NSM: Prinsipalen for norsk cybersikkerhet?

Bacheloroppgave i statsvitenskap

Universitetet i Stavanger

Olav Persson Flatabø & Frida Fjeldstad

Studentnummer: 250903 / 250908

Kandidatnummer: 5532 / 5512

Veileder: Lars Gjesvik

Antall ord: 12983

SAMMENDRAG

Vi har i denne oppgaven undersøkt hvordan NSM og deres virkemidler er med på å påvirke sikkerheten i anskaffelser hos virksomheter tilknyttet kritisk infrastruktur. Konkret har vi hatt stor vekt på hvordan NSM har påvirket virksomhetens anskaffelser og verdikjeder. Dette er gjennomført gjennom en rekke kvalitative case-studier av virksomheter vi har ansett relevante for oppgaven: Kongsberg Satellite Services, Telenor, Lyse, Forsvarsdepartementet og Nedre Romerike Vannverk. For å belyse dette har vi tatt utgangspunkt Jensen & Mecklings prinsipal-agent teori (1976). Vi betegner i denne sammenhengen NSM som en overordnet aktør som gjennom ulike virkemidler insentiverer underlagte agenter til å holde sikkerheten til nivået ønsket av NSM. Som et andre trinn i analysen har vi pekt på et nytt PA-forhold: virksomhetene som prinsipal overfor sine underleverandører. På denne måten belyser oppgaven hvordan NSM direkte og indirekte virker inn på virksomhetene og deres anskaffelser.

Gjennom innholdsanalyser og semi-strukturerte intervjuer har vi identifisert og vurdert to former for virkemidler under NSM: sikkerhetsloven og veiledere - og med dette, et skille mellom myke og harde virkemidler. De viktigste funnene kan oppsummeres til at NSM har i varierende grad påvirket alle aktørene, særlig de som er underlagt og/eller forventer å underlegges sikkerhetsloven. Vi ser hos de samme virksomhetene at sikkerhetsfokuset knyttet til anskaffelser og verdikjeder er svært høyt. Som en slutning ser vi at NSM har en tydelig prinsipalrolle overfor virksomhetene og at dette kan sees i sammenheng med et tungt fokus på sikkerhet hos virksomhetene.

Innholdsfortegnelse

INNLEDNING

Introduksjon

Temaet for denne oppgaven er digital sikkerhet og hvordan vekting av digital sikkerhet påvirker anskaffelsesprosesser og underleverandører. Bakgrunnen for temaet er vår interesse for digital sikkerhet som et noenlunde nytt og svært viktig aspekt i samfunnet. Vårt globale verdenssamfunn er i konstant endring, og ifølge Nasjonal Sikkerhetsmyndighet (NSM) har den digitale utviklingen eskalert kraftig de siste årene. (NSM, 2020. s. 7-8). Det er viktig å holde tritt med den teknologiske utviklingen. Nye teknologiske løsninger har gjort det både enklere og mer effektivt for virksomheter, men det utgjør også større risikoer å benytte seg av en teknologi vi knapt kan holde følge med. Dermed blir fokuset på digital sikkerhet stadig viktigere, og vi er nødt til å tenke sikkerhet i flere ledd. Ettersom teknologi infiltrerer og påvirker samtlige kritiske infrastrukturer vi som samfunn er avhengig av er det viktig å vite hvordan vi skal tette hullene i sikkerhetssystemer.

Vi har sett en utvikling de siste årene der digitale angrep foregår mer og mer i det skjulte. Et eksempel på dette finner vi hos hackere, som har gått bort fra å infiltrere de store målene direkte, men går heller via underleverandører med mindre avansert sikkerhet. (Atlantic Council, 2019) Dermed har fokuset på digital sikkerhet skiftet fra å primært dreie seg om de større selskapene med og deres forvaltning av sensitiv informasjon, til å også omfavne mindre virksomheter. Det kom en ny sikkerhetslov i 2019 som fokuserer i mye større grad på digital sikkerhet enn hva den har tidligere, særlig krav om bedre sikkerhetsløsninger.

Med utgangspunkt i dette, er vi interessert i å se på hvorvidt private aktører med ansvar for kritisk infrastruktur i samfunnet vektlegger digital sikkerhet hos sine underleverandører i en anskaffelsesprosess. Her legger vi særlig vekt på de som benytter seg av tjenesteutsetting, og om deres fokus på digital sikkerhet påvirkes av NSM som offentlig sikkerhetsmyndighet. Dermed lyder problemstillingen som følger:

Hvordan påvirker NSM sine virkemidler den digitale sikkerheten i anskaffelser tilknyttet kritisk infrastruktur?

Avgrensning og struktur

Denne oppgaven er avgrenset til å omhandle vektleggingen av digital sikkerhet i anskaffelsesprosesser. Videre har vi avgrenset til virksomheter knyttet til kritisk infrastruktur i Norge. Ettersom vår ambisjon har vært å se på forholdet mellom aktørene i bestiller rollen og underleverandører har vi valgt å benytte Principal-Agent-teorien fra Jensen og Meckling (1976) som et teoretisk rammeverk. Videre ser oppgaven særlig nærme på hvordan NSM opptrer som sektorovergripende sikkerhetsmyndighet overfor virksomheter knyttet til kritisk infrastruktur, og hvordan de følgelig påvirker virksomhetenes sikkerhetsarbeid både direkte og indirekte.

Strukturen i oppgaven er lagt opp case-orientert, med en underordnet tematisk inndeling.

Oppgavens oppbygging

Denne oppgaven består av totalt 7 kapitler. I det kommende kapittelet vil det teoretiske rammeverket bli gjennomgått, der vi også i korte trekk vil gjøre rede for reformstrategien «New Public Management». I kapittel 3 vil den metodiske tilnærmingen bli gjennomgått, der vi presenterer vurderingene av valgene vi har tatt i den forbindelse. Kapittel 4 danner bakteppet for NSM og deres rolle i forbindelse med anskaffelsesprosessene vi vektlegger i denne oppgaven. I kapittel 5 presenteres den innsamlede og behandlede dataen innhentet fra intervjuene og rapportene vi har brukt som sekundærkilder. I kapittel 6 analyseres empirien med utgangspunkt i det teoretiske rammeverket. I det siste kapittelet presenteres konklusjonen for denne oppgaven, med avsluttende kommentar.

TEORI

I teoridelen vil vi først beskrive den politiske sammenhengen som er relevant for oppgaven vår ved å kort redegjøre for noen av trekkene ved New Public Management. Deretter vil vi redegjøre de delene av Prinsipal-agent-teorien som vi mener er anvendelige for å kunne undersøke problemstillingen. Videre vil vi drøfte om hvordan Prinsipal-agent-teori passer inn i arbeidet for cybersikkerhet i Norge.

Ettersom digitaliseringen har blitt svært fremtredende de siste tiårene, i kombinasjon med et omfattende samarbeid mellom privat og offentlig sektor, mener vi PA-teori blir en veldig relevant og viktig teori å belyse tematikken med for å sikre at aktørene i en slik kompleks verdikjede har sammenfallende interesser også når det gjelder cybersikkerhet.

New Public Management (NPM)

NPM refereres ofte til som en reformstrategi, der målet er å integrere markedsorientert tenkning inn i offentlig sektor. (Christensen, Egeberg, Lægreid, Aars, 2016, s.202-203) Utviklingen av dette begynte ved midten av 80-tallet, i samtid med Reagan og Thatcher sine styringsperioder. Det innebar en overgang fra de klassiske tunge og stive byråkratiene. De klassiske byråkratiene var stabile, strukturerte og forutsigbare, men var samtidig preget av tunge og ufleksible strukturer og var svært lite kostnadseffektive. Følgelig ble det lagt opp til å introdusere prinsipper fra markedet til offentlig sektor gjennom reformer.

Et sentralt virkemiddel for denne overgangen, var å i økende grad engasjere private aktører til å utføre arbeid på vegne av offentlige institusjoner. Samtidig ble ledelsestro et viktig tema - ledere på lavere nivåer ble delegert mer ansvar ved at de ble målt på resultater og måloppnåelse, fremfor å bli detaljstyrt gjennom byråkratiske reguleringer. Disse to momentene i kombinasjon førte til at private aktører fikk mulighet til å øke kostnadseffektiviteten drastisk innen virksomhet som i utgangspunktet var offentlig ansvar, men dette introduserte også en rekke nye interessekonflikter.

Prinsipal-agent-teori (PA)

Som teoretisk utgangspunkt har vi valgt å benytte oss av Principal-Agent-teori med opprinnelse fra Jensen og Meckling (1976).
Prinsipal-Agent-teorien beskriver forhold og problematikk som oppstår i sammenhenger der en aktør utfører en oppgave på vegne av noen andre. Parten som utfører arbeidet har da en agent-rolle, mens parten agenten handler på vegne av står som prinsipalen. Hovedproblemet teorien dreier seg rundt, er at interessene hos prinsipalen og interessene hos agenten er ikke nødvendigvis sammenfallende. Dette problemet betegnes som prinsipal-agent-problemet og er utgangspunktet for teorien.

Denne teorien har vært særlig sentral innenfor bedriftsøkonomi, da dette er treffende mellom ledere og medarbeidere i en organisasjon. Kanskje enda viktigere, finner vi dette forholdet mellom ledere og eiere i en organisasjon, der eierskap og kontroll over daglig drift er separert. Det antas at prinsipalen ønsker å optimalisere sin fortjeneste, mens innsats fra agenten er å anse som krevende og uønskelig. Dette kan lede til motstridende interesser. Agenten vil yte nok til å tilfredsstille uttrykte krav, men å jobbe videre for å ytterligere optimalisere resultatene, vil stride imot agentens interesser

Til tross for at prinsipal-agent-forhold ofte sees i sammenheng med bedriftsøkonomi, finner vi eksempler på denne typen forhold tilnærmet overalt.
Samtidig som kan dreie seg om en uformell transaksjonsavtale mellom to enkeltpersoner, kan prinsipal-agent forhold dreie seg om aktører på helt andre nivåer og andre former for nytte.
For eksempel kan en større offentlig institusjon bestille inn tjenester fra mindre underleverandører. Samtidig som kostnadseffektivitet er et sentralt fokus, har bærekraftige alternativer blitt mer og mer vektlagt. Samtidig vil de færreste bedrifter vektlegge bærekraft i seg selv, fremfor mulige inntekter. Dette betyr at partene i utgangspunktet har motstridende interesser.

Prinsipal-agent teori foreslår at slike tilfeller kan løses ved å kontraktfeste passende insentiver, som fører til at det blir i agentens egeninteresse å optimalisere arbeidet og dermed handle i tråd med prinsipalens egeninteresse. Det finnes mye utdypende PA-litteratur om akkurat hva disse insentivene skal være, men oppgaven vår vil handle om bruk av insentiver fra et generelt perspektiv. (Jensen & Meckling, 1976).

Prinsipal-agent og cybersikkerhet i Norge

Vi ønsker å se nærmere på hvordan denne tematikken kan anvendes innen statsvitenskapen. Lane (2013) beskriver i sin tekst to sentrale sider ved P-A i sammenheng med offentlig politikk og administrasjon.

Den første handler om forholdet mellom folket og de folkevalgte. Her vil folket ha rolle som prinsipalen, i det de velger frem politikere til å representere deres interesser.

Den andre varianten handler om forholdet mellom offentlige myndigheter og aktørene de involverer til å drifte funksjoner som er av samfunnets interesser, både offentlige og private. (Lane, 2013)

Disse forholdene har det blitt mange flere av, ettersom dagens utvikling innen kostnadseffektivitet og globalisering har ført til at nesten alle større operasjoner støtter seg på leverandørkjeder. (Telenor, 2020) Samtidig som dette har sine åpenbare fordeler, fører utviklingen innen automatikk og digitalisering til nye nivåer av kompleksitet og avhengigheter, som igjen fører til nye sårbarheter, både kjente og ukjente. Dette kan vi se komme til uttrykk gjennom Njå (2020) sin omtalelse av komplekse systemer i dagens samfunn der det som eksempel vises til hvordan vannforsyning i dag er avhengig av telekommunikasjon, software, hardware og energiforsyning. (Njå, 2020, s131)

En viktig del av oppgaven blir å se på bruk av insentiver, da insentiver vil lede virksomhetene til å oppfylle og maksimere kravene som vektlegges. Disse kan komme i form av økonomisk godtgjørelse, men kan også komme i form av forbud og ansvarliggjøring. (Kåre P. Hagen, 1990) Hvorvidt insentiver er i bruk i leverandørkjedene og deres effekt på berørte aktører vil være sentralt for å vurdere hvor anvendelig teorien er til empirien.

Vi har pekt ut en bestemt kategori av PA-forhold: forholdet mellom aktører som er ansvarlige for kritisk infrastruktur og deres bruk av underleverandører. Dette dreier seg både om offentlige og private aktører. Disse aktørene opererer med en overlapp av både prinsipal- og agentrolle, da de gjennom offentlig regulering pålegges å stille krav til sine underleverandører om digital sikkerhet.

Styrker og svakheter

Vi valgte å benytte oss av sentral litteratur fra Jensen & Meckling tilknyttet PA-teorien for å ha et teoretisk rammeverk til oppgavens senere drøfting og analyse. Til tross for at litteraturen frembringer viktige aspekter ved PA-teorien, er den avgrensende og det er ikke alle aspekter ved teorien vi kan anvende.

PA-teori er i utgangspunktet tilpasset mikroøkonomiske settinger og mye av litteraturen omhandler konkrete kostnader og konkrete midler for å motvirke ulempene PA-forhold leder til. For eksempel kan dette være å betale ansatte i form av aksjer og opsjoner hos bedriften de jobber på vegne av. (Jensen & Meckling, 1976) Samtidig som økonomisk insentiv har vært et sentralt resultat av NPM, er dette ikke et fremtredende virkemiddel i samarbeidet vi studerer. Insentiver som følger av sikkerhetsloven har snarere vært negative insentiver, da lovbrudd i ytterste konsekvens kan ende med dom og straff, både mot virksomhetene, men også mot enkeltpersoner. Kapittel 11 i sikkerhetsloven går inn på en rekke virkemidler som kan rettes mot de ansvarlige. For eksempel kan et forsettlig eller grovt uaktsomt brudd på taushetsplikten medføre bøter og fengselsstraff. (Sikkerhetsloven, 2019, kapittel 11)
Myndigheter har en veldig ulik prinsipal-rolle, sammenlignet med en typisk bedrift sin rolle overfor sine ansatte. Det offentlige systemet er i posisjon til å utforme og vedta lover, og videre kreve at underlagte virksomheter nærmest kompromissløst retter seg etter disse. Dette blir ulikt typiske insentivprogrammer som foreslås i Jensen & Meckling (1976), men likevel relevant, ettersom det sjeldent vil være i aktørenes egeninteresse å begå lovbrudd.

PA-forhold handler om implikasjonene ved å skille kontroll over driften fra de overordnede interessentene i arbeidet. Denne strukturen er svært relevant generelt innen politikken de siste tiårene, både ved desentralisering innen det offentlige, men også ved å inkludere private aktører i arbeidet rundt kritisk infrastruktur. Å belyse interesseforholdene i samarbeidet, vil være sentralt for å forstå dynamikkene de fragmenterte systemene. (Kåre P. Hagen, 1990)
Samtidig som vi måtte avgrense og til dels tilpasse litteraturen fra Jensen & Meckling, fant vi flere kilder som beskriver PA-forhold i moderne politikk. Dette ga oss både en forsikring om at teorien er anvendelig innen offentlig forvaltning, og bidro videre med faglige innspill vi kunne bruke for å utfylle redegjørelsen. Oppsummert har vi derfor vurdert PA til å være relevant for problemstillingen vår.

METODE

I denne delen av oppgaven skal vi gjøre rede for våre valg og begrunnelser knyttet til metodisk tilnærming. Vi har valgt en kvalitativ tilnærming, og benyttet oss av intervjuer samt offentlige dokumenter og artikler for å undersøke problemstillingen.

Tilnærming

Vi tok først utgangspunkt i cybersikkerhet som tema. Deretter oppsøkte vi faglitteratur og rapporter knyttet til cybersikkerhet. Disse fant vi ved å søke etter kilder på nettet gjennom nøkkelord vi plukket opp underveis, slik som verdikjedeangrep, sikkerhetsloven og sikkerhetsgraderte anskaffelser. Et gjennomgående tema er at begrensede ressurser og kompetanse i offentlig sektor har ledet til at norsk cybersikkerhet i svært høy grad er avhengig av offentlige og private virksomheter. Etter gjennomgang av tidligere fag, så vi at PA virket som et veldig relevant perspektiv og vi begynte å jobbe videre ut fra dette.

Vi så på muligheten for å forsøke å finne noen standardiserte variabler som kunne indikere noe om digital sikkerhet hos virksomheter, men konkluderte med at digital sikkerhet hos enkeltvirksomheter er rimelig individuelt og at vi heller burde undersøke færre virksomheter i dybden. Følgelig bestemte vi oss for å heller utføre en rekke case-studier, som både gir oss et grundig innblikk i noen større og viktige aktører og samtidig kan gi oss et bedre sammenligningsgrunnlag.

Da vi startet med utformingen av denne oppgaven så vi for oss å fokusere på private aktører knyttet til kritisk infrastruktur, med spesielt fokus på sikkerhetsloven. Etterhvert som vi gjennomførte intervjuene kom det frem et større fokus på NSM som tilsynsmyndighet og deres veiledere i tillegg til sikkerhetsloven, hvilket gjorde at vi omformulerte problemstillingen og spørsmålene vi stilte i de neste intervjuene.

Forskningsdesign

Denne oppgaven utføres med en kvalitativ tilnærming. Årsaken til dette er at tematikken vi ønsker å undersøke er svært omdiskutert og komplekst, og består av mange grå-soner. Skillet mellom kvalitativ og kvantitativ forskning går på hvorvidt studiet er case-orientert eller variabel-orientert.
Med et case-orientert studie har man mulighet til å endre forskningen underveis, og er mer interessert i helheten enn i enkelte variabler. Målet blir dermed å forklare hvordan noe skjer heller enn hvorfor noe skjer. (Ragin, 1999, s 1137-1138).

I denne oppgaven benytter vi oss av en iterativ prosess, hvilket er spesielt nyttig i en kvalitativ studie. Dette vil si at vi utvikler teori og data sammen ved å gå frem og tilbake, og koble det med ny innsikt. På denne måten oppnår vi gradvis en mer raffinert innsikt og forståelse. (Srivastava, P & Hopwood, N. 2009).

Denne prosessen står i kontrast med den rendyrkede hypotetisk-deduktive metoden der en starter med en forutinntatt hypotese og tester denne. Ettersom det er relativt lite kunnskap på området vi har valgt å undersøke, og dette er et nytt fagfelt for oss, vurderte vi oss frem til at en iterativ prosess er mest hensiktsmessig. Det har også vært begrenset med standardisert og offentlig tilgjengelig datamateriale. Dermed har vi brukt en blanding av rapporter, intervjuer og avisartikler. Dette medførte et begrenset antall caser, men har samtidig gitt oss muligheten til å gå i dybden på casene vi har. Det finnes flere styrker ved å fordype seg i færre caser, og metoden er bredt akseptert innen akademia. Blant annet argumenteres det for at det blir utfordrende å plukke opp på alle viktige områder ved hver case dersom utvalget blir for stort, hvilket kan resultere i et feilaktig inntrykk av helheten. På en annen side er det like vanskelig å få et helhetlig inntrykk med for få caser å ta utgangspunkt i. (Geertz, C. 2003)

Datainnsamling

Da vi begynte å se etter data, ble det fort tydelig at veiledende informasjon om cybersikkerhet og informasjon om tidligere sikkerhetshendelser var lett å få tak i på internett. Det var imidlertid svært få enkeltvirksomheter som legger ut utfyllende sikkerhetsrapporter, så selv om vi primært så etter informasjon virksomhetene har publisert selv, kom vi frem til at det ble behov for intervju i tillegg, hos de fleste virksomhetene.

Dataens validitet (gyldighet) og reliabilitet (pålitelighet) er et sentralt fokus i utvelgingen av metoder for innsamling av kvalitativ data. (Halvorsen 2018). Både dataen hentet fra intervjuene og sekundærkildene vi benyttet oss av har blitt analysert ved bruk av innholdsanalyse, som betyr at den mest relevante empirien er forenklet og senere fremstilt kategorisert etter case-studier og tematikk.

Vår sekundærdata er i all hovedsak Telenors årlige digital sikkerhetsrapport. Denne rapporten var svært informativ og relevant til temaet vårt, samt utfyllende nok om leverandørbruk til å kunne benyttes som case i seg selv. Rapporten hadde et eget kapittel dedikert til digital sikkerhet rundt bruk av underleverandører, noe som både ga oss et godt innblikk i Telenor, og var opplysende om hvilke problemstillinger som er på dagsorden. Dette hjalp oss videre med å finne ut hvilke spørsmål vi burde ta med videre til intervjuobjektene.
Vi fant frem til Kongsberg Satellite Services og Nedre Romerike Vannverk etter å ha lagt ut en post i en IT-gruppe på Facebook. Gjennom denne posten fikk vi kontakt med en relevant person i Forsvarsdepartementet, som hjalp oss med å komme i dialog med relevante aktører og avtale intervjuer. Disse informantene ble dermed rekruttert via snøballutvelging.[1]

Intervjuene

Da intervjuobjektene var på plass begynte vi å skissere opp en intervjuguide for å få tilstrekkelig informasjon om hvor mye virksomhetene vektlegger cybersikkerhet i anskaffelsesprosesser. Vi var interessert i å finne ut av hvorvidt store virksomheter med kritiske ansvarsområder vektla cybersikkerheten til sine underleverandører, om de benyttet seg av insentiver i form av krav for samarbeidet, eller om de anså underleverandørenes sikkerhetsnivå som mindre relevant dersom deres egen sikkerhet var sterk nok.

Intervjuguiden var semi-strukturert[2], der vi har latt kilden snakke relativt fritt innenfor rammer vi har satt.

[1] "Fra en informant får man oppgitt navnet fra andre informanter som det kan være aktuelt å intervjue, slik fortsetter det." (Halvorsen, 2014:164)

[2] «I denne metoden er spørsmålene forhåndsbestemt og de samme spørsmålene blir stilt til samtlige kandidater, i samme rekkefølge. Du velger selv oppfølgingsspørsmål ut ifra det kandidaten forteller og ikke ut fra det du vil at kandidaten skal fortelle om. Alle kandidater får altså samme hovedspørsmål, noe som gjør at alle behandles likt, samtidig som intervjuet til en viss grad formes ut ifra kandidatens svar.» (Academicwork, u.å.)

En av utfordringene semi-strukturerte intervjuer fører med seg, er at mye ligger på informantene. Vi tok utgangspunkt i intervjuguiden, men lot informasjonen vi fikk underveis føre samtalen naturlig dit informantene selv styrte den. Dette resulterte i at vi satt igjen med svært forskjellig informasjon fra de forskjellige virksomhetene. I tillegg er det viktig at informantene er tilstrekkelig motivert når en benytter seg av et semi-strukturert intervju.
Til tross for at alle informantene var engasjerte og motiverte under hele samtalen, opplevde vi litt forskjeller virksomhetene imellom. Noen snakket uoppfordret om flere aspekter og områder ved spørsmålene vi stilte, mens andre ga oss mer konkrete og lukkede svar. Dette er en svakhet ved oppgaven, som delvis har blitt løst ved å gå frem og tilbake underveis og knytte ny informasjon opp mot utviklingen av data og teori i en iterativ prosess.

Vi valgte å ta notater underveis i intervjuene, ettersom informantene godtok dette. Dermed byttet vi på hvem som ledet intervjuet, og hvem som transkriberte underveis. Vi opplevde denne måten å jobbe på som effektiv da vi hadde notatene ferdig transkribert med en gang, men noe utfordrende da det ikke var mulighet for å gå tilbake på ting vi var usikre på slik vi ville hatt mulighet til ved å benytte oss av båndopptager. Vi løste denne utfordringen ved å sende oppfølgingsspørsmål på e-post til de aktuelle virksomhetene.

Grunnet Covid-19 pandemien har gjennomføringen av intervjuene blitt løst på en annen måte enn ønsket. Vi hadde ikke mulighet til å møte med intervjuobjektene personlig, og tok samtalen over Teams. Dette medfører at vi mister muligheten til å lese kroppsspråk, og skaper en noe kunstig setting. På en annen side eliminerer vi risikoen for undersøkelseseffekten[3], hvilket styrker oppgavens reliabilitet.

Styrker og svakheter

En kvalitativ tilnærming bringer med seg både styrker og svakheter. Noen av styrkene er blant annet at vi har fått god kjennskap til hver case, og er i stand til å legge frem grundige beskrivelser i motsetning til variabler eller tall som vi måtte ha brukt med en kvantitativ metode.

[3] Undersøkelseseffekten kan være en utfordring i det å skille mellom årsakens virkning og virkningen av selve undersøkelsesopplegget. Kritikken innebærer at ulike eksperimenter kan skape kunstige situasjoner og med det kunstige resultater. (Jacobsen 2018, s.117)

Når det gjelder spørsmål om sikkerhet og virksomheters vektlegging av dette drar vi dermed stor nytte av å ha muligheten til å analysere dataene kvalitativt. Svakheter med denne tilnærmingen er at den gir oss mindre mulighet til å konkludere og generalisere.

Fem informanter kan være for få til å sitte igjen med et helhetlig inntrykk av den generelle vektleggingen av cybersikkerhet i anskaffelsesprosesser hos virksomheter knyttet til kritisk infrastruktur i Norge. Dette er et altfor lite utvalg til å generalisere funnene vi har gjort oss i denne oppgaven. Dersom denne undersøkelsen skulle blitt gjort på ny, ville fler ressurser i form av bredere utvalg og lengre tid legge til rette for en bedre mulighet til å få et helhetlig inntrykk. I tillegg hadde informantene vi intervjuet svært forskjellige stillinger og ansvarsområder innad i deres virksomheter. Det varierer fra ansvar for anskaffelsesprosesser, sjefsstillinger i IKT-sektorer til teknisk sikkerhet. Ved å intervjue kandidater med forskjellige stillinger og ansvarsområder medfører dette at vi sitter igjen med svært forskjellig informasjon fra intervju til intervju.

Det er også viktig å poengtere at informantene kan ha valgt å holde tilbake informasjon eller ordlegge seg annerledes ettersom temaet gjelder egen virksomhets sikkerhet. Dette er gjerne gradert informasjon, hvilket gjør at det er vanskelig for oss å danne et helhetlig bilde av virksomhetens cybersikkerhet. I informasjonsskrivet vi sendte ut til alle informantene i forkant av intervjuet informerte vi om taushetsplikt og anonymitet, men ettersom vi nevner virksomhetene med navn er det ingen garanti på at informasjon ikke ble tilbakeholdt.

BAKGRUNN – NSM, sikkerhetsloven og kritisk infrastruktur

For å supplere vårt bilde av det norske cybersikkerhetsbildet har vi valgt å redegjøre for og drøfte rundt Nasjonal Sikkerhetsmyndighet sin rolle i forbindelse med anskaffelsene vi omtaler. NSM er underlagt Justis- og Beredskapsdepartementet og har et generelt ansvar for å sikre at sikkerhetsloven blir overholdt. Sikkerhetsloven beskriver NSM sin rolle som sektorovergripende fagmyndighet innen forebyggende sikkerhetsarbeid innen norsk virksomhet. (Sikkerhetsloven, 2019, § 2-2)

Sikkerhetsloven og anskaffelser

Den nye sikkerhetsloven ble vedtatt i 2019 og opphevet med det sikkerhetsloven fra 1998. Denne loven har som endelig formål å sikre Norges sikkerhetsinteresser og grunnleggende samfunnsfunksjoner og prinsipper. Alle Norges offentlige organer på lokalt, regionalt og statlig nivå er underlagt både nåværende og tidligere sikkerhetslov.
En viktig utvikling i den nye sikkerhetsloven er å i større grad ta høyde for rollen private virksomheter spiller i norsk sikkerhet. Et resultat av dette er at omfanget av sikkerhetsloven har blitt utvidet til å omhandle både private og offentlige virksomheter generelt hvis drift i vesentlig grad påvirker samfunnets kritiske infrastruktur. (Sikkerhetsloven, 2019, § 1-3)

Den nye sikkerhetsloven måtte ta høyde for den raske teknologiske utviklingen vi har hatt de siste årene. Dette kommer særlig til uttrykk ved at formuleringene i den gamle sikkerhetsloven var mer konkrete og stive, men som nå har blitt erstattet av rettslige standarder. (Sikkerhetsloven, 1998) Rettslige standarder er i seg selv vage, men innholdet presiseres gjennom forskrifter, veiledere og tilsyn. Den viktige fordelen er at lovteksten kan forbli det samme, samtidig som betydningen endres over tid og sammenheng. For eksempel fremgår det av sikkerhetsloven § 7-3 at «Virksomheten skal iverksette «nødvendige» sikkerhetstiltak for å opprettholde et «forsvarlig» sikkerhetsnivå». (Sikkerhetsloven, 2019, § 7-3) Slike formuleringer åpner for at kravene kan konkretiseres gjennom blant annet forskrifter, veiledere og tilsyn og følgelig blir prosessene rundt endringer raskere, noe som gir jussen bedre mulighet til å følge den teknologiske utviklingen. (NSM, 2019: 8:30)

Virksomhetene selv er ansvarlige for å gjøre egne risikovurderinger som en del av sikkerhetsarbeidet. Sikkerhetslovens rettslige standarder gir virksomhetene anledning til å utforme egne sikkerhetsstrategier basert på eget risikobilde, men tilsynsmyndigheten kan gi pålegg om tiltak der sikkerheten finnes utilstrekkelig.
NSM har i tillegg publisert ulike veiledere, som skal hjelpe virksomhetene til å oppfylle sikkerhetskravene. Disse er imidlertid ikke juridisk bindende i seg selv, men vil kunne gi sikre svar på tilfredsstillende sikkerhetspraksis.

En viktig utvikling i den nye sikkerhetsloven er å i større grad ta høyde for rollen private virksomheter spiller i norsk samfunnssikkerhet. Et resultat av dette er at omfanget av sikkerhetsloven har blitt utvidet til både private og offentlige virksomheter generelt dersom driften i vesentlig grad påvirker «grunnleggende nasjonale funksjoner» eller behandler sikkerhetsgradert informasjon. Departementet innenfor det aktuelle ansvarsområdet vil ha ansvar for utpekingsvedtak og medfølgende tilsyn mot disse virksomhetene. (Sikkerhetsloven, 2019, § 1-3)

I den hensikt at det skal være forholdsmessighet mellom tiltak og sårbarhet, har sikkerhetsloven to forskjellige skalaer som kategoriserer ulike nivåer av potensielle skadefølger. Disse er i utgangspunktet gjeldende for virksomhetene selv som tilvirker sikkerhetsgradert informasjon, men blir også gjeldende for deres underleverandører som kan få adgang til slik informasjon.
Den første skalaen omhandler sikkerhetsgradert informasjon. Informasjon som kan skade nasjonale sikkerhetsinteresser skal etter § 5-3 graderes etter fire kategorier. Kategoriene går i stigende rekkefølge, etter alvorlighetsgrad av potensielle skadefølger: BEGRENSET, KONFIDENSIELT, HEMMELIG og STRENGT HEMMELIG. (Sikkerhetsloven, 2019, § 5-3)
Graderingen som følger med informasjonen avgjør hvor strenge krav loven stiller til involverte aktører og prosessene rundt. For eksempel stiller sikkerhetsloven krav om leverandørklarering dersom leverandøren kan få tilgang til og/eller oppbevare informasjon gradert KONFIDENSIELT eller høyere.
Den andre skalaen klassifiserer skjermingsverdige objekter ut ifra hvilken grad de anses som «kritiske» og lyder: VIKTIG, KRITISK og MEGET KRITISK. Etter virksomhetssikkerhetsforskriften § 58 vil denne graderingen avgjøre hvilket sikkerhetsnivå som er ansvarlig. (Virksomhetssikkerhetsforskriften, 2019)

Forskrifter

NSM lister opp to viktige forskrifter under sikkerhetsloven. (NSM, u.å.) Blant supplementene til ny sikkerhetslov står virksomhetssikkerhetsforskriften helt sentralt. Forskriftens bestemmelser er gjeldende for enhver virksomhet underlagt sikkerhetsloven. Denne går nærmere inn på hvilke krav som fremgår av sikkerhetsloven. Før 2019 var det flere forskjellige forskrifter om virksomhetens arbeid med forebyggende sikkerhet, mens denne forskriften har samlet de tidligere forskriftene til én.

Virksomhetsforskriften fungerer til å presisere bestemmelsene og standardene som følger med sikkerhetsloven. Forskriften går nærmere inn på blant annet hvordan risikovurderinger, tiltak og oppfølging skal foregå, samt sikkerhetskrav ut fra de ulike graderingsnivåene. (Virksomhetsikkerhetsforskriften, 2019)

Den andre viktige forskriften NSM viser til er klareringsforskriften. Denne forskriften inneholder mer konkrete krav til blant annet prosedyrer og klareringskriterier, med basis i sikkerhetslovens bestemmelser. (Klareringsforskriften, 2019)

Veiledere og grunnprinsipper

NSM sitt kanskje viktigste virkemiddel for å heve digital sikkerhetsstandard er deres veiledere. Veilederne, som tidligere nevnt, er ikke juridisk bindende. De er likevel en viktig ressurs enhver virksomhet kan benytte seg av for å videreutvikle egen forståelse av det aktuelle trusselbildet og hvordan man kan sikre seg på best mulig måte. Veilederne er i utgangspunktet ment å hjelpe virksomhetene som er underlagt sikkerhetsloven med å etterleve loven. NSM anbefaler samtidig at enhver virksomhet benytter seg av veilederne, ettersom et godt sikkerhetsnivå er ønskelig uavhengig av om virksomheten er underlagt sikkerhetsloven eller ikke. (NSM, u.å.)

NSM sine grunnprinsipper for IKT-sikkerhet står sentralt blant deres nettressurser. Disse prinsippene handler om grunnleggende steg enkeltvirksomheter kan gjøre. Som de andre veilederne fra NSM, omhandler dette oppfordringer og veiledning, som anbefales til enhver norsk virksomhet, men særlig virksomhetene med ansvar for samfunnskritiske funksjoner. (Nasjonal Sikkerhetsmyndighet (NSM), 2020)

Grunnprinsippene er fordelt i fire kategorier i prosessen for digital sikkerhet.

Det første leddet handler om å identifisere og kartlegge. Dette trinnet om å lage og holde oversikt over risikobildet og egen sikkerhetspraksis.

Dette innebærer kartlegging av egne systemer, samt avhengigheter til eksterne systemer og leveranser, samt tekniske vurderinger av digitale systemer og enheter og deres forhold til sluttbrukere.
Blant foreslåtte tiltak finner vi tilstrekkelig risikovurdering og risikostyring, anbefalinger som henger i tråd med sikkerhetsloven. (ibid)

Det andre leddet heter «beskytte og opprettholde». Her går NSM nærmere inn på konkrete sikkerhetsområder og tilhørende vurderinger og tiltak. Dette er neste trinn og handler om å etablere sikre praksiser og kontroll rundt blant annet anskaffelser, administratorrettigheter, programvare og e-post. (ibid)

Neste trinn går inn på å oppdage. Dette trinnet handler om mulige midler for å deteksjon av og tiltak mot sårbarheter og trusler. Dette kan oppnås gjennom diverse programvare og produkter, samt overvåkningssystemer og oppfølging. NSM anbefaler også å gjennomføre inntrengingstester for å avdekke sårbarheter som kan utnyttes. (ibid)

Siste trinn heter «håndtere og gjenopprette» og retter seg mer mot beredskap ved uønskede hendelser. NSM innleder med at dataangrep har blitt en del av dagliglivet og at virksomheter må innstille seg deretter. Det oppfordres til å ha ferdig utarbeidede beredskapsplaner og prosedyrer klart før hendelsen inntreffer, som da vil gjøre at virksomheten kan møte sikkerhetshendelser så effektivt som mulig. Dette trinnet består av en prosess som omfatter forberedelse av virksomheten, klassifisering og håndtering av hendelsen og til slutt evaluering og læring. (Ibid)

Sikkerhetsgraderte anskaffelser

Blant punktene sikkerhetsloven og virksomhetssikkerhetsforskriften dekker, finner vi sikkerhetsgraderte anskaffelser. Sikkerhetsgraderte anskaffelser handler om anskaffelser der leverandøren som benyttes kan få tilgang på «skjermingsverdige verdier».

NSM har i sin veileder om anskaffelser under sikkerhetsloven, listet opp kriteriene for hva som etter sikkerhetsloven er å anse som sikkerhetsgraderte anskaffelser:

- «Leverandøren kan få tilgang til sikkerhetsgradert informasjon,
- Leverandøren tilvirker sikkerhetsgradert informasjon,
- Leverandøren kan få tilgang til et skjermingsverdig objekt, eller
- Leverandøren kan få tilgang til skjermingsverdig infrastruktur» (Nasjonal Sikkerhetsmyndighet (NSM), 2019, s5)

Etter § 1-2 er sikkerhetsloven gjeldende for leverandører i forbindelse med sikkerhetsgraderte anskaffelser. I en slik prosess vil det med få unntak foreligge krav om sikkerhetsavtale med leverandør, uavhengig av graderingsnivå. Virksomhetsikkerhetsforskriften utdyper hva innholdet i en slik avtale må inkludere, deriblant hvor og hvordan sikkerhetsgradert informasjon skal behandles under samarbeidet. Sikkerhetsgraderte anskaffelser er blant temaene NSM dekker i sin veiledning, både gjennom sine grunnprinsipper og gjennom en egen veileder for anskaffelser under sikkerhetsloven.

Sikkerhetsloven og kritisk infrastruktur

Som tidligere nevnt skiller Sikkerhetsloven fra 2019 seg vesentlig fra den tidligere loven. Blant annet dreier dette seg om de overnevnte rettslige standardene. Den andre viktige endringen som kan ha betydning for vårt utvalg er de nye kriteriene for underleggelse av sikkerhetsloven som ble omformulert til å kunne inkludere en rekke nye virksomheter, både offentlige og private. Om en virksomhet blir utpekt eller ikke er blant annet avhengig av hvorvidt virksomheten har betydning for grunnleggende nasjonale funksjoner (GNFer).

GNFer blir i sikkerhetsloven § 1-5 definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2019, § 1-5). Nasjonale sikkerhetsinteresser defineres i samme paragraf.

DSB har i en rapport fra 2016 kartlagt og beskrevet den kritiske infrastrukturen og tilknyttede samfunnsfunksjoner det norske samfunnet er avhengig av. Kritisk infrastruktur og ny sikkerhetslov henger tett sammen, men det er verdt å understreke at denne rapporten ble skrevet før den nye loven. Med formål om å operasjonalisere begrepet «kritiske samfunnsfunksjoner» benytter DSB seg av en tidsdimensjon i definisjonen av begrepet: ved frafall av funksjonen i syv dager eller mindre er befolkningens sikkerhet og/eller trygghet i fare. Således henger begrepet tett sammen med GNFene sikkerhetsloven viser til.
Kritisk infrastruktur brytes her ned til tre hovedkategorier: Styringsevne og suverenitet, befolkningens sikkerhet og samfunnets funksjonalitet. (DSB, 2016)

Innledende om virksomhetene

Forsvarsdepartementet

Ifølge Regjeringens oversikt over departementene og deres ansvarsområder, presenteres Forsvarsdepartementet som et regjeringskontor med ansvar for utforming og iverksetting av norsk sikkerhets-og forsvarspolitikk. Videre nevner de overordnet styring og kontroll av, samt tilsyn med, underlagte etaters virksomhet som departementets ansvarsområder. (Regjeringen, 2014).

I en oversikt over kritiske samfunnsfunksjoner presentert av DSB finner vi Forsvarsdepartementet i flere kategorier. Hovedsakelig står Forsvarsdepartementet oppført innenfor styring og kriseledelse samt under forsvar, men også i sammenheng med helsetjenester, matforsyning, drivstofforsyning og sikkerhet i elektronisk kommunikasjon. De spiller også en rolle innenfor satellittbaserte tjenester, der Forsvarsdepartementet gjennom Forsvarets forskningsinstitutt bidrar til romforskning og jordobservasjon. Med ansvarsområder som strekker seg til alle de overnevnte områdene ser vi at Forsvarsdepartementet er helt uunnværlig for at samfunnet skal gå rundt. Dette innebærer at deres vektlegging av digital sikkerhet blir særlig interessant. (Direktoratet for samfunnssikkerhet og beredskap, 2016, s.12-105)

Telenor

Telenor Norge AS er landets største digitale tjenesteleverandør innenfor innhold-, telekommunikasjon- og datatjenester. Ettersom vår oppgave fokuserer på virksomheter knyttet til kritisk infrastruktur faller Telenor naturlig inn under denne kategorien.

Telenor Norge jobber for å maksimere telekommunikasjonens samfunnsnytte, og de både eier og forvalter samfunnskritisk infrastruktur som er kritiske for funksjonen til det norske samfunnet. Dette innebærer blant annet deres tjenester på mobil, fastnett og bredbånd. Ifølge Telenor går nesten 80 prosent av hele Norges datatrafikk gjennom deres tjenester og infrastruktur, hvilket åpner opp for avanserte trusselaktører. Dermed står Telenor med et betydelig samfunnsansvar der de må levere trygge og stabile tjenester i alle deler av kriseskalaen. (Nilsen u.å)

Utgangspunktet for bruken av Telenor som kildemateriell er litt annerledes enn de andre virksomhetene. Samtidig som vi har intervjuet kandidater fra virksomhetene vi har konsentrert oss om i utvalget vårt, benytter vi oss av en rapport om digital sikkerhet som Telenor publiserte i 2020. Hovedforskjellen blir dermed metoden vi har brukt for å trekke ut informasjon, samt vektleggingen av denne informasjonen. Dette til tross er det flere likheter det er verdt å trekke frem. Felles for alle virksomhetene i utvalget er deres posisjon i sine leveransekjeder, der de både innehar bestillerrollen overfor sine underleverandører, og i varierende grad er underlagt statlig myndighet. I tillegg har alle ansvar for kritisk infrastruktur, og er ansett som en samfunnsnødvendighet.
Det bidrar til at sikkerhetsaspektet i deres arbeid er ekstra viktig. Dermed mener vi Telenor Norge AS en viktig virksomhet å trekke frem i en oppgave som tar for seg vektleggingen av digital sikkerhet i anskaffelsesprosesser.

KSAT

Kongsberg Satellite Services, forkortet til KSAT, er en verdensledende tjenesteleverandør for mottak av satellittdata. KSAT har tre bakkestasjoner for å kalibrere satellitter. Disse bakkestasjonene står på deres lokasjoner, der KSAT står ansvarlige for å levere strøm, nett, kjøling og andre nødvendigheter. Dette er i aller høyeste grad kritisk infrastruktur. Tilgangen til satellitter har lenge vært en stor nødvendighet for at samfunnet går rundt, ettersom de fleste systemer vi er helt avhengige av benytter seg av denne teknologien. (KSAT, personlig kommunikasjon, 23.04.2021).

Til forskjell fra de andre virksomhetene i utvalget vårt, er store deler av KSATs kundemasse - omlag 90% - utenlandske leverandører. Likevel forholder de seg til norske myndigheter og reguleringer, i likhet med de andre virksomhetene i Norge.

Nedre Romerike Vannverk

Nedre Romerike Vannverk er et interkommunalt aksjeselskap eid av fire tilknyttede kommuner i Viken.

Selskapets arbeid dreier seg om vannforsyning til eierkommunene Lillestrøm, Rælingen, Lørenskog og Nittedal. Vi har tatt kontakt med og intervjuet en sikkerhetsleder i NRV for å samle inn informasjon om selskapet tilknyttet oppgaven. Vi har valgt å avgrense til vannverket, men sikkerhetssjefen representerer både Nedre Romerike Vannverk og Nedre Romerike Avløpsselskap.

Lyse

Lyse er et norsk industrikonsern eid av 14 forskjellige kommuner, med Stavanger, Sandnes og Sola som de tre største eierne. Selskapet er et resultat av en fusjon av lokale E-verk gjennom 90-tallet. (Lyse, u.å.)

Konsernet har en rekke underlagte selskaper som står for en bred portefølje av tjenester for kunder i Norges sør-vest region. Tjenesteområdene Lyse jobber med gjennom datterselskapene inkluderer flere ledd innenfor kritisk infrastruktur, deriblant strømnett og fibernett.

Vi har hatt et intervju med tre ansatte i Lyse for datainnsamling. I intervjuet fikk vi tak i to anskaffelsesrådgivere og leder for informasjonssikkerhet i Lyse.

EMPIRI

I dette kapittelet vil den tilgjengelige, relevante empirien på cybersikkerhet i anskaffelsesprosesser bli presentert. Empirien presenteres tematisk innunder virksomhetene.

Lyse

Lyse opplyser at arbeidet deres kan knyttes opp til både kritisk infrastruktur og kritiske samfunnsfunksjoner. Disse to er underlagt svært forskjellige lovverk. Lyses rolle i kraftsektoren foregår gjennom underselskapet Lyse Elnett. Lyse Elnett er et infrastrukturselskap som i deres region har monopol på distribuering av strøm.

Lyse regner med at deres underselskap Altibox kommer til å bli underlagt sikkerhetsloven. Dette er grunnet betydningen fibernettet har fått for samfunnet. De sier videre at å bli underlagt sikkerhetsloven vil bety betydelige endringer for deres sikkerhetspraksis. Blant nye mulige tiltak blir det nevnt sperrede soner og adgangskontroll, nye krav til lokalene og strengere regler rundt oversending av informasjon som sikkerhetsgradert på høyere nivå. Som et resultat har de allerede begynt å «rigge til» for de nye sikkerhetskravene og understreker at «compliance» med sikkerhetsloven er kostbart. Samtidig som å bli underlagt sikkerhetsloven ikke er ønskelig, gir Lyse imidlertid uttrykk for å støtte den nye loven. De peker på at den nye loven er mye mer dynamisk og handler mer om risikovurdering og risikostyring, en overgang fra den gamle loven som handlet mer om gradering og merking.

Kraftforsyning blir også etter DSB-rapporten betegnet som kritisk samfunnsfunksjon. Begrepet omfatter systemene og leveransene samfunnet har behov for, blant annet til husholdninger, produksjon og transport. Dette deles opp i to former for leveranser: elektrisk energi og fjernvarme. Forsyning av elektrisk energi handler om at sluttbrukere skal ha tilgang på tilstrekkelig mengde strøm. Ved langvarig mangel på tilstrekkelig strømmengde skal systemene rasjonere energien etter behov. Forsyning av fjernvarme handler om å sikre husholdninger virksomheter tilstrekkelig fjernvarme etter behov. I tillegg kan det regnes med at kraftforsyning er sentralt i å støtte opp under de andre kritiske samfunnsfunksjonene. (DSB, 2016)

Under formidling av krav til underleverandørene er det et stort fokus på å skrive ned kravene som forventes oppfylt for leverandørene, slik at leverandørene kan bekrefte eller avkrefte at de oppfyller disse. Dersom anskaffelsen dreier seg som sensitiv informasjon, kan man begrense antallet leverandører i forkant.

I forhold til pris understreker Lyse at sikkerhet går under betegnelsen «Skal-Krav». Dersom kravene ikke oppfylles er man diskvalifisert. «Bør-krav» og «Kan-krav» på den andre siden, regnes som pluss, men ikke obligatorisk.

Når det kommer til underleverandørenes sikkerhetsnivå og hvorvidt dette har endret seg de siste årene, mener sikkerhetssjefen hos Lyse at dette er blandet. De større leverandørene har et mer bevisst forhold til sin digitale sikkerhet fordi kundene deres stiller strenge krav. Amerikanske leverandører på sin side er gode på sikkerhet, men stiller ikke like sterkt når det kommer til personvern – dermed blir de diskvalifisert.

Videre får Lyse mange unntaksforespørsler fra leverandører som gjerne vil benytte seg av personell utenfor EU/EØS avtalen, men kravene Lyse stiller til dette blir ofte så strenge at leverandørene velger å finne tilsvarende ressurser i Europa. Dette kommer av at sikkerhetssjefen i slike tilfeller er nødt til å få detaljert informasjon om hvilke data de har fått tilgang på, hvilke systemer de skal jobbe med, hvilke tilganger de får og liknende – i tillegg til hvem som tar konsekvensen og en eventuell regning dersom det skulle oppstå en hendelse.

Ettersom Lyse regner med å bli underlagt den nye sikkerhetsloven, er de nødt til å følge opp allerede eksisterende leveranser samt stille krav til nye leverandører. Her drar de frem skygge-IT [4] som en svært viktig del, særlig med tanke på verdikjedeangrep som de jobber hardt for å bli kvitt.

Det er heller ingen bruk av insentiver for å oppmuntre deres underleverandører til å ha høyere fokus på sikkerhet, ettersom det er et «Skal-krav». De opererer med andre ord med fastsatte krav som leverandørene er nødt til å forholde seg til, det samme gjelder insentiver fra det offentlige til Lyse.

Ved spørsmål om myndighetenes innvirkning på Lyses sikkerhetsarbeid blir NSM nevnt som en viktig aktør. Videre blir Norges vassdrag- og energidirektorat (NVE) pekt ut som spesielt viktig i samspillet med det offentlige. NVE har rolle som tilsynsmyndigheten til Lyse.

Lyse beskriver veilederne fra NSM som gode og at man som en organisasjon med sikkerhetsfokus bør bruke disse. Som et eksempel trekker vi frem veileder for anskaffelser under sikkerhetsloven og spør hvordan de forholder seg til denne. Lyse trekker da et skille mellom å bruke veilederen og det å implementere den. Veilederen kan brukes, men den har ikke blitt implementert fordi de ikke er underlagt sikkerhetsloven. Dette vil imidlertid endre seg ved et utpekingsvedtak. Lyse sier videre at dersom et selskap under Lysekonsernet blir underlagt, vil endringene sannsynligvis skje hos det aktuelle selskapet, framfor på konsernnivå, avhengig av hvor omfattende og kostnadseffektive endringene blir.

[4] «Skygge-IT defineres gjerne som at virksomhetens ansatte eller fagavdelinger tar i bruk eksterne IT-tjenester fra skyen, uten at IT-avdelingen hverken er involvert i, eller kjenner til anskaffelse eller bruk» (Helse Nord IKT, 2018, s49)

Lyse trekker frem International Organization for Standardization (ISO). Dette er en internasjonal organisasjon som formidler standarder på en rekke områder, deriblant informasjonssikkerhet. Lyse jobber for å etterleve disse standardene og trekker ytterligere inspirasjon fra amerikanerne, som er enda strengere på sikkerhet, sett bort fra personvern.
Grunnprinsippene fra NSM beskrives som viktige og gode at de legges til grunn i deres sikkerhetspraksis. Samtidig sies det at prinsippene er nokså grunnleggende og ingen «rocket science», men at de ligger i bunn når de implementerer ISO-standarder. De opplyser videre at deres tilsynsmyndighet NVE holder prinsippene svært tett til brystet.

Som tidligere nevnt jobber Lyse hardt for å bli kvitt verdikjedeangrep, hvilket er en av grunnene til at skygge-IT blir kjempeviktig. De mener at verdikjedeangrep er den mest alvorlige risikoen de står overfor, både på lokalt, regionalt og nasjonalt nivå. Vurdering, håndtering og styring av tredjeparter blir viktigere og viktigere ifølge Lyse.

Som tidligere forklart, opplyser Lyse at de opererer i både telesektoren og kraftsektoren. Disse to er underlagt veldig forskjellig regulering. Dermed er det viktig å ha struktur på sikkerheten – et godt styringssystem og full kontroll på verdikjeden. Lyse jobber for at infrastrukturselskapet Elnett ikke skal bli underlagt sikkerhetsloven, men de tviler på at det ikke blir underlagt.
På telesiden vet de at Altibox Norge vil bli underlagt sikkerhetsloven og at to andre selskaper kan bli underlagt. Dermed gjør de seg klare til sikkerhetskravene, og mener at nøkkelen i det hele er å få på plass kontrollene og risikostyring – dette går på å få kontroll på verdiene sine.

Lyse eier fremdeles mange vannkraftverk, blant annet Lyse Kraft DA. De har fusjonert med Hydro som nå eier ca 24% av Lyse Kraft, og har operasjon på disse vannkraftverkene. I etterkant av verdikjedeangrepet på Hydro der en e-post ga tilgang til hovedleverandør gjennom en underleverandør, har Hydro hatt et enormt fokus på sikkerhet som igjen stiller krav til ledelsen i Lyse Kraft. Verdikjeder kommer dermed til å bli viktigere på kraftisden ifølge Lyse – spesielt med underleverandører som leverer komponenter inn i kontrollsystemene. Dette sier Lyse er kjempeviktig å beskytte, ettersom en trusselaktør som ønsker å gjøre sabotasje i deres kontrollsystemer vil utgjøre en stor risiko. Et eksempel Lyse tar opp i denne sammenhengen er kontroll på slusene til dammene. Dersom en trusselaktør får kontroll på disse slusene vil det være veldig kritisk og potensielt resultere i oversvømmelse, så det er viktig å ha god kontroll på disse områdene.

NRV

Nedre Romerike Vannverk opplyser at de ikke er underlagt sikkerhetsloven, samtidig som de har ansvar for vann og avløp. Intervjuobjektet opplyser at han ikke er kjent med grunnen til dette og viser til at Vann- og avløpsetaten i Oslo kommune er underlagt sikkerhetsloven. Intervjuobjektet sier at det har tidligere blitt vurdert om de skal bli underlagt grunnet deres rolle i vannforsyning, men det ble bestemt at de ikke underlagt.
Selskapene NRA og NRV drifter to separate renseanlegg, et for vannrensing til drikkevann og det andre for avløpsrensing. Sikkerhetsavdelingen vi er i kontakt med er felles for begge to.

Samtidig som vannverket ikke har blitt underlagt sikkerhetsloven, er vann og avløp blant punktene som dekkes DSB-rapporten. DSB skriver at forsyning av drikkevann i tilstrekkelig grad er å betegne som en kritisk samfunnsfunksjon. Nøyaktig hva som ansees som tilstrekkelig, vil være opp til overordnede myndigheter å defineres. Det påpekes at drikkevann ikke bare er vann til drikking, men inkluderer også andre bruksområder for vann knyttet til boliger, næringsliv og samfunnet ellers.

NRV gir ikke uttrykk for at de benytter seg av NSMs veiledere, utover NSMs grunnprinsipper. Grunnprinsippene blir imidlertid omtalt som en «bibel» norske virksomheter bør etterstrebe og følge og at NRV legger prinsippene til grunn.

Formidlingen av sikkerhetskrav til underleverandørene hos NRV bygger i stor grad på lange relasjoner. I samtale med intervjuobjektet hos NRA har man historisk sett hatt sikkerhetskomponenter fra mange produsenter, men én antiviruspakke på klientene og en annen på e-post. Dette har utviklet seg over tid, nå jobber hver av produsentene av sikkerhetsprodukter i sitt eget økosystem. De passer på å ha produkter som samspiller, og kommunikasjonen har utviklet seg. De er også av den oppfatning av at sikkerhetsnivået på underleverandørene har endret seg de siste årene. Holdningene i bransjen har utviklet seg, og det er et mye større fokus på sikkerhet fra leverandørene. I tillegg merker de at løsningene også er mer ivaretatt på sikkerhet.
På spørsmålet vedrørende typiske krav NRV/A stiller til sine leverandører kommer kompetanse frem som en betydelig stor del av anskaffelsesprosessen. Kartlegging av kompetansen hos leverandørene er den første fasen i deres anskaffelser, etterfulgt av en leverandørsamtale. Sertifiseringer og referanser vektlegges i stor grad, og blir fulgt opp. Disse faktorene veier tyngre enn prisen på tjenestene.

Telenor

Telenor er ifølge et saksdokument fra Nasjonal Kommunikasjonsmyndighet underlagt sikkerhetsloven på grunn av deres rolle tilknyttet kritisk infrastruktur. (Nasjonal Kommunikasjonsmyndighet, 2019, s1-2) Vi kan også finne en side for Telenor Security Operation Center (TSOC), en del av Telenor som beskrives som hjertet og kjernen i sikkerhetsarkitekturen. Blant kravene til sine medarbeidere finner vi «Forsvarets sikkerhetsklarering for «Hemmelig» i henhold til sikkerhetsloven». (Telenor, u.å.)

Telenor som i en sentral aktør innen ekom blir også omfattet av DSB-rapporten under elektroniske kommunikasjonsnett og tjenester. Dette omhandler å dekke samfunnsbehovene for ekom, både kommersielle nett og Nødnett.
Videre påpekes det at å ivareta sikkerhetsaspekter som konfidensialitet og integritet i ekom er av kritisk karakter. På lik linje med kraftforsyning kan dette antas å være sentrale funksjoner som støtter om øvrige kritiske samfunnsfunksjoner. (DSB, 2016)

Telenor peker på både sikkerhetsfaglig kompetanse og domenekompetanse som viktige faktorer når det kommer til identifisering av relevante og gode krav til en leverandør. Domenekompetanse går utpå leverandørens virksomhet og leveransen man mottar. Årsaken til at Telenor understreker viktigheten av kompetanse i flere ledd er at utilstrekkelig kompetanse i kravstillerrollen er en av de vanligste årsakene til mangelfulle krav.
For å bidra til å gjøre kravene mer akseptable for begge parter, foreslår Telenor at bruken av referanser kan bidra til å forenkle og lette kravstillingen. Relevante referanser kan blant annet være anerkjente rammeverk og standarder, lover og regler, veiledninger, bransjenormer og sertifiseringsordninger. Slike referanser kan også gi en form for automatikk i vedlikehold av kravene ved at kildene i takt med teknologi og det generelle trusselbildet, utvikles og fornyes over tid. (Telenor, 2020)

Rett risikovurdering er en nødvendig forutsetning for kravstilling, ettersom krav kan ha skyhøye kostnader. Kostnadene virksomheten velger å ta, må samsvare med gevinsten (risikoreduksjonen). Uten god risikoforståelse er den balansen vanskelig å treffe, og valgene vanskelige å ta. Avtalefestede krav stilles gjerne på relativt høyt eller prinsipielt nivå. For å forstå hvilken risikoreduksjon kravene faktisk vil gi, og ikke minst for å realisere denne gevinsten, vil det, spesielt i større avtaler, være viktig å avklare hvordan de mest sentrale kravene vil bli innfridd. Dette bør avklares før endelig leverandørvalg og avtaleinngåelse.

Ifølge Telenors erfaring er sikkerhetsmessig kvalitet og forbedring nødt til å bli drevet av etterspørsel fra kjøperens side, samt en viss vilje til å betale for sikkerhet og risikoreduksjon.
Å stille et krav om at leverandøren må pålegge sikkerhetskravene videre til sine underleverandører er et virkemiddel for å gi sikkerhetskrav en etterspørselsdrevet effekt videre nedover i leveransekjedene. (ibid)

Videre poengterer Telenor viktigheten av å stille krav om kontroll av mottatte leveranser. De hevder at mange virksomheter undersøker forhold knyttet til potensielle leverandører, men at det er svært få som stiller krav om transparens for hvem disse underleverandørene er. De påpeker at evnen til å dokumentere dette effektiv vil ofte avhenge av løpende vedlikehold i gode styrings- og rapporteringssystemer hos leverandøren. (ibid)

Telenor definerer leveransekjeder som både tjenester og produkter. De omfatter både direkte leveranser, altså direkte leverandører og innsatsfaktorer, og indirekte leveranser, altså underleverandører og deres ytterligere underleverandører og innsatsfaktorer. Underleverandører kan også opptre som «overleverandører». Det vil si at de leverer på andres vegne, slik som support og kundeservice.
Videre peker de på hvordan rekkene av underleverandører og underleveranser har en tendens til å bli svært lange og omfattende, ettersom ytterst få bedrifter som ikke benytter seg for noen form av tjenesteutsetting. Dermed finnes det et stadig mer komplekst, fragmentert og langstrakt nett av underleveranser bak enhver leveranse. Dette betyr også at leddene er mindre transparent jo mer innviklet leveransekjeden blir. Dette peker Telenor på som en direkte årsak av et mer globalt og kostnadsoptimalisert verdensbilde. (ibid)

Telenor definerer leveransekjedene som angrepsflater sett fra et sikkerhetsperspektiv.
«Enhver virksomhet eller person som bidrar til en underleveranser, og underleveransen i seg selv, gir mulighet til å påvirke sikkerheten lengre opp i leveransekjeden. Denne angrepsflaten øker sannsynligheten for negative operasjonelle hendelser, enten de oppstår som følge av sårbarheter i kode og mangelfull håndtering av disse, konfigurasjonsfeil, mangelfull herding, vellykket kompromittering av personell eller alminnelige uhell. Jo lenger og mer fragmentert leveransekjeden er, desto lenger unna er kompetansen som vil være i stand til å håndtere hendelser, og mulighet til å påvirke håndteringen.» (Telenor, 2020, s30).

På bakgrunn av dette utsagnet i Telenors årlige sikkerhetsrapport anbefaler de virksomheter å forstå eget trusselbilde for å ha mulighet til å møte denne angrepsflaten på en hensiktsmessig måte.
«Du må vite hvilke verdier du og dine kunder besitter sett fra relevante trusselaktørers perspektiv, og hvilken evne og vilje relevante aktører har til å utøve sikkerhetstruen - de virksomhet mot disse verdiene. Forstå verdiene – for trusselaktøren.» (Telenor, 2020, s30).

Det viktige her, som Telenor poengterer, er å skille mellom det virksomheter kan ha identifisert som sin «kjernevirksomhet», altså verdier vurdert som viktigst fra et økonomisk perspektiv eller strategiske vurderinger på områder virksomheten kan tilføre noe unikt, og de «negative» verdiene, altså de som har en verdi for potensielle trusselaktører.

- Viktigheten av å se på verdiene fra trusselaktørens perspektiv, og ikke nødvendigvis hva virksomheten selv anser som sine største verdier, er stor.

- Telenors Digitale Sikkerhets rapport fra 2018 pekte på viktigheten av formalisert samarbeid med leverandører og viktige samarbeidspartnere.

Et viktig poeng Telenor illustrerer i sin digitale sikkerhetsrapport er at en er nødt til å forstå seg selv som en del av samfunnsmaskineriet. Med dette mener de at en kan danne en form for flokkimmunitet dersom alle tar høyde for at de både kan være et mål, men også en mulighet for trusselaktører til å infiltrere andre virksomheter som via en leverandør eller en annen form for et samarbeid.
«Det egentlige målet for angriperen kan være noen helt andre, og i så henseende bør alle prioritere de viktigste sikkerhets - tiltakene som underbygger forsvarbar IKT slik vi i 2019 omtalte som digital flokkimmunitet». (Telenor, 2020, s33)

KSAT

I vårt intervju med KSAT kommer det frem at sikkerhetsledelsen jobber med sikkerhet på forskjellige områder, men ettersom 90-95% av deres virksomhet foregår utenfor Norge har ikke sikkerhetsloven hovedfokus i det daglige. De opplyser videre at deler av virksomheten deres er underlagt sikkerhetsloven grunnet deres rolle i prosjektet «Galileo».

Dette prosjektet dreier seg om et EU-eid prosjekt som tar sikte på å utvikle leveranser som tilsvarer de amerikanske GPS-systemene. De sier videre at Galileo er et system som handler om å bidra til EU sin selvstendighet innen satelittnavigasjon, ved å begrense avhengigheten til amerikanske systemer. KSAT nevner en rekke leveranser dette prosjektet bidrar til, deriblant stedstjenester, navigasjon og timing. Dette legger til rette for flere viktige samfunnsfunksjoner som banktjenester, handel og transport, samt en "search and rescue" funksjon kalt SAR. I dette samarbeidet er KSAT en leverandør av infrastruktur prosjektet er avhengig av, blant annet bygg/lokasjoner, førstelinje teknisk støtte og tre ulike bakkestasjoner som fungerer til å kalibrere satellittene, hvor KSAT har ansvar for oppgaver som strøm, nett og kjøling.
KSAT tar videre opp et noe vanskelig forhold til sikkerhetsloven og NSM tilknyttet sikkerhetsklarering av utenlandske arbeidere. Her peker de på at vage formuleringer og mangel på forutsigbarhet fører til utfordringer i rekruttering.

KSAT viser videre til et flynavigasjonssystem de bidrar til, EGNOS, som per dags dato ikke er underlagt sikkerhetsloven, men er etter dialog med NSM forberedt på at deres rolle i dette systemet også kan bli underlagt sikkerhetsloven etter hvert. De peker senere på at slik utpeking går gjennom en omfattende og tidkrevende prosess på myndighetsnivå.

Regjeringen har publisert et dokument på sine nettsider, der virksomheter med kritisk samfunnsfunksjon og nøkkelpersonell kartlegges i forbindelse med barnehageplasser under Covid-19 pandemien. Her blir KSAT nevnt som virksomhet med avgjørende betydning for tjenester som støtter opp under ekom og transport. (Regjeringen, 2021) KSAT påpeker imidlertid at deres rolle i arbeidet ikke har blitt underlagt sikkerhetsloven.

Blant punktene nevnt som kritisk infrastruktur i DSB-notatet, finner vi satellittbaserte tjenester. DSB nevner blant annet navigasjon, kommunikasjon og vitenskapelige undersøkelser som bruksområder.
Her pekes det på at kritikaliteten bak norske satellittjenester i seg selv er varierende, men at leveransene ofte spiller en rolle i en større helhet knyttet til kritiske funksjoner. Konkret blir også begge prosjektene KSAT snakket om, omtalt i dokumentet. Her blir Norsk romsenter nevnt som ansvarlig for å ivareta norske interesser og NSM har i oppgave å følge opp sikkerhet knyttet til sikkerhetsgradert informasjon og godkjenninger av dette.

I intervjuet med KSAT får vi vite at de for øyeblikket er midt i en prosess med å endre deres sikkerhetskrav til underleverandører. Det kommer flere og strengere sikkerhetskrav fra både myndigheter og kunder, som gjør at en endring i sikkerhetskrav blir aktuelt. Hovedsakelig er det innkjøpsprosessen som skal gjøres om på.

Slik det er nå starter KSAT med en innledende dialog med leverandøren, der de presenterer sine standard klausuler og Non-disclosure agreement (NDA) avhengig av hva man kjøper. Da starter en intern prosess der innkjøper er nødt til å sette seg inn i hvor mye informasjonssikkerhet som er relevant i den spesifikke sammenhengen. Her prøver de å gjøre det så enkelt som mulig, men dersom en behøver informasjonssikkerhet blir det en litt tyngre prosess.

De siste årene har det vært en utvikling i hele bransjen vedrørende vektlegging av digital sikkerhet hos underleverandører. KSAT melder om en økt bevissthet rundt sikkerhet der fokuset generelt retter seg mer mot vektleggingen av sikkerhet i alle ledd, blant annet når det kommer til hvilke og hvor høye krav virksomhetene har til sine leverandører. Ifølge KSAT vil leverandørene de er i dialog med komme nærmere dersom de har et stort fokus på digital sikkerhet, og at de generelt er svært opptatt av sikkerhet i anskaffelsesprosesser. Denne endringen i fokus på digital sikkerhet har utviklet seg fra å se på innkjøp som en rent økonomisk transaksjon, der de i all hovedsak skilte på økonomisk størrelse. Effekten av denne endringen er positiv for KSAT. De får kontrakter som kan håndheves dersom noe skulle skje, i tillegg til at det reduserer risikoen for at noe skulle skjedd i utgangspunktet. I tillegg opplever de en økt bevissthet internt i virksomheten rundt anskaffelsene de gjør. Dersom det er brudd på den digitale sikkerheten hos deres leverandører eller de ikke leverer de sikkerhetstjenestene som inngår i avtalen, medfører dette kontraktsbrudd der leverandøren må stå for kostnadene for kompensasjon eller en eventuell opprydding.

KSAT skildrer et utfordrende forhold til et NSM-tilsyn i kort etterkant av at virksomhetssikkerhetsforskriften trådte i kraft. Dette blir begrunnet med at NSM sine veiledere ikke var klare på dette punktet, samtidig som tilsyn under ny forskrift var nytt for KSAT, men også for NSM. Dette resulterte i at spørsmål om hvorvidt etablerte sikkerhetsløsninger var tilstrekkelig, ikke alltid kunne besvares fra NSMs side.
Blant viktige ressurser som legger grunnlag for sikkerhetspraksisen tar KSAT opp NSMs grunnprinsipper på eget initiativ.

KSAT sier at de bruker grunnprinsippene aktiv i sitt sikkerhetsarbeid og således trekker en viss inspirasjon fra sikkerhetsloven, men at sikkerhetsloven i seg selv ikke har en betydelig veiledende virkning for ugraderte anskaffelser.

Forsvarsdepartementet

I intervjuet opplyser intervjuobjektet at Forsvarsdepartementet (FD), på lik linje med alle andre departementer, er underlagt sikkerhetsloven. Dette har de vært siden den gamle sikkerhetsloven trådte i kraft i 1998. FD står også bak forslaget til den nye sikkerhetsloven og tilhørende forskrifter. (Regjeringen, 2018) FD beskriver sikkerhetsloven som svært betydelig i deres arbeid generelt, og blir stadig nevnt gjennom hele intervjuet. Sikkerhetsloven og virksomhetsikkerhetforskriften gir strenge krav til hvordan virksomhetene skal behandle og forholde seg til gradert informasjon og tilhørende systemer, noe som svært ofte er et tema i FD. FD forteller videre at når de skal velge ut underleverandører, stilles det krav om at firmaet selv skal være underlagt sikkerhetsloven. Dersom en aktuell leverandør ikke enda er underlagt sikkerhetsloven, kan de fortsatt bli vurdert, men dette forutsetter at virksomheten sender inn en ny verdi- og risikovurdering til NSM. Denne vil da være oppdatert med deres tilknytning til FD og vil med det bli underlagt sikkerhetsloven og kan da bli benyttet som leverandør.
FD sier at overgangen til ny sikkerhetslov har ført til at sikkerhetskravene både til FD, samt deres krav til underleverandørene blitt rundere og at den har flyttet mye av ansvaret over på virksomhetene som underlegges. Virksomhetene må selv ha kompetanse til å gjøre selvstendige risikovurderinger som skal være tilstrekkelige for å oppfylle standardene gitt i sikkerhetsloven.

I den tidligere nevnte DSB-rapporten fra 2016 er forsvar blant de kritiske sektorene og støtter opp under de grunnleggende behovene «styringsevne og suverenitet». Forsvarets rolle under dette området oppsummeres gjennom tre punkter: overvåking og etterretning, militær respons og forebyggende sikkerhet.
Oppsummert handler sektoren i hovedsak om å ivareta Norges grunnleggende sikkerhets- og suverenitetsinteresser i en internasjonal sammenheng. FD blir listet opp som relevant aktør i alle de overnevnte punktene.
FD blir videre nevnt som relevant aktør under en rekke kritiske samfunnsfunksjoner, deriblant styring- og kriseledelse, forsyningssikkerhet og elektroniske kommunikasjonsnett og -tjenester. (DSB, 2016).

Veilederne til NSM blir beskrevet som svært viktige i sikkerhetsarbeidet. FD er avhengig av godkjenning av NSM under tilsyn og veilederne fungerer i denne sammenheng som et løsningsforslag, der man mer eller mindre er garantert godkjenning. Intervjuobjektet forklarer at innholdet er tilnærmet umulig å etterleve helt, men at man i hovedsak følger veiledere, begrunner avvik og implementerer kompenserende tiltak.
Grunnprinsippene fra NSM omtales som prinsipper for hvordan man skal drive forsvarlig IKT og at dette er noe enhver virksomhet i Norge bør etterstrebe å være «compliant» med. Videre blir media trukket frem som en relevant aktør, da glipper i sikkerheten kan føre til negative avisoppslag. Som eksempel trekker FD frem at dette kunne blitt aktuelt dersom det kommer frem at deres sikkerhet ikke er i tråd med grunnprinsippene.

Forsvarsdepartementet benytter seg ikke i like stor grad av tjenesteutsetting. De forsøker å kjøpe tjenester som er produktspesifiserte slik at de kan ha det i egne datasentre. Dersom de ser seg nødt til å kjøpe tjenester utenfra, er disse tjenestene nødt til å bli levert av en virksomhet underlagt sikkerhetsloven. Dette er et absolutt krav fra Forsvarsdepartementet. En av grunnene til dette er at det er vanskelig å få personell og konsulentselskaper sikkerhetsklarering dersom de ikke er underlagt sikkerhetsloven. Nå som de skal implementere IKT-løsninger for hele departementsfellesskapet, planlegger Forsvarsdepartementet å benytte seg av tjenesteutsetting både med servicetest og telefoni-videokonferanse tjenester på ugradert og lavgradert nivå. Servicetest er der brukerne kan henvende seg hvis de har problemer. Disse tjenestene kan man legge på Doffin, nettsiden der alle aktører gir beskjed om at de går ut med en forespørsel, og stille tilhørende krav.

Videre trekker Forsvarsdepartementet frem virksomhetssikkerhetsforskriften som sier noe om vektleggingen av systemene en jobber på. Her poengterer de at selv om systemet i seg selv er ugradert, er det den samlede verdien av informasjon som ligger der som kan være gradert.
Derfor er virksomhetene Forsvarsdepartementet gir tjenesteoppdrag, konsulentoppdrag og liknende, alle underlagt sikkerhetsloven. Virksomheter som ikke er underlagt sikkerhetsloven kan fremdeles være med i den prosessen, men de forplikter seg til å oppdatere sin verdi og sikkerhetsvurdering slik at de faller inn under sikkerhetsloven. Forsvarsdepartementet avslutter med å presisere at alle som leverer tjenester til forsvars - og justissektoren, blir mer eller mindre automatisk underlagt sikkerhetsloven.

I en eventuell anbudskonkurranse viser Forsvarsdepartementet til flere aspekter som spiller inn. Vurderinger i forhold til pris, hvilke tjenester leverandørene kan tilby, hvilken måte det blir gjort på og fasiliteter blir nevnt som eksempler på ting som vektlegges. Forsvarsdepartementet skiller også på Må-krav eller Bør-krav, og presiserer at sikkerhet vektlegges høyere, også over pris i mange tilfeller. Videre påpeker de at pris er en avgjørende faktor, men ikke på bekostning av sikkerhet – det må alltid være en balanse involvert.

På spørsmål om hvorvidt Forsvarsdepartementets underleverandører har endret sitt sikkerhetsnivå de siste årene, er svaret tydelig ja. De fleste av deres leverandører har gjort store endringer for å kunne levere tjenester videre. Dette gjør seg gjeldende også før den nye sikkerhetsloven kom på banen i begynnelsen av 2019. I 90% av tilfellene kjøper Forsvarsdepartementet tjenester i en tidsbegrenset periode, hvilket vil si at kontrakten mellom dem og leverandøren vil gå ut. For å fornye denne kontrakten er man da nødt til å gjøre eventuelle tiltak, dersom kravene til sikkerheten har endret seg.

Dersom underleverandøren ikke har den sikkerheten de skal ha, kan kontrakten med Forsvarsdepartementet sies opp. Videre legger de til at de gjerne tar inn leverandøren og går gjennom hva problemet er før dette skulle forekomme. Forsvarsdepartementet har ingen sanksjonsmuligheter, og kan ikke pålegge noe de ikke vet noe om. De er dermed nødt til å hvile seg på den verdi – og sikkerhetsvurderingen underleverandøren har gjort og står for, slik at de kan få tilsyn av enten riksrevisjonen eller NSM. Dette avhenger av hvorvidt underleverandøren er offentlig eller privat. Som kontraktspartner av Forsvarsdepartementet vil de få informasjon basert på kritikkverdige forhold.

Insentivering blir heller ikke brukt hos Forsvarsdepartementet. De har en rekke kravsett som enten blir møtt eller ikke, og preferer ikke noen leverandører over andre basert på positive omtalelser rundt egen sikkerhet. Forsvarsdepartementet stiller nøytrale som offentlig aktør.

ANALYSE OG DISKUSJON

Virksomhetene og sikkerhetsloven

I vår analyse av NSM og virksomhetene definerer vi to sentrale PA-forhold. Det første er NSM som prinsipal overfor virksomhetene. Dette innebærer at virksomhetene har en selvstendig rolle, men at de ved hjelp av styringsvirkmidler fra NSM sin side blir insentivert til å drive sikkerhetsarbeid på et høyere nivå enn det de i utgangspunktet ville gjort. For å vurdere dette vil vi først se på hvordan virksomhetene gir uttrykk for at de uten virkemidlene ville hatt en annerledes sikkerhetspraksis uten virkemidlene - og med det muligens en lavere sikkerhetsstandard. I det andre PA-forholdet vurderer vi virksomheten selv som prinsipal overfor sine underleverandører. Her vil vi da vurdere hvorvidt sikkerhetskrav og sikkerhetsfokus fra prinsipalsiden former sikkerhetsnivået til underleverandørene, som står med agentrollen. Dette vil igjen bli sett i sammenheng med PA-forholdet mellom NSM og virksomhetene.

KSAT opplyser i intervjuet at deres valg av personell fra utlandet har blitt komplisert og vanskeligere grunnet uklarheter i formuleringene fra lovverket og uforutsigbarhet i NSM sin praksis. Ut fra dette kan vi trekke ut at KSAT i utgangspunktet ville hatt en mildere tilnærming til utvalg av personell dersom sikkerhetsloven og klareringsforskriften ikke var gjeldende for dem. KSAT sier videre at de har begynt å forberede seg på utpekingsvedtak for deler av virksomheten, som et resultat av utvidelsene som fremgår av ny sikkerhetslov. Dette kan vi tolke i retning av at utpekingsvedtaket vil føre til at KSAT vil måtte skjerpe sikkerhetsnivået dersom sikkerhetsloven blir gjeldende, til tross for at sikkerhetskravene de allerede blir møtt med allerede er krevende. Dette gjelder imidlertid en nokså liten andel av arbeidet deres, ettersom en stor majoritet av anskaffelsene deres ikke er sikkerhetsgraderte.

Lyse beskriver en lignende utvikling. Lyses Altibox er enda ikke underlagt sikkerhetsloven, men de regner med at de blir det grunnet deres rolle innen fibernettet. Denne endringen beskriver Lyse som uønskelig, da utpeking vil føre til betydelige kostnader. De gir videre uttrykk for at de muligens ikke vil implementere de medfølgende endringene på konsernnivå, men kun de selskapene som blir underlagt. Dette tyder også på at Lyse uten sikkerhetsloven som virkemiddel ville hatt en annen tilnærming til sikkerheten.

Dermed vil underleggelse av sikkerhetsloven bli et hardt virkemiddel som kan sies å til en viss grad tvinge Lyse til å holde et høyere sikkerhetsnivå.
I følge intervjuobjektet vårt i NRV er ikke NRV underlagt sikkerhetsloven per dags dato og det blir gitt uttrykk for at denne vurderingen allerede er foretatt. Følgelig kan vi ikke se at sikkerhetsloven har hatt en direkte innvirkning på sikkerheten hos NRV.
I saksdokumentet om Telenor kommer det frem at Telenor er underlagt sikkerhetsloven, inkludert den gamle loven. Det kommer likevel ikke frem i vårt kildemateriale hvorvidt sikkerhetsloven har hatt innvirkning på deres sikkerhetspraksis.

FD på sin side skildrer en drift tungt preget av sikkerhetsloven. Som et resultat av dette er det strenge og omfattende krav rettet mot FD i det daglige. NSM som tilsynsmyndighet får en ekstra tydelig prinsipalrolle overfor FD.
Fordi de har vært underlagt siden starten av den gamle sikkerhetsloven er det vanskelig å finne noe sammenligningsgrunnlag angående hvordan deres praksis rundt digital sikkerhet hadde vært foruten sikkerhetsloven. Det kommer uansett tydelig frem at sikkerhetsloven i betydelig grad påvirker arbeidet deres. FD trekker frem to måter sikkerhetsloven treffer anskaffelsesprosessene deres: sikkerhetsloven som stiller krav direkte til FD og FDs krav om at underleverandørene er underlagt sikkerhetsloven. Dette forteller oss at kravene som fremgår av sikkerhetsloven er av stor betydning for FDs sikkerhet og særlig blir dette tydeliggjort når kravene speiles videre til underleverandører.

I utvalget vårt kommer det tydelig frem at NSM som prinsipal kan tvinge gjennom betydelige og kostbare sikkerhetsendringer. Virkemiddelet kommer i form av lovverk, gjennom sikkerhetsloven, virksomhetsikkerhetforskriften og klareringsforskriften. Til tross for noen ujevnheter rundt hvorvidt de er underlagt sikkerhetsloven, ga både KSAT og Lyse tydelig uttrykk for at underleggelse av sikkerhetsloven vil i vesentlig grad påvirke sikkerhetsarbeidet deres. Dette gjelder imidlertid kun virksomhetene underlagt sikkerhetsloven. Et annet interessant funn er at NRV ikke har blitt underlagt sikkerhetsloven, til tross for at de er tilknyttet den kritiske infrastrukturen vannforsyning. Insentivene i denne sammenhengen vil være konsekvenser og implikasjonene ved brudd på loven, som blir beskrevet i bakgrunnen. Dette er negative insentiver, mens vi ikke ser antydninger til positive insentiver.

Veiledere

Vi går over på et nytt aspekt ved PA-forholdet mellom NSM og virksomhetene. Dette handler om hvordan NSMs bruk av veiledere har innvirkning på sikkerheten hos virksomhetene. Vi tar i utgangspunkt at god sikkerhet er i utgangspunktet i virksomhetenes egeninteresse, men samtidig at dette må sees opp mot kostnadseffektivitet, da høyt sikkerhetsnivå medfører kostnader. Følgelig kan et sikkerhetsnivå ønsket av prinsipalen stå i strid med agentens egeninteresse. Veiledere vil da kunne bidra til å gi virksomhetene verdifull informasjon om trusselbilde og foreslåtte tiltak mot disse, fremfor at virksomhetene skal bruke ressurser på å finne ut av dette selv. Slik vil dette bli et virkemiddel fra prinsipalens side for at forholdet mellom sikkerhetsnivå og kostnad blir bedre, og at det følgelig blir i agentens egeninteresse å holde et høyere sikkerhetsnivå.

Telenor trekker frem kompetanse hos prinsipalen som sentralt for god sikkerhet i anskaffelser og at manglende kompetanse er en vanlig årsak til mangelfulle krav og kan dermed bidra negativt til sikkerheten. De mener dette kan motvirkes av ulike referanser, deriblant lovverk og veiledere. Dette er ressurser hvor NSM vil stå sentralt med sikkerhetsloven og sine veiledere. Gjennom dette gir Telenor uttrykk for at NSM som prinsipal er med på å styre sikkerhetsnivået i anskaffelser gjennom veiledning. Videre trekker de frem at bruk av slike referanser vil ikke bare gi et bedre utgangspunkt, men at referansene oppdateres stadig og med det gir en form for vedlikehold som utvikles i takt med et trusselbilde i utvikling, som ytterligere bidrar til å redusere tyngden i sikkerhetsarbeidet.

Under intervjuet med Lyse blir det nevnt at veilederne til NSM er gode og at disse bør brukes. Angående sikkerheten i Altibox, som antakelig underlegges, påpeker Lyse at veilederne ikke implementeres direkte enda, men at de har bruker innholdet. Men implementering av veilederne vil trolig bli aktuelt når sikkerhetsloven blir gjeldende. Dette kan fortelle oss at først og fremst at veilederne blir brukt som en viktig ressurs som bidrar til å lette på kostnadene og innsatsen nødvendig for å ellers oppnå sikkerhetsnivået de har. Slik kan vi se at NSM som prinsipal bidrar gjennom myke virkemidler til at Lyse kan holde et høyere sikkerhetsnivå og at dette blir særlig aktuelt ved utpeking.

Grunnprinsippene fra NSM blir av NRV omtalt som en «bibel». Det sies videre at dette er det viktigste dokumentet for de fleste virksomheter. Dette forteller oss at grunnprinsippene har en tydelig veiledende effekt på NRV sin sikkerhet, blant annet innen anskaffelser. NRV går ikke inn på at ytterligere veiledere aktivt brukes.

FD trekker også frem grunnprinsippene står sentralt i deres sikkerhet og de mener selv at enhver norsk virksomhet bør etterstrebe å følge disse. Veiledningene blir også omtalt som sentralt, men at full compliance ofte er urealistisk. Fordi FD er underlagt sikkerhetsloven, må imidlertid punktene følges opp og implementeres i den grad det er praktisk hensiktsmessig.

Blant veiledningsressursene til NSM, er det et gjennomgående tema fra samtlige virksomheter at grunnprinsippene i stor grad anvendes i sikkerhetsarbeidet. Dette tolker vi til at NSM sine veiledninger er med på å styrke synet på NSM som prinsipal i deres forhold til virksomhetene, gjennom myke virkemidler, til motsetning fra hvordan sikkerhetsloven påvirker partene.

Verdikjede og underleverandører

I denne delen av analysen skifter vi perspektiv over til PA-forholdet mellom virksomhetene og deres underleverandører. Virksomhetene har i denne sammenhengen prinsipalrollen overfor både allerede underleverandører, men også potensielle leverandører. Knyttet opp til sikkerhetsaspektet ved samarbeidet dreier forholdet seg om at underleverandørene utgjør sårbarheter og en slags angrepsflate hos prinsipalen. Dette leder til at prinsipalen er avhengig av at underleverandørene har en tilstrekkelig standard på egen sikkerhet for å redusere egne sårbarheter. NSM dekker bruk av underleverandører både i grunnprinsippene, egen veileder og gjennom sikkerhetsloven med forskrifter.

Lyse er svært tydelige på fokuset på den digitale sikkerheten hos sine underleverandører. Verdikjedeangrep trekker de frem som den kanskje største sikkerhetstrusselen i dagens risikobilde, et tema de har blitt godt kjent med etter deres fusjon med Hydro. De trekker et stramt skille mellom «bør-krav» og «skal-krav» og at alle sikkerhetskrav, deriblant digitale sikkerhetskrav, er absolutte.

Brudd på avtalt sikkerhetspraksis blir tatt på alvor og sjefen for informasjonssikkerhet sier videre at hans avdeling er i posisjon til å «velte» hele anskaffelser dersom sikkerheten ikke ivaretas.

FD, likhet med Lyse, forteller at kvalifikasjoner i anskaffelser deles opp i «bør-krav» og «skal-krav». De har også til felles med Lyse at samtlige sikkerhetskrav de stiller er absolutte «skal-krav». De sier videre at samtidig som pris er en viktig faktor, blir sikkerheten vektlagt langt tyngre enn pris og slår fast at pris skal ikke gå på bekostning av sikkerheten.

KSAT opplyser at stadig strengere sikkerhetskrav fra både myndigheter og kunder der KSAT er underleverandører, er med på å forme sikkerhetskravene KSAT stiller til sine underleverandører. De forteller videre at de former kontraktene med underleverandørene sine på en måte som tillater dem virkemidler for å håndheve sikkerhetskrav, som de mener vil både ha en preventiv effekt, samt fungere som en «pisk». De trekker også frem at de bruker «pisk» mye mer enn «gulrot» når de opererer rundt sikkerhet. Samtidig peker de på et viktig positivt insentiv gjennom at de deres sikkerhetsmessige erfaringer med leverandørene er et sentralt punkt når de skal vurdere underleverandører til et nytt oppdrag eller forlengelser (ikke i empiri enda). På denne måten blir underleverandørene insentivert til å drive god sikkerhet gjennom samarbeidet.

Intervjuobjektet fra NRV trekker frem to viktige momenter når de skal velge frem leverandører. Først blir det nevnt at prisen på tjenesten er av betydning, men at det ikke er det viktigste. NRV vektlegger sikkerheten hos leverandøren, samt kompetansen, sertifiseringer og omdømme i bransjen. Videre trekkes det frem at lange relasjoner er av stor betydning, nemlig at leverandører som har vist seg å tilfredstille krav i tidligere samarbeid har et konkurransefortrinn. Ut fra dette ser vi at sikkerhetsfokuset er tydelig, men virkemidlene direkte knyttet til NSM er relativt lite fremtredende.

Forholdene som Lyse og FD skildrer forteller oss to viktige elementer som underleverandørene må rette seg etter. Først vil dette dreie seg om anskaffelsesprossesen. Underleverandørene som holder sikkerheten i tråd med kravene, vil favoriseres fremfor de andre.
Fra dette kan vi se at potensielle leverandører blir møtt med positive insentiver, da god sikkerhet fører at man er bedre stilt i konkurranser. Vi ser omvendt virkning på hos leverandørene som ikke oppfyller sikkerhetskravene.

Det andre elementet handler om insentiver virksomhetene bruker overfor leverandørene som allerede er utvalgt. Lyse, KSAT og FD snakker om at kravene som har blitt stilt vil følges opp gjennom leveranseløpet. Dersom sikkerheten ikke ivaretas som avtalt, vil virksomhetene gjennom de kontraktsfestede sikkerhetsbetingelsene være i posisjon til å ansvarliggjøre leverandørene. Med en antakelse om at det er i leverandørenes egeninteresse å holde på kontraktene sine og ha et glatt samarbeid, vil det da være i deres egeninteresse å etterleve kravene som stilles av prinsipalen.

Telenor på sin side skriver ikke konkret om sine forhold til egne underleverandører, men sier på generelt grunnlag at underleverandører representerer store angrepsflater oppover i verdikjeden. Som tidligere nevnt er kompetanse i bestillerrollen viktig for å redusere risikoen og at dette kan bedres gjennom referanser knyttet til blant annet NSM. Lyse og KSAT trekker imidlertid frem andre former for referanser de tar i bruk, deriblant krav som fremgår av internasjonale standarder, som krav fra kunder i større prosjekter og ISO-standardene. Dette forteller oss at samtidig som NSMs veiledning er viktig, er det andre ressurser som også tas i bruk i sikkerhetsarbeidet.

KONKLUSJON

Vi har i analysen vurdert NSM som prinsipal i sitt forhold overfor private og offentlige selskaper tilknyttet kritisk infrastruktur og undersøkt hvordan dette påvirker deres forhold til egne underleverandører.
Gjennom intervjuene og kildematerialet har vi funnet at NSM gjennom ulike kanaler har påvirket sikkerheten hos samtlige virksomheter vi undersøkte. Hvordan og i hvilken grad dette har foregått har riktignok variert mellom virksomhetene.

I lys av PA-teoriens antakelser har vi tatt utgangspunkt i at virksomhetene til en viss grad har hatt interesser i konflikt med sikkerhetsnivået ønsket av NSM. Vi har identifisert to virkemidler tilknyttet NSM som har hatt innvirkning på dette: sikkerhetsloven og veiledere.
Sikkerhetsloven har vært det tydeligste og hardeste virkemiddelet. KSAT, Telenor, FD og Lyse er alle helt eller delvis underlagt sikkerhetsloven, og/eller regner med å bli det. FD og KSAT som allerede er underlagt loven, forteller om enkeltområder hvor sikkerhetsloven har hatt direkte innvirkning på hvordan bestemte prosesser må foregå. KSAT og Lyse forventer at nye deler av virksomheten skal underlegges og forteller at dette vil kreve omstilling.
Gjennom intervjuene og utvalgt kildemateriale har vi sett et tydelig mønster av at de underlagte virksomhetene i vesentlig grad påvirkes/vil bli påvirket av loven. Slik kan vi se at sikkerhetsloven har vært et gjennomgående effektivt virkemiddel i utvalget vårt. NRV var den eneste virksomheten som ikke knyttet seg til sikkerhetsloven og ga heller ikke uttrykk for å bli direkte påvirket av denne.

Veiledere har kommet frem som et midlere virkemiddel og er betinget på virksomhetenes frivillighet. Flere av virksomhetene nevnte NSM-veiledere som gode og viktige å bruke. Det viktigste som kom frem av veiledningsressurser var NSMs grunnprinsipper, som ble nevnt indirekte av Telenors rapporten, og ellers noe alle intervjuobjektene tok opp. Gjennom alle intervjuene ble grunnprinsippene omtalt som en god og viktig ressurs. Dette styrker opp under synet på NSM som prinsipal for sikkerheten.

Alle virksomhetene vi har undersøkt har fortalt oss at sikkerhet veier er blant de tyngste faktorene, både når de skal velge leverandør og gjennom samarbeidet med leverandørene.
Som et resultat ser vi har virksomhetene har tatt en tydelig prinsipalrolle overfor underleverandørene med tanke på sikkerhet. Leverandørene insentiveres gjennom favorisering i anskaffelsesprosessene og gjennom konsekvenser ved kontraktsbrudd knyttet til sikkerhet. Vi ser også at virksomhetene er tydelige på at sikkerheten i anskaffelser er vel så viktig som prisen og at de gjerne kan betale en høyere pris dersom tjenesten kan leveres med en høyere sikkerhetsstandard.

Begge virkemidlene vi omtaler fra NSM er tydelige på at den digitale sikkerheten i anskaffelser er et viktig element i sikkerhetsbildet - NSM har publisert en egen veileder om anskaffelser under sikkerhetsloven og sikkerhet i anskaffelser er et eget tema under trinn 2 i grunnprinsippene. Sikkerhetsloven og forskriftene regulerer også bruk av eksterne aktører. Alle virksomhetene understreker at de stiller strenge krav nedover i verdikjeden, som kan sees i sammenheng med deres forhold til NSM og sikkerhetsloven.
Særlig vil vi trekke frem FD i denne sammenhengen. FD stiller krav om at sikkerhetsloven er gjeldende sine underleverandører og viser med det helt klart at NSMs sikkerhetsstandarder til FD selv, speiles videre ned i verdikjeden.

Et viktig poeng rundt denne oppgaven er at utvalget består av virksomheter som tilhører bestemte grupper, og at vi jobbet ut noe sammenligningsgrunnlag til andre grupper, og at vi har sett i hovedsak på én side. For eksempel kunne det vært interessant å undersøke og sammenligne med sikkerheten hos virksomheter som ikke noe forhold til NSM, virksomheter av mindre størrelse og lenger ned i verdikjeden eller virksomheter. Dette kunnet bidratt til å styrke en teori om kausalitet mellom NSMs virkemidler og virksomhetenes prinsipalforhold overfor egne underleverandører, og bekrefte/avkrefte om andre faktorer avgjør sikkerhetsnivået.

Resultatet vi likevel kan trekke ut fra analysen er at vi ser klart mønster av sikkerhetsfokus fra NSM rettet mot virksomhetene. De samme virksomhetene har et klart mønster av sikkerhetsfokus rettet mot egne underleverandører. Vi ser en tydelig korrelasjon i oppgaven, men grunnet begrensninger i utvalget, er det vanskelig å konkludere med har en årsakssammenheng mellom NSM og virksomhetenes anskaffelsesprosesser.

LITTERATURLISTE

Hagen, K. P. (1990). Prinsipal-agentteori: Implikasjoner for offentlig styring og politikk. *ØKONOMENE OG VELFERDSSTATEN*.

Jensen, M., & Meckling, W. (1976). *Theory of the firm: Managerial behavior, agency costs and ownership structure*.

Jacobsen, D. I. (2018). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (3. utgave). Oslo: Cappelen Damm akademisk.

Halvorsen, K. (2018). *Å forske på samfunnet: En innføring I samfunnsvitenskapelig metode* (5. utgave). Oslo: Cappelen Damm akademisk.

Christensen, T., Egeberg, M., Lægreid, P., Aars, J. (2016) *Forvaltning og politikk* (4) Oslo: Universitetsforlaget

Regjeringen. (2018). *Saksgang: Ny sikkerhetslov.* Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/dokument/dep/fd/sak/saksgang-ny-sikkerhetslov/id2607089/

Regjeringen. (2014). *Ansvarsområder og oppgaver i Forsvarsdepartementet*. Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/dep/fd/ansvarsomraader/id405/

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner*. (ISBN: 978-82-7768-412-3) Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Nilsen. H. T. Felles og helt, ikke stykkevis og delt. Hentet fra: https://www.telenor.no/om/digital-sikkerhet/forord.jsp

Ragin, C. C. (1999). The Distinctiveness of Case-oriented Research. *Health Services Research, 1999,* 1137-1151. Hentet fra https://stavanger.instructure.com/courses/3682/files/folder/Pensum%3A%20artikler%20som%20skal%20leses?preview=414801

Srivastava, P & Hopwood, N. (2009). A Practical Iterative Framework for Qualitative Data Analysis. *International Journal of Qualitative Methods, 8*(1), 76-84. https://doi.org/10.1177/160940690900800107

Kregnes, S. B. *Nasjonal sikkerhetsmyndighet* (Audio podkast) Hentet fra: https://nsm.no/hold-deg-oppdatert/podcaster/ nr. 21 – ny sikkerhetslov

Academicwork (u.å.) 3 intervjuteknikker – hvilke velger du? Hentet fra: https://www.academicwork.no/insights/arbeidsgivere/3-intervjuteknikker

NSM (u.å.) Sikkerhetsloven og forskrifter. Hentet fra: https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-

forskrifter/?fbclid=IwAR3OIfUDSKPFoQAcOBbNbzfkT7Lkh1rJQCPsQFb1pN4uHlKE3wXzcScQ_2g

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet.* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Virksomhetsikkerhetsforskriften. (2019). *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (FOR-2018-12-20-2053). Lovdata. https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

Klareringsforskriften. (2019). *Forskift om sikkerhetsklarering og annen klarering* (FOR-2018-12-20-2054) Lovdata. https://lovdata.no/dokument/SF/forskrift/2018-12-20-2054?fbclid=IwAR2uN32dATriQsJ1DLaWp_GpUCRk2SV2PnGmvxYpvR6H19WGHffvLcF0m_M

NSM (u.å.) Veiledere og håndbøker til sikkerhetsloven. Hentet fra: https://l.facebook.com/l.php?u=https%3A%2F%2Fnsm.no%2Fregelverk-og-hjelp%2Fveiledere-og-handboker-til-sikkerhetsloven%2F%3Ffbclid%3DIwAR2C5OhrPW_j5kzDiNAcF7051BCfBLnWCXPwNW1Zu5q6S1BzAFY152tWrfo&h=AT1jH30CvieqoRTeV4nk42IgUrkFIBfGLnRi4MjeilwnaUZvDvU4N3dNuzA7h52bf0yXEgThpbZg2AqB0LMgd1digWslxnv32cgxKbWWZ96fXCb7Jd6HH8_P2ayPOSaGmIj4375

Nasjonal sikkerhetsmyndighet. (2020) *NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0.* Hentet fra: https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf?fbclid=IwAR0WxwVlZUTzblfyhvnJwZt9e8tpgVTWZWPJmXS5dU12O7AsO3g16Go-w_c

Nasjonal sikkerhetsmyndighet. (2019) *Veileder i anskaffelser etter sikkerhetsloven.* Hentet fra: https://nsm.no/getfile.php/133651-1592813221/Demo/Dokumenter/Veiledere/veileder-i-anskaffelser-etter-sikkerhetsloven-versjon-1.pdf?fbclid=IwAR0amyi4wuAYD4hfoGTO4GnYxvIcWMIZxCdV2pIDqEzro63Vut8pJHKvjhs

LYSE. (u.å.) *Hovedside.* Hentet fra: https://www.lysekonsern.no/

Helsenord IKT (14.06.2018) *Framtidig arbeidsflate.* Hentet fra: https://helsenordikt.no/Documents/Styret/Styrem%C3%B8ter/2018/20180830/20180831/Styresak%20040-2018-1%20vedlegg%20-%20Konseptutredning%20Del%20I.pdf

Nasjonal kommunikasjonsmyndighet (2019) *Til informasjon: Brannvern – klarering av personell.* Hentet fra: https://www.dsb.no/globalassets/dokumenter/brann-og-redning-bre/prinsippavgjorelser/2019-06-04-tilsyn_skjermingsverdige-objekter_personell-ma-sikkerhetsklareres_brannvesen_sak-2019_3119.pdf

Telenor. (u.å.) Telenor Security Operation Centre (TSOC). Hentet fra: https://www.telenor.no/bedrift/sikkerhet/tsoc/?fbclid=IwAR0qpdRw_vASlCQZx-7XTDrTGVw72DuzxDx1moR5FmXUd4dEnKa-BwfHXRE

Telenor. (23.06.2020). *De lange linjene – Digital sikkerhet 2020.* Hentet fra: https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf

Geertz, C. (2003) *Thick Description: Toward an Interpretive Theory of Culture.* Oxford, UK. Hentet fra: https://books.google.no/books?hl=en&lr=&id=8aXWAQAAQBAJ&oi=fnd&pg=PA143&dq=geertz+thick+descriptions&ots=lh6YN_COGs&sig=iW-EZteWUAq3aG506S8j81SM9kM&redir_esc=y#v=onepage&q=geertz%20thick%20descriptions&f=false

NSM. (2020) *Helhetlig digitalt risikobilde 2020.* Hentet fra: https://nsm.no/getfile.php/134267-1601027852/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf?fbclid=IwAR0WWcGvmNz1NDVeR140kYMF6VfTqcFoRVkDeJPm_1OL1IupFhgJgv5tD7Q

Hagen, K. P. (1990). Prinsipal-agent teori : implikasjoner for offentlig styring og politikk.

Lane, J.-E. (2013). *The Principal-Agent Approach to Politics: Policy Implementation*, ss. 85-89.

Njå, O. (2020). Samfunnssikkerhet i et systemperspektiv. I *Samfunnssikkerhet : analyse, styring og evaluering* (ss. 129-149). Oslo: Universitetsforlaget.

Regjeringen (28.04.2021). Liste over kritiske samfunnsfunksjoner. Hentet fra: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/liste-over-kritiske-samfunnsfunksjoner/id2695609/

Atlantic Council (2019). Breaking Trust. Hentet fra: https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/