange verktøy, inkludert fysisk inntrengning via sosial manipulasjon. De vil også kunne gjøre skade med veldig høy konsekvens dersom de lykkes.
Statlige etterretnings tjenester	Velorganisert gruppe ansatt på oppdrag for statlige etterretningstjenester. De har onde hensikter og utnytter sårbarheter i Skatteetatens eksternt eksponerte tjenester, samt interne tjenester.	I følge PST sin trusselvurdering 2019 er russisk og kinesisk etterretning mest aktive med forsøk på innhenting av informasjon, drive påvirkning og utføre cyberoperasjoner mot Norge og norske interesser. De vil også ha klare mål og motivasjon.	Statlig etterretning har stor kapasitet til rådighet. Det de velger ut som prioriterte operasjoner vil de ha tilstrekkelig kapasitet til å gjennomføre, alt fra hacking, sabotasje til fysisk inntrengning via sosial manipulasjon. Konsekvensene kan være kritiske for etaten.

Tabell 1: Viser trusselbildet til Skatteetatens IT-systemer

3.3 Tidligere forskning

Etter brede søk på tidligere forskning gjort på områdene innovasjon og informasjonssikkerhet sammen, fant jeg lite relevant i norsk sammenheng. I internasjonalt sammenheng var det mer dekkende, men likevel mindre enn på andre temaer. Det har derfor vært en utfordring å finne noen gode studier og forskningsbasert dokumentasjon der innovasjon og informasjonssikkerhet blir studert sammen. Hva dette skyldes er det ikke noe enkelt svar på, men en studie som ble gjort for 15 år siden viste at antall forskningsbaserte studier på informasjonssikkerhetsområdet var lavere enn på andre områder. De mente at dette kan skyldes at det er vanskelig å gjennomføre en studie på sikkerhetstemaet fordi

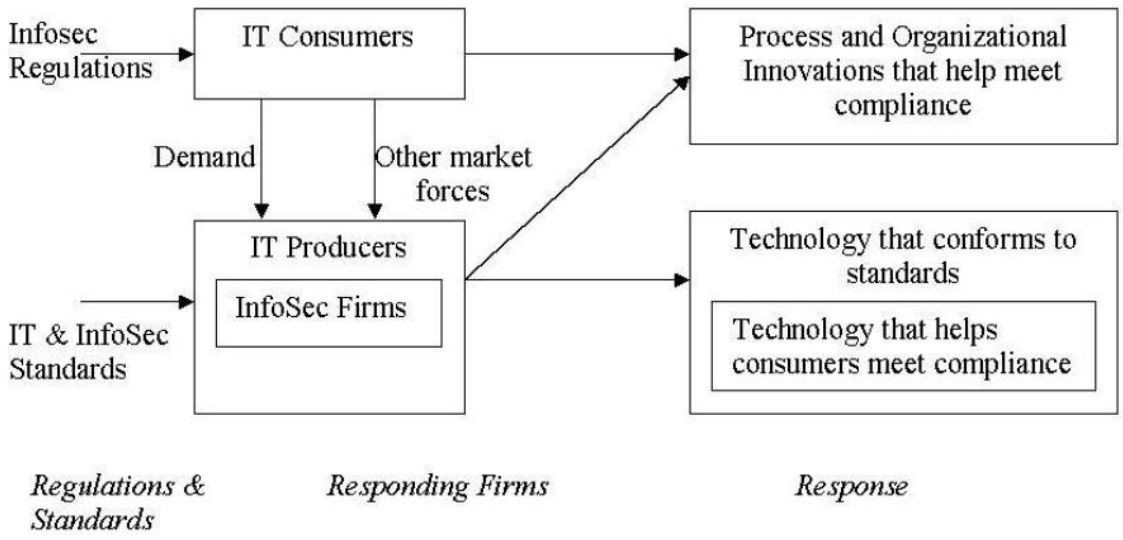
man blir sett på som "en fra utsiden". Sikkerhet er et sensitivt tema og organisasjoner vil ikke dele informasjon om dette temaet med utenforstående uten å ha fått forsikringer om at det som deles ikke vil kunne utgjøre en risiko for dem, (Kotulic & Clark, 2004).

3.3.1 Innovasjon og informasjonssikkerhet

Det nærmeste og beste eksemplet jeg kom over var en artikkel fra 2007 hvor forskere så på hvilken innflytelse de regulatoriske endringene hadde på innovasjonen på området informasjonssikkerhet, (Khansa & Liginla, 2007). De hevdet at det er tre hovedargumenter for å forsvare innovasjonskostnaden til firmaer som driver med informasjonssikkerhet;

1. Organisasjoner har blitt mer sårbare for nye avanserte metoder av ondsinnede angrep hvor motivasjonen er økonomisk vinning
2. Informasjonsteknologien har opplevd mye innovasjon på områdene telekommunikasjon og datamaskinarkitektur
3. Regulatoriske endringer og krav har tvunget organisasjoner til å endre strategi og få på plass sikkerhetsmekanismer og kontroll over IT-systemene og prosessene.

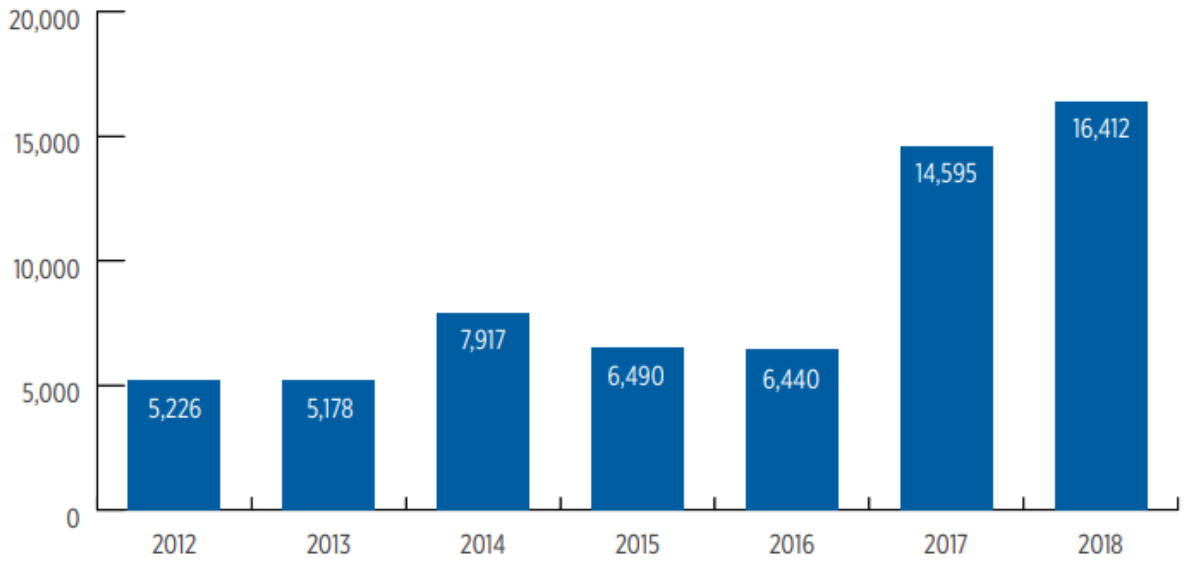
Videre har de dykket ned i punkt 3 og påpeker at regulatoriske endringer påvirker innovasjonen til teknologi, prosesser og organisasjoner, selv om det ikke er hovedintensjonen til endringen. Hensikten med de regulatoriske endringene er å sikre organisasjoner, samt samfunnet, slik at konfidensialitet, integritet og tilgjengelighet av informasjon er ivaretatt. De argumenterer for at regulatoriske endringer fører til at det må settes en annen standard som gjør at virksomheter som driver med informasjonssikkerhet innoverer og finner opp nye produkter som vil føre til at deres kunder kjøper disse produktene og tjenestene for å være compliant. Samtidig som studien viser at innovasjon i informasjonssikkerhet er drevet av etterspørsel, må en organisasjon ha støtte fra toppledelsen for at innovasjonen skal bli en suksess.



Figur 12: Viser konseptuell modell av regulatoriske endringer som påvirker innovasjonen, (Khansa & Liginla, 2007)

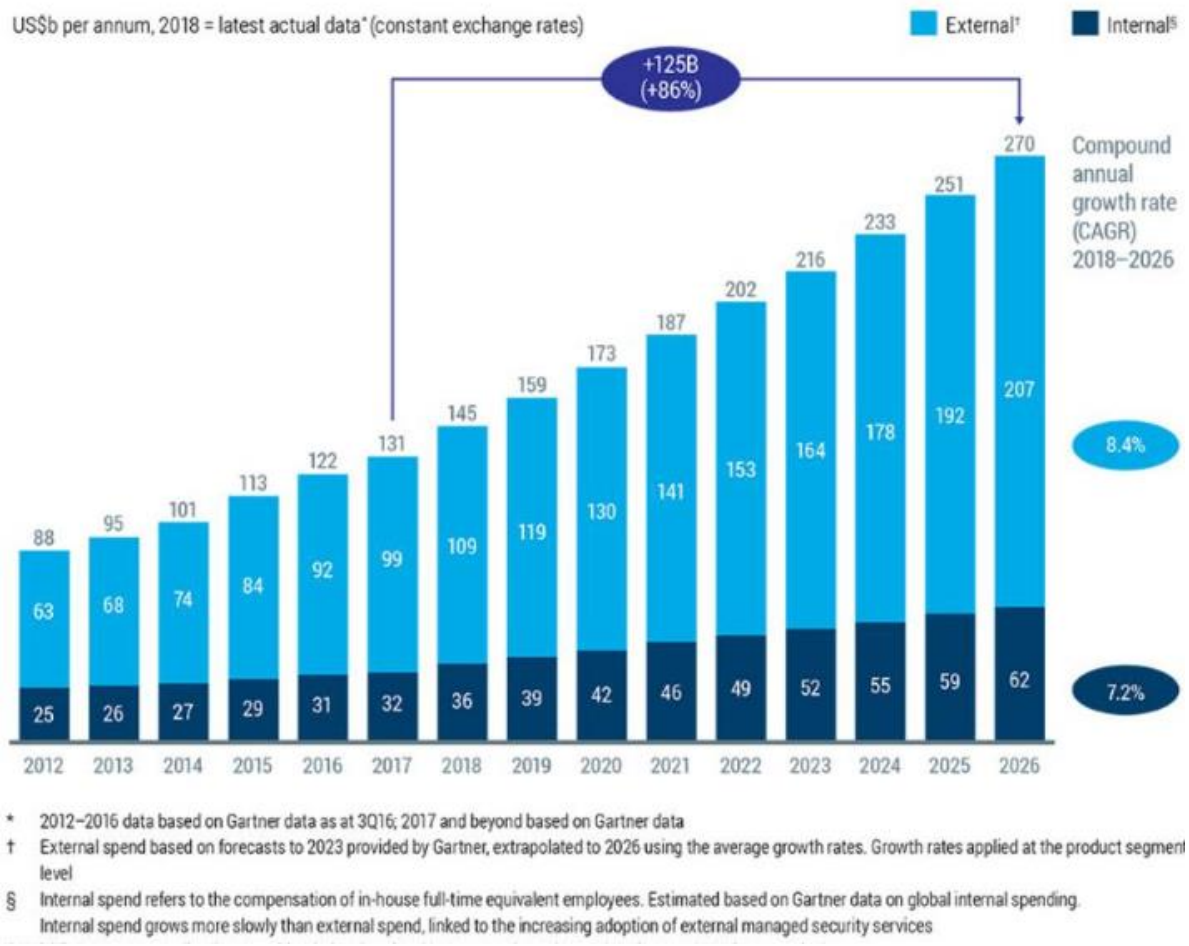
På en annen side ble det i 2017 gjennomført en studie som så på sårbarheter og motstandsdyktighet i Norges olje- og gassinfrastruktur. Den påpekte at det tok over 10 år før regulatoriske endringer krevde identifisering og beskyttelse av kritisk infrastruktur, noe som er lenge sammenlignet med farten på teknologiutviklingen. Det ble tatt utgangspunkt i den nasjonale strategien for digital sikkerhet fra 2012 der det ble påpekt at det var begrenset fokus på motstandsdyktighet, samtidig som det var fokus på reaktive handlinger framfor proaktive, (Johnsen, 2017).

Økning i antall sårbarheter fører også til innovasjon. For å imøtekomme økningen av sårbarhetene prøver produsentene å fylle markedet med nye innovative og mer effektive produkter. Antall nye sikkerhetsprodukter utgitt av Microsoft økte i takt med rapporterte sårbarheter i Microsoft sine produkter, (James, Khansa, Cook, Bruyaka & Keeling, 2013). Det er selvsagt en fordel at det finnes verktøy for å sikre systemer og tette sårbarheter, men de må komme raskt nok og være effektive. Innovasjon på IT-systemer, skiller seg ikke nevneverdig ut fra innovasjon generelt. Det må eksistere et behov, strategi, kultur, støtte fra ledelsen, kompetanse, øremerkede midler, rom for fleksibilitet og kreativitet på teknologisiden for å lykkes med innovasjon, (Johannessen, 2007).



Figur 13: Nye registrerte og bekreftede sårbarheter etter år, (Skybox Research Lab, 2019)

En studie som så på potensialet til kunnskapsbasert innovasjon innenfor forskjellige IT områder fant også ut at det var høyest innovasjonstakt og intensivitet på områdene multimedia og IT-sikkerhet. Disse to områdene hadde også størst påvirkning på kunnskapsbasert innovasjon, (Ružičić & Micic, 2013). Det er derfor ingen tvil om at IT-sikkerhet også er avhengig av innovasjon og at det skjer endringer på det området. Ettersom virksomheter er avhengig av å fornye for å henge med trusselbildet, overholde lover og ikke minst for å være konkurransedyktige og compliant, er det forventet en global økning i forbruk på IT-sikkerhet i årene frem mot 2026.



Figur 14: Viser globalt forbruk på IT-sikkerhet og estimering fram til år 2026, (Colombus, 2020)

3.3.2 Styringssystem og ansatte

Når det kommer til forskning som omfatter hvorvidt informasjonssikkerhet og sikkerhetsregler hemmer innovasjonsarbeidet, fant jeg ikke noe konkret forskning på akkurat det. Likevel var det en del interessante studier som tok for seg samspillet mellom sikkerhetsprosedyrer og ansatte. En studie som forsket på motivasjonsfaktorer blant ansatte i en organisasjon i Finland som hadde ambisjon om å bli compliant med organisasjonens sikkerhetsregler og prosedyrer, hadde interessante funn. Det ble der påpekt at halvparten av alle sikkerhetsbrudd skyldes at ansatte direkte eller indirekte ikke fulgte organisasjonens policyer og regler, noe som presiserer viktigheten av et godt styringssystem og ansvarsbevisste ansatte, (Vance, Siponen & Pahnila, 2012). Har man ikke etablert et styringssystem for informasjonssikkerhet som er mulig å etterleve og som ikke er tilpasset brukerne, vil ansatte i større grad omgå sikkerhetsmekanismene eller nekte å etterleve sikkerhetsreglene og prosedyrene, (Gyõry, Cleven, Uebernickel & Brenner, 2012). Denne samme studien viste til lignende andre studier som påviste at hver tredje ansatt omgår sikkerhetsmekanismer for å få gjort jobben sin. Begge de to ovennevnte studiene påpekte at dette kunne skyldes mangelen på holdningsskapende arbeid i organisasjonen. En annen tredje studie viste at effektive regler og sikkerhetskontroller er

kritiske for å håndtere store IT-systemer. Uten sikkerhetsmekanismer på utstyret er det umulig å detektere, forhindre og håndtere sikkerhetshendelser. Der det er mennesker involvert viser det seg at brukerne av systemer omgår sikkerhetskontroller, ikke for å bevisst utgjøre en sikkerhetsrisiko, men for å få utført jobben sin effektivt, (Blythe, Koppel & Smith, 2013).

3.3.3 Motstandsdyktighet / Resilience

Tradisjonelt har man forsøkt å forstå sikkerhet gjennom å fokusere på inntrufne uønskede hendelser og konsekvensene av dem, for eksempel gjennom å granske dem i etterkant. Noe som kalles safety 1 i teorien. I de tilfellene vil man finne ut at sikkerheten ikke var tilstede da hendelsen inntraff. Hollnagel mener det er et paradoks at man forsøker å studere et fenomen når det ikke er tilstede. Han mener derfor at dersom sikkerhet skal forstås må de hendelsene der sikkerhet faktisk er tilstede granskes. Det vil være de situasjonene hvor man har tatt beslutninger og gjennomført arbeid som gjør at situasjonen ikke resulterer i uønskede hendelser, noe som kalles safety 2, (Hollnagel, 2014). I dette prinsippet vil man endre fokuset fra å unngå at noe går galt til å sikre at det går bra, gjennom for eksempel forsterking av de menneskelige, tekniske og organisatoriske ressursene. Han argumenterer med at dette er nødvendig for å ha en forebyggende tilnærming til sikkerhet, ettersom safety 1 vil fokusere på å lære av feil som allerede har truffet – en form for erfaringsbasert tilnærming. Disse prinsippene er viktig å ha med når vi ser på motstandsdyktighet i forbindelse med angrep på IT-systemer.

At en organisasjon skal være motstandsdyktig i enhver situasjon og samtidig til enhver tid kunne kjøre virksomhetskritiske prosesser, er en tøff oppgave. Dette er spesielt utfordrende i en digitalisert og tilkoblet verden som eksisterer i dag. Systemer som er tilkoblet internett vil alltid være eksponert for trusler, det kreves en konstant risikobasert tilnærming. Antall trusler og hvor sofistikerte de er, har økt jevnt de siste årene. Dette fører til at organisasjoner får utfordringer med å ivareta sikkerheten, samtidig som de ansatte krever mer fleksible og mobile arbeidsløsninger, (Borrett et al., 2013). Tidligere var angrep tilfeldige og relativt korte, mens dagens angrep er avanserte, ofte målrettet, langtidsplanlagt, persistente og vanskeligere å oppdage. Angriperne tar i bruk alt de har av verktøy og har ingen etiske eller moralske forpliktelser ovenfor andre parter samtidig som motivasjonen deres er høy, (Borrett et al., 2013). Under ser vi en grov inndeling av angrepsmetoder en trusselaktør kan benytte seg av.

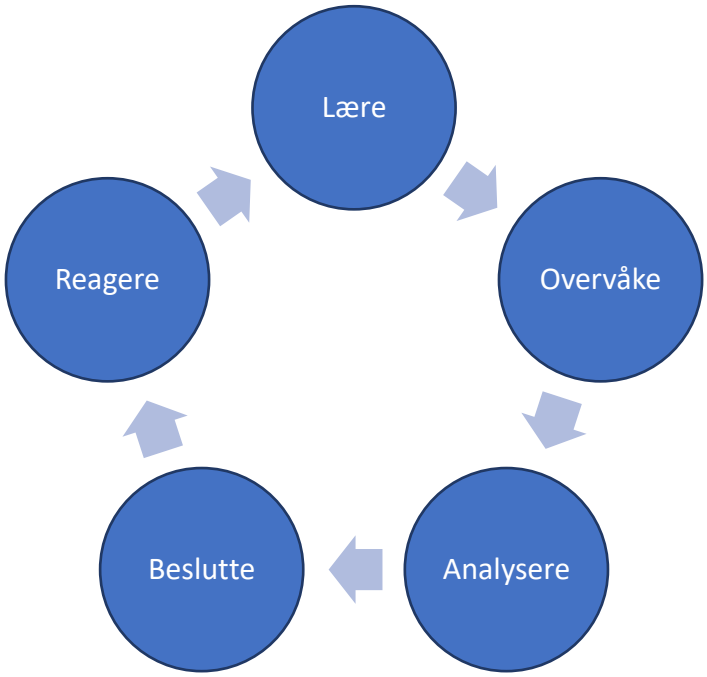
Angrepsmetode	Kort beskrivelse
Hacking	Innbrudd i en datamaskin eller nettverk med hensikt å ta over kontrollen. Teknikker inkluderer SQL injection, tjenestenekt, autentisering med standard påloggingsinformasjon eller stjålet påloggingsinformasjon
Ondsinnet programvare	Software laget for å infiltrere eller gjøre skade på en datamaskin eller system uten eiers kjennskap eller bevissthet; for eksempel keylogger, spyware, trojaner
Misbruk	Misbruk av en datamaskin eller system gjennom en brukers tilganger for ondsinnet aktivitet eller misbruk av systemtilganger.

Sosial manipulering	Manipulere en person til å utføre handlinger på vegne av angriperen med hensikt for å tilegne seg tilgang til en datamaskin, system eller nettverk; for eksempel phishing.
Fysisk	True eller angripe fysisk med hensikt å få tilgang til datamaskin, system eller nettverk; for eksempel kabelavlytting, sette opp falske nettverksstasjoner.

Tabell 2: Viser overordnede angrepsmetoder en trusselaktør tar i bruk, (Borrett et al., 2013 – oversatt av meg)

Jakten på slike angrep gjør jobben til de som arbeider med sikkerhet vanskeligere og kostnadene større. Mer data må analyseres, flere loggkilder må inkluderes og flere sensorer må etableres for å kunne skille normal trafikk og oppførsel fra ondsinnet.
Avanserte angrep er noe alle stater bekymrer seg for ettersom angrepet kan pågå årevis og konsekvensen kan være høy. I studien til Borrett, Carter og Wespi fra 2013, påpekes det at statlige aktører ser etter forsvarsmekanismer mot denne type angrep, som ofte er finansiert av andre stater. For organisasjoner som skal forsvare seg mot slike angrep er ikke spørsmålet nødvendigvis hvordan de skal forsvare seg om de blir angrepet, men hva man skal unngå når angrepet kommer; brudd på nettverkskommunikasjonen, informasjonslekkasje, etc. og hvordan man skal reagere på et slikt angrep.

En organisasjon må jobbe med holdningsskapende arbeid rettet mot ansatte, det er en av de største mangelvarene på god informasjonssikkerhet og god sikkerhetskultur i organisasjonen er et av de viktigste virkemidlene for å oppnå god informasjonssikkerhet, (Borrett et al., 2013). Det er derfor viktig å ha rutinene på plass og ha tenkt og øvd på situasjoner som kan oppstå. Angrep går fort og det er viktig å automatisere og være tilpasningsdyktig i forsvaret, ettersom angrepene er dynamiske og sjelden helt like. Borrett, Carter og Wespi fremhever i sin studie viktige elementer en organisasjon må ha på plass for å kunne være motstandsdyktige mot dynamiske angrep og et trusselbilde i stadig endring.



Figur 15: Hovedfasene i livssyklusen til en IT-sikkerhetshendelse, (Borrett et al., 2013 – grafisk fremstilt av meg)

Lære; forstå IT landskapet, inkludert nettverkstopologien og de potensielle risikoene så organisasjonen skjønner hvilke sårbarheter som finnes i organisasjonens infrastruktur.

Overvåke; logg og sett hendelsene i et system og tidstabell. Ha med så mange kilder som mulig for å få et real-time bilde. Detekter at en hendelse har skjedd eller at et program eller informasjon har blitt manipulert.

Analysere; Forstå en hendelse og hva som har skjedd. Undersøk skadeomfanget og potensialet til et angrep og visualiser det i analysen.

Beslutte; Finn ut hvordan man skal reagere på denne hendelsen, balansert og opp mot forretningsmessige konsekvenser.

Reagere; Handling. Rydd opp og reparer skaden. Finn ut hvorfor angrepet var suksessfullt. Implementer tiltak slik at kjente sårbarheter ikke blir utnyttet.

Lære; Livssyklusen begynner igjen. Ved å bruke analysen og beslutningene som ble tatt, forbedre risikostyringen. Informer andre relevante om angrepet og hvilke tiltak som ble gjennomført.

I hver av fasene må man vurdere tre viktige aspekter og hvilken påvirkning de vil ha på hverandre; teknologi, tjenestespekteret til organisasjonen og risiko, (Borrett et al., 2013). Under ethvert angrep er det veldig fristende å slå av alle datamaskiner eller dra dem ut av nettet, men det vil samtidig ta ned alle andre tjenestene til organisasjonen, det vil kunne skape medieoppslag og det vil kanskje utgjøre en enda større risiko for organisasjonen. Samtidig vil en slik handling føre til at det ikke er mulig å gå videre i livssyklusen til en sikkerhetshendelse, som gjør at man ikke kan analysere og lære av hendelsen og vil dermed fortsatt være sårbar. Det er derfor viktig å ha gjennomtenkt reaksjonene og handlingene før de faktisk tre i kraft.

4 Forskningsdesign og metode

For å få frem gode argumenter for drøfting fra en undersøkelse er man avhengig av å ha forskningsdesign som er godt gjennomtenkt. Det vil gjøre at vi klarer å tolke data som samles inn og at vi systematisk kan presentere det som er observert under datainnsamlingen. Samtidig er det viktig å ivareta objektiviteten i undersøkelsen, slik at det er mulig å gjennomføre en kritisk vurdering av resultatene. Påliteligheten av en undersøkelse er minst like viktig og vil sammen med det ovennevnte forhåpentligvis danne grunnlaget for en analyse som kan bidra til økt kunnskap. Jeg vil i dette kapittelet derfor gå inn på hvilken metode og strategi jeg har valgt for oppgaven, i håp om å besvare problemstillingen så godt som mulig. I dette kapittelet begrunner jeg mine metodevalg og fremgangsmåter, før jeg i neste kapittel gir en grov oversikt over resultatene.

Hensikten med denne studien og de undersøkelsene gjort i den er todelt; jeg ønsker å studere fenomenene innovasjon og informasjonssikkerhet opp mot hverandre ved å finne ut om sikkerhetsmekanismer er hemmende for innovasjonsarbeidet i etaten. På veien dit ønsker jeg også å høste anbefalinger til bedre og mer innovativt sikkerhetsarbeid i etaten, som kan bidra til å øke Skatteetatens motstandsdyktighet.

Først vil jeg ha en eksplorerende tilnærming, der jeg ser på sammenhenger mellom fenomenene informasjonssikkerhet og innovasjon. Utforskningen på disse områdene er noe spesielt da det eksisterende teorigrunnlag på samspillet mellom disse to fenomenene er tynnere enn på andre områder. Målet vil derfor være å gi økt forståelse og innsikt av samspillet mellom disse to. Basert på funnene vil jeg mot slutten ha en normativ tilnærming i håp om at dette er noe som kan brukes til videre arbeid.

Som nevnt tidligere er jeg ansatt i Sikkerhetsstaben og har dermed med meg en del erfaringer og forkunnskaper når det kommer til prosessene brukt i arbeid med informasjonssikkerhet, samt utfordringene og forbedringspotensialet på det området. Jeg ønsket ikke å bekrefte eller avkrefte en eller flere hypoteser i denne analysen, og valget falt på at jeg primært skulle gjennomføre en kvalitativ studie basert på dybdeintervjuer. Selv om jeg mistenkte at informasjonssikkerhet og innovasjon kunne være to motpoler, ønsket jeg ikke å utforske akkurat det, men ville heller utforske samspillet mellom de to og forhåpentligvis finne måter der de eventuelt drar i samme retning. Jeg var overbevist og er fortsatt overbevist om at sikkerhet, som mange forbinder med kontroll og begrensninger, også er avhengig av innovasjon. Ettersom det også er mulighet for å kombinere kvantitativ og kvalitativ forskningsmetode, valgte jeg underveis å berike denne studien med en kvantitativ spørreundersøkelse.

4.1 Datainnsamling

4.1.1 Dybdeintervju

For å finne ut om sikkerhetsmekanismer hemmer innovasjonsarbeidet har jeg benyttet meg av kvalitativ forskningsmetode basert på dybdeintervjuer. Ved å intervjue ansatte i avdelingene Forretningsutvikling og Planleggingsstaben, har jeg hatt fokus på å studere meningene, holdningene og erfaringene, samt hva slags arbeid og prosesser de har. Disse avdelingene ble valgt da de arbeider med innovasjon på sine respektive områder og har en viktig rolle i innovasjonsarbeidet til hele etaten og dets IT portefølje. Selv har jeg liten kjennskap til deres metoder og arbeid, og ønsket spesielt å finne mer ut av deres relasjon til informasjonssikkerhet, sikkerhetsmekanismer og samarbeid med Sikkerhetsstaben under arbeidsprosessene deres. Intervjuene mine skulle i utgangspunktet ikke samle inn personopplysninger, men for å være på den sikre siden kontaktet jeg NSD (Norsk Senter for Forskningsdata) og sendte inn en melding om datainnsamlingen. 15 desember 2019, fire uker etter at søknaden var sendt, fikk jeg tillatelse fra NSD og startet planleggingen av intervjuene.

For å få forankring og ressurser til intervjuene kontaktet jeg avdelingsdirektørene for Forretningsutvikling og Planleggingsstaben på e-post. Jeg forklarte litt om oppgaven og hensikten med den og ba i utgangspunktet om å få tildelt 5 ressurser fra hver avdeling til disposisjon som jeg kunne intervjue. Grunnen til at jeg valgte 10 personer totalt er på bakgrunn av at det bør være mellom 8-12 dybdeintervjuer i en masteroppgave basert på kvalitativ forskningsmetode, (Tjora, 2017). Jeg sendte skriftlig samtykkeerklæring til hvert intervjuobjekt på e-post før intervjuet og ba om skriftlig bekreftelse på at de har mottatt, lest og forstått samtykkeerklæringen, i tillegg til at de samtykker til deltakelse.

Jeg startet mitt første intervju i slutten av januar 2020 og hadde estimert å gjennomføre 1-2 intervjuer i uken frem til påskeuken som startet 3 april 2020. Alt gikk etter planen helt frem til 12 mars 2020 da koronaviruset spredte seg i Norge, og det ble innført smittereduserende tiltak i samfunnet. Skatteetaten besluttet at samtlige ansatte skulle ha hjemmekontor og oppgaver skulle omprioriteres, noe som førte til at jeg ikke fikk gjennomført resterende intervjuer. Gitt den spesielle situasjonen fikk jeg likevel gjennomført 8 intervjuer, hvorav 5 med informanter fra Forretningsutvikling og 3 fra Planleggingsstab, som er akkurat nok etter Tjoras anbefaling.

Intervjuene ble gjennomført i et lydisolert møterom i lokalene til Skatteetaten, dette ble gjort for å skape et trygt og avslappende miljø for intervjuobjektene, uten støy, samtidig som det var det mest praktiske da alle informantene var geografisk plassert på samme sted som meg. Dette er også noe Tjora anbefaler i sin bok, ettersom det vil øke sjansene for at intervjuobjektene føler seg mer komfortable og åpne på temaet og har dermed stor betydning i intervjusituasjoner.

Dybdeintervju er avhengig av en god dialog mellom forsker og informant for å få fram refleksjoner, det er noe jeg ønsket å ha fokus på, og valgte derfor å gjennomføre lydopptak. Da kunne jeg aktivt lytte og følge med på hva som ble sagt og stille relevante oppfølgingsspørsmål slik at dialogen ble god. Samtidig kunne jeg trekke frem eksempler fra konkrete problemstillinger de daglig møter, i håp om å motivere informanten til å åpne seg enda mer, (Tjora, 2017). I tillegg ville oppfølgingsspørsmål bidra til bedre diskusjon av

konkrete problemstillinger slik at vi fikk en dypere og mindre generell diskusjon. Dette hjalp meg også under selve databehandlingen og analysen av intervjuene, for da kunne jeg gå tilbake til det som ble sagt. Alle intervjuobjektene fikk beskjed om at det ville bli gjort lydopptak, både skriftlig i e-post innkallingen til intervjuet og muntlig før selve intervjuet startet. De ble også opplyst om at de kunne velge å gjennomføre intervjuet uten lydopptak, samt trekke seg fra intervjuet når som helst. Jeg var også tydelig på at lydopptakene og svarene deres likevel kunne bli brukt i senere forskning, noe som også var skrevet i samtykkeerklæringen. Ingen av de 8 intervjuobjektene valgte bort lydopptakeren eller trakk seg fra intervjuet.

På bakgrunn av et spisset og uproblematisk tema og min rolle i organisasjonen, som jeg antok ville etablere tillit raskt, var selve dybdeintervjuet satt opp til å vare 45 minutter. Mine 32 forhåndsdefinerte og i hovedsak åpne spørsmål, var seksjonert opp etter Tjora sin anbefaling; 7 på oppvarming, 21 på hoveddel og 4 som avslutning. I tillegg til dette fulgte jeg opp med oppfølgingsspørsmål for å komme til roten av hva informantene mente på enkelte temaer. Intervjuguiden i sin helhet finnes vedlagt i kapittel 9.

For å ivareta kollegiale og etiske hensyn valgte jeg, selv om det ikke var personopplysninger involvert eller et problematisk tema, å sende det bearbeidede datagrunnlaget til intervjuobjektene. Dette gjorde jeg for at de skulle føle seg trygge på at ingenting ble tatt ut av kontekst eller identifiserbart på noen måte. Samtidig ble de også tilbudt å lese gjennom eventuelle sitater som jeg hadde planlagt å bruke for å øke troverdigheten av forskningen.

4.1.2 Spørreskjema

Ettersom jeg også har med en del bagasje på området informasjonssikkerhet, har jeg valgt å benytte meg av digital anonym spørreskjemaundersøkelse for å kartlegge motstandsdyktigheten til Skatteetatens trusselaktører. Dette er også noe Tjora anbefaler i sin bok dersom forskeren har mye kunnskap om et fenomen, for å ivareta objektiviteten og for at forkunnskapen skulle bli en ressurs fremfor støy, (Tjora, 2017). Samtidig ønsket jeg å finne ut hvor mye fokus det er på innovasjon i metodene, verktøyene og prosessene til Skatteetatens IRT, et team sammensatt av ni personer som daglig arbeider med å detektere, oppdage og håndtere trusler mot IT-systemene til Skatteetaten. Jeg lagde derfor 21 spørsmål i verktøyet ConfirmIT som jeg sendte link til på e-post til alle i Skatteetatens IRT. De ulike spørsmålene hadde også forskjellige svaralternativer i form av graderinger, dette ble brukt for å få fram eventuelle variasjoner de enkelte intervjuobjektene skulle ha. For å få flest mulig svar, forankret jeg først undersøkelsen hos lederen for IRT med informasjon om denne oppgaven. Deretter sendte jeg først ut en e-post med samtykkeerklæring og ba om skriftlig bekreftelse på at den er mottatt, lest og forstått, i tillegg til at mottaker bekrefter samtykke til deltakelse. Til slutt sendte jeg ut en lenke til undersøkelsen fra min e-post konto på arbeidsplassen til hver enkelt informant.

Når alle hadde svart ble svarene samlet inn av ConfirmIT som autogenererte statistikk på hvert av spørsmålene som ble stilt. Jeg har ikke endret dem i etterkant og presenterer dem i denne oppgaven slik som den totale besvarelsen er på de forskjellige spørsmålene.

Den eneste endringen er at jeg har erstattet noen svar som potensielt kan utgjøre en risiko for Skatteetaten med N/A, noe man kan se i kapittel 9 der alle spørsmålene er vedlagt.

Dette har jeg gjort da jeg dessverre ikke kan gjengi alle detaljene fra besvarelsene i en uklausulert oppgave. Innenfor informasjonssikkerhetsfeltet kan informasjon om IRT være nyttig for en angriper, og selv om det er få personvernbekymringer i oppgaven min, er det største skadepotensialet at jeg kan avsløre informasjon som skader IT-sikkerheten. Likevel kan jeg trekke noen konklusjoner og samtidig ivareta sikkerheten til Skatteetaten. Et eksempel på dette var der et av spørsmålene gikk på hvor godt rustet IRT er mot identifiserte trusselaktører. Svarene derfra vil potensielt kunne gi en indikasjon på hvor sårbare Skatteetaten er ovenfor disse. Jeg har også gjennomført en kvalitetssjekk med en kollega som har sett på disse opplysningene, for å avdekke eventuelle utsagn som kan identifisere potensielle sårbarheter jeg trekker ut fra spørreundersøkelsen.

4.2 Utvalg av kandidater

Avdelingene for både dybdeintervjuene og spørreundersøkelsen ble valgt ut på bakgrunn av deres tilknytning til henholdsvis innovasjon og informasjonssikkerhet i Skatteetaten. Hvordan informanter blir valgt ut og hva slags relasjoner det er mellom forsker og informanter, kan ha betydning for påliteligheten, (Tjora, 2017). Dette var også en av hovedgrunnene til at jeg valgte å gå via avdelingsleder, for da kunne jeg få et tilfeldig utvalg av informanter til disposisjon. Jeg var også klar over at min posisjon kunne farge svarene ettersom jeg er ansatt i Sikkerhetsstaben. I et forsøk på å unngå dette påpekte jeg tidlig min uavhengighet, ved å forklare at dette var til læring for avdelingene våre, etaten og oppgaven, samtidig som opplysningene ville være anonyme. Dette opplyste jeg om i den første e-posten som gikk til avdelingslederne og det var dette jeg innledet alle intervjuene med.

4.3 Pålitelighet, validitet og overførbarhet

Ved å intervjue to forskjellige avdelinger på to forskjellige forretningsområder, der begge arbeider med innovasjon, mener jeg bidrar til å få frem forskjellige synspunkter og øker studiens troverdighet. Det at de samme spørsmålene ble stilt til begge avdelingene, støtter også opp under dette. I tillegg har jeg benyttet spørreskjema mot Skatteetatens IRT, altså to ulike metoder dog med noe ulikt fokus men som likevel utfyller hverandre, for å bidra til styrking av undersøkelsen min. Der dybdeintervjuene påpeker hvilke sikkerhetsmekanismer som hemmer innovasjonsarbeidet og hvordan sikkerhet kan bli mer innovative, forteller spørreskjemaundersøkelsen mer om trusselhåndteringen og hvordan metodene, verktøyene og prosessene holdes effektive og innovative. Hele fremgangsmåten og innsamlingen av data er forklart grundig i denne oppgaven, inkludert utfordringer underveis og svakheter i oppgaven, slik at også transparens er ivaretatt.

Gjennom å samle inn data direkte fra de som jobber med innovasjon og håndtering av angrep på IT-systemer, mener jeg at resultatene er pålitelige og gyldige. Ressursene ble også valgt ut av avdelingslederne, som gjør at intervjuobjektene vurderes som troverdige, samtidig som antall informanter i utgangspunktet var satt til å være høyere enn det antall intervjuer som faktisk ble gjennomført. Sist og ikke minst har jeg forsøkt å ivareta min

objektivitet gjennom flere gjennomførte tiltak i dybdeintervjuene, men også gjennom å bevisst velge anonyme spørreskjema mot IRT.

Når det gjelder overførbarhet av resultatene, så er det i teorien beskrevet at ikke alle kvalitative data vil egne seg for gjenbruk, (Tjora, 2017). Alle dataene i denne oppgaven vil heller ikke egne seg for gjenbruk, men likevel mener jeg at observasjonene, synspunktene og anbefalingene som kommer frem i denne oppgaven, vil egne seg for gjenbruk eller sekundæranalyse. Ettersom problemstillingene og utfordringene er ganske like på tvers av organisasjoner, spesielt i organisasjoner med samme størrelse og kompleksitet som Skatteetaten, mener jeg at innsikten, analysen og anbefalingene gjort i denne oppgaven også vil være mulig å overføre til andre sammenlignbare organisasjoner. Det gjelder spesielt for organisasjoner som, i likhet med Skatteetaten, baserer seg på standarder som ISO-27000 serien hva gjelder informasjonssikkerhet, men også ITIL[1] prosesser. Det at prosessene innenfor informasjonssikkerhet er standardiserte og ganske like, vil også øke sannsynligheten for at funnene, analysen og anbefalingene kan overføres til andre organisasjoner.

4.4 Analyseprosessen

Som Tjora beskriver så kan det være tungt å sette i gang med analyseprosessen, dette er også noe jeg erfarte ved dybdeintervjuene ettersom det var mye data å fordøye, noe som gjorde det litt uoversiktlig i begynnelsen, (Tjora, 2007). Men etter å ha fått en struktur på databearbeidelsen, gjennom inspirasjon av stegvis-deduktiv induktiv sin anbefaling om å gå fram og tilbake mellom datamaterialet og analytiske konsepter, overkom jeg den barrieren.

Redningen min ble at jeg opprettet et Excel ark der jeg la inn alle spørsmålene fra intervjuguiden som rader, samt unike informantnummer som kolonner. På en separat fil hadde jeg beskrevet hvem informant som hadde hvilket informantnummer, dette gjorde jeg for å ivareta anonymiteten til informantene dersom Excel arket skulle komme på avveie eller leses av noen andre. Deretter spilte jeg av intervju for intervju og skrev ned korte stikkord hver informant svarte på det enkelte spørsmålet. På den måten lagde jeg en grov oversikt før jeg skulle dykke ned i svarene på de enkelte spørsmålene, som gjorde det lettere for meg å se hvilke informanter som svarte hva. Ved å ha slike knagger som jeg kunne henge svarene og informantene på, var det lettere for meg å huske tilbake til hvem som sa hva og se sammenhengen mellom svarene til informantene.

Etter dette gikk jeg tilbake til teorien min og fant noen interessante temaer og viktige punkter som svarene hadde fellestrekk med. Eksempler på dette er safety 1 og safety 2 prinsippet, samt modell 1 og modell 2 tilnærmingene. Jeg kategoriserte deretter de forskjellige punktene fra teorien med farger i Excel arket, før jeg gikk tilbake til lydopptakene og prøvde å fange opp utsagn som kan knyttes opp mot temaene fra teorien. Hver gang jeg fanget opp at en informant hadde nevnt noe som kan knyttes opp og brukes i diskusjon opp mot et tema, ble utsagnet notert i Excel arket og gitt en fargekode tilhørende det temaet. Når jeg hadde gjort dette på alle lydopptakene og informantene, gikk jeg enda en gang på de mest interessante utsagnene og spolte frem og tilbake på lydfilen for å se etter flere sammenhenger. Slik gikk jeg frem og tilbake og knyttet dataene opp mot

[1] ITIL er et rammeverk for kvalitetssikring av leveranse, drift og støtte innen IT

konsepter, modeller og punkter fra teorien, som skulle besvare på problemstillingen min relatert til hvilke praktiske utfordringer det er med høy innovasjonstakt og eksisterende sikkerhetsmekanismer.

Når det gjelder datagrunnlaget fra spørreundersøkelsen som ble sendt ut via ConfirmIT, et digitalt verktøy Skatteetaten har avtale på, ble besvarelsene fra disse kvantitative dataene autogenerert for meg. Likevel måtte jeg tolke besvarelsene for å knytte det opp mot den delen av oppgavens problemstilling som omfatter trusselbildet til Skatteetaten. Jeg måtte også kamuflere noen av svarene, som beskrevet i kapittel 4.1.2, og generalisere dem slik at det likevel ga verdi for oppgaven. Svarene fra spørreundersøkelsen bygget også opp under en del utsagn jeg fant i dybdeintervjuene, noe som gjorde at disse to metodene utfylte hverandre. Eksempel på dette er der dybdeintervjuene påpekte at det må innoveres og effektiviseres på sikkerhetssiden, svarte spørreskjemaundersøkelsen på hvordan dette blir ivaretatt hos IRT.

4.5 Svakheter i undersøkelsen

I og med at intervjuene ble gjort på egen arbeidsplass og jeg har en stabsposisjon, er det en risiko for at dette kan ha påvirket svarene. Informasjon samlet inn her kunne jeg også brukt i mitt sikkerhetsarbeid for etaten, noe jeg var klar over. Men jeg har hele tiden hatt fokus på disiplin og bevissthet, slik at jeg ikke skulle bruke den innsamlede informasjonen med det formålet. Jeg har forsøkt å unngå dette med virkemidler beskrevet tidligere i dette kapittelet, gjennom blant annet å deklarere min uavhengighet tidlig og sende den bearbeidede dataanalysen til informantene, og fikk i liten grad tilgang til den type informasjon i denne undersøkelsen. Temaet for denne oppgaven er også for øvrig lite kontroversielt.

Når det gjelder annen lignende forskning og studier, så er det som jeg nevnte i teorikapittelet, relativt færre som har tatt for seg sammenhengen mellom informasjonssikkerhet og innovasjon sammenlignet med studier på andre områder. Dette er ikke en svakhet i denne undersøkelsen, men gjør det utfordrende å sammenligne resultatene fra denne undersøkelsen med annen fagfellevurdert forskning.

Som jeg nevnte i bakgrunnskapittelet så er innovasjonen ganske spredt i Skatteetaten og innovasjon finner derfor sted i alle divisjonene i etaten. Dette vil si at antallet informanter kunne helt sikkert vært høyere og mer spredt i organisasjonen. På grunn av tids- og kapasitetsbegrensninger har jeg forsøkt å intervjue de som har hovedansvaret for innovasjonen i etaten og jobber direkte med det, og har derfor ikke fått intervjuet alle som bidrar til innovering av etaten. Deres synspunkt og mening er minst like viktig som informantene i denne undersøkelsen, da de mest sannsynlig har kunnskap om innovasjon på sine respektive fagområder.

Selv om hovedintensjonen for å gå via avdelingsleder var å få forankring av intervjuene, tilfeldige ressurser og styrke pålitelighet til denne oppgaven, er det er også noen mulige svakheter ved dette. Det jeg oppdaget underveis i dette arbeidet var at avdelingslederne kan ha valgt ut de flinkeste medarbeiderne sine som også vil svare det som er mest gunstig for avdelingen deres. I tillegg så vil lederen vite hvem som har svart og bidratt til utfallet av oppgaven. Selv er jeg ikke bekymret for at dette har skjedd, men muligheten er tilstede.

Tolkning av svar som kom opp under intervjuene, som er et fagfelt i seg selv, har også vært en utfordring. Dette forsøkte jeg å kompensere med å stille oppfølgingsspørsmål og gjøre lydopptak av intervjuet, slik at jeg kunne fokusere på kroppsspråk, tonefall og selve svaret. Under analyseprosessen beskrevet i kapittel 4.4, kunne jeg kvalitetssikret mine observasjoner gjennom metoden jeg benyttet, men ettersom denne typen tolkning ikke er mitt fagfelt, er det en risiko for at jeg ikke fikk med alle detaljer som kom frem under intervjuene.

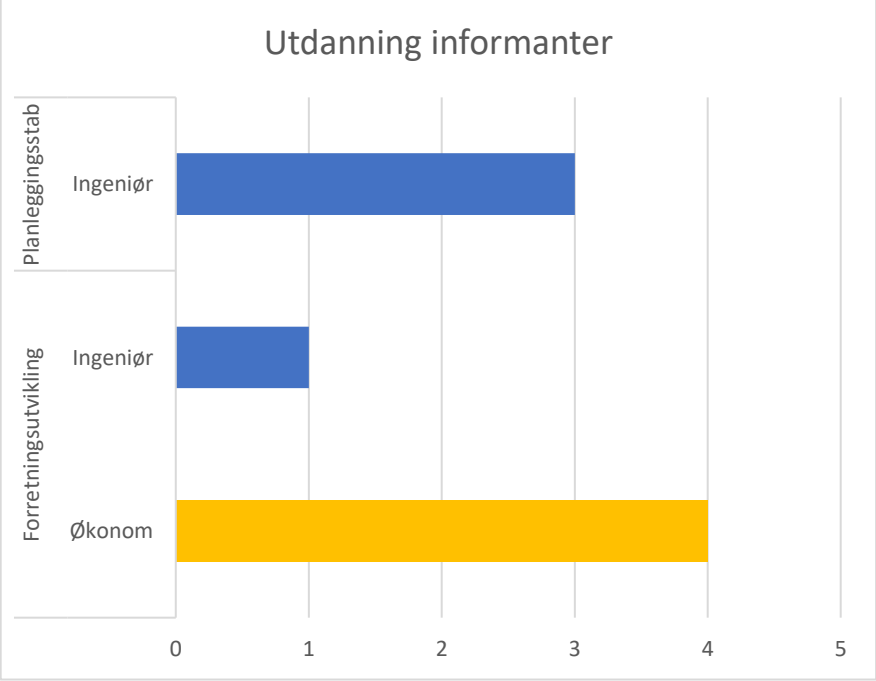
5 Empiri og resultat

Dette kapittelet gir en grov oversikt over resultatene fra både dybdeintervjuene og spørreundersøkelsen, før de blir analysert mer inngående og satt i sammenheng med hverandre i neste kapittel.

5.1 Dybdeintervjuene

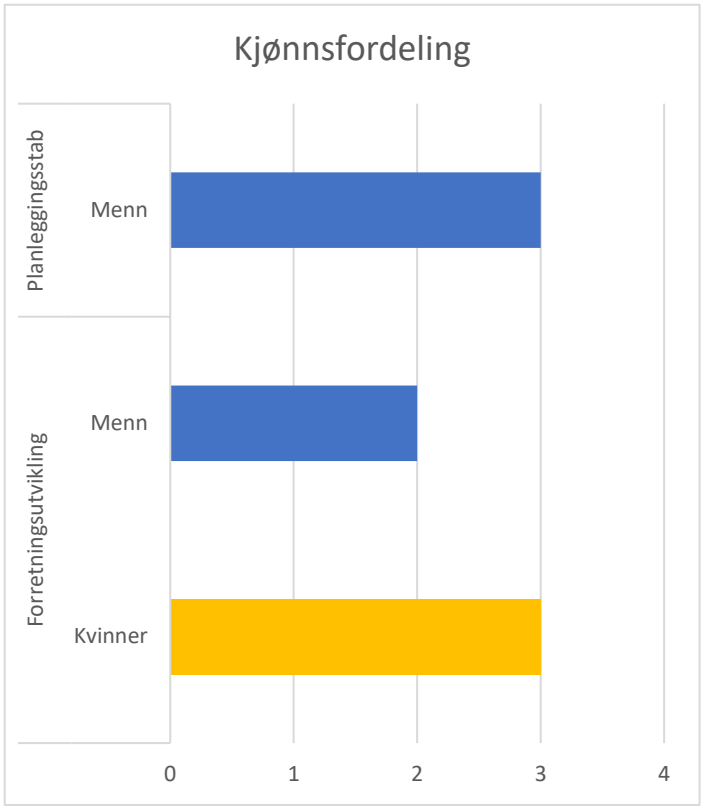
De samme spørsmålene ble stilt til ansatte fra avdelingen Forretningsutvikling i divisjon Utvikling og Planleggingsstaben som er organisert under IT divisjonen. Totalt 8 intervjuer ble gjennomført; 5 informanter fra Forretningsutvikling og 3 fra Planleggingsstaben. Deres ansiennitet i etaten var mellom 5 og 13 år og gjennomsnittet var på 8,25 år.

Bakgrunnen og utdanningen til disse to gruppene var delt opp med ganske klart skille. Mens 80% av informanter fra Forretningsutvikling var økonomer, var alle informantene fra Planleggingsstab ingeniører innenfor informatikk.



Figur 16: Viser utdanningen til informanter i dybdeintervjuene

Kjønnsfordelingen mellom informantene her var det også relativt klart skille på. Mens alle informantene fra Planleggingsstaben var menn, stilte Forretningsutvikling med 3 kvinner og 2 menn.



Figur 17: Viser kjønnsfordelingen blant informantene i dybdeintervjuene

I dybdeintervjuene var svarene fra Forretningsutvikling naturlig nok mer begrunnet i anvendt metodikk og arbeidsprosesser, mens Planleggingsstab hadde en mer teknisk tilnærming i sine svar og eksempler. Dette skyldes mest sannsynlig at Forretningsutvikling har en veldokumentert prosess som de er trofaste mot samtidig som de arbeider på et konseptuelt nivå. Planleggingsstaben på sin side består for det meste av IT-arkitekter som har teknisk bakgrunn og som jobber tettere på IT-løsninger og har sånt sett mer detaljkunnskap. De var også mer fleksible og pragmatiske i sine tilnærminger og mente at de har arbeidsprosesser, men at de ikke alltid fulgte dem slavisk fordi de ikke passet inn i alle jobbsituasjoner de kom opp i.

Samtlige informanter ga uansett utfyllende svar som ga denne oppgaven et godt datagrunnlag. I begynnelsen fikk jeg inntrykk av at de fleste informantene var litt forvirret hvorfor akkurat de var valgt ut til å bli intervjuet. Etter at jeg forklarte dem hva oppgaven gikk ut på, at det gagnet avdelingen og etaten og at det var lederen deres som pekte dem ut, var de veldig fornøyde med å kunne bidra. De aller fleste informantene ga etter intervjuet uttrykk for at spørsmålene var veldig gode, relevante og til tider vanskelig å svare på da de ikke har tenkt på sikkerhet på denne måten. Samtlige var også veldig interessert i å få tilsendt masteroppgaven slik at de kunne lese utfallet og hvordan dette vil kunne påvirke innovasjon og sikkerhet i etaten.

Dybdeintervjuene viser at de som jobber med innovasjon, både på forretningssiden og IT-siden svarer ganske likt på noen av spørsmålene, samtidig som det er noen nyanser og forskjeller i svarene. På noen av spørsmålene gjennom hele dybdeintervjuet måtte enkelte informanter tenke seg godt om før de svarte, mens på noen var de veldig raske med å svare som om de forventet å bli spurt om dette. Uansett, hadde alle mye på hjertet og svarte utfyllende noe som ga et godt datagrunnlag. Samtlige var godt fornøyd i jobben sin og følte at de fikk utnyttet potensialet sitt. De opplevde også forskjellige hindringer i sitt

arbeid, men ingen av intervjuobjektene nevnte direkte sikkerhet som en hindring eller ulempe. Informantene påpekte også at de får utnyttet sine ressurser og kunnskap, samtidig som de ser på eksisterende sikkerhetsmekanismer på utstyret de jobber på som en trygg ramme i deres arbeid. Alle informantene følte også trygghet på sin arbeidsplass og har heller ikke opplevd sikkerhetshendelser relatert til brudd på konfidensialitet, integritet eller tilgjengelighet i deres arbeid for etaten. Dette er positive og interessante funn som er viktige å ta med seg i videre arbeid på innovasjon og sikkerhet.

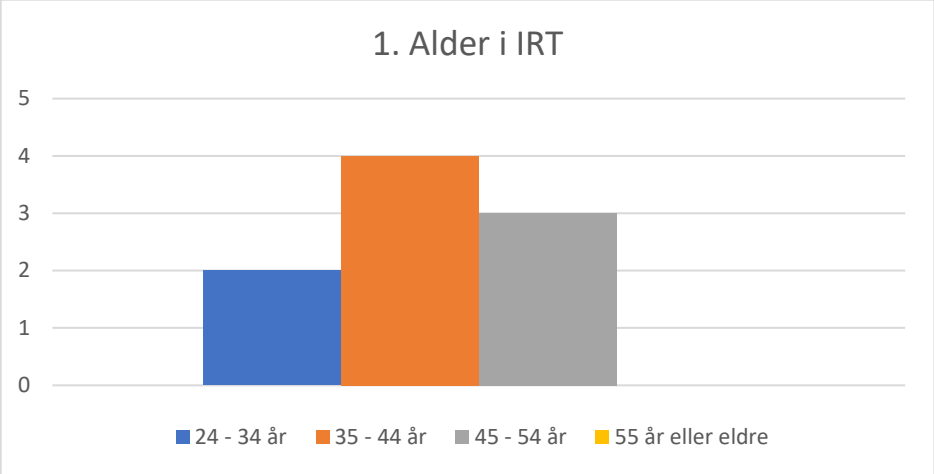
På den andre siden mente alle at det var potensiale for å innovere på sikkerhetsområdet i etaten. Den største forskjellen mellom intervjuobjektene var at Forretningsutvikling antok at innovasjon også innebar mindre endringer i en prosess eller rutine, mens Planleggingsstaben så på innovasjon som noe revolusjonerende og stort. De hadde også en ulik tilnærming til hvordan Sikkerhetsstaben bør innovere og forbedre seg for å møte morgendagens trusler og være mer motstandsdyktige, som jeg vil diskutere mer i neste kapittel.

5.2 Spørreskjema

Hensikten med denne digitale spørreundersøkelsen, som var veldig spisset mot informasjonssikkerhet, var å bekrefte at Skatteetaten har et dynamisk trusselbilde på IT-siden og kartlegge motstandsdyktigheten til Skatteetaten opp mot trusselaktørene. Informantene her var også geografisk plassert i Grimstad, mens jeg har kontor i Oslo, noe som gjorde denne formen for datainnsamling enklere. På veien dit ønsket jeg også å finne ut hvor mye innovasjon som faktisk foregår i deres prosesser, metoder og verktøy. Ettersom det var et spisset tema som informantene hadde fått informasjon om på forhånd, var det ikke behov for omfattende oppvarming. IRT, med 9 ansatte, er også en enhet som er svært opptatt og presset på ressurser, og deres oppmerksomhet på våre IT-systemer er påkrevd til enhver tid. Det var derfor viktig for meg å ikke ha for mange spørsmål og samtidig sørge for at spørsmålene var klare og konsise. Jeg valgte derfor å stille spørsmålene slik at de var enkle å forstå og at det var mulig å få med de forskjellige variasjonene i svarene.

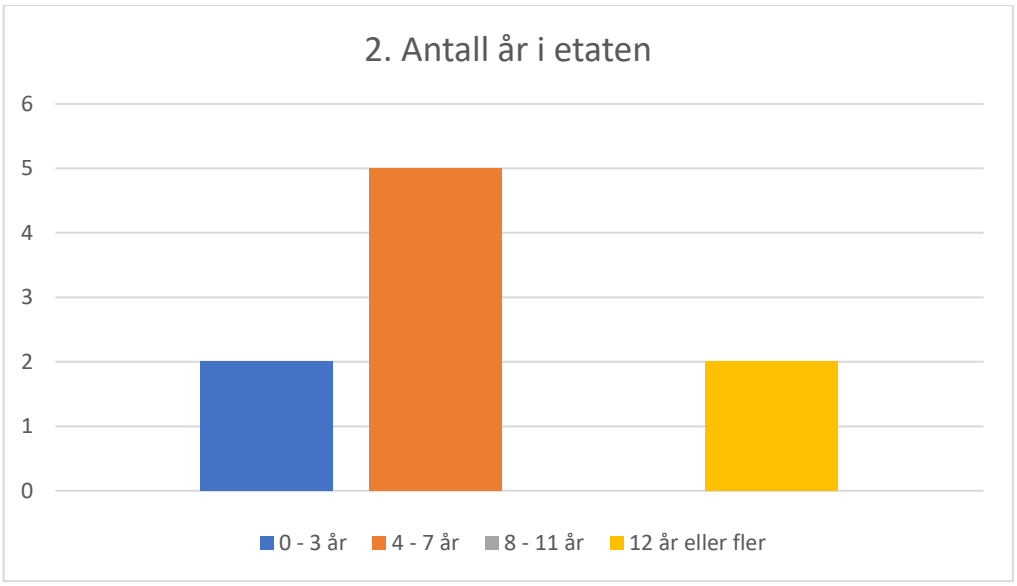
Totalt ble det stilt 21 spørsmål, der noen av dem ble stilt sammen fordi de var relatert til hverandre og dermed var det lettere å synliggjøre forskjellen på dem. Spørsmål 5 og Spørsmål 9 er eksempler på dette hvor det i teksten på spørsmål 5 er stilt to forskjellige spørsmål der det er et ord som skiller de fra hverandre; *oppdage* og *stoppe*. Ved å ha de to spørsmålene samtidig ved siden av hverandre og visuelt fremheve det ordet, ville det være lettere for informantene å se forskjellen på dem før de svarer. Det andre som skiller seg litt ut er spørsmålene 12 og 13. Den totale svarsummen på disse spørsmålene blir tilsammen over 100%. Dette skyldes at disse to spørsmålene ble stilt som multiple choice, der informantene hadde mulighet til å krysse av for flere valg.

Skatteetatens IRT består av 9 personer i alderen 24 til 54 og alle bekreftet at de jobber med å oppdage/stoppe angrep og/eller mistenkelig trafikk. Gjennomgående gjennom hele spørreundersøkelsen var det disse 9 personene som besvarte undersøkelsen, noe man kan se på kolonnen *Total* på hvert spørsmål som er vedlagt i denne oppgaven.



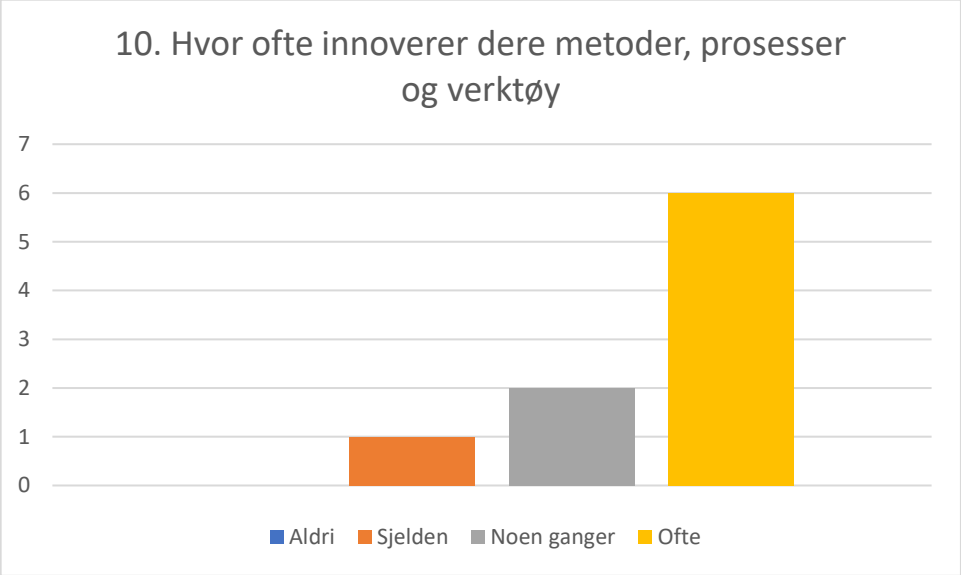
Figur 18: Statistikk over aldersfordelingen i IRT

Over halvparten av IRT har mellom 4 og 7 års erfaring i etaten, mens to ansatte har opptil 3 års erfaring. To av de ansatte har også lang fartstid i etaten med mer enn 12 års erfaring.



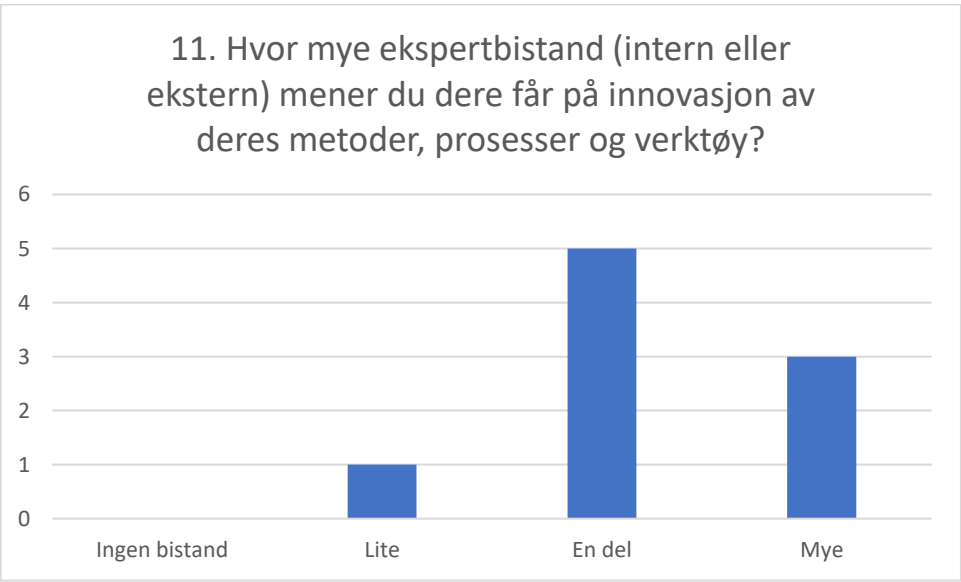
Figur 19: Viser ansiennitet blant Skatteetatens IRT medlemmer

Svarene på spørsmålene 10, 11, 12 og 13 har jeg valgt å ikke erstatte med N/A, som jeg forklarte tidligere, ettersom de er sentrale for denne oppgaven og det er disse svarene som beriker den. På spørsmål 10 og 11 er det en liten svakhet da disse svaralternativene kan tolkes relativt. For noen kan svaralternativet *ofte* eller *mye* være 2 ganger i måneden, mens det for andre må være et mye høyere tall for at det skal anses som ofte. Uansett så svarer 6 informanter, som utgjør ca 67%, at IRT ofte innoverer sine metoder, prosesser og verktøy. To svarer at de gjør det noen ganger og en ansatt svarer at de sjelden gjør det. Ingen svarer at de aldri innoverer.



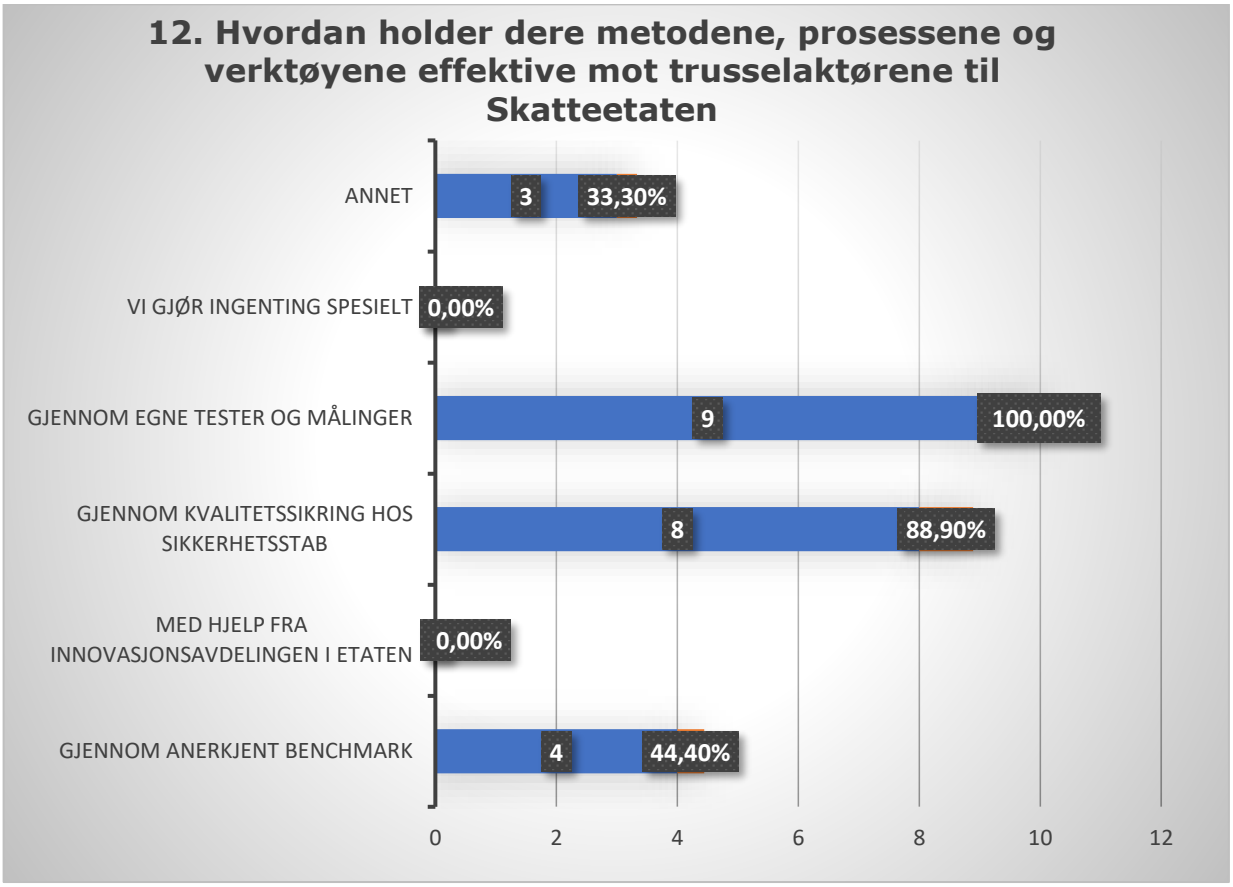
Figur 20: Viser innoveringsfrekvensen på metoder, prosesser og verktøy

Når det gjelder ekspertbistand på innovering av metoder, prosesser og verktøy, så er det bare 1 informant som svarer at de får lite av det. Samtidig svarer over halvparten av informantene at de får *en del* ekspertbistand, mens 3 informanter sier at de får *mye* ekspertbistand til innovasjon. Dette er klare signaler på at IRT i hvert fall får bistand for å innovere sine metoder, verktøy og prosesser i kampen mot å oppdage og begrense skadeomfang av angrep. Her kan det også være en liten svakhet ettersom mennesker kan ha forskjellig oppfatning av hva ekspertbistand innebærer.



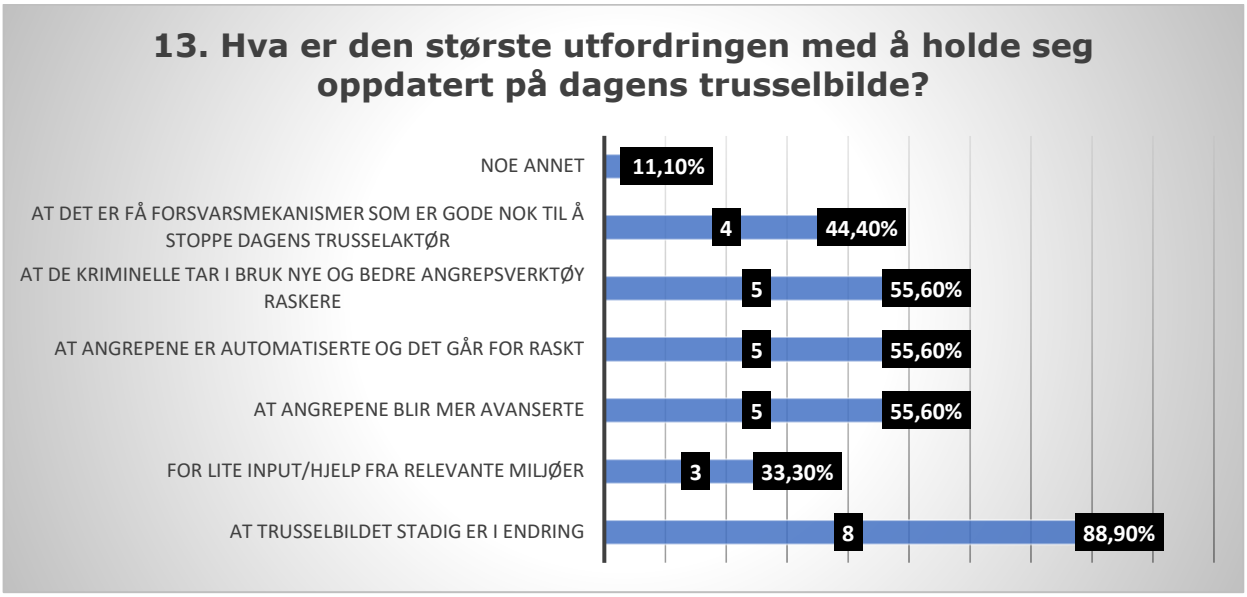
Figur 21: Viser hvor mye ekspertbistand IRT får på innovasjon

Svarene på spørsmål 12 samsvarer godt med besvarelsene på spørsmål 11, ingen svarte at de ikke gjør noe spesielt. Alle sluttet opp mot at IRT holder sine metoder, prosesser og verktøy effektive mot trusselaktørene gjennom egne tester og målinger. Samtidig svarte 8 av 9 at de kvalitetssikret dem gjennom Sikkerhetsstaben. 4 av informantene svarte også at de holdt effektiviteten oppe via anerkjente benchmark og 3 benyttet seg av feltet *noe annet*, hvor de beskrev at de brukte markedet, trening og øvelser for å holde tritt.



Figur 22: Svarfordeling på effektivisering av metoder, prosesser og verktøy

På siste spørsmål, som kanskje er det mest interessante i denne spørreundersøkelsen sammen med spørsmål 12, er hva IRT mener den største utfordringen er med å holde seg oppdatert på dagens trusselbilde. Hele 8 av 9 medlemmer i Skatteetatens IRT svarte at *et trusselbilde i stadig endring* er den største utfordringen. Over halvparten av de spurte anså også avanserte, automatiserte og raskere angrep som noen av de største utfordringene, sammen med at *kriminelle tar i bruk nyere og bedre angrepsverktøy raskere*, som er kjennetegn relatert til et dynamisk trusselbilde. Dette er noe som peker på at innovasjon og effektivisering er viktig for å henge med i utviklingen på trusselbildet. På den andre siden, hevdet litt under halvparten at det er få forsvarsmekanismer som er gode nok for å stoppe dagens trusler og bare en tredjedel mente at det var en stor utfordring at de får for lite input fra relevante miljøer.



Figur 23: Oversikt over utfordringer med dagens trusselbilde

5.2.1 Spørsmål som kunne utgjøre sikkerhetsrisiko

I kapittel 4 forklarte jeg at svarene på noen spørsmål ble erstattet med N/A for at denne oppgaven ikke skulle bli klausulert. For potensielle angripere vil informasjon om dette teamet og hva IRT anser som trusler og sårbarheter være nyttig. Få ressurser på et arbeidsområde kan for eksempel avsløre hvor effektivt trusler håndteres. Hvor effektive metodene, verktøyene og prosessene er for å oppdage og stoppe en trusselaktør kan danne et bilde av hvor Skatteetaten er mest sårbare. Selv om disse dataene inngår i mine tolkninger på et generalisert nivå, kan de ikke presenteres i oppgaven, men jeg har valgt å fremheve de aktuelle spørsmålene her slik at leseren er klar over dem. Alle spørsmålene er for øvrig vedlagt i denne oppgaven i kapittel 9.

- Hva er ansvarsområdet ditt
- Føler du at angrepene har blitt vanskeligere å oppdage de siste to årene?
- Føler du at angrepene har blitt vanskeligere å stoppe de siste to årene?
- Hvem av disse mener du utgjør den største trusselaktøren til Skatteetaten?
- Mener du, på generelt grunnlag, at dere har gode nok metoder, prosesser og verktøy til å oppdage angrep eller mistenkelig trafikk før brudd på IKT har inntruffet?
- Mener du, på generelt grunnlag, at dere har gode nok metoder, prosesser og verktøy til å stoppe angrep eller mistenkelig trafikk før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å oppdage et angrep fra en statlig aktør med store ressurser før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å stoppe et angrep fra en statlig aktør med store ressurser før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å oppdage et angrep fra en organisert kriminell gruppe før brudd på IKT har inntruffet?

- Hvilke mulighet tror du dere har for å stoppe et angrep fra en organisert kriminell gruppe før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å oppdage et angrep fra ekstern enkeltperson før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å stoppe et angrep fra ekstern enkeltperson før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å oppdage et angrep fra en intern ansatt eller konsulent før brudd på IKT har inntruffet?
- Hvilke mulighet tror du dere har for å stoppe et angrep fra en intern ansatt eller konsulent før brudd på IKT har inntruffet?

6 Analyse og diskusjon

I begynnelsen av dette kapittelet vil jeg analysere svarene fra dybdeintervjuene og spørreskjemaene hver for seg. Ettersom det var mange interessante svar fra dybdeintervjuene og spørreskjemaene, vil jeg fokusere på de spørsmålene og svarene som er mest interessante i forhold til oppgavens problemstilling. Jeg har gjort det på denne måten for å ta svarene og informanten på alvor før jeg går inn i en dypere diskusjon i siste del av dette kapittelet, der interessante observasjoner fra både dybdeintervjuene og spørreskjemaene blir diskutert på tvers og opp mot relevant teori.

6.1 Analyse

Under her har jeg valgt å analysere og fremheve spørsmålene som ble stilt i dybdeintervjuene der svarene var mest interessante og gjenfortelle observasjoner, sitater og svar fra informantene på de spørsmålene. Overskriftene gir indikasjon på temaet som blir diskutert, etterfulgt av spørsmål fra intervjuguiden. Alle spørsmålene som ble stilt under dybdeintervjuene er også vedlagt i kapittel 9 i denne oppgaven.

6.1.1 Generelle utfordringer i innovasjonsarbeidet

Dette punktet vil belyse hva informantene så på som utfordring ved innovasjonsarbeidet. Jeg hadde en formening før første intervju at mange ville nevne sikkerhet her og ønsket derfor ikke å lede informantene til å nevne sikkerhet som en utfordring. Derfor stilte jeg spørsmålet på denne måten, slik at de kunne svare fra et fritt perspektiv, i håp om å få frem så ærlig svar som mulig og fange opp det som var den faktiske utfordringen deres.

Spørsmål 8: *Hvilke utfordringer har dere i deres dagligdagse arbeid? Eks: Er det noe som bremser opp eller som ikke utnytter potensialet til ressursene og kunnskapene i innovasjonsarbeidet?*

Svarene som dukket opp ved dette spørsmålet var veldig interessante da sikkerhet ikke ble nevnt som en utfordring eller brems av noen informanter.

Alle informantene fra Planleggingsstaben nevnte tid som en utfordring, der ting tar veldig lang tid før det faktisk blir implementert og at de er avhengig av andre for beslutninger og gjennomføring. Ansatte i denne gruppen er også relativt tekniske og opptatt av å være oppdatert på teknologisiden, og min oppfatning av svarene gitt på dette spørsmålet var relatert til at tidsbruken ved beslutninger gjør at Skatteetaten henger etter på teknologisiden. Som teknologer er man som regel opptatt av å følge teknologiutviklingen og vil ikke bli hengende etter, noe som kan forklare deres frustrasjon på dette.

Informantene fra Forretningsutvikling nevnte også utfordringer i sin hverdag, men var mer opptatt av å adressere organisatoriske hindringer. Flesteparten nevnte ressurstilgang og økonomi, samt nedprioritering og allerede etablert praksis som de store utfordringene. Jeg følte at dette gjorde dem ganske oppgitt og at de følte det som en kraftig begrensning. Informant 01 refererte også til Conveys lov på dette spørsmålet; *Organisasjoner som lager komplekse systemer bygger ubevisst disse slik at de gjenspeiler sine egne kommunikasjonsstrukturer*. Etter min oppfatning var dette frustrerende og informanten mente at de dermed drev med innovasjon innenfor sterkt begrensede rammer og ikke fikk utnyttet sitt potensiale fullt ut.

Dette spørsmålet var for øvrig også der informantene var veldig engasjerte. Dette kan være fordi det var det første spørsmålet på hoveddelen etter oppvarmingsspørsmålene, men det kan også skyldes at de endelig hadde fått et talerør slik at de kunne påpeke deres utfordringer i håp om at de ville bli utbedret. Samtlige informanter hadde utdypende svar på dette spørsmålet og det var i mindre grad behov for oppfølgingsspørsmål.

6.1.2 Dokumenter på nivå 3 i SFI passer ikke alltid inn

Ettersom det var en del teori på samspillet mellom sikkerhetsprosedyrer og ansatte, ønsket jeg å ha et spisset spørsmål rettet mot SFI og om det er hemmende for innovasjonsarbeidet. I diskusjonsdelen vil funn herfra kobles opp mot relevant eksisterende teori, noe som var utfordrende på enkelte steder i oppgaven grunnet tynt teorigrunnlag.

Spørsmål 17: Føler du at SFI (styringssystemet for informasjonssikkerhet) hemmer innovasjonsarbeidet? I så fall, kan du utdype?

På dette spørsmålet fant jeg den største forskjellen på svarene til informantene fra de respektive avdelingene. Alle informantene var glade og forståelsesfulle for at vi har et styringssystem for informasjonssikkerhet og synes Sikkerhetsstaben er viktig å involvere og avklare med. Det som derimot kom tydelig frem var at Forretningsutvikling ikke benytter seg av SFI på samme måte som Planleggingsstaben og dermed hadde ulik grad av kjennskap til dokumentene som var nedfelt der. De hadde kjennskap til styringssystemet som sådan og visste at det finnes, men "det var ikke en del av verktøykassa" deres og leser dem ikke. Planleggingsstaben på sin side ser på detaljer ved implementering av en ny IT løsning og kjenner til hele SFI godt, men er mest avhengig av de detaljerte dokumentene på nivå 3.

Alle informantene fra Planleggingsstaben mente at dokumentene i SFI fungerte fint på de to første nivåene, altså SFI-1.1 og SFI-2.n, men at dokumentene på nivå 3 skapte utfordringer for dem. Dette mente de skyldtes blant annet at de var altfor detaljerte og spisset, i noen tilfeller også bundet opp mot eksisterende teknologivalg, som gjorde det vanskelig å realisere løsninger som hadde passet bedre i flere sammenhenger. Samtlige ønsket de mer fleksibilitet på dette nivået slik at de kunne gjøre IT porteføljen til etaten enda bedre og mer attraktiv.

"SFI fungerer fint, men ikke over nivå 2. Alt på nivå 3 blir altfor detaljert og passer ofte ikke inn i de forskjellige situasjonene." – Alle informantene fra Planleggingsstab

"Teknologi endrer seg fortere enn dokumentene på nivå 3" – Informant 05 fra Planleggingsstab

Ingen fra Forretningsutvikling svarte at SFI'en er hemmende for deres arbeid på noen måte og jeg følte at jeg måtte grave litt her for å verifisere at de faktisk mente det. Under samtalen kom det da frem at Forretningsutvikling for det meste jobber på det konseptuelle nivået, og da benytter de ikke SFI aktivt i sitt arbeid. De har heller ikke et sjekkpunkt med Sikkerhetsstaben eller sikkerhetsansvarlige i sin prosess og det er da opp til den enkelte som holder i prosessen hvor tidlig eller sent man vurderte problemstillinger knyttet til sikkerhet og personvern. Dette er den rake motsetningen til informantene fra Planleggingsstab som hadde jevnlige møter med representanter fra Sikkerhetsstaben og brukte SFI aktivt i sitt arbeid. Når slike vurderinger skulle taes opp så gikk ikke informantene fra Forretningsutvikling inn i SFI og vurderte problemstillingen opp mot gjeldende regler, men kontaktet istedenfor noen direkte i Sikkerhetsstaben og luftet problemstillingen for å høre om det er noen såkalte umiddelbare "showstoppere". Var det problematisk, prøvde man å diskutere alternativer for å gå videre med idéen eller løsningen, eller i verste fall droppe idéen. De synes også at vurderingene fra Sikkerhetsstaben kan ta litt tid og at svaret de får ofte er varierende, "avhengig av hvem man spør og man spør ofte de som man tror gir positive svar".

"Jeg vet det finnes masse policyer, men jeg leser dem ikke og de ligger ikke veldig synlig" – Informant 03 fra Forretningsutvikling

6.1.3 Råd for et bedre og mer innovativt sikkerhet

Her har jeg valgt å ta med fire spørsmål og oppsummere dem fordi alle informantene var samstemte i sine svar på de tre første spørsmålene, som i utgangspunktet var ja/nei spørsmål. Dette er også kjernen av denne oppgaven da spørsmålene fokuserer på involvering av innovasjon i prosesser relatert til sikkerhet. På det siste spørsmålet var informantene mer varierende i svaret, noe som er logisk ettersom informantene hadde forskjellig utgangspunkt, relasjon og erfaring med sikkerhet og innovasjon – likevel var alle anbefalingene verdifulle.

Rådene som kom frem her sier også noe om hva informantene mener er problematisk og hva de har observert forbedringspotensial på. Ettersom innovasjon er deres ekspertise bør rådene taes på alvor og arbeides videre med.

Spørsmål 23: Har din avdeling vært involvert i utarbeidelsen av informasjonssikkerhetsstrategien i etaten?

Spørsmål 24: Er din avdeling involvert i utarbeidelsen av andre strategier enn dets egen eller etatens overordnede strategi?

Spørsmål 30: Tror du Sikkerhet kunne ha behov for å være mer innovative?

Spørsmål 31: Hva er dine råd for et bedre og mer innovativt sikkerhet?

Informasjonssikkerhetsstrategien har vært under arbeid i cirka et år og er fortsatt under arbeid. Det som er interessant her er at ingen av informantene kjenner til at avdelingen deres som sådan har vært involvert i arbeidet med den strategien, selv om alle

informantene fra begge avdelingene svarer at avdelingen de jobber i har som oppgave å bidra inn i strategiarbeidet til andre enheter i etaten.

Samtidig svarer alle informantene at de mener Sikkerhetsstaben kunne ha behov for å være mer innovative, bortsett fra en informant som ikke kunne svare på det spørsmålet da vedkommende ikke kjente godt nok til Sikkerhetsstaben. Noen av informantene svarte "ja" veldig raskt på dette spørsmålet, som om de var veldig sikre i sin sak, mens 3 av dem måtte tenke seg om litt og forklare mer og påpekte at det har blitt bedre med årene. Ved utdypingen mente de at det spørs hvor man ser og hvor detaljert man graver. For eksempel dersom man ser på teknologi brukt for å understøtte sikkerhet og sikkerhetsmekanismer brukes det ny teknologi for å løse problemstillinger relatert til sikkerhet på IT området. På en annen side ble det nevnt at dersom man ser på prosesser relatert til sikkerhetsgodkjenning av ny teknologi så er det potensiale for mer innovasjon og forbedring. De 3 svarte også tidligere at de "ikke ser på innovasjon og sikkerhet som to motsetninger, men at det fort kunne bli det ettersom sikkerhet gir føringer og retninger".

Alle informantene hadde gode råd å komme med når det gjaldt et bedre og mer innovativt sikkerhet, samtlige uttrykte også engasjement på dette spørsmålet. De aller fleste hadde utfyllende og gode svar på dette spørsmålet og jeg måtte i mindre grad stille oppfølgingsspørsmål. Det kan ha noe å gjøre med at det var her ekspertisen og domenet deres kom inn i bildet, men kan også være relatert til at det var det siste spørsmålet og informantene å hadde blitt varme i trøya eller rett og slett følte at her kunne de bidra til forbedring – noe som er hele tankegangen med innovasjon. Her måtte jeg også, for noen informanter, presisere at det gjelder sikkerhet i etaten og måten vi arbeider på, både prosesser, metoder og verktøy. Det var også her jeg fant forskjell på tilnærmingene og rådene de to avdelingene kom med. Informantene fra Forretningsutvikling ga råd som var mer rettet mot organisatoriske tilnærminger. De var generelt mer opptatt av å forankre og involvere andre enheter i organisasjonen i vårt sikkerhetsarbeid. "Se mer på sikkerhet i hverdagen" og "Vær mer oppsøkende og synlig" i organisasjonen var to konkrete råd, som vi også har økt fokus på i Sikkerhetsstaben ettersom vi er relativt få hvis man ser på totalt ansatte i etaten. Det andre som dukket opp som råd fra denne gruppen informanter var mer åpenhet og deling, to ting man ofte finner utfordrende i sikkerhetssammenheng da mye av arbeidet og informasjonen vi besitter er taushetsbelagt. Allikevel er det viktige punkter som ikke overraskende kommer fra disse informantene, der alle tidligere svarte at de ikke jobber med sensitive opplysninger. De er med andre ord vant til å dele sitt arbeid, som er avhengig av åpenhet og involvering av andre og ser derfor på det som nødvendig. Ingen av dem anser arbeidet sitt som konkurransesensitivt og noen av informantene svarte også at de inviterer private kommersielle aktører for å videreutvikle idéene og konseptene sine, da de gjerne vil ha deres mening.

"Få øremerkede midler, ressurser og tid til innovasjon på sikkerhetsområder inn i mandatet deres slik at det blir ivaretatt" – Informant 06 fra Forretningsutvikling

Planleggingsstaben sine informanter hadde på sin side en mer teknisk og pågående tilnærming i sine råd. Deres råd gikk mer på at Sikkerhetsstaben må være mer i forkant og tørre å ta i bruk nyere teknologi og mer utforsking. En mer "prøv dere fram og lær av feil og erfaringer fra dere selv og andre" tilnærming, noe som dreier mot safety 2 prinsippet. De oppfordret også til mer samarbeid og dialog med andre i samme situasjon slik at man kan hjelpe hverandre og dele erfaringer. En av informantene påpekte at det var en risiko å ikke fornye seg, men samtidig en risiko å ta i bruk noe som er altfor prematurt, og oppfordret Sikkerhetsstaben til å finne en riktig balanse på dette. "Man må endre seg med trusselbildet

og tørre å utfordre seg selv for å få med at ting forandrer seg" var et råd som er meget sentralt i denne oppgaven. Dette viser at de har en proaktiv, fleksibel og innovativ innstilling, altså at de tenker på safety 2 måten. I dialogen med dem var jeg også under det inntrykket av at ting går bra på sikkerhetssiden i Skatteetaten, men at vi likevel må følge med i utviklingen, ikke bare sitte i vår lille sikre boble. Vi måtte bruke den kunnskapen og erfaringen vi har og bygge videre på den for å bli enda bedre, noe som er kjernen i safety 2 prinsippet forklart tidligere i denne oppgaven.

6.1.4 Trusselbildet er i endring

Når det gjelder svarene til IRT og spørsmålene besvart i spørreskjemaet, så har jeg som tidligere nevnt ikke ønsket å klausulere oppgaven og kunne derfor ikke gjengi svarene på alle spørsmålene da det potensielt kunne utgjøre en risiko for Skatteetaten. Videre i oppgaven vil jeg derfor bruke de spørsmålene og svarene jeg kunne presentere uten at det utgjør en sikkerhetsrisiko for Skatteetaten. Spørsmålene i sin helhet er dog å finne som vedlegg i denne oppgaven. Selv om jeg i denne oppgaven ikke har brukt de svarene som er erstattet med N/A, har jeg brukt dem til å bekrefte egne mistanker da IT-sikkerhet er mitt spesialfelt. En av mine oppgaver i Sikkerhetsstaben er å bidra til rapportering av Skatteetatens trusselbilde til toppledelsen, og svarene fra spørreundersøkelsen samsvarer godt med etatens trusselbilde. Dette er også noe av grunnen til at spørreskjema ble benyttet for å samle inn data om trusselbildet slik IRT ser det, da det er en velegnet metode for å ivareta objektiviteten og for at forkunnskapen skal bli en ressurs fremfor støy, (Tjora, 2007).

Alle i IRT var samstemte om at det har skjedd en endring i oppdagelsen og forhindring av angrep de to siste årene, noe som er veldig interessant i denne oppgaven som blant annet ser på et trusselbilde i endring. 7 av de 9 som svarte pekte også ut den samme trusselaktøren på spørsmål om hvem som utgjør den største trusselaktøren for Skatteetaten. De var også samstemte om hvor godt rigget de er for å oppdage og stoppe angrep fra den aktøren. Dette er svar jeg har måttet erstatte med N/A i vedlegget, men som jeg likevel kan trekke disse konklusjonene fra uten at det utgjør en sikkerhetsrisiko for Skatteetaten.

6.1.5 IRT innoverer og kvalitetssikrer gjennom Sikkerhetsstab

Det andre som er interessant å trekke frem fra spørreundersøkelsen relatert til denne oppgaven, var om og hvordan IRT holder sine metoder, prosesser og effektive mot trusselaktørene til Skatteetaten. Her svarer over halvparten av IRT at de får *en del* ekspertbistand, mens 3 informanter sier at de får *mye* ekspertbistand til innovasjon. Dette er klare signaler på at IRT i hvert fall får bistand for å innovere sine metoder, verktøy og prosesser i kampen mot å oppdage og begrense skadeomfang av angrep på IT-systemene.

Ca 90% av IRT svarte at de kvalitetssikret metoder, prosesser og verktøy gjennom Sikkerhetsstaben, noe som er interessant i seg selv, da det stiller forventninger til at Sikkerhetsstaben vet hva som skal til for å oppdage og stoppe trusselaktørene IRT og Skatteetaten står ovenfor. Dette betyr at når man har et trusselbilde i endring, er det

nødvendig at Sikkerhetsstaben har en oversikt over det til enhver tid, samtidig som de har forslag til gode løsninger for å oppnå motstandsdyktighet. Andre resultater på dette spørsmålet viser også at det faktisk er en god del fokus på effektivisering av metoder, prosesser og verktøy og at det skjer på flere måter. De benytter seg blant annet av egne målinger og anerkjente benchmark også. Det andre som er verdt å nevne i den sammenhengen er at ingen mener at de får bistand fra innovasjonsavdelingen i etaten.

6.2 Diskusjon

Som nevnt tidligere består denne oppgaven av innsamlede data fra både dybdeintervju og spørreskjema, altså en kombinasjon av kvalitative og kvantitative data. Informasjonen fra disse to datakildene bidrar på hvert sitt vis til med å kaste lys over problemstillingen min; *"… om de etablerte sikkerhetsmekanismene utgjør en hindring for de som arbeider med innovasjon og hvordan vi kan være mer innovative og forbedre oss på sikkerhetssiden slik at vi er bedre rustet mot et trusselbilde i stadig endring".*

Dybdeintervjuene forteller om samspillet mellom innovasjon og informasjonssikkerhet og praktiske utfordringer knyttet til disse to fenomenene. Intervjuene har jeg derfor konkret benyttet for å blant annet finne ut om sikkerhet hemmer innovasjonsarbeidet i etaten, samt høste tips og anbefalinger på hvordan vi kan være mer innovative i sikkerhetsarbeidet i etaten.

Spørreundersøkelsen brukt mot IRT forteller mer om motstandsdyktigheten og trusselbildet til Skatteetaten, hvor mye fokus de har på innovasjon i det arbeidet, samt hva som gjør det utfordrende å holde seg oppdatert på dagens trusselbilde. Denne datakilden har jeg dermed benyttet for å bekrefte min forutgående forståelse av at vi har et komplisert og dynamisk trusselbilde som vi må være godt rustet mot, men at vi også er avhengig av innovasjon på forsvarssiden. Det var ikke aktuelt å gjennomføre dybdeintervju med Skatteetatens IRT da den rollen og kunnskapen jeg har på sikkerhetstemaet kunne skape støy, i tillegg til at det var mest praktisk grunnet den geografiske avstanden.

Funnene fra disse to datakildene vil bli diskutert nedenfor, både på tvers og opp mot relevant teori.

6.2.1 Hvorfor oppleves SFI utfordrende?

Mens ingen fra Forretningsutvikling mente at styringssystemet for informasjonssikkerhet (SFI) var hemmende for deres arbeid, svarte alle fra Planleggingsstab at det var rom for forbedringspotensial. Spesielt når det gjelder kravene stilt på nivå 3 i SFI var det en del synspunkter fra denne gruppen. De hadde behov for mer fleksibilitet enn hva dokumentene på nivå 3 ga dem og de mente at teknologien endret seg raskere enn dokumentene på dette nivået, noe som viser betydningen av safety 2 prinsippet. Det er en mulighet for at bakgrunnen til informantene er en forklaring på hvorfor de oppfatter styringssystemet så forskjellig. Ettersom 80% av informantene fra Forretningsutvikling var økonomer, mens alle informantene fra Planleggingsstab var ingeniører, kan det skyldes at de leser dokumentene på forskjellig vis. Dette er ikke forsket mer på i denne oppgaven, men noe som kanskje bør ses på i videre arbeid. Uansett er dette observasjoner som er meget interessant å se opp

mot hvordan reglene ble skrevet når dokumentene på nivå 3 ble etablert, altså modell 1 og modell 2 tilnærmingene beskrevet i teorikapittelet.

Sikkerhetsstaben er en stab som har det overordnede ansvaret for både fysisk sikkerhet, informasjonssikkerhet og personsikkerhet, samt krisehåndtering og beredskap. Dette er et bredt, men viktig område å dekke i enhver organisasjon. Med et så bredt spekter vil det være en stor utfordring å kjenne til alle detaljene ved implementering og gjennomføring av reglene, da det vil være mange forhold å ta hensyn til som gjør at man ikke har hele oversikten.

Sikkerhetsstaben var, før omorganiseringen i 2019, organisert under IT og hadde dermed tettere kjennskap og kontakt med IT-divisjonen. Det var ganske naturlig at vi da kjente til mange detaljer om IT-systemene til etaten og hadde som sådan bedre oversikt over hvordan teknologi hang sammen på IT-systemene våre. Dette er noe som har blitt mer overlatt til nyopprettede IT-sikkerhet, der de har arvet noen av oppgavene vi tidligere hadde i vårt mandat. Av den grunn kan man si at når disse dokumentene på nivå 3 i SFI ble laget i sin tid, var de laget basert på modell 2 prinsippet som vil si at det var vi som skrev reglene og det var vi som operasjonaliserte dem. Vi kjente da til mange detaljer om IT systemene og i de fleste tilfeller deltok vi i gjennomføringen av reglene og var tungt inne i prosjekter som implementerte dem.

Ettersom tiden har gått og vi har fått et mer overordnet ansvar for etaten har Sikkerhetsstaben, ved å bli organisert i direktoratet, mindre oversikt over hvordan ting henger sammen på IT siden. Vi dykker ikke like mye i detaljer og er mest fokusert på å ha det overordnede ansvaret. Med 10 ansatte i Sikkerhetsstaben og det brede ansvaret som ligger på dem, er det heller ikke kapasitet til å være like mye involvert i dybden. Dette samsvarer godt med observasjonene gjort i dybdeintervjuene der de på forretningssiden ikke følte at SFI var hemmende for deres arbeid, siden de jobber på det konseptuelle nivået og bruker mest nivå 2 dokumenter, mens informanter i Planleggingsstab mente at dokumentene på nivå 3 gjorde det utfordrende for dem i deres arbeid. Ettersom de jobber med å innovere IT-porteføljen til Skatteetaten kan man si at dette er en indikasjon på at policyene på nivå 3 i SFI kan være hemmende for innovasjonen på IT-siden. Dette er uansett noe som bør forskes mer på før en endelig konklusjon trekkes. Det man derimot mest sannsynlig kan påstå, er at den organisatoriske avstanden til IT, etter siste omorganisering, gjør at det nå kan se ut som om de er skrevet med modell 1 prinsippet – eksternalisert kunnskap. Reglene kan derfor virke altfor teoretiske og virkelighetsfjerne og gjøre dem vanskelig å etterleve, (Heldal & Dehlin, 2017). En annen mulig grunn til at det føles som om dokumenter på nivå 3 i SFI kan være utfordrende å gjennomføre, er dersom dokumentene er utdaterte ettersom teknologien endrer seg raskt på IT siden. Uansett grunn fører det til at de som faktisk bruker disse dokumentene ikke føler at de er hensiktsmessige og da øker risikoen for at de finner egne måter å løse ting på.

Samtidig ble det påpekt av de fleste informanter fra Forretningsutvikling at SFI ikke ble aktivt brukt og ikke lå veldig synlig. Ansatte fra Forretningsutvikling, som er lokalisert i samme bygg som Sikkerhetsstaben, gikk direkte til ansatte Sikkerhetsstaben for å spørre om råd istedenfor å lese dokumentene i SFI. Denne handlingen, der de bevisst ikke vil lese hva policyene og reglene sier, grenser til policybrudd, men er likevel ikke problematisk fordi de oppsøker Sikkerhetsstaben for råd. Dette er meget interessant funn som danner grunnlag for nærmere undersøkelser om hva som faktisk skjer på andre lokasjoner der Sikkerhetsstaben ikke er tilstede, noe jeg etterlater til videre arbeid. Med over 6500 ansatte spredd på 56 kontorer i landet, der Sikkerhetsstaben fysisk er tilstede på kun to av dem,

må det kompenseres med systematisk opplæring og holdningsskapende arbeid innenfor SFI slik at det skapes god sikkerhetskultur. Ettersom holdningsskapende arbeid er en av de største mangelvarene på god informasjonssikkerhet, er det viktig at Skatteetaten har et bra opplegg for sine ansatte på det området da mangelen på det kan føre til bevisste brudd på sikkerhetsregler, (Borrett et al., 2013). Brukerne av systemer som omgår sikkerhetskontroller, gjør ikke dette bevisst for å utgjøre en sikkerhetsrisiko, men for å få utført jobben sin effektivt - noe som uansett ikke bør skje, (Blythe et al., 2013). Oppdagelsen av slike brudd vil neppe komme før en etterlevelsekontroll finner sted, eller det faktisk har ført til en konsekvens og rotårsaksanalysen viser at en ansatt ikke har fulgt en sikkerhetsprosedyre. Dette er også en økende trend og kan være en utløsende årsak til sikkerhetsbrudd, ettersom halvparten av sikkerhetsbruddene skyldes nettopp at ansatte ikke etterlever regler og krav fra styringssystemet, (Gyõry et al., 2012). Det skal ikke mer enn ett sikkerhetsbrudd til før konsekvensene kan bli store for en viktig nasjonal aktør som Skatteetaten. Det er derfor viktig å ha oppdaterte, relevante policyer som er mulig å etterleve og som det blir gitt opplæring i.

6.2.2 Motstandsdyktighet og forberedelse

Et trusselbilde i endring krever proaktiv tankegang som safety 2 med rask omstilling, dette er også noe informantene fra Planleggingsstaben gjennomgående påpekte i sine intervju. Det er en endring i angrepsmetodikken og varigheten av angrepene i dag, noe som gjør at mer informasjon må samles, analyseres og bearbeides, og at det generelt må arbeides på en annen måte. Tidligere var angrep tilfeldige og relativt korte, mens dagens angrep er avanserte, ofte målrettet, langtidsplanlagt, persistente og vanskeligere å oppdage. Også IRT til Skatteetaten bekrefter, i spørreundersøkelsen utført i denne oppgaven, at det har skjedd en endring i oppdagelsen og forhindring av angrep de to siste årene. I tillegg svarte ca 90% av IRT at *et trusselbilde i stadig endring* er den største utfordringen med å holde seg oppdatert på dagens trusselbilde. Mye av grunnen til det er at jakten på slike angrep gjør jobben til de som jobber med sikkerhet vanskeligere, spesielt de som tilbyr offentlige tjenester må være forberedt mot avanserte trusselaktører, (Borrett et al., 2013, s. 169). For å komme dette i møte, må man ha rutinene og prosessene på plass for å kunne forsvare seg mot dette og begrense skadeomfanget, (Borrett et al., 2013, s. 171). Dette krever at man prøver ut nye metoder og verktøy, for å være mer effektiv på forsvarssiden og øke motstandsdyktigheten. Antall nye sikkerhetsprodukter øker i takt med sårbarheter og ved innføring av regulatoriske endringer, som vil si at produkter finnes men man må finne informasjon om forsvarstrender, noe som kan være utfordrende, (James et al., 2013). Regulatoriske endringer og standardisering, som for eksempel GDPR, har ført til mange nye tjenester og produkter for at virksomheter skal bli compliant. De løfter standarden og det er spesielt viktig når det eksisterer trusler som krever oppmerksomhet og håndtering, (Johnsen, 2017). Samtidig er det noen ulemper ved å endre seg i takt med regulatoriske endringer. Utfordringen er blant annet at de ofte kommer sent på banen når det er en endring i trusselbildet. I tillegg er det meldt om at regulatoriske endringer, slik som GDPR, mulig hemmer innovasjon i banksektoren, (Capgemini, 2019, s. 9). Dette forsinkede tidsvinduet kan gi våkne trusselaktører en mulighet til utnyttelse og angrep. Spørreundersøkelsen i denne oppgaven pekte også på noe av det samme. 4 av 9 informanter fra IRT i Skatteetaten mente at det er få forsvarsmekanismer som er gode nok for å stoppe dagens trusler. Dette kan tyde på at forsvarsmekanismene er ineffektive mot

avanserte trusselaktører, men kan også tyde på at produkter som øker i takt med sårbarheter kommer sent på banen i forhold til endringen i trusselbildet.

Å være forberedt mot slike angrep, krever at planen er klar på forhånd. For å ha en plan klar må strategien ligge til grunn og da kommer man ikke unna det å se hva informasjonssikkerhetsstrategien fokuserer på. Ettersom Skatteetatens informasjonssikkerhetsstrategi fortsatt er under arbeid, har jeg ikke kunnet bruke den i denne oppgaven. Allikevel er det interessant å nevne her at ingen av informantene kjente til at avdelingen deres som sådan har vært involvert i arbeidet med den strategien. Selv om alle informantene fra begge avdelingene svarer at avdelingen de jobber i har som oppgave å bidra inn i strategiarbeidet til andre enheter i etaten. Dette kan selvsagt skyldes at informasjonssikkerhetsstrategien fortsatt er under arbeid, men kan også skyldes manglende forankring av informasjonssikkerhetsstrategien. Det hadde likevel vært interessant å se om strategien fokuserte på motstandsdyktighet, proaktivitet og innovasjon.

Ettersom Sikkerhetsstaben benytter seg blant annet av nasjonale strategier som input til sitt styringssystem for informasjonssikkerhet (SFI), har jeg istedet valgt å se på den relativt ferske norske nasjonale strategien for digital sikkerhet. Dette er et dokument fra 2019, altså en nyere versjon av dokumentet Johnsen så på i sin studie i 2017, der konklusjonen var at det var begrenset fokus på motstandsdyktighet og at det var fokus på reaktive handlinger framfor proaktive, (Johnsen, 2017). Overraskende nok var det heller ikke fokus på motstandsdyktighet eller resilience i 2019 versjonen. Dette er bekymringsverdig når Norge, et av verdens rikeste land og samtidig et av verdens mest digitaliserte, ikke har nevnt dette i sin strategi for digital sikkerhet. Det nærmeste som blir nevnt i den ferske strategien er at *sikkerhetsutfordringer som stadig er i endring bør møtes med intensivt samarbeid mellom offentlige og private aktører*. Dette er en lite ambisiøs strategi ettersom et angrep av ressurssterke aktører kan gi store konsekvenser, både på den økonomiske siden, men også omdømmet til Norge. Særdeles viktig er det å trekke frem folkeregisteret og helseopplysninger som attraktive mål for slike trusselaktører, der informasjon stadig blir mer digitalisert gjennom nasjonale fellesløsninger. Samarbeid er fint og viktig, men med en slik formulering samtidig som statlige aktører utgjør den største digitale risikoen mot viktige samfunnsfunksjoner og nasjonale interesser, er ordene *motstandsdyktighet* og *resilience* dypt savnet i den nasjonale strategien for digital sikkerhet, (Departementene, 2019).

6.2.3 Endring og innovasjon på sikkerhetsområdet

Offentlige aktører, slik som Skatteetaten, ser stadig etter forsvarsmekanismer mot avanserte angrep og det eksisterer ikke en "quick fix" på utfordringene nevnt ovenfor som man bare kan plugge i veggen og så er man tilstrekkelig beskyttet. Skal man kunne motstå denne type angrep må man lære, overvåke, analysere, beslutte og reagere på kort varsel og ta med seg de erfaringene raskt inn i en oppdatert plan og rutine, (Borett et al., 2013). Mennesker er raske, men de kan uansett ikke måle seg med datakraft, spesielt ikke når kunstig intelligens er involvert. Det som tar månedsvis for mennesker å utføre, blir gjort på sekunder med hjelp av kunstig intelligens. Dette var noe vi så i praksis på Def Con konkurransen i 2016, nevnt i innledningen av denne oppgaven, (Darpa, 2016). Med en kombinasjon av komplisert trusselbilde i stadig endring og avanserte ressurssterke trusselaktører må ambisjonen være å komme seg på det nivået og det må man innovere og

ta i bruk AI for å få til. Som informant 02 fra Forretningsutvikling nevnte i intervjuet; "*AI er viktig og kommer, men den enkelte er ikke forberedt på det".*

Det er ingen tvil om at det er mye å hente på dette området og at det er mange muligheter i et bedre samvirke mellom innovasjon og sikkerhetstenkning, noe også informantene påpekte. Det er også et stort potensiale på IT-sikkerhetsområdet hva gjelder løsninger og produkter, (Ružičić & Micic, 2017). Produsentene forsøker å fylle markedet med nye innovative og mer effektive produkter, men det er ikke sikkert det er riktige veien å gå for Skatteetaten. Ettersom Skatteetaten har veldig mye på plass allerede, både når det gjelder styringssystem og ressurser for å følge opp trusler, er det ikke behov for å finne opp kruttet helt på nytt men heller starte forsiktig. En prøv og feil strategi, som en informant fra Planleggingsstab anbefalte, kan være utfordrende i sikkerhetssammenheng ettersom eksperimentering og feil med sikkerhetssystemer kan få store konsekvenser. Her er det derfor viktig å ta fornuftige valg og finne den riktige balansen. Læringsfasen er viktig og uunngåelig i arbeidet med innovasjon, og da kan det i arbeid som er følsomt for feilsituasjoner, passe godt med mål om *forbedret forståelse* i denne fasen fremfor *prøv og feil*, *(*Fagerberg et al., 2006). Siden noen informanter også anbefalte økt fokus på samarbeid og dialog med andre i samme situasjon, er dette en tilnærming man kunne brukt i en innovasjonsprosess som ville økt forståelsen om mulighetene som finnes på sikkerhetsområdet.

I dybdeintervjuet der informanten nevnte Conveys lov var det en følelse av at man bygger på eksisterende teknologi og at det begrenset en god del for valgmuligheter. Det er veldig viktig at de som jobber med innovasjon ikke blir begrenset i sitt arbeid. Slike begrensninger kan være hemmende for innovasjonsarbeidet og bør ikke forekomme dersom man ønsker å fokusere på suksessfaktorene ved innovasjon, (Johannessen, 1994). Samtidig er det også viktig å ikke fokusere på en "gamechanger" ved innovasjon, men heller ha en inkrementell innovasjonsstrategi til å begynne med og gradvis innføre større endringer ved behov. Funnene i denne oppgaven bekreftet at flere forskjellige hindringer er tilstede i innovasjonsarbeidet og da kan inkrementell innovasjon være lurt å starte med. Teorien støtter denne fremgangsmåten som kan være mindre utfordrende ved innføring av nye måter å gjøre ting på i tradisjonsrike organisasjoner som Skatteetaten, (Davila et al., 2007). Det kan være for eksempel være en endring i en allerede etablert rutine ved håndtering av hendelser forårsaket av en kjent trusselaktør. Uten større investering, som for eksempel gjennom workshops, kan en slik rutine forbedres slik at oppdagelsen skjer på et tidligere tidspunkt ved angrep på IT-systemer. Det vil da kunne føre til innføring av inkrementell innovasjon på sikkerhetssiden. Det samme prinsippet kan innføres dersom man har manuelle flerstegs prosesser for å stoppe angrep. Det kan innføres en AI basert prosess eller produkt, som vil øke motstandsdyktigheten mot et trusselbilde i endring betraktelig. Slikt arbeid krever vesentlig endring i teknologien og vil da bli ansett som semi-radikalt, noe som også vil kunne påvirke forretningsmodellen ettersom de påvirker hverandre, (Davila et al., 2007). Teorien støtter også en kombinasjon av flere innovasjonsmetoder, da det er å anse som langsiktig suksess. Det fører til nye muligheter og forbedringer på sikkerhetssiden, men krever at organisasjonen er godt forberedt og har kapasitet nok for å gjennomføre den fullt ut, egenskaper Skatteetaten har vist å inneha gjennom flere tyngre omorganiseringer, (Davila et al., 2007).

Det er også ingen tvil om at det er en kostnad ved å innovere og at en investeringskostnad ofte må forsvares, (Khansa & Liginlal, 2007). Økningen av antall sårbarheter globalt og forventninger til at det skal brukes mer midler på IT-sikkerhet fram mot 2026, trenger ikke å falle i god smak hos ledelsen som er opptatt av å kutte kostnader. Ikke gjør det lettere å

forsvare en fremtidig innovativ investeringskostnad når innovasjon er usikkert, da det er umulig å forutse eksakte kostnader, ytelse og effekt av en ny gjenstand, (Fagerberg et al., 2007). Spesielt kan en investeringskostnad på sikkerhetssiden være utfordrende å argumentere for da man ikke kan vise til positive effekter før et angrep har blitt stoppet, i motsetning til en idé som kutter produksjonskostnader der investeringen vises lønnsom fra start. Uansett, et uforutsigbart trusselbilde i stadig endring, der trusselaktørene benytter angrepsmetoder med AI, er derimot et godt argument for å innovere på sikkerhetssiden. Et annet argument som er med på å forsvare en slik investeringskostnad, er at man uten AI teknologi på forsvarssiden, ikke vil være i stand til å oppdage, analysere, reagere og lære av avanserte angrep. Dette er spesielt viktig å ha på plass når såpass store pengesummer og Norges folkeregister forvaltes i en og samme organisasjon.

Det at det er relativt lenge siden et sikkerhetsbrudd har skjedd i Skatteetaten, trenger ikke å være et argument som skal slå ned en slik investering. For det betyr ikke nødvendigvis at ansatte følger alle sikkerhetsregler eller at vi er motstandsdyktige mot våre trusselaktører. Det kan hende at etterlevelsessjekken ikke er god nok eller at det ikke er tilrettelagt for etterlevelse, noe denne oppgaven ikke tar for seg, men som absolutt bør undersøkes. På en annen side kan den lave risikoappetitten ha bidratt til at Skatteetaten har levd i en liten sikker boble lenge og at dette er grunnen til at ingen informanter hadde opplevd sikkerhetshendelser relatert til brudd på konfidensialitet, integritet eller tilgjengelighet i deres arbeid for etaten. Samtidig mente alle informantene i dybdeintervjuene at Sikkerhetsstaben har behov for å være mer innovative og offensive, noe som bør taes på alvor. Det ble blant annet påpekt at Sikkerhetsstaben må mer på banen og at vi har et rom for forbedringspotensial hva gjelder innovasjon. Ettersom det er lenge siden et sikkerhetsbrudd har funnet sted kan det også være en bekreftelse på at vi har tatt riktige valg hva gjelder informasjonssikkerhet og det kan vi ta med videre på den reisen. Safety 2 prinsippet, som bygger på å lære av ting som går bra, forteller oss at dette faktisk er mulig å gjennomføre når risikoappetitten økes i håp om å forbedre og fornye seg. Dersom det ikke innoveres og tas i bruk AI på forsvarssiden, er det en stor risiko for at de vil bli hengende etter de kriminelle og da vil den gode historikken uten sikkerhetshendelser fort bli glemt. Som en informant fra Planleggingsstab påpekte; "Det en risiko å ikke fornye seg, men samtidig en risiko å ta i bruk noe som er altfor prematurt". På lik linje som man benytter ALARP prinsippet i sine tilnærminger i etaten ellers, bør man innføre samme prinsipp ved innovering på sikkerhetssiden. På den reisen er det derfor viktig å benytte seg av safety 2 prinsippet, ta med seg det som er sikkerhetsmessig positivt, spesielt når et trusselbilde i endring er lite forutsigbart. For sikkerhet på IT-systemer er nesten usynlig, man ser ofte ikke nytten av det før man har klart å oppdage en hendelse eller trussel.

7 Konklusjon

Svarene fra både dybdeintervjuene og spørreundersøkelsene viser at det må gjøres endringer på sikkerhetssiden både for å være enda mer motstandsdyktige, men også for å forenkle arbeidet til de som jobber med innovasjon i etaten og minimere risikoen for brudd på SFI. Samtidig må Skatteetaten ha sikkerhetsmekanismer og sikkerhetsregler for å opprettholde akseptabelt risikonivå og være motstandsdyktige mot trusselaktører.

For å redusere risikoen av bevisste sikkerhetsbrudd i SFI og samtidig tilrettelegge for de som jobber med innovasjon på teknologisiden, må dokumentene på nivå 3 i styringssystemet for informasjonssikkerhet være skrevet med modell 2 tilnærming. Dokumentene på nivå 1 og 2 er mer generelle og fungerer fint, men reglene og prosedyrene beskrevet på nivå 3 må være mulig å etterleve. De må ikke oppleves som ulempe for de som skal implementere og gjennomføre dem, eller for de som skal innovere IT-porteføljen. Ifølge informanter fra Planleggingsstab passer ikke dokumentene på nivå 3 i SFI alltid inn da de er for detaljerte og endrer seg heller ikke i takt med teknologien. Dette bør være grunnlag nok for å revurdere eierskapet til dokumentene på dette nivået. Sikkerhetsstaben har et stort overordnet ansvar med bredt spenn og det kan være utfordrende for Sikkerhetsstaben å ha ansvaret for disse detaljerte dokumentene nå som de har fått et annet fokus etter omorganiseringen og en mer overordnet rolle i organisasjonen. Denne oppgaven har også vist at de som har tilgang til sikkerhetsressurser bruker dem, noe som er positivt. Allikevel det gir det grunn for å undersøke hva som skjer på lokasjoner der Sikkerhetsstaben ikke er tilstede, og der bør det kompenseres med holdningsskapende arbeid mot ansatte hva gjelder SFI.

Ser vi på svarene til IRT temaet til Skatteetaten som bekrefter at det har skjedd en endring i trusselbildet de to siste årene, er det god grunn til å være forberedt og kjenne til trusselaktøren sin kapabilitet. IRT svarte at de kvalitetssikret metoder, prosesser og verktøy gjennom Sikkerhetsstaben og det stiller forventninger til at Sikkerhetsstaben til enhver tid er oppdatert på Skatteetatens trusselbilde. I tillegg til dette så mener de som jobber med innovasjon i Skatteetaten at sikkerhet har behov for å være mer innovative, noe som er unngåelig for å henge med et trusselbilde i stadig endring. Alt dette peker mot at sikkerhetsarbeidet må ha en safety 2 tilnærming. Man kan ikke vente på trusselrapporter som utgis en gang i året eller at regulatoriske endringer skal komme og løfte standarden hvert tiår. Det kan ta altfor lang tid før et krav kommer i form av et direktiv og et trusselbilde med motiverte angripere vil forsøke å utnytte det tidsvinduet, noe som vil kunne få store konsekvenser for en organisasjon som Skatteetaten og det ansvaret som ligger på dem.

For å kunne være rustet og motstandsdyktig mot et dynamisk trusselbilde må det, ifølge informantene og spørreundersøkelsen, benyttes ny teknologi med større grad av automatisering og AI. Mennesker alene kan ikke være motstandsdyktige mot en trusselaktør som er innovativ og tar i bruk nye og mer effektive verktøy. Trusselaktørene vil forbedre seg hele tiden og har ingenting å tape på å omstille seg, spesielt når motivasjonen og gevinsten er høy, samtidig hvis konsekvensene og oppdagelsen av deres angrep er lav.

Skatteetaten er en kompleks og tradisjonsrik organisasjon som er forpliktet til å modernisere og innovere gjennom både nasjonale og egne strategier, men ikke til enhver pris. Det må jobbes mer med innovasjon på sikkerhetsområdet i Skatteetaten nå som denne oppgaven har identifisert at behovet er tilstede. Rom for fleksibilitet og kreativitet på teknologisiden må etableres hos de som jobber med sikkerhet, aksepten for endring av allerede etablerte praksiser må forankres i toppledelsen, sikkerhetsinnovasjon må inkluderes i strategier og ikke minst finansieres med øremerkede midler, samtidig som det må allokeres ressurser og tid til dette viktige arbeidet. Endringer i et område som sikkerhet, der feil valg kan få store konsekvenser, bør tenkes godt gjennom og planlegges nøye. På veien mot endringer og forbedringer bør ALARP prinsippet benyttes, der man tar en kalkulert risiko. Er man redd for å innovere på IT-sikkerhetssiden fordi det kan føre til feil, kan man tape mer på å ikke innovere da man blir hengende etter trusselaktørene og mindre motstandsdyktige. Anbefalingene relatert til et bedre sikkerhet bunner i at det er lurt å starte i små steg på et risikofylt område. Inkrementell innovasjon kan bidra til å identifisere forbedringer i rutiner for å øke effektiviteten av oppdagelse og skadebegrensning mot et dynamisk angrep. Deretter kan en gå dypere til verks med semi-radikal innovasjon og se på forsvarsmekanismer basert på AI teknologi som vil kunne effektivisere manuelle stegene i forsvarsjobben mot disse angrepene. For angrep fra en avansert trusselaktør vil komme, enten det er gjennom eksterne eller interne eksponerte tjenester eller fordi en ansatt har brutt en regel i styringssystemet for informasjonssikkerhet (SFI).

En viktig del av min oppgave er å bidra til forbedring og her kommer oppsummering av konkrete anbefalinger basert på funnene i denne oppgaven:

- Revurder eierskap på nivå 3 dokumenter i styringssystemet for informasjonssikkerhet, slik at det ikke hemmer innovasjonsarbeidet på IT-siden og for å ta ned risikoen for brudd på sikkerhetsregler
- Sikkerhetsstaben må være kontinuerlig oppdatert på Skatteetatens dynamiske trusselbilde - Ikke vent på trusselrapporter som utgis en gang i året eller regulatoriske endringer for å gjennomføre endringer
- Benytt automatisering og AI på forsvarssiden
- Forankring og planlegging av innovasjon på sikkerhetssiden, gjennom kalkulert risiko, er nødvendig

8 Referanser

Berg, T. (2019, 29. August). Her er Norges 25 mest innovative virksomheter! *Innomag*. Hentet fra https://www.innomag.no/

Bergsjø H. & Windvik, R. (2018). *Datasikkerhet for ledere*. Oslo: Universitetsforlaget.

Blythe, J., Koppel,R. & Smith, S. (2013). Circumvention of Security: Good Users Do Bad Things. *Security & Privacy, IEEE*. 11. 80-83. https://doi.org/10.1109/MSP.2013.110

Borrett M., Carter R. & Wespi A. (2013). How is cyber threat evolving and what do organisations need to consider? *Journal of Business Continuity & Emergency Planning 7(1),* 163-171.

Capgemini. (2019) *World Payments Report 2019.* Hentet fra https://www.mynewsdesk.com/no/capgemini-norge/documents/world-payments-report-2019-90346

Columbus, L. (2020, 5. april). 2020 Roundup Of Cybersecurity Forecasts And Market Estimates. *Forbes*. Hentet 29. mai 2020 fra https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/

Darpa (2016, 4. august) "Mayhem" Declared Preliminary Winner of Historic Cyber Grand Challenge. Hentet 24. mai 2020 fra https://www.darpa.mil/news-events/2016-08-04

Davila, T., Epstein, M. & Shelton, R. (2007). *Making innovation Work*. Upper Saddle River, NJ: Wharton School Publishing

Departementene. (2019). *Norges strategi for digital sikkerhet.* (Strategi G-0444 B) Hentet fra https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Dobbs R., Manyika J. & Woetzel J. (2015). *The four Global Forces Breaking all the trends.* Mckinsey. Hentet fra https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-four-global-forces-breaking-all-the-trends

Fagerberg, J., Mowery D.C. & Nelson R.R. (2006). *The Oxford handbook of Innovation*. Oxford; New York: Oxford University Press.

Gjelsvik, M. (2007). *Innovasjonsledelse.* Bergen: Fagbokforlaget

Gordon, S., Tarafdar, M., Cook, R., Maksimoski, R. & Rogowitz, B. (2008). Improving the Front End of Innovation with Information Technology. *Research-Technology Management. 51.* 50-58. https://doi.org/10.1080/08956308.2008.11657505

Györy, A., Cleven, A., Uebernickel, F. & Brenner, W. (2012). Exploring The Shadows: IT Governance Approaches To User-Driven Innovation. *ECIS 2012(222).*

Heldal, F. & Dehlin, E. (2017). Drop your rules! i Antonsen, S., Heldal F. & Kvalheim S.A.(red) *Sikkerhet og ledelse* (1. utg.). Oslo: Gyldendal s. 63-82.

Hollnagel, E. (2010). *Resilience Engineering in Practice.* Aldershot, UK: Ashgate.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Farnham, UK: Ashgate

ISO-standards, "STANDARDS", Hentet 29. mai 2020 fra https://www.iso.org/standards.html

James, T., Khansa, L., Cook, D. & Bruyaka, O. (2013). Using network-based text analysis to analyze trends in Microsoft's security innovations. *Computers & Security. 36.* 49–67. https://doi.org/10.1016/j.cose.2013.02.004

Johannessen, J.A. (1994). Information Technology and Innovation: Identifying Critical Innovation Factors. *Inf. Manag. Comput. Security*. 2. 4-9. https://doi.org/10.1108/09685229410059532

Johansen, J.P., Almklov, P.G. & Mohammad, A.B. (2016). What can possibly go wrong? Anticipatory work in space operations. *Cogn Tech Work* 18, 333–350. https://doi.org/10.1007/s10111-015-0357-8

Johnsen S. (2016). MITIGATING EMERGENT VULNERABILITIES IN OIL AND GAS ASSETS VIA RESILIENCE. *Critical Infrastructure Protection X*, 43–61. https://doi.org/10.1007/978-3-319-48737-3

Khansa, L. & Liginlal, D. (2007). The Influence of Regulations on Innovation in Information Security. *AMCIS 2007 Proceedings*. 180. http://aisel.aisnet.org/amcis2007/180

Kommunal- og moderniseringsdepartementet (2020). *Nasjonal strategi for kunstig intelligens.* (Strategi H-2458 B) Hentet fra https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

Kongsvik, T., Albrechtsen E., Antonsen, S., Herrera, I.A., Hovden, J. & Schiefloe, P.M. (2018). *Sikkerhet i arbeidslivet* (1. utg.). Oslo: Fagbokforlaget

Kotulic, A. & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management. 41*. 597-607. https://doi.org/10.1016/j.im.2003.08.001

Lord, N. (2018, 14. Desember). Uncovering Password Habits: Are Users' Password Security Habits Improving? *DataInsider.* Hentet fra https://digitalguardian.com

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn*. Oslo: Justis- og beredskapsdepartementet

NSM. (2020). *Nye krav til tryggleik.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-aarsrapport-2019_enkelts_3004.pdf

Ruefle, R. (2007, 24. Januar). Defining Computer Security Incident Response Teams. Hentet 29. mai 2020 fra https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

Ružičić, V. & Micic, Z. (2017). Creating a Strategic National Knowledge Architecture: A Comparative analysis of knowledge source innovation in the ICS subfields of multimedia and IT security. *Computers & Security. 70*. https://doi.org/10.1016/j.cose.2017.07.007

Skybox Research Lab. (2019) *VULNERABILITY AND THREAT TRENDS.* Hentet fra https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_and_Threat_Trends_2019.pdf

Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis* (3. utg). Oslo: Gyldendal

Tomter L., Remen A.C. & Helljesen V. (2018, 14. juni). Helse Sør-Øst skroter milliardavtale om utflagging av IT*. NRK*. Hentet 10. oktober 2019 fra https://www.nrk.no

Tomter L., Remen A.C. & Wernersen C. (2017, 30. juni). Statoil henter hjem sikkerhetskritiske IT-oppgaver fra India. *NRK*. Hentet 10. oktober 2019 fra https://www.nrk.no

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management. 49*(3-4). 190–198. https://doi.org/10.1016/j.im.2012.04.002

9 Vedlegg

9.1 Skatteetatens overordnede policy for informasjonssikkerhet (SFI-1.1)

Skatteetatens overordnede policy for informasjonssikkerhet (SFI-1.1)

Versjon 2.1

2. desember 2019

Godkjenning

Skattedirektøren godkjenner Skatteetatens overordnede policy for informasjonssikkerhet (dette dokumentet). For nivå 2, spesifikke sikkerhetspolicyer, og nivå 3, sikkerhetsstandarder, sikkerhetsinstrukser og sikkerhetsveiledninger, kan godkjenning delegeres til sikkerhetsdirektør.

Iverksettelse

Denne policyen etterfølger versjon 2.0 fra den dag Skattedirektøren har godkjent versjonen. Spesifikke policyer og standarder i styringssystemet gis iverksettelsesdato ved godkjenning.

Etter iverksettelsesdato skal elementene i styringssystemet anvendes for all løpende manuell aktivitet i etaten, og for alle krav / spesifikasjoner til nye IT-systemer og –løsninger. Eksisterende systemer skal normalt tilpasses til dette styringssystemet for informasjonssikkerhet ved neste hovedversjon. For gamle systemer der det ikke er sikkerhetsmessig lønnsomt å gjøre inngrep før systemet erstattes, og der systemet og rutinene totalt sett ligger innenfor akseptabel risiko, kan avvik aksepteres fram til avvikling.

Versjonshåndtering

Dette dokumentet angir Skatteetatens overordnede målsetting og strategi for informasjonssikkerhet. Dokumentet er basert på trusselbildet og utviklingstrender per november 2019. Oppdateringer kan være påkrevd ved endringer i forretningsmessige behov, organisasjonen eller større endringer i trusselbildet. Sikkerhetsstaben har ansvar for å vurdere oppdatering en gang per år i forbindelse med ledelsens gjennomgang, eller ved behov.

INNHOLD

Innledning

Skatteetaten har en sentral rolle i det norske samfunn gjennom sitt ansvar for fastsetting og innkreving av skatter og avgifter og føring av et sentralt folkeregister. Dette medfører forvaltning av store mengder informasjon om virksomheter og enkeltpersoner, noe som stiller høye krav til sikkerhet. Informasjons-sikkerhet i Skatteetaten er viktig for å sikre tillit og respekt hos borgerne slik at etaten oppnår god etterlevelse og effektiv beskatning og folkeregistrering.

Informasjon kan finnes i mange formater og utgaver. Den kan være trykket eller skrevet på papir, lagret elektronisk, sendt per post eller elektronisk, vist på film eller uttrykt muntlig. Uavhengig av hvordan informasjonen foreligger, må den ha tilfredsstillende beskyttelse gjennom sikkerhetstiltak som gir akseptabel risiko. Krav til sikkerhet gis av bestemmelser i lover og forskrifter, nasjonale retningslinjer for informasjonssikkerhet samt Skatteetatens egen fastsettelse av akseptabelt risikonivå.

Den informasjon som Skatteetaten besitter skal ikke benyttes til aktiviteter i strid med lov- og regelverk og etatens ansvar og interesser. Skatteetatens IT-systemer og tjenester er tilrettelagt for å støtte saksbehandlingen i etaten og skal benyttes med dette utgangspunktet.

Større krav til samhandling og digitalisering av informasjonstjenester medfører at Skatteetaten øker sin eksponering. Dette gir mer synlighet i samfunnet, høyere krav til tilgjengelighet og sikring, samt forventninger og leveringsevne til og fra andre etater, skattyter/borger, parter og partnere.

Hva er informasjonssikkerhet?

Informasjonssikkerhet omfatter i praksis alle aktiviteter som iverksettes for å sikre korrekt og sikker håndtering og formidling av informasjon. Informasjonssikkerhet er definert som ivaretakelse av egenskapene:

- **Konfidensialitet**: Informasjon er beskyttet mot innsyn fra uautoriserte.
- **Integritet**: Informasjon er korrekt og kan kun oppdateres som følge av autoriserte handlinger. Oppdateringer skal være dokumentert og sporbare til person som har utført handlingen.
- **Tilgjengelighet**: Informasjon er tilgjengelig for autoriserte til rett tid.

Kriteriene kan basert på en risikovurdering, gis ulik prioritet ut fra informasjonens egenskaper eller påtenkte anvendelse. Informasjonssikkerhet favner over hele sikkerhetsområdet inkludert fysisk sikkerhet, kontinuitet, beredskap, mislighold og personellsikkerhet.

Styringssystem for informasjonssikkerhet

Skatteetatens Styringssystem For Informasjonssikkerhet (SFI) består av en overordnet sikkerhetspolicy (dette dokumentet) som er forankret hos etatens øverste ledelse og spesifikke sikkerhetspolicyer som skal forankres på riktig nivå og i riktige organisasjonsenheter i linjen avhengig av innhold og målgruppe. Den overordnede

policyen gir føringer for alle sikkerhetspolicyene for håndtering av sikkerhet, mens de spesifikke sikkerhetspolicyene setter krav til informasjonssikkerhet på underliggende sikkerhetsområder.

Følgende liste er områder innenfor informasjonssikkerhet der spesifikke sikkerhetspolicyer er godkjente:

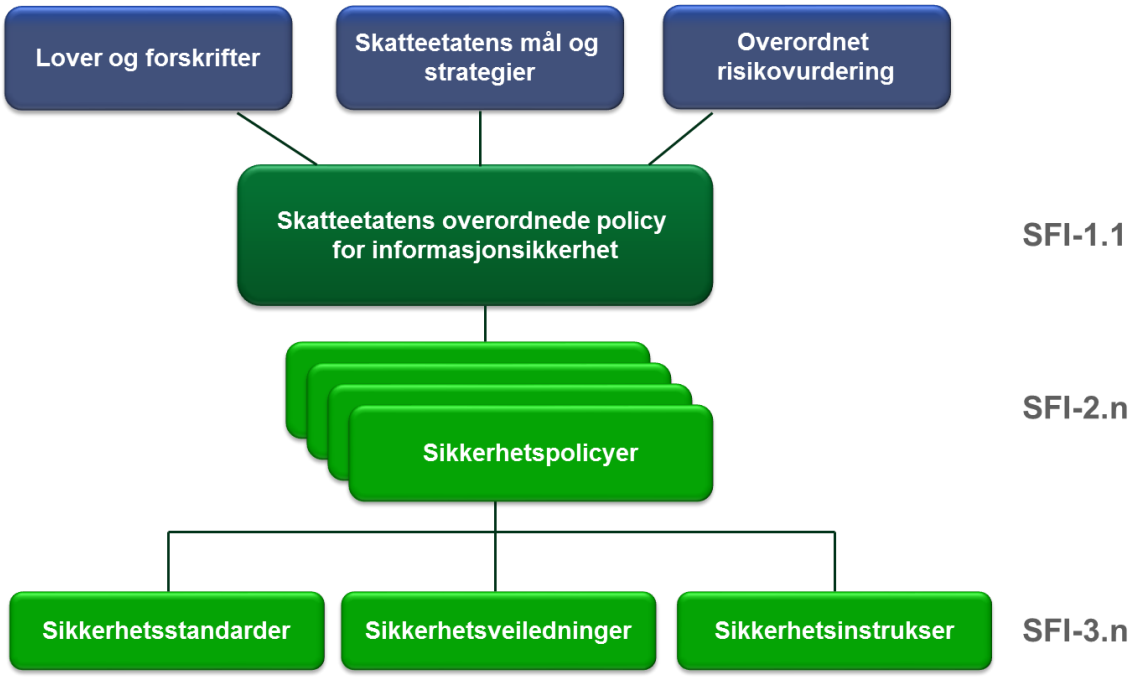
- Sikkerhetsansvar
- Risikostyring av sikkerhet
- Internkontroll av informasjonssikkerhet
- Personellsikkerhet
- Identitetsforvaltning
- Sikkerhetsgradert informasjon
- Sikkerhet i informasjonshåndtering
- Driftssikkerhet
- Nettverkssikkerhet
- Kontinuitet
- Fysisk sikkerhet
- Systemsikkerhet
- Logging
- Kryptografi

Med basis i spesifikke policyer foreligger nødvendige sikkerhetsstandarder, sikkerhetsinstrukser og/eller sikkerhetsveiledninger:

- *Sikkerhetsstandarder* er detaljerte beskrivelser av hvordan sikkerhetskravene i en policy oppfylles. En standard kan i noen tilfelle inneholde mer detaljerte krav til hvordan sikkerhet skal løses for eksempel i ulike IT-systemer. Det kan være flere standarder som understøtter en policy.
- *Sikkerhetsinstrukser* beskriver konkret sikkerhetsansvar og oppgaver/prosesser tillagt ulike ansatte og/eller funksjoner i Skatteetaten, for eksempel brukere, ledere, driftspersonell og sikkerhetspersonell.
- *Sikkerhetsveiledninger* er gode råd, forklaringer og hjelp til implementering av informasjonssikkerhet. Dokumentene skal forankres på riktig nivå i organisasjonen avhengig av innhold og målgruppe.

Dokumentene som utgjør styringssystemet for informasjonssikkerhet (SFI) er delt i nivåer i henhold til beskrivelsen ovenfor. Overordnet policy er på nivå 1, de spesifikke policyene er på nivå 2 og tilhørende standarder, instrukser og veiledninger er på nivå 3. Nummereringen av dokumentene bygges opp i henhold til dette.

Strukturen på styringssystemet for informasjonssikkerhet er visualisert i følgende figur:



Mål og strategi for informasjonssikkerhet

Den overordnede policyen for informasjonssikkerhet har, i samsvar med den internasjonale standarden ISO/IEC 27002, som mål å sikre ledelsens styringssignaler og støtte i forebyggende sikkerhetsarbeid. Styringssystemet skal være en integrert del av etatens totale styringsprosess.

Skatteetatens mål og strategi for informasjonssikkerhet skal understøtte etatens mål og virksomhetsstrategier. Den skal både understøtte og tas hensyn til i etatens IT-strategi.

Hovedmål for informasjonssikkerhet

Skatteetaten har følgende hovedmål for informasjonssikkerhet:

- Informasjonssikkerhet i Skatteetaten bidrar til at etaten oppfyller krav i lover og forskrifter.
- Etatens informasjon, IT-systemer, anlegg, bygninger, kontorer og verdier beskyttes slik at konsekvensene ved sikkerhetsbrudd ikke er større enn det ansvarlig ledelse vurderer som akseptabelt risikonivå.
- Informasjonssikkerhet i etaten bidrar til et godt omdømme og til å opprettholde tillit til norsk offentlig forvaltning, skattyter/borger og etatens partnere.
- Informasjonssikkerheten bidrar til at etaten når etatens mål og følger etatens strategier med hensyn til akseptabel risiko.
- Etatens informasjonssikkerhet understøtter nasjonale retningslinjer for informasjonssikkerhet og internasjonale retningslinjer for informasjonssikkerhet gitt fra OECD.
- Etatens ansatte og avtalepartnere er bevisste på sikkerhetsbestemmelser og overholder disse.
- Etaten har akseptabel virksomhetskontinuitet ved uforutsette hendelser.

Strategiske virkemidler

I samsvar med ISO/IEC 27002 og personopplysningsloven med forskrifter samt andre relevante lover og forskrifter skal risikovurderinger og basis sikkerhetskrav fastlagt i styringssystem for informasjonssikkerhet legges til grunn for sikkerhetstiltak. Iverksatte sikkerhetstiltak skal gjennomgås og revideres på basis av regelmessig gjennomførte risikovurderinger.

Følgende strategiske virkemidler er identifisert som spesielt viktige:

- Ledelsesforankring og ledelsesgjennomgang
- Et effektivt styringssystem for informasjonssikkerhet
- Veldefinerte prosesser for beslutning og aksept av risiko
- Internkontroll
- Kontinuerlig opplæring, bevisstgjøring og holdningsskapende arbeid
- En risikobasert tilnærming
- Teknologiske, personellmessige, organisatoriske og fysiske sikringstiltak basert på identifisert risiko
- En organisasjon med evne til oppdagelse, reaksjon, håndtering og evaluering av uønskede hendelser
- Ansvarliggjøring av aktivitet og handlinger
- Kontinuitetsplanlegging og øvelser i krisehåndtering
- Sikkerhetsrevisjoner og uavhengige sikkerhetstester
- Sertifisering av eget personell
- Kvalitetssystem med gode prosesser
- En imøtekommende, profesjonell og nytenkende sikkerhetsorganisasjon

Viktige styringsprinsipper

Arbeidet med informasjonssikkerhet i Skatteetaten følger en del viktige styringsprinsipper:

i. **Akseptabelt risikonivå**

Oppbevaring og behandling av informasjon med tilhørende IT-systemer og rutiner i Skatteetaten skal basere seg på risikovurdering og holde seg innenfor akseptabelt risikonivå.

Ved kryssende sikkerhetsbehov skal behovene for sikring av konfidensialitet og integritet som hovedregel gå foran hensynet til tilgjengelighet.

ii. **Sikkerhetsmessig lønnsomhet**

For hendelser som etter en risikovurdering havner i området der tiltak skal vurderes, gjelder prinsippet om sikkerhetsmessig lønnsomhet. Et sikkerhetstiltak skal normalt koste mindre i anskaffelse og drift enn det koster å leve med den risiko tiltaket vil eliminere. Før etablering av prioriterte tiltak skal derfor ansvarlig ledelse vurdere hvilke kostnader tiltaket medfører, målt opp mot den nytte og de fordeler som redusert risiko kan medføre. Hendelser med særlig høy konsekvens skal vurderes nærmere selv om sannsynligheten er lav.

iii. **Minste privilegiums prinsipp**

Ansatte og avtalepartnere skal bare gis tilgang til de IT-systemer og den informasjon vedkommende har behov for i sitt arbeid. Skatteetaten skal praktisere minste privilegiums prinsipp, slik at akseptabel sikkerhetsrisiko oppnås ved avveiing mellom behovet for sikkerhetstiltak, behovet for fleksibel og effektiv administrasjon og oppgaveløsning, samt behov for informasjonsutveksling som virkemiddel for samarbeid og kompetanseutvikling.

iv. **Arbeidsdeling**

Ansvarlige ledere skal så langt praktisk mulig innføre arbeidsdeling ved utførelse av kritiske oppgaver innen sitt ansvars- og myndighetsområde. Arbeidsdeling innebærer at forskjellige personer utfører ulike arbeidssteg for å fullføre oppgaven. På denne måten reduserer etaten muligheten for at enkeltpersoner kan utføre vinningskriminalitet eller på annen måte undergrave tillit til Skatteetaten eller skade etatens omdømme.

v. **Eierskap til produkter og interne tjenester**

Ansvaret for produkter og interne tjenester er plassert i linjen. Ansvarlige i linjen skal klassifisere produkter og tjenester med utgangspunkt i det aktuelle bruksområdet og den informasjon som behandles. Formålet er å indikere den kritikalitet produktet/tjenesten har for Skatteetaten. Ansvarlige i linjen har også ansvar for gjennomføring av risikovurdering av informasjonssikkerhet jevnlig og ved endringer som påvirker risikobildet.

vi. **Sikkerhet i dybden**

Etatens tjenester og løsninger skal utformes slik at prinsippet om sikkerhet i dybden ivaretas. Prinsippet setter krav om at det skal eksistere flere lag av uavhengige sikkerhetsmekanismer. Hensikten er å øke vanskelighetsgraden av å kunne gjennomføre en uønsket hendelse ved å måtte passere flere lag enn kun ett, samt at èn feil i et lag ikke alene vil resultere i en uønsket hendelse.

vii. **Sikkerhetsbetingelser for avtalepartnere**

Tredjepart som skal ha tilgang til Skatteetatens informasjon eller IT-systemer, skal inngå en kontrakt som inneholder eller refererer til alle nødvendige krav for å sikre overensstemmelse med etatens styringssystem for informasjonssikkerhet.

Akseptabelt risikonivå

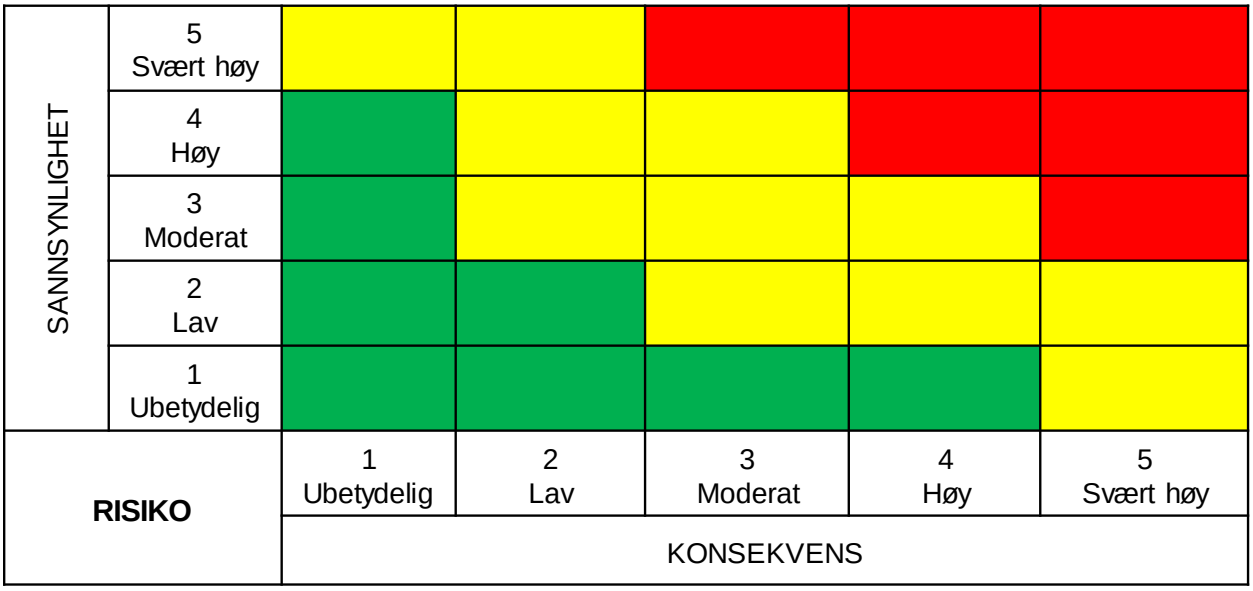
Ved fastsetting av akseptabelt risikonivå, er følgende generelle målsetting lagt til grunn:

- Det er et mål at personer utenfor Skatteetaten ikke skal kunne forårsake hendelser med høy konsekvens for enkeltmenneskers personvern, bedrifters konkurransesituasjon, Skatteetatens evne til å levere tjenester eller det norske samfunnet
  - gjennom sosial manipulering av medarbeidere i etaten, eller
  - med mindre de samarbeider med utro tjenere i nøkkelposisjoner internt i etaten.
- Det er et mål at egne medarbeidere ikke skal kunne forårsake hendelser med høy konsekvens for enkeltmenneskers personvern, bedrifters konkurransesituasjon, Skatteetatens evne til å levere tjenester eller det norske samfunnet,
  - med mindre de har spesialiserte ressurser og god/fullstendig kjennskap til

sikkerhetstiltak, eller
- det er flere som samarbeider.

- Det er et mål at egne medarbeidere ikke uaktsomt skal kunne forårsake hendelser med høy konsekvens for enkeltmenneskers personvern, bedrifters konkurransesituasjon, Skatteetatens evne til å levere tjenester eller det norske samfunnet.
- Det er et mål at fysiske hendelser ikke skal gi høy konsekvens for enkeltmenneskers personvern, bedrifters konkurransesituasjon, Skatteetatens evne til å levere tjenester eller det norske samfunnet.

Akseptabelt risikonivå er oppsummert i figuren nedenfor.



De ulike nivåene er beskrevet i *SFI-3.19 Standard for risikostyring av informasjonssikkerhet*.

Ansvar og organisering

Førende krav til ansvarsfordeling og organisering av forebyggende sikkerhetsarbeid er beskrevet i personopplysningsloven, sikkerhetslovens forskrift om sikkerhetsadministrasjon og den internasjonale standarden ISO/IEC 27002.

Skattedirektørens ansvar

Skattedirektøren er virksomhetsleder for hele Skatteetaten og har derfor det overordnede ansvar for styring og kontroll med etatens informasjonssikkerhet. Overordnet policy for informasjonssikkerhet skal godkjennes av skattedirektøren.

Øvrige lederes ansvar

Ivaretakelse og kontroll av informasjonssikkerhet er integrert i etatens aktiviteter. Enhver leder har ansvar for informasjonssikkerheten innen sitt ansvars- og myndighetsområde, og for oppfølging som en integrert del av etatens internkontroll. Dette innebærer at leder har et ansvar for å føre tilsyn med at aktuelle sikkerhetstiltak som er iverksatt for å beskytte data som vedkommende har et ansvar for fungerer etter hensikten. Dersom en slik kontroll avdekker at tiltakene ikke virker etter hensikten, må det foretas en vurdering av nye/endrede tiltak. Ansvaret gjelder også der utførelsen av sikkerhetsoppgaver er overlatt til avtalepartnere og andre virksomheter.

Enhver leder skal:

- ta ansvar for informasjonssikkerhet innen sitt respektive ansvars- og myndighetsområde
- påse at sine medarbeidere har en atferd som bidrar til å ivareta sikkerheten
- veilede sine medarbeidere, og søke bistand hvis nødvendig
- påse at vedtatte sikkerhetstiltak er iverksatt og fungerer etter hensikten
- varsle linjen oppover samt sikkerhetsdirektør ved hendelser som har medført, eller kan medføre sikkerhetsrisiko

Den enkeltes ansvar

Faste og midlertidige ansatte, samt innleid personell, skal i sitt arbeid / oppdrag for etaten medvirke til en effektiv sikkerhetstjeneste. Personellet skal:

- overholde sikkerhetsinstruks for brukere
- kjenne til overordnet policy for informasjonssikkerhet og policyer relevant for sitt arbeidsområde
- kjenne til prinsippene for risikostyring
- påpeke feil og mangler ved sikkerheten og sikkerhetstjenesten
- omgående rapportere sikkerhetstruende hendelser til nærmeste leder og/eller sikkerhetsdirektør

Etatens Sikkerhetsstab

I samsvar med sikkerhetsloven og andre relevante lover skal skattedirektøren ha utpekt en sikkerhetsdirektør med stedfortreder og et tilstrekkelig antall personer i en Sikkerhetsstab i forhold til etatens sikkerhetsbehov.

Sikkerhetsstaben skal ha myndighet innenfor sitt ansvarsområde i hele Skatteetaten. Sikkerhetsdirektøren skal rapportere direkte til skattedirektør ved kritiske sikkerhetshendelser eller ved observerte situasjoner som medfører høy risiko.

Sikkerhetsstaben skal dekke skattedirektørens behov for styringssystemer, fagkompetanse og oppfølging innenfor informasjonssikkerhet, inkludert fysisk sikkerhet og beredskap. Sikkerhetsstaben har en viktig rolle i forhold til å stille krav, gi føringer og følge opp utviklingsprosjekter. Sikkerhetsstaben skal tidlig involveres i arbeidet med spesifisering, design, utvikling og implementering for å sikre en kosteffektiv tilnærming til at løsninger har akseptabel risiko. Sikkerhetsstaben skal formidle styringssystemet for informasjonssikkerhet på en hensiktsmessig måte til alle ansatte og avtalepartnere.

9.2 Intervjuguide dybdeintervju

Oppvarming

1. Hva er din alder?
2. Hva er din rolle og avdeling?
3. Hvor lenge har du jobbet i etaten?
4. Hva er din bakgrunn/utdanning? Fra hvilket år?
5. Hvordan ser arbeidsdagen din ut til daglig?
6. Føler du at du får utnyttet dine ressurser og kunnskaper fullt ut i innovasjonsarbeidet?
7. Med utgangspunkt i arbeidsprosessen deres, hva er du mest opptatt av ift arbeidet ditt? Eks: At en idè skal kunne implementeres raskt og effektivt? At den skal dekke et stort behov?

Hoveddel

8. Hvilke utfordringer har dere i deres dagligdagse arbeid? Eks: Er det noe som bremser opp eller som ikke utnytter potensialet til ressursene og kunnskapene i innovasjonsarbeidet?
9. Føler du at du i ditt dagligdagse arbeid har en sikker arbeidsplass? I form av at informasjonsbehandlingen er trygg på enhetene i arbeidsprosessene deres?
10. Vil du anse en innovasjonsarbeidet som konkurransesensitivt? Hva om andre stjeler ideèn din og tjener penger på den eller får berømmelse pga den?
11. Har du vært borti, enten ved denne arbeidsplass eller tidligere, at arbeidet ditt eller kollegaens har kommet på avveie? Hvis ja, fortell mer om det.
12. Har dere eget spesialutstyr eller bruker dere standardutstyr med sikkerhetsmekanismer?
13. Foretrekker du å arbeide uten noen form for begrensninger på det digitale utstyret, som for eksempel på pc'en din, eller ser du på sikkerhetsmekanismene rundt arbeidsflaten din som en trygg ramme/lekekasse?
14. Hvilke sikkerhetsmekanismer ser du på som unødvendige og hvorfor?
15. Omgår du noen av sikkerhetsmekanismene for å utnytte potensialet i en idè i arbeidet ditt? Hvor ofte?
16. Anser du sikkerhetstankegangen i etaten som lite innovativt og rigid eller fleksibelt og imøtekommende ift ditt arbeid?
17. Kjenner du til styringssystemet for informasjonssikkerhet (SFI)?
18. Føler du at SFI hemmer innovasjonsarbeidet? I så fall, kan du utdype?
19. Hvem samarbeider du med vanligvis i arbeidet ditt?
20. Hvordan er samarbeidet med sikkerhetsavdelingen i Skatteetaten?
21. Hvor ofte har dere kontakt med sikkerhetsavdelingen og hvilke problemstillinger taes opp der?
22. På hvilken måte inkluderer dere sikkerhetsavdelingen i deres arbeid med innovasjon og strategimålene til etaten?
23. Kjenner du til informasjonssikkerhetsstrategien i etaten?
24. Kjenner du til prosesser for å innovere informasjonssikkerhet? I så fall hvilke?
25. Hvor ofte har du vært involvert i innovasjonsarbeid relatert til et sikkerhetstema?
26. Har din avdeling vært involvert i utarbeidelsen av informasjonssikkerhetsstrategien i etaten?
27. Er din avdeling involvert i utarbeidelsen av andre strategier enn dets egen eller etatens overordnede strategi?
28. Hvor tidlig involverer dere sikkerhet i innovasjonsarbeidet? I hvilken fase mtp arbeidsprosessene deres?

Avslutning

29. Ser du på sikkerhet og innovasjon som to motsetninger?
30. Tror du Sikkerhet kunne ha behov for å være mer innovative?
31. Hva er dine råd for et bedre og mer innovativt sikkerhet?
32. Er det noe du ønsker å få frem som vi ikke har tatt opp her?

9.3 Spørsmål og svar fra spørreskjema

Spørsmål til IT- sikkerhet 2020

(Spørsmål 1)

IT-sikkerhet 2020 Vennligst oppgi din alder:

24 - 34 år	2	22,2 %
35 - 44 år	4	44,4 %
45 - 54 år	3	33,3 %
55 år eller eldre	0	0,0 %
Total	9	100,0 %

(Spørsmål 2)

Antall år i etaten:

0 - 3 år	2	22,2 %
4 - 7 år	5	55,6 %
8 - 11 år	0	0,0 %
12 år eller fler	2	22,2 %
Total	9	100,0 %

(Spørsmål 3)

Hva er ansvarsområdet ditt?

IRT	N/A	N/A
Overvåking	N/A	N/A
Gjenoppretting/backup	N/A	N/A
Logger	N/A	N/A
Analyse	N/A	N/A
Total	9	100,0 %

(Spørsmål 4)

Jobber du med å stoppe/oppdage mistenkelig aktivitet/angrep?

Ja	9	100,0 %
Nei	0	0,0 %
Total	9	100,0 %

(Spørsmål 5)

Føler du at angrepene har blitt vanskeligere å oppdage de siste to årene? (1)

1Tvert i mot det har blitt enklere	N/A	N/A
2Noe enklere	N/A	N/A
3Det er ingen endring	N/A	N/A
4Noe vanskeligere	N/A	N/A
5Mye vanskeligere	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 5)

Føler du at angrepene har blitt vanskeligere å stoppe de siste to årene? (2)

1Tvert i mot det har blitt enklere	N/A	N/A
2Noe enklere	N/A	N/A
3Det er ingen endring	N/A	N/A
4Noe vanskeligere	N/A	N/A
5Mye vanskeligere	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 6)

Hvem av disse mener du utgjør den største trusselaktøren til Skatteetaten?

Utro tjener/ansatt/konsulent	N/A	N/A
Ekstern hacker (enkeltperson)	N/A	N/A
Organisert kriminell gruppe	N/A	N/A
Statlig etterretningstjeneste	N/A	N/A
Andre, beskriv:	N/A	N/A
Total	9	100,0 %

(Spørsmål 7)

Mener du, på generelt grunnlag, at dere har gode nok metoder, prosesser og verktøy til å oppdage angrep eller mistenkelig trafikk før brudd på IKT har inntruffet? (1)

1Nei, vi klarer ikke å oppdage det	N/A	N/A
2Det er sjelden vi oppdager det	N/A	N/A
3Vi oppdager det i halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 8)

Mener du, på generelt grunnlag, at dere har gode nok metoder, prosesser og verktøy til å stoppe angrep eller mistenkelig trafikk før brudd på IKT har inntruffet? (1)

1Nei, vi klarer ikke å stoppe det	N/A	N/A
2Det er sjelden vi klarer det	N/A	N/A
3Vi stopper det i halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å oppdage et angrep fra en statlig aktør med store ressurser før brudd på IKT har inntruffet? (1)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A

Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å stoppe et angrep fra en statlig aktør med store ressurser før brudd på IKT har inntruffet? (2)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å oppdage et angrep fra en organisert kriminell gruppe før brudd på IKT har inntruffet? (3)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å stoppe et angrep fra en organisert kriminell gruppe før brudd på IKT har inntruffet? (4)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å oppdage et angrep fra ekstern enkeltperson før brudd på IKT har inntruffet? (5)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å stoppe et angrep fra ekstern enkeltperson før brudd på IKT har inntruffet? (6)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å oppdage et angrep fra en intern ansatt eller konsulent før brudd på IKT har inntruffet? (7)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 9)

Hvilke mulighet tror du dere har for å stoppe et angrep fra en intern ansatt eller konsulent før brudd på IKT har inntruffet? (8)

1Ingen mulighet	N/A	N/A
2Liten mulighet	N/A	N/A
3I halvparten av tilfellene	N/A	N/A
4I de fleste tilfeller	N/A	N/A
5I alle tilfellene	N/A	N/A
Total	9	100,0 %
AVG		N/A

(Spørsmål 10)

Hvor ofte mener du dere innoverer metoder, prosesser og verktøy for å øke oppdagelsen og begrense angrep? (1)

1Aldri	0	0,0 %
2Sjelden	1	11,1 %
3Noen ganger	2	22,2 %
4Ofte	6	66,7 %
Total	9	100,0 %
AVG		3,6

(Spørsmål 11)

Hvor mye ekspertbistand (intern eller ekstern) mener du dere får på innovasjon av deres metoder, prosesser og verktøy? (1)

1Ingen bistand	0	0,0 %

2Lite	1	11,1 %
3En del	5	55,6 %
4Mye	3	33,3 %
Total	9	100,0 %
AVG		3,2

(Spørsmål 12)

Hvordan holder dere metodene, prosessene og verktøyene effektive mot trusselaktørene til Skatteetaten?

Gjennom anerkjent benchmark	4	44,4 %
Med hjelp fra innovasjonsavdelingen i etaten	0	0,0 %
Gjennom kvalitetssikring hos Sikkerhetsstab	8	88,9 %
Gjennom egne tester og målinger	9	100,0 %
Vi gjør ingenting spesielt	0	0,0 %
Annet, beskriv:	3	33,3 %
Total	9	100,0 %

(Spørsmål 13)

Hva er den største utfordringen med å holde seg oppdatert på dagens trusselbilde for deg?

At trusselbildet stadig er i endring	8	88,9 %
For lite input/hjelp fra relevante miljøer	3	33,3 %
At angrepene blir mer avanserte	5	55,6 %
At angrepene er automatiserte og det går for raskt	5	55,6 %
At de kriminelle tar i bruk nye og bedre angrepsverktøy raskere	5	55,6 %
At det er få forsvarsmekanismer som er gode nok til å stoppe dagens trusselaktør	4	44,4 %
Noe annet, beskriv:	1	11,1 %
Total	9	100,0 %

NTNU
Kunnskap for en bedre verden

Skatteetaten