Samfunnsøkonomisk vurdering av anbefalinger fra IKT-sikkerhetsutvalget

Utarbeidet for IKT-sikkerhetsutvalget

osloeconomics

Om Oslo Economics

Oslo Economics utreder økonomiske problemstillinger og gir råd til bedrifter, myndigheter og organisasjoner. Våre analyser kan være et beslutningsgrunnlag for myndighetene, et informasjonsgrunnlag i rettslige prosesser, eller et grunnlag for interesseorganisasjoner som ønsker å påvirke sine rammebetingelser. Vi forstår problemstillingene som oppstår i skjæringspunktet mellom marked og politikk.

Oslo Economics er et samfunnsøkonomisk rådgivningsmiljø med erfarne konsulenter med bakgrunn fra offentlig forvaltning og ulike forsknings- og analysemiljøer. Vi tilbyr innsikt og analyse basert på bransjeerfaring, sterk fagkompetanse og et omfattende nettverk av samarbeidspartnere.

Samfunnsøkonomisk utredning

Oslo Economics tilbyr samfunnsøkonomisk utredning for departementer, direktorater, helseforetak og andre virksomheter. Vi har kompetanse på samfunnsøkonomiske analyser i henhold til Finansdepartementets rundskriv og veiledere.

Fra samfunnsøkonomiske og andre økonomiske analyser har vi bred erfaring med å identifisere og vurdere virkninger av ulike tiltak. Vi prissetter nyttevirkninger og kostnader, eller vurderer virkninger kvalitativt dersom prissetting ikke lar seg gjøre.

Samfunnsøkonomisk vurdering av anbefalinger fra IKT-sikkerhetsutvalget /OE rapport 2018:37

Kontaktperson:
Asbjørn Englund / Senior Partner
aen@osloeconomics.no, Tel. 91318802

Innhold

Sammendrag og konklusjoner

Oslo Economics har på oppdrag fra IKT-sikkerhetsutvalget foretatt samfunnsøkonomiske vurderinger av tiltak utvalget foreslår i sin utredning. Vi har gjennomført informasjonsinnhenting fra relevante aktører gjennom semi-strukturerte intervjuer og det er foretatt samfunnsøkonomiske analyser av hvert tiltak. IKT-sikkerhetsutvalget har foreslått i alt fem tiltak:

Tiltak 1: Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
Tiltak 2: Sikkerhet ved anskaffelser
Tiltak 3: Tydeligere styring og bedre koordinering
Tiltak 4: Opprette et IKT-sikkerhetssenter
Tiltak 5: Tydeligere ansvar og regulering på tilkoblede produkter og tjenester

Denne rapporten starter med en beskrivelse av bakgrunnen og mandatet for Oslo Economics' analyser, og deretter presenteres metoden som er benyttet. Metoden er basert på DFØs veileder for samfunnsøkonomiske analyser, og det er særlig vurdering av ikke-prisede effekter som er relevant. Etter metodekapitlet følger en oversikt over informasjonsgrunnlaget Oslo Economics har benyttet seg av, altså hvilke personer og virksomheter som er intervjuet. Totalt er 13 virksomheter intervjuet, og disse omfatter både offentlig og privat sektor, samt én internasjonal aktør.

I kapittel 4 presenterer vi en samfunnsøkonomisk problembeskrivelse av IKT-sikkerhetsområdet. Det er fire problemstillinger som fremheves spesielt i kapitlet: insentivproblemer, kompetansebehov, kapasitetsutfordringer og koordineringsproblemer. Senere i kapittelet illustreres en målstruktur, der samfunnsmålet om bedre IKT-sikkerhet dekomponeres i mål om bedre håndtering og bedre forebygging, før disse igjen dekomponeres i en rekke effektmål.

I kapittel 5, 6, 7 og 8 foretas de samfunnsøkonomiske vurderingene av de respektive tiltakene. Disse følger arbeidsfasene fra DFØ, og en beskrivelse av nullalternativene og målene følges av en beskrivelse av tiltakene, før det foretas identifisering og vurdering av virkninger. Etter vurderingen av virkningene, følger en vurdering av usikkerheten, et perspektiv som er særlig viktig i denne rapporten. Til slutt vurderes samfunnsøkonomisk lønnsomhet av hvert tiltak, før Oslo Economics presenterer sin samlede vurdering og sine anbefalinger.

Den samfunnsøkonomiske vurderingen av tiltaket om å etablere en tverrsektoriell IKT-sikkerhetslov er at en slik lov har potensielt stor positiv virkning på IKT-sikkerheten, men at ytterligere utredninger kan være nødvendig. Det er usikkerhetsmomenter i Oslo Economics' forventede virkninger av tiltaket, både om behovet for en lov og hvordan den eventuelt bør formuleres. Usikkerhetsomfanget bør trolig reduseres før man beslutter å etablere en ny lov. Det er også en forventet positiv virkning av å stille krav til IKT-sikkerhet i anskaffelsesregelverket, men potensielle markedseffekter må tas i betraktning når disse reglene eventuelt skal formuleres.

På anbefalingen om at Justis- og beredskapsdepartementet (JD) skal ta tydeligere lederskap, er den samfunnsøkonomiske vurderingen at tydeligere styring og koordinering på IKT-sikkerhetsområdet vil være samfunnsøkonomisk lønnsomt, selv om vi ikke har hatt nok informasjon til å vurdere kostnadene. Det er imidlertid en del usikkerhet også rundt dette forslaget, blant annet om IKT-sikkerhetsområdets tverrsektorielle natur begrenser JDs muligheter til å ta en lederrolle.

Tiltaket om opprettelsen av et IKT-sikkerhetssenter er det som utgjør den mest omfattende delen av denne rapporten. Det er gjort en samfunnsøkonomisk vurdering av både det å etablere et IKT-sikkerhetssenter underlagt NSM, slik det er planlagt per i dag, og en vurdering av et alternativ der et IKT-sikkerhetssenter er frittstående og sivilt. I den samfunnsøkonomiske vurderingen gjøres grove anslag på kostnadene ved de to alternativene, samt en vurdering av de kvalitative virkningene. Det er en del usikkerhet i virkningene også her, både når man sammenligner omfanget av virkningene på tvers av de to alternativene og om man sammenligner med nullalternativet. Oslo Economics vurderer at en del nyttevirkninger vil være sterkere ved et rent sivilt senter, men at det er enkelte viktige usikkerhetsmomenter, for eksempel ved betydningen av

militær etterretningsinformasjon som kanskje forsvinner ved ren sivil forankring. Hovedanbefalingen fra Oslo Economics er at ytterligere utredninger behøves, både på om det faktisk er et behov for et IKT-sikkerhetssenter, og om det burde ligge under NSM eller være mer frittstående.

På det femte tiltaket, om å skape tydeligere ansvar og regulering på tilkoblede produkter og tjenester, presenterer Oslo Economics en vurdering av hvilke konsekvenser som er relevante for et slikt tiltak. Også her vurderes virkningene å være samfunnsøkonomisk lønnsomme, men det er betydelig usikkerhet i virkningene. Foruten at tydeligere myndighetsansvar på området vurderes å kunne være samfunnsøkonomisk lønnsomt, konkluderer Oslo Economics at reguleringsforholdet på tilkoblede produkter og tjenester er en viktig problemstilling. Ettersom markedet for tingenes internett kan ha betydelige eksternaliteter, støtter Oslo Economics anbefalingen om å foreta en vurdering av produktansvarsregelverket.

1. Bakgrunn og mandat

Digitaliseringen endrer samfunnet i rekordfart. Den gjør at vi jobber på nye måter, at næringslivet og offentlig sektor effektiviseres og at nye næringer oppstår og erstatter gamle næringer. Digitaliseringen har imidlertid også gjort oss sårbare for feil, naturkatastrofer eller bevisste angrep mot den digitale infrastrukturen.

Regjeringen har oppnevnt IKT-sikkerhetsutvalget for å gjennomføre en utredning av IKT-sikkerheten i Norge samt identifisere tiltak for å forbedre den.

IKT-sikkerhetsutvalget definerer IKT-sikkerhet som beskyttelse av IKT-systemene, tjenestene de leverer og informasjonen de behandler. Utvalget presenterer følgende sikkerhetsmål:

- **Tilgjengelighet**: IKT-systemene, informasjonen som behandles i systemene og tjenestene som er tilknyttet systemene er tilgjengelig for brukerne
- **Integritet**: IKT-systemene, informasjonen som behandles i systemene og tjenestene som er tilknyttet systemene endres ikke utilsiktet eller uautorisert
- **Konfidensialitet**: IKT-systemene, informasjonen som behandles i systemene og tjenestene som er tilknyttet systemene er kun tilgjengelig for de som rettmessig skal ha tilgang

Utvalgets mandat er å vurdere:

- Om dagens regulering er hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet
- Om vi har en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet
- Hvilke regulatoriske og organisatoriske grep som bør gjøres for å styrke nasjonal IKT-sikkerhet

Utgangspunktet for mandatet er at regjeringen mener det er behov for å utrede både den rettslige reguleringen på IKT-sikkerhetsområdet og organiseringen av det tverrsektorielle ansvaret.

I sin melding til Stortinget[1] identifiserer regjeringen følgende sentrale tiltak:

- Utarbeide en ny nasjonal strategi for IKT-sikkerhet, inkludert en handlingsplan
- Etablere et forum for offentlig-privat samarbeid for å støtte opp under det nasjonale arbeidet med IKT-sikkerhet
- Videreutvikle nettverk for informasjonssikkerhet for å sikre at strategiske spørsmål om IKT-sikkerhet i Norge og internasjonalt blir diskutert og koordinert
- Videreutvikle totalforsvaret og øke motstandsdyktigheten i samfunnskritiske funksjoner, blant annet innenfor robuste kommunikasjonssystemer

IKT-sikkerhetsutvalget har identifisert i alt fem anbefalinger til tiltak:

Tiltak 1: Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
Tiltak 2: Sikkerhet ved anskaffelser
Tiltak 3: Tydeligere styring og bedre koordinering
Tiltak 4: Opprette et IKT-sikkerhetssenter
Tiltak 5: Tydeligere ansvar og regulering på tilkoblede produkter og tjenester

Da denne rapporten ble skrevet var ikke anbefalingene endelige, og vi har derfor vurdert utkast til anbefalinger parallelt med utvalgets arbeid. Tiltak 1 og 2 er vurdert i sammenheng, i kapittel 5.

Oslo Economics er engasjert av utvalget for å vurdere samfunnsøkonomiske effekter av de anbefalte tiltakene. Arbeidet er gjennomført i tidsrommet august 2018 til oktober 2018.

[1] (Meld. St. 38, 2016-2017)

2. Metode

IKT-sikkerhetsutvalget har identifisert fem tiltak for å bedre IKT-sikkerheten i Norge. Tiltakene har nyttevirkninger, men også kostnader som må veies opp mot nytten. I det følgende beskriver vi vår metodiske tilnærming til analysen av de fem tiltakene.

2.1 Samfunnsøkonomisk analyse

For å vurdere utvalgets anbefalinger har vi tatt utgangspunkt i veilederen til Direktoratet for økonomistyring (DFØ, 2018), som er basert på Finansdepartementets krav og prinsipper. Veilederen til DFØ beskriver åtte steg i en samfunnsøkonomisk analyse, vist i Figur 2-1: Arbeidsfasene i en samfunnsøkonomisk analyseFigur 2-1. Vi har fulgt veilederen så langt det passer i vurderingen av anbefalingene.

Figur 2-1: Arbeidsfasene i en samfunns-økonomisk analyse

Steg 1 baseres på de tre sikkerhetsmålene, men det vil også være nødvendig å identifisere mer konkrete effektmål. Effektmålene beskriver den ønskede direkte effekten av tiltakene. Effektmålene utformes fra et brukerperspektiv, og utledes fra de mer grunnleggende sikkerhetsmålene. «Bedre koordinering» er ett eksempel på et effektmål, som i kombinasjon med andre effektmål kan lede til oppnåelse av sikkerhetsmålene.

Vi vil identifisere effektmål for hvert enkelt tiltak, og det er disse som vil legge grunnlaget for den samfunnsøkonomiske analysen. Det skal altså vurderes om tiltakene fra IKT-sikkerhetsutvalget vil kunne oppnå effektmålene. Denne vurderingen består av å identifisere virkninger (nytte og kostnad), vurdere virkningene, og til sist gjøre en vurdering av den samfunnsøkonomiske lønnsomheten. Tiltakene har ulik karakter, og noen er mer utførlig beskrevet enn andre. Derfor er vi mer grundige i våre analyser for enkelte tiltak enn andre.

Ikke-prissatte virkninger

Ikke-prissatte effekter er virkninger som ikke kan eller bør tallfestes, men som likevel skal vurderes opp mot kostnadene. Eksempler kan være hvorvidt et tiltak fører til bedre koordinering i offentlig sektor eller bedre rådgivning til befolkningen, og slike virkninger vil utgjøre en betydelig del av en samfunns-økonomisk analyse på IKT-sikkerhetsområdet. Disse virkningene vurderes kvalitativt, og inngår i den samlede vurderingen av tiltakenes samfunnsøkonomiske lønnsomhet.

For å vurdere de ikke-prissatte effektene benytter vi oss av pluss-minusmetoden slik den er beskrevet i DFØs veileder. Pluss-minusmetoden skal vurdere både betydning og omfang for virkningene, som til sammen angir virkningenes anslåtte konsekvens. Både hvilken betydning hver av virkningene vurderes å ha, samt hvilket omfang, baseres på en helhetsvurdering av informasjonsgrunnlaget fra dybdeintervjuene, samt skriftlige kilder.

Tabell 2-1: Konsekvensmatrise ikke-prissatte virkninger

		Betydning		
		Liten	Middels	Stor
Omfang	Stort positivt omfang	++	+++	++++
	Middels positivt omfang	+	++	+++
	Lite positivt omfang	0	+	++
	Intet omfang	0	0	0
	Lite negativt omfang	0	÷	÷÷
	Middels negativt omfang	÷	÷÷	÷÷÷
	Stort negativt omfang	÷÷	÷÷÷	÷÷÷÷

Kilde: (DFØ, 2018)

I Tabell 2-1 kan man se hvordan både betydningen og omfanget av en virkning spiller inn på den endelige konsekvensen for samfunnet. Når man til slutt bestemmer konsekvensene, vil de baseres på følgende nidelte skala:

Tabell 2-2: Nidelt konsekvensskala

++++	Meget stor positiv konsekvens
+++	Stor positiv konsekvens
++	Middels positiv konsekvens
+	Liten positiv konsekvens
0	Ubetydelig/ingen konsekvens
÷	Liten negativ konsekvens
÷÷	Middels negativ konsekvens
÷÷÷	Stor negativ konsekvens
÷÷÷÷	Meget stor negativ konsekvens

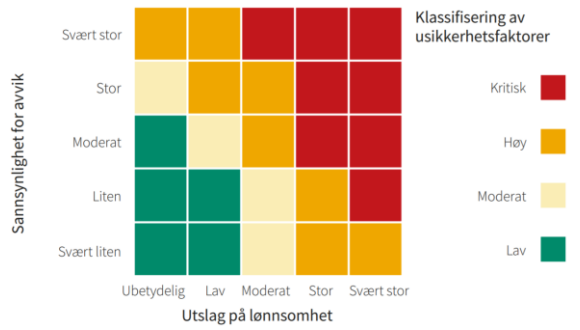
Usikkerhetsanalyse

I våre analyser har vi vært nødt til å ta en del forutsetninger, og det kan være nyttig å drøfte hvor følsomme og robuste lønnsomhetsvurderingene er til disse forutsetningene. Vi lener oss derfor på DFØs veileder for kartlegging av usikkerhetsfaktorer.

Både prissatte og ikke-prissatte virkninger vil kunne være preget av usikkerhet, og det kan være nyttig å si noe om hvor mye støy de ulike virkningene har. For noen effekter, der det er en tydelig og direkte kausal sammenheng mellom tiltaket og virkningen, vil usikkerheten kunne være lav. For andre virkninger kan utfallsrommet være slik at en forventet positiv virkning plutselig kan bli negativ ved en liten endring i forutsetningene.

Figur 2-2 viser hvordan DFØs veileder overordnet foreslår å gjennomføre en usikkerhetsanalyse. Usikkerhet er et produkt av to faktorer: Sannsynlighet for avvik og utslag på lønnsomhet. Kombinasjonen av disse faktorene resulterer i en vurdering av usikkerheten som «kritisk», «høy», «moderat» og «lav», illustrert med fargekoder i figuren. Selv om det er dette rammeverket som ligger til grunn for vår vurdering av usikkerhet, har vi valgt å fremstille våre vurderinger uten konkret henvisning til begrepene i Figur 2-2.

Figur 2-2: Usikkerhetsanalyse



Kilde: (DFØ, 2018)

2.2 Metode for datainnsamling

For å få innsikt om hvilke virkninger utvalgets anbefalinger potensielt kan ha, har vi gjennomført semi-strukturerte intervjuer med relevante aktører på IKT-sikkerhetsområdet. Vi har sendt ut intervjuguider i forkant av intervjuene, som ligger i Vedlegg A.

Et semi-strukturert intervju innebærer at man har en fleksibel tilnærming til intervjuguiden, og vi har bevisst fokusert på de temaene som har vært mest relevante for de ulike intervjuobjektene. Hvert intervju har hatt et omfang på 1–2 timer. En beskrivelse av intervjuobjektene følger i neste kapittel.

3. Informasjonskilder

I gjennomføringen av den samfunnsøkonomiske analysen har vi benyttet oss av både kvalitative og kvantitative data og analyser av disse.

For den kvalitative datainnsamlingen har vi gjennomført semi-strukturerte intervjuer med ulike interessenter for å få identifisert virkninger av anbefalingene, samt å vurdere betydning og omfang av virkningene. Vi har intervjuet representanter fra en rekke offentlige departementer og etater, samt andre aktører sentrale på IKT-sikkerhets-området.

3.1 Offentlige virksomheter og etater

Offentlig sektors tverrsektorielle samarbeid og koordinering er viktig for å kunne forhindre og håndtere cybersikkerhetsangrep. Derfor er også mange offentlige etater og virksomheter viktige informanter for å vurdere problemstillingen.

Det er to fremtredende departementer på IKT-sikkerhetsområdet: Justis- og beredskaps-departementet og Forsvarsdepartementet. Disse to har til sammen ansvar for den nasjonale IKT-sikkerheten, med ansvar for henholdsvis sivil og militær sektor. Videre er det en rekke etater som er underlagt hvert av disse departementene (og andre departe-menter) som også spiller viktige roller. Styringen av etatene, samt koordineringen og samarbeidet mellom dem, er et gjennom-gående tema i vurderingene våre.

Vi har gjennomført dybdeintervjuer med følgende offentlige virksomheter, departementer og etater:

- Justis- og beredskapsdepartementet (JD)
  - Martin Kjellsen, avdelingsdirektør
- Forsvarsdepartementet (FD)
  - Ole Felix Dahl, avdelingsdirektør
  - Rita Edvardsen, seniorrådgiver
  - Mia Harlyng, seniorrådgiver
  - Ørnulf Storm, fagdirektør
- Nasjonal sikkerhetsmyndighet (NSM)
  - Bente Hoff, avdelingsdirektør
  - Annette Tjaberg, assisterende direktør
  - Hans Christian Pretorius, avdelingsdirektør
- Kripos
  - Ketil Haukaas, sjef
- Nasjonalt cyberkrimsenter (NC3)
  - Olav Skard Jørgensen, leder
- Direktoratet for samfunnssikkerhet og beredskap (DSB)
  - Erik Thomassen, fagdirektør
- Direktoratet for forvaltning og IKT (Difi)
  - Remi Longva, seniorrådgiver
  - Øyvind Grinde, seksjonssjef
- Datatilsynet
  - Martha Eike, fagdirektør
  - Gullik Gundersen, juridisk rådgiver
- Nasjonal kommunikasjonsmyndighet (Nkom)
  - Elise Lindeberg, avdelingsdirektør
  - Bjørn Erik Eskedal, fagdirektør
  - Rune Kanck, seksjonssjef
  - Frank Stien, seksjonssjef
  - Svein Sundfør Scheie, seksjonssjef

I intervjuene fikk informantene anledning til å komme med innspill om generelle utfordringer på IKT-sikkerhetsområdet, forklare hvordan de opplever koordineringen og samarbeidet i offentlig sektor, samt vurdere relevansen og effektene av de ulike anbefalingene fra IKT-sikkerhetsutvalget.

3.2 Næringsliv

Utvalget trekker frem offentlig-privat samarbeid som viktig for IKT-sikkerheten, og fremhever at det private næringslivet er viktig for den totale IKT-sikkerheten. Vi har intervjuet representanter fra næringslivet for å vurdere dette nærmere. Ett av spørsmålene vi ville undersøke var om private virksomheter er mindre opptatte av IKT-sikkerhet enn de burde være og om man kan ha et insentivproblem på området. Videre ville vi undersøke om det er kompetansemangler på IKT-sikkerhetsområdet blant private aktører. Det var også nyttig å få innspill om hvordan privat sektor vurderer myndighetenes arbeid på området.

Vi har intervjuet følgende aktører for å belyse disse spørsmålene nærmere:

- Norsk senter for informasjonssikring (NorSIS)
  - Peggy Heie, administrerende direktør
- Næringslivets sikkerhetsråd
  - Arne Røed Simonsen, seniorrådgiver
- Telenor
  - Hanne Tangen Nilsen, Chief Security Officer
  - Rolv R. Hauge, Head of Telco Security
  - Storm Jarl Landaasen, Chief Intelligence Officer

I likhet med de offentlige virksomhetene og etatene, fikk også representantene for det private næringslivet anledning til å komme med generelle innspill, samt vurdere IKT-sikkerhetsutvalgets anbefalinger.

3.3 IKT-sikkerhetssenter

For å få et innblikk i hvordan et IKT-sikkerhetssenter fungerer i praksis har vi samlet inn informasjon om internasjonale IKT-sikkerhetssentre. I den forbindelse har vi også intervjuet følgende senter:

- National Cyber Security Centre (NCSC), Storbritannia
  - Simon Parsons, Deputy director for strategy

NCSC fikk tilsendt en intervjuguide tilpasset deres britiske forankring. En del norske forhold ble dermed ikke belyst i intervjuet av det britiske IKT-sikkerhetssenteret.

4. Problembeskrivelse

IKT-sikkerhet påvirker mange deler av samfunnet vårt, og den raske digitaliseringen fører med seg utfordringer. Cyberangrep har potensielt store skadevirkninger på samfunnet, så det er et problemområde hvor myndighetene ser behov for utredning.

I det følgende presenteres noen samfunnsøkonomiske betraktninger ved IKT-sikkerhetsområdet. Et sentralt tema er at IKT-sikkerhet innebærer markedssvikt ved at negative eksterne virkninger ikke fanges opp av aktørene i samfunnet.

4.1 Problemstillinger

4.1.1 Insentivproblemer

Et kjent problem i fagfeltet «economics of information security» er at bedrifter kan ha insentiver som fører til underinvestering i IKT-sikkerhet. Gordon-Loeb-modellen illustrerer det optimale investeringsnivået i IKT-sikkerhet. Generelt viser modellen at selskaper som er profittmaksimerende og følger sine egeninteresser kun burde investere en liten andel av det forventede tapet ved IKT-sikkerhetsbrudd (Gordon & Loeb, 2002).

Dersom man inkluderer de negative eksternalitetene ved IKT-sikkerhetsbrudd, altså samfunnsvirkninger utenfor virksomhetene, viser Gordon et al. (2015) at det bedriftsøkonomisk rasjonelle investeringsnivået vil være for lavt i et samfunnsøkonomisk perspektiv. Den teoretiske prediksjonen er derfor at det vil skje en underinvestering i IKT-sikkerhet. Det verste som kan skje med selskapene er en konkurs, mens samfunnet blir sittende igjen med hoveddelen av kostnadene.

Et annet poeng er at virksomheter kan velge å investere mindre i sikkerhetstiltak fordi investeringene er synlige som kostnader i regnskapene. Sikkerhetsinvesteringene har derfor normalt negativ innvirkning på lønnsomheten i virksomhetene. Derfor kan agentproblemer oppstå om ledelsen i selskapene er mer opptatte av kortsiktig lønnsomhet (som for eksempel sin egen bonus) enn sikkerhetstruslene.

Som konkludert av Gordon et al. (2015) vil den mulige samfunnsøkonomiske underinvesteringen kunne skape en trussel mot nasjonal sikkerhet, og det rettferdiggjør trolig at myndigheter regulerer eller setter inn virkemidler for å påvirke insentivene i det private næringslivet. Dette argumentet understøtter behovet for at IKT-sikkerhetsutvalget foreslår tiltak som har som formål å forbedre IKT-sikkerheten i private virksomheter.

Bekymringen for at det potensielt kan foregå en underinvestering i IKT-sikkerhet i det private næringslivet erkjennes av IKT-sikkerhetsutvalget. Utvalget drøfter derfor hvorvidt man bør ta i bruk juridiske-, økonomiske-, pedagogiske- eller organisatoriske virkemidler for å få bedrifter til å prioritere IKT-sikkerhetstiltak i større grad.

I tillegg til potensielle insentivproblemer i det private næringslivet, kan det også oppstå insentivproblemer i offentlig sektor. Det er for eksempel ikke utenkelig at noen etater har insentiver til først og fremst å drive digitaliseringen fremover med siktemål om økt effektivitet, mens andre i første rekke ønsker å ha god IKT-sikkerhet. Dette er en form for målkonflikt, som kan føre til incentivproblemer. Et annet eksempel kan være at mens noen etater ønsker å fremme personvern og dermed er motstandere av for eksempel lang lagringstid for logger, kan andre etater ønske lengre lagringstid for å få bedre etterretningsinformasjon.

4.1.2 Kompetansebehov

Det er komplekse sammenhenger på IKT-sikkerhetsområdet, noe som gjør at det ofte kreves en viss kompetanse for å kunne forstå risikoen, herunder både sårbarheter og trusler. Mange enkeltpersoner, private og offentlige virksomheter vil ikke ha godt nok informasjonsgrunnlag til å kunne identifisere de gode tiltakene for å hindre IKT-sikkerhetsbrudd. Én hypotese kan derfor være at det investeres for lite i IKT-sikkerhet fordi individer og virksomheter ikke forstår truslene godt nok til å håndtere dem rasjonelt.

At det er et kompetansebehov på IKT-sikkerhetsområdet er også konklusjonen i

Lysneutvalgets rapport, som videre etterspurte mer forskning (NOU, 2015:13). Det ble senere vist i en rapport av NIFU at det er et økende gap mellom tilbud og etterspørsel etter IKT-sikkerhetskompetanse, ettersom etterspørselen er forventet å vokse mer enn tilbudet frem mot 2030 (NIFU, 2017).

Én måte å redusere problemene knyttet til kompetansebehovene på IKT-sikkerhetsområdet er å gjøre befolkningen bedre informert. Dette kan gjøres gjennom digital opplæring og vil trolig kunne føre til at flere vil gjennomføre hensiktsmessige tiltak, ettersom man bedre forstår risikoen man er eksponert for og som man også kan utsette andre for. Et eksempel på dette kan være at individer forstår viktigheten av å ha sikre passord.

En annen tilnærming for å redusere utfordringen er å erkjenne at IKT-sikkerhetskompetanse delvis er en knapp ressurs, og derfor øke kompetansen i en sentralisert enhet og derfra innføre virkemidler som kan lede virksomheter og personer til å ta formålstjenlige beslutninger.

En del av kompetanseutfordringen i privat sektor er knyttet til «sourcing». Dersom en virksomhet for eksempel velger å outsource IKT-sikkerhetsområdet, vil graden av IKT-sikkerhet avhenge mye av hvem man velger å samarbeide med og sette ut deler av porteføljen til. For små virksomheter med lav IKT-sikkerhetskompetanse, vil outsourcing trolig kunne føre til bedre IKT-sikkerhet. I denne delen av IKT-sikkerhetsstrategien trekker informantene frem at mye handler om økonomiske og administrative planer. Næringslivets Sikkerhetsråd (2018) viser at mens 17 prosent av virksomhetene outsourcer IT-driften fullt ut, outsourcer 31 prosent av virksomhetene IT-driften delvis.

I offentlig sektor virker det også å være stort kompetansebehov på IKT-sikkerhetsområdet. I en rapport fra Difi (2018) fremkommer det at 68 prosent av virksomhetene i statsforvaltningen ikke klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet. I rapporten anbefaler Difi at virksomhetene kartlegger sin kompetanse og sikkerhetskultur, og basert på kartleggingen utformer eventuelle tiltak til forbedring.

4.1.3 Kapasitetsutfordringer

En faktor som vil påvirke IKT-sikkerheten er ressursene som blir lagt inn i IKT-sikkerhetsforbedringer. At etatene med myndighetsansvar på IKT-sikkerhetsområdet har nok ressurser, er derfor en forutsetning for å forebygge og håndtere trusler. I IKT-sikkerhetsutvalgets undersøkelser, der de ba om skriftlige innspill fra 186 virksomheter i offentlig og privat sektor, påpekte respondentene at de ikke opplever at de får tilstrekkelig veiledning på IKT-sikkerhetsområdet. Dette kan være et tegn på at det finnes kapasitetsutfordringer i offentlig sektor.

4.1.4 Koordineringsproblemer

IKT-sikkerhetsområdet er tverrsektorielt av natur ettersom alle sektorer har en viss sårbarhet mot IKT-sikkerhetshendelser. Det er i dag sektorvise responsmiljøer på IKT-sikkerhetsområdet, og flere sektorer har sin egen sektor-CERT. Videre er det tverrsektorielle responsmiljøer, slik som NSMs NorCERT, som skal avdekke og håndtere truslene som har nasjonal betydning.

NSM er administrativt underlagt Forsvarsdepartementet, med faglig rapporteringslinje til Justis- og beredskapsdepartementet om saker i sivil sektor. Overordnet er det Justis- og beredskapsdepartementet som har ansvar for å utforme politikk på IKT-sikkerhet i sivil sektor. Justis- og beredskapsdepartement har også ansvar for den tverrsektorielle styringen, koordineringen og samarbeidet.

Det er mange etater og veiledningsaktører på IKT-sikkerhetsområdet, og respondentene i spørreundersøkelsen til IKT-sikkerhetsutvalget peker på at veiledningsaktørene har ulik begrepsforståelse og gir forskjellige råd innenfor samme tema. Dette kan være et tegn på at det er koordineringsproblemer blant myndighetsorganene. Fordi råd og veiledning vil være nødvendig for å kunne imøtekomme kompetansebehovet, i tråd med diskusjonen under 4.1.2, vil disse koordineringsproblemene kunne ha negative samfunnsøkonomiske effekter.

4.2 Målstruktur

Figur 4-1 viser målstrukturen vi tar utgangspunkt i for de samfunnsøkonomiske analysene. Vi har etter innspill fra informanter valgt å bryte opp samfunnsmålene i

to: forebygging og håndtering av IKT-sikkerhetshendelser. Disse understøttes igjen av en rekke effektmål. Dekomponeringen er i første rekke en illustrasjon, og flere av effektmålene understøtter i realiteten både forebygging og håndtering.

4.2.1 Bedre forebygging

For sikkerhetsmålet om bedre forebygging av IKT-sikkerhetshendelser har vi identifisert fire effektmål. Som drøftet i 4.1.1 og 4.1.2 vil potensielt viktige problemstillinger være knyttet til insentivproblemer og kompetanse-mangler. Basert på disse argumentene vil viktige effektmål for eventuelle IKT-sikkerhetstiltak være å redusere både insentivproblemene og øke kompetansen på IKT-sikkerhet. Disse elementene vil derfor være sentrale i målstrukturen, og flere av tiltakene som analyseres i denne rapporten vil måles opp mot disse effektmålene.

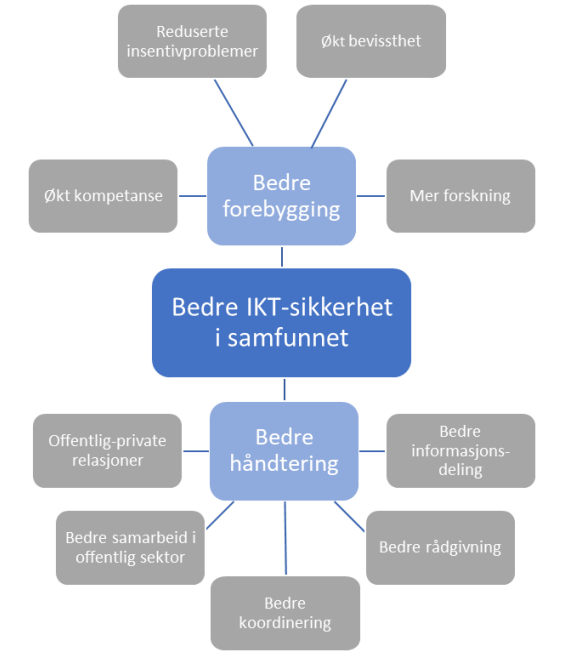
For forebygging av IKT-sikkerhetshendelser vil det også være et mål å skape økt oppmerksomhet og bevissthet rundt IKT-sikkerhet. Mørketallsundersøkelsen foretatt for NSR viser at 61 prosent av virksomhetene i utvalget har det siste året gjennomført aktiviteter for å øke de ansattes bevissthet rundt sikkerhet.

IKT-sikkerhet er et komplekst felt, og vi tror at mer forskning på området vil styrke evnen til forebygging. Dette var også en av konklusjonene til Lysneutvalget. Utviklingen på IKT-området er svært rask, og relevant og velinformert forskning er avgjørende for å kunne følge med på trusselbildet, og samtidig bidra til innsikt på hvilke forebyggende tiltak som gir best effekt.

4.2.2 Bedre håndtering

Vi har identifisert fem effektmål relatert til håndteringen av IKT-sikkerhetstrusler.[2] God informasjonsdeling er viktig, slik at myndighetsorganer og andre relevante aktører kan ha det nødvendige informasjons-grunnlaget for å håndtere hendelser korrekt og effektivt. Dette relaterer til både den rent tekniske infrastrukturen for varslingene, samt silingen og koordineringen av informasjonen.

Figur 4-1: Målstruktur



Illustrasjon: Oslo Economics

For å bedre håndteringsevnen er det også viktig med god, relevant og enhetlig rådgiving. For at etater og virksomheter også kan forholde seg til informasjonen som deles, må de ha kompetansen som skal til, og denne kan komme fra god rådgivning fra kompetansemiljøene. At IKT-sikkerhetskompetansen, som delvis er en knapp ressurs, dermed blir nyttiggjort ved å gi råd om hva aktører skal gjøre, kan skape bedre IKT-sikkerhet.

Relatert til diskusjonen i 4.1.4, vil også hensiktsmessige mål på området være at man kan skape bedre koordinering, samarbeid og relasjoner mellom offentlige og private virksomheter. At dette fungerer godt vil være avgjørende for at man både skal kunne gi gode råd og veiledning, og for at aktørene skal trekke i samme retning.

En viktig del av å håndtere IKT-sikkerhets-truslene er også det tekniske utstyret. For å kunne avdekke hendelsene i det hele tatt, er det nødvendig at man har sofistikerte systemer som fanger dem opp. For den praktiske håndteringen vil dette være viktig, og det er nylig, etter det vi forstår, investert en halv milliard i NSM for å forbedre sensorene for deteksjon.

[2] Nå vi omtaler håndtering, mener vi både oppdaging/deteksjon og håndtering av trusler. I teksten skiller vi i liten grad mellom disse.

5. Tiltak 1 og 2 – Innføre ny lov om IKT-sikkerhet og stille krav til IKT-sikkerhet i anskaffelser

IKT-sikkerhetsutvalget foreslår at det utarbeides et forslag til en tverrsektoriell IKT-sikkerhetslov. Loven anbefales å inneholde krav til forsvarlig IKT-sikkerhet, og bør også omfatte samfunnskritiske virksomheter og offentlig forvaltning. Videre mener utvalget at det bør stilles krav til IKT-sikkerhet i anskaffelsesregelverket, og at man bør vurdere å endre statens standardavtaler.

5.1 Nullalternativet

Det er ulike regelverk som er med på å regulere IKT-sikkerhet i Norge. Ingen av disse dekker samtlige elementer. IKT-sikkerhets-utvalget har gjennomført en kartlegging som viser at det er over 500 lover og forskrifter som *kan* inneholde krav til IKT-sikkerhet. Noen av lovene regulerer IKT-sikkerhet eksplisitt, mens andre inneholder generelle krav til sikring som mer indirekte regulerer IKT-sikkerhet.

Tilbakemeldinger til utvalget tyder på at dagens regler er vanskelige å etterleve fordi de er vagt utformet og kan være vanskelige å forstå. Det er også stor variasjon i språkbruk, begreper og definisjoner mellom regelverkene, noe som kan skape forvirring for brukerne.

5.2 Mål

Et effektmål som følger av samfunnsmålet om å skape bedre IKT-sikkerhet er å løse insentiv-problemene diskutert i delkapittel 4.1.1. Det er også slik at fragmentert regulering innebærer en fare for at enkelte forhold faller mellom stoler og ikke er regulert tilstrekkelig av denne grunn.

Virksomheter som har valgt å ikke prioritere IKT-sikkerhetsinvesteringer basert på kost-nytte-vurderinger, vil ved innføringen av en tverrsektoriell IKT-sikkerhetslov kunne risikere sanksjoner ved å ikke sikre seg. Dette legges til den bedriftsøkonomiske nedsiden ved å ikke sørge for forsvarlig IKT-sikkerhet i virksom-hetene, og kan føre til bedre sikring av systemene. Et av målene med en ny lov kan også være å skape økt bevissthet om IKT-sikkerhet, som kan bli resultatet dersom virksomheter gjøres oppmerksomme på krav og relaterte sanksjoner.

Diskusjonen i kapittel 4.1.2 tyder på at kompetanseheving blant virksomhetene vil kunne ha positive effekter på IKT-sikkerheten. Ved å etablere en lettfattelig lov, eller ved å sørge for i fremtiden å ha enhetlig begrepsbruk i lover og forskrifter, kan en målsetning også være å øke kompetansen blant virksomhetene. Dette følger av at virksomheter som IKT-sikkerhetsutvalget har vært i kontakt med hevder at dagens regler er vagt utformet og vanskelige å forstå.

5.3 Beskrivelse av tiltaket

Utvalget anbefaler at det utarbeides et forslag til en tverrsektoriell lov om forsvarlig IKT-sikkerhet. Loven bør ta utgangspunkt i NIS-direktivet og utvide virkeområdet til også å omfatte alle virksomheter som er kritiske for samfunnets infrastruktur, samt alle forvaltnings-virksomheter på statlig, regionalt og kommunalt nivå.

Utvalget mener at loven bør inneholde funksjonelle krav til forsvarlig IKT-sikkerhet. De anbefaler videre at kravene utformes slik at de er fleksible for tverrsektorielle utfordringer og teknologisk utvikling. Utvalget mener loven bør inneholde hjemler til å føre tilsyn og for sanksjoner for manglende etterlevelse, og at det bør vurderes nærmere om det skal innføres en varslingsplikt om brudd på kravene. Det foreslås at man bør vurdere å innføre rapporteringskrav for både offentlige og private virksomheter om arbeidet med IKT-sikkerhet.

Utvalget mener også at det bør vurderes om den foreslåtte tverrsektorielle loven skal ha en egen bestemmelse om krav til IKT-sikkerhet i anskaffelser. Videre mener utvalget det bør vurderes å stille krav om IKT-sikkerhet i anskaffelsesverket, og at det bør vuderes å

legge inn krav om IKT-sikkerhet i Statens Standardavtaler (SSA).

5.4 Identifisering av virkninger

5.4.1 Kostnader

Den mest åpenbare kostnaden som påløper ved utarbeidelse av en ny tverrsektoriell IKT-sikkerhetslov er arbeidsinnsatsen som må legges inn i utformingen av loven. Økt regulering innebærer dessuten kostnader for virksomheter, som Oslo Economics' intervjuobjekter også trekker frem. Virksomhetene vil være nødt til å bruke mer tid på å forholde seg til regelverk hvis det øker i omfang, og det oppstår derfor en potensiell alternativkostnad av ressursene som kunne vært benyttet på operativ drift.

Flere vi har snakket med ønsker at man heller rydder i eksisterende regelverk istedenfor å innføre et nytt. Skal man innføre et nytt regelverk mener flere at det bør komme istedenfor og ikke i tillegg til eksisterende regelverk.

Hvis man i lov skal stille krav i anskaffelser og til leverandører vil dette, ifølge flertallet av intervjuobjektene, kunne ha en effekt på markedene som blir omfattet av loven. Det antas imidlertid at dersom det stilles sikkerhetskrav til leverandørene i et marked, vil det kunne trekke markedet i retning av mindre konkurranse. For noen virksomheter kan slike krav være for kostbare å innfri i et kost-nytte-perspektiv, og da vil man potensielt risikere at markedet konsentreres blant leverandørene som evner å bære disse sikkerhetskostnadene. Samtidig er det antagelig ønskelig at noen av de useriøse aktørene forsvinner fra markedet.

Det vil også være kostnader tilknyttet et eventuelt rapporteringskrav til offentlige og private virksomheter. Virksomhetene vil være nødt til å bruke tid og ressurser på rapporteringen, og dette vil medføre både direkte og indirekte kostnader. Enkelte av intervjuobjektene trakk frem at før man begynner å pålegge rapporteringer, så må man grundig vurdere hva man skal bruke rapporteringen til. Videre ble det trukket frem at hvis man gir noe tilbake i form av veiledning eller bistand, vil rapporteringsviljen komme av seg selv. Det er derfor uklart om man er nødt til å pålegge det.

5.4.2 Nyttevirkninger

En virksomhet kan redusere innsatsen for IKT-sikkerhet hvis sikringen er for kostbar sammenlignet med forventet gevinst med å redusere risikoen. Det er ikke utenkelig at virksomheter vurderer at det er mer lønnsomt å prioritere andre investeringer enn IKT-sikkerhet, eller prioriterer en viss type IKT-sikkerhetssårbarhet, som også den teoretiske modellen til Gordon og Loeb (2002) predikerer. En måte for virksomhetene å ta rasjonelle kost-nytte-beslutninger på IKT-sikkerhetsområdet er å gjennomføre en risiko- og sårbarhetsanalyse (ROS-analyse), eller ta utgangspunkt i rammeverket fra Gordon og Loeb (2002) og å dekomponere parameterne ytterligere. I sistnevnte rammeverk vil man vurdere *verdien* på det som skal sikres, altså hvor stort tapet ved et angrep vil være; vurdere *trusselen*, med andre ord sannsynligheten for at man blir angrepet; samt *sårbarheten,* altså sannsynligheten for verditapet gitt at et angrep har skjedd.[3]

Sanksjoner fra myndighetene kan endre kost-nytte-vurderingen blant virksomhetene og dermed atferden på IKT-sikkerhetsområdet. Ved å innføre krav om grunnsikring med tilhørende sanksjoner, blir det relativt mindre kostbart å ha grunnsikring. Det vil med andre ord for en enkelt virksomhet komme en ytterligere kostnad ved å ikke sikre seg, slik at flere forebyggende sikkerhetsinvesteringer vil bli gjort enn de basert på en ren risikoanalyse. Virksomhetene vil internalisere noen av de eksternalitetene som oppstår ved underinvestering i IKT-sikkerhet.

Myndighetene kan påvirke virksomheter slik at de opplever det som mer lønnsomt å sikre seg enn å ikke gjøre det. Flere av informasjonskildene til Oslo Economics trekker frem dette, og fremhever eksemplet med hvordan personvernforordningen (GDPR) har gjort virksomheter bevisste på håndteringen av personopplysninger. GDPR medførte strenge sanksjoner, og dette vil naturligvis påvirke kost-

[3] En relatert metode for å vurdere IKT-sikkerhetsrisiko er å gjennomføre en skjønnsmessig vurdering av de samme parameterne, ved hjelp av en VTS-analyse, lansert av Næringslivets Sikkerhetsråd (https://vtsanalyse.no/vts-analyse/hva-er-vts-analyse).

nytte-vurderinger.[4] I mørketallsundersøkelsen foretatt av Næringslivets Sikkerhetsråd (2018) fremkommer det at nær halvparten av virksomhetene i utvalget gjorde endringer eller forbedringer som følge av innføringen av GDPR.

Å stille krav til anskaffelser kan også ha nyttevirkninger på IKT-sikkerhetsområdet. Det at man må gjøre IKT-relaterte vurderinger ved innkjøp, kan gjøre virksomhetene sikrere. Blant Oslo Economics' informanter som er tilhengere av dette tiltaket trekkes det frem at anskaffelsesregelverket er et uutnyttet rom for å skape IKT-sikkerhetsforbedringer, og at anbefalingen derfor vil ha positive virkninger.

Rapporteringskrav er også noe som noen av informantene trekker frem som hensiktsmessig, og det konkluderes i forskning av Moore (2010) at det er hensiktsmessig at selskaper rapporterer sine cyberovervåkningssaker samt kommuniserer ut potensiell svindel og andre hendelser som påvirker deres IKT-systemer. Å innføre rapporteringskrav vil i hovedsak være rettet mot et mål om å gjøre virksomhetene mer bevisste om IKT-sikkerhetsområdet, og det er etter Oslo Economics' vurdering ikke usannsynlig at et rapporteringskrav vil kunne skape et skift i virksomhetenes fokus. Dette vil igjen kunne ha positive nyttevirkninger på IKT-sikkerheten.

5.5 Vurdering av virkninger

5.5.1 Kostnader

Å tallfeste de samfunnsøkonomiske kostnadene ved å etablere nye reguleringer er ikke uten videre enkelt. Som nevnt i 5.4.1 kan det tenkes at en ny tverrsektoriell IKT-sikkerhetslov kan føre til alternativkostnader for virksomhetene, ettersom mer tid vil gå til å forstå og håndheve de nye reglene. Det er for eksempel ikke utenkelig at GDPR har medført betydelige kostnader for private virksomheter, og at dette eksemplet kan fungere som en analogi for en potensiell innføring av en tverrsektoriell IKT-sikkerhetslov.

Det er heller ikke enkelt å tallfeste kostnadene ved eventuelle IKT-sikkerhetskrav i anskaffelsesregelverkene, selv om de kvalitativt lar seg identifisere. Hvis det er slik at noen leverandører får konkurransefortrinn og større markedsmakt, kan det føre til at de tar høyere priser slik at det potensielt oppstår samfunnsmessige effektivitetstap.

Å tallfeste en aggregert samfunnsmessig alternativkostnad ved økt regulering vil kreve analyser som vil ligge utenfor denne rapportens vurderinger. Det vil likevel være nødvendig å trekke inn effektivitetstapsperspektivene inn i vurderingen av samfunnsøkonomisk lønnsomhet under 5.8.

5.5.2 Øvrige virkninger

Virkningene av dette tiltaket vil hovedsakelig være av en art som gjør at de bør vurderes kvalitativt. Styrken på virkningene, både basert på betydningen de har og virkningsomfanget, vil derfor baseres på pluss-minus-metoden.

Det er flere virkninger som kan oppstå ved å etablere en tverrsektoriell IKT-sikkerhetslov. Basert på vår informasjonsinnhenting og egne vurderinger, har vi fremhevet virkninger i Tabell 5-1 under, med deres respektive samfunnsøkonomiske betydning.

Tabell 5-1: Betydning av virkninger

Virkning	Betydning
Økt kompetanse	Stor
Reduserte insentivproblemer, privat	Stor
Økt bevissthet	Middels
Bedre informasjonsdeling	Middels

Økt kompetanse

Oslo Economics' informanter trekker frem at det er et stort kompetansebehov på IKT-sikkerhetsområdet. Selv om det påpekes at Norge er langt fremme på målinger både med tanke på forebygging og håndtering, og at det er en gradvis økende oppmerksomhet, kommer mye av dette trolig av at Norge er langt fremme i digitaliseringen generelt.

Basert på både intervjurunden og tidligere utredninger fra blant annet Lysneutvalget, vurderer Oslo Economics at økt kompetanse på

[4] Sanksjonene tilsvarer opptil 4 % av den globale årsomsetningen i en virksomhet, vist i personvernforordningens artikkel 83 nummer 5.

IKT-sikkerhetsområdet vil ha stor samfunnsøkonomisk betydning. En tverrsektoriell IKT-sikkerhetslov kan føre til en økning i kompetanse hvis den formuleres på en pedagogisk måte. Det trekkes frem av informanter at dagens regelverk oppleves å være fragmentert og vagt utformet, så hvis en mer forståelig IKT-sikkerhetslov kan stille krav som er enklere å begripe, kan dette ha en middels positiv konsekvens på det reduserte kompetansebehovet – både i offentlige og private virksomheter (++).

Reduserte insentivproblemer

At IKT-sikkerhetsområdet har insentivproblemer, i tråd med de teoretiske prediksjonene fra 4.1.1, bekreftes i de intervjuene vi har gjennomført. Flere trekker frem at det i enkelte virksomheter opereres med et risikonivå som samfunnsmessig ikke er akseptabelt; fordi mens kostnadene for samfunnet kan være betydelig ved alvorlige IKT-sikkerhetsbrudd, er de bedriftsøkonomiske kostnadene gjerne mindre. På tross av en viss usikkerhet om hvor kraftig problemet er, og at enkelte informanter mener det er kompetansebehovet som er viktigst, vurderer Oslo Economics at insentivproblemene i privat sektor har stor betydning på IKT-sikkerhetsområdet. Å redusere insentivproblemene har derfor, etter vår vurdering, stor samfunnsøkonomisk betydning for IKT-sikkerheten.

Fordi juridiske virkemidler i stor grad retter seg mot atferd, vil en ny IKT-sikkerhetslov potensielt påvirke insentivene til IKT-sikkerhetsområdets aktører. Når vi har gitt en stor positiv konsekvens på insentivproblemene i privat sektor (+++), er det fordi vi vurderer at denne anbefalingen kan ha en virkning på insentivene med middels omfang. Dette følger av argumentene i 5.4.2, nemlig at lovfestede krav kan gi et skift i kost-nytte-vurderingen blant virksomhetene, slik at de tilpasser seg og investerer mer i IKT-sikkerhet.[5] Oslo Economics vurderer for øvrig at dette tiltaket vil ha en mindre konsekvens for offentlige virksomheter – fordi insentivvirkningene trolig vil være mindre kraftfulle i offentlige virksomheter som i større grad har spesifiserte regelverk og oppfølging fra for eksempel Difi.

Økt bevissthet

Vi gir økt bevissthet middels samfunnsøkonomisk betydning. Innspill i intervjuene, samt rapporter fra Difi og NSR, viser at det har vært en gradvis økt erkjennelse blant aktørene av betydningen av IKT-sikkerhet. Fordi man dermed kan anta at samfunnsaktørene kjenner til viktigheten av IKT-sikkerhet på et generelt nivå, er rekkevidden av virkningene ved å øke bevisstheten noe begrenset, og middels betydning virker således å være rimelig.

Det stilles spørsmål blant Oslo Economics' intervjuobjekter om endringer i lovverket er veien å gå, og et argument er at lovregulerte krav til IKT-sikkerhet kan bli en sovepute for virksomhetene. Likevel vurderer vi at en tverrsektoriell lov med tilhørende sanksjoner vil gjøre at virksomhetene blir nødt til å være mer bevisste. Også potensielle rapporteringskrav kan gjøre at virksomhetene må snu fokuset i større grad mot IKT-sikkerheten. Vår forventning er at virkningsomfanget vil være lite og positivt, og at konsekvensen dermed blir liten og positiv (+), men fordi det er argumenter i ulike retninger, vil det være usikkerhet rundt denne prediksjonen, diskutert i 5.6.

Bedre informasjonsdeling

Både utvalget og flere av Oslo Economics' intervjuobjekter trekker frem behovet for informasjonsdeling. Fordi rasjonelle beslutninger om IKT-sikkerhet avhenger av at man har informerte aktører, er det viktig at informasjonsflyten er tilstrekkelig friksjonsløs, og dette erkjennes av flere av informasjonskildene. Bedre informasjonsdeling vurderes generelt å ha middels samfunnsøkonomisk betydning.

Effekten på informasjonsdelingen vil ved dette forslaget trolig være mer indirekte, slik at man kan få bedre deling av at både kompetansebehovene og insentivproblemene reduseres, samt at bevisstheten øker. Hvis en privat virksomhet gjennom lovregulering får sterkere insentiver til å investere i IKT-sikkerhet, vil det for eksempel ikke være utenkelig at den ønsker å se følgene av disse investeringene ved å ta del i informasjonsdeling. Dette vil i så fall henge sammen med at dersom virksomheter investerer i IKT-sikkerhet i større grad, vil den også ønske å ta del i liaisonordninger eller å

[5] Dette er under forutsetning av at lovene er utformet på en god måte. Gitt at det er insentivproblemer på IKT-sikkerhetsområdet, vil man kunne skape bedre IKT-sikkerhet ved å skrive en altomfattende lov som spesifiserer konsekvenser i alle mulige fremtidige tilstander. I praksis vil det naturligvis være stor usikkerhet rundt selve utformingen. Dette diskuteres i 5.6.

samarbeide med NorCERT med sensorer. Vi vurderer derfor at tiltaket kan ha et lite, positivt omfang og forventningen er derfor at det blir en liten positiv konsekvens.

Tabell 5-2: Omfang av virkninger

Virkning	Omfang
Økt kompetanse	Lite positivt
Reduserte insentivproblemer, privat	Middels positivt
Økt bevissthet	Lite positivt
Bedre informasjonsdeling	Lite positivt

Tabell 5-3: Konsekvens av virkninger

Virkning	Tverrsektoriell IKT-sikkerhetslov og anskaffelseskrav
Bedre forebygging:	
Økt kompetanse	++
Reduserte insentivproblemer, privat	+++
Økt bevissthet	+
Bedre håndtering:	
Bedre informasjonsdeling	+

5.6 Vurdering av usikkerhet

Det kan være stor økonomisk usikkerhet ved innføringen av nye reguleringer. Å etablere lover kan være et effektivt virkemiddel for å endre atferd blant økonomiske aktører, men det er ikke alltid de formuleres slik at atferden går i retningen myndighetene ønsker. Fordi lovverket allerede i dag oppfattes som vanskelig å forstå blant virksomhetene som IKT-sikkerhetsutvalget har vært i kontakt med, er den forventede store positive konsekvensen på insentivene under en forutsetning av at loven blir formulert godt og ikke kompliserer ytterligere. Det er derfor betydelig usikkerhet rundt dette virkningsomfanget, for hvis den nye loven ikke formuleres godt, vil det kunne betraktelig redusere omfanget av virkningen.

Det trekkes frem at kravene ikke bør omfatte alle virksomheter, men at man bør sette en grense for størrelsene til bedriftene. Kravene anbefales derfor kun å gi en minimums-regulering inntil et visst samfunnskritisk nivå. En begrensning ved de positive effektene av tiltaket er da at også virksomheter under en slik grense vil kunne være en del av et større økosystem og kilde til sårbarhet i samfunnet.

En annen usikkerhet som trekkes frem av flere av Oslo Economics' intervjuobjekter er hvor stort rom en tverrsektoriell lov om IKT-sikkerhet kan dekke. Det påpekes at det i Norge allerede er sektorlover på plass, og at en ny sikkerhetslov med forskrift kan gjøre at man treffer bredere enn man gjorde før. Man vil ikke komme utenom de sektorielle regelverkene, så det vil stilles krav i en del av disse sektorene uansett. Enkelte har overfor oss trukket frem at en tverrsektoriell lov ikke vil rydde i kompleksiteten som allerede er, men heller føre til mer kompleksitet. Noen av informantene foreslår derfor at det først og fremst trengs en revisjon av eksisterende regelverk. Et spørsmål som stilles er også hvorvidt bestepraksis kan ha like god effekt som en ny lov på området.

Det hevdes blant noen av informantene at sektorielle lover, sammen med ny sikkerhetslov, vil gi fullstendig dekning – med andre ord være en tilstrekkelig bred grunnplanke – og at det som kommer utenfor bør løses av andre verktøy og mekanismer enn lovverket. Det påpekes også at det er vanskelig å vurdere i dag hvor stort behovet for en slik lov er, ettersom sikkerhetsloven først trer i kraft 1. januar 2019, og at man heller ikke ser effektene av NIS-direktivet ennå.

En utfordring når man skal etablere lover på IKT-området er den raske teknologiske utviklingen. Det er en risiko for at man ved å innføre krav, ender opp med å innføre krav som blir utdatert i løpet av relativt kort tid. Ifølge flere informanter er personopplysnings-loven et eksempel hvor dette har skjedd tidligere, ettersom loven over tid ikke traff så godt.

En annen type usikkerhet er hvorvidt en lov vil føre til økt bevissthet om IKT-sikkerhetstruslene blant virksomhetene. Noen av informantene frykter at konkrete krav kun vil bli en «check-box» for virksomhetene, eller en «sovepute», og at man derfor ikke tilegner seg kompetansen som kanskje er nødvendig.

5.7 Vurdering av samfunnsøkonomisk lønnsomhet

Det vil være potensielle samfunnsøkonomiske nyttevirkninger av å etablere en tverrsektoriell IKT-sikkerhetslov, og tiltaket vil dermed være lønnsomt hvis forventningen om disse overstiger forventningen om kostnadene. Virksomheter vil være nødt til å forholde seg til et nytt regelverk hvis det etableres en ny IKT-sikkerhetslov, og kostnadene forbundet med dette må veies opp mot nyttevirkningene.

Spørsmålet om tiltaket er samfunnsøkonomisk lønnsomt vil avhenge i veldig stor grad av hvordan en ny lov formuleres. Tiltaket vil kun være lønnsomt om det faktisk er et tomt rom i det eksisterende lovverket, og om en tverr-sektoriell IKT-sikkerhetslov evner å fylle dette. Hvis disse forutsetningene innfris, vil tiltaket kunne ha samfunnsøkonomiske nyttevirkninger, vist i Tabell 5-3, og tiltaket vil trolig være samfunnsøkonomisk lønnsomt.

Oslo Economics vurderer på samme måte at det er vil kunne være samfunnsøkonomisk lønnsomt å stille krav til IKT-sikkerhet i anskaffelsesregelverket, men at potensielle markedseffekter må vurderes når disse kravene utformes. Dette er fordi kravene vil kunne påføre tilbydere og innkjøpere kostnader, og at konkurransen kan reduseres.

5.8 Samlet vurdering og anbefaling

De predikerte virkningene av dette tiltaket er preget av en del støy. En «perfekt» IKT-sikkerhetslov vil utvilsomt kunne føre til bedre IKT-sikkerhet, men det er antakelig for mange usikkerhetsfaktorer til at man kan etablere en slik lov uten at det foretas ytterligere utred-ninger. I tillegg til at det må utredes om det i det hele tatt er behov for ny regulering, må man også vurdere om det kan være mest hensiktsmessig å implementere endringene i eksisterende regelverk.

Hvis man får orden på usikkerhetsfaktorene, med andre ord hvis man får redusert støyen i prediksjonene under Tabell 5-3, viser de estimerte virkningene at det en tverrsektoriell lov kan ha positive konsekvenser for IKT-sikkerheten. Oslo Economics' anbefaling er derfor at det godt kan vurderes nærmere, ved hjelp av ytterligere utredninger, om en tverrsektoriell IKT-sikkerhetslov skal etableres. Oslo Economics mener også at man kan vurdere nærmere om man bør stille IKT-sikkerhetskrav i anskaffelsesregelverket Usikkerheten gjør imidlertid at man først bør vurdere spørsmålet nærmere.

6. Tiltak 3 – Tydeligere styring og bedre koordinering

IKT-sikkerhetsutvalget anbefaler at Justis- og beredskapsdepartementet må ta et tydeligere lederskap for de forvaltningspolitiske utfordringene nasjonal IKT-sikkerhet fører med seg.

6.1 Nullalternativet

Mange av utfordringene utvalget har identifisert er knyttet til tverrsektoriell styring, koordinering og samarbeid, som er Justis- og beredskapsdepartementets (JD) ansvar. Det er horisontale styringsutfordringer på IKT-sikkerhetsområdet, og informantene Oslo Economics har vært i kontakt med beskriver JDs håndtering som oppstykket og uten visjoner eller klare grep. Det er også liten grad av koordinering mellom tilsynsmyndigheter med ansvar for IKT-sikkerhet.

Det hevdes fra flere av informantene at JD har vært mer aktive på enkeltproblemstillinger enn på å se det store bildet. Det stilles spørsmål ved om JD har nok kompetanse på IKT-sikkerhetsområdet. Videre stilles det også spørsmål ved om JD i for stor grad støtter seg på andre fagmiljøer og selv blir hengende etter.

6.2 Mål

Overordnet er tiltaket rettet mot samfunnsmålet om å skape økt IKT-sikkerhet, og effektmålene er å sikre bedre koordinering og samarbeid om IKT-sikkerhet i offentlig sektor. Dersom JD tar tydeligere lederskap, er målet at dette skal føre til en samordning av styringen av de tverrsektorielle etatene. Dette vil igjen kunne føre til en bedre håndteringsevne på IKT-sikkerhetsområdet.

6.3 Beskrivelse av tiltaket

Utvalget mener at Justis- og beredskaps-departementet i større grad må utvise lederskap når det gjelder styring og samordning av etater som berører IKT-sikkerhetsområdet. Denne styringen kan innebære å samordne styringssignalene fra Justis- og beredskapsdepartementet til både NSM og DSB når det gjelder oppgaver innenfor nasjonal IKT-sikkerhet.

Tilsyn innenfor IKT-sikkerhetsområdet bør koordineres bedre. Samarbeidet som har funnet sted mellom en rekke etater og departementer når det gjelder HMS-tilsyn kan være et godt eksempel for hvordan IKT-sikkerhetstilsyn kan koordineres. For å oppnå dette, foreslås det at JD blir tydeligere i sitt lederskap.

Utvalget trekker fram to eksempler som skal presisere hva tiltaket innebærer. Den første er at JD i 2017 la fram den første stortings-meldingen om IKT-sikkerhet. Dette er i hovedsak et strategidokument. Det andre eksemplet er JDs arbeid med nasjonal digital sikkerhet i 2018. Som en del av dette arbeidet arrangerte JD og Forsvarsdepartementet «Strategikonferansen» i mars 2018. Ved å trekke fram disse eksemplene kan det virke som at utvalget mener det er initiativ og lederskap på strategisk nivå som er kjernen i tiltaket.

Anbefalingen fra utvalget om tydeligere lederskap er i en generell form. Vi benytter derfor på samme måte en generell tilnærming når vi vurderer anbefalingen.

6.4 Identifisering av virkninger

6.4.1 Kostnader

Anbefalingen om at JD må ta tydeligere lederskap har ingen klar betydning på kostnader, men vi vil peke på de mest nærliggende kildene til økte kostnader.

Enkelte av intervjuobjektene som Oslo Economics har snakket med mener JD trenger sterkere kompetanse på IKT-sikkerhet. I den grad tydeligere lederskap krever økt kompetanse på IKT-sikkerhet, vil eventuelle kostnader være knyttet til nye ansettelser, samt eventuelle kurs eller andre kompetansehevende tiltak for eksisterende ansatte og ledelse. Tiltaket kan også ha alternativkostnader i form av at ansatte og ledelse må bruke mer av sin arbeidstid på IKT-sikkerhetsspørsmål, noe som går ut over andre arbeidsoppgaver. Til slutt kan det være kostnader knyttet til opprettelse og drift av samarbeidsarenaer, samt periode-vise IKT-sikkerhetsfora (for eksempel konferanser).

6.4.2 Nyttevirkninger

Bedre og mer tydelig styring av fagmiljøene på IKT-sikkerhetsområdet kan føre til bedre forebygging og håndtering. Dette vil hovedsakelig skje ved å legge bedre til rette for koordinering når hendelser oppstår. Økt fokus og mer ressurser til strategisk samarbeid kan særlig bidra til bedre forebygging, men også bedre hendelseshåndtering på lengre sikt.

Tydeligere lederskap fra departementet kan også bidra til å redusere interessekonflikter mellom ulike offentlige etater, i tilfeller hvor ønsker om mer digitalisering kommer i konflikt med økt sikkerhet.

6.5 Vurdering av virkninger

6.5.1 Kostnader

Tiltaket inneholder ingen konkrete forslag som gir åpenbare kostnadsvirkninger, og det er derfor vanskelig å tallfeste disse virkningene. I den grad tydeligere lederskap krever nyansettelser for å øke kompetansen, samt en vridning i arbeidsoppgaver for eksisterende ansatte og ledelse, vil kostnadene være foreliggende. Vi anser likevel utvalgets forslag som for lite konkret til å tallfeste disse kostnadene.

6.5.2 Øvrige virkninger

Vår vurdering av betydningen av hver virkning kan ses i Tabell 6-1.

Intervjuobjektene påpeker at det kan være interessekonflikter mellom ulike offentlige etater. Vi mener derfor at dette har en viss betydning, fordi det ligger implisitt i etatenes ansvarsområder at slike interessekonflikter kan og vil oppstå. Det kan for eksempel oppstå konflikter knyttet til informasjonsdeling. Deling av sensitiv og konfidensiell informasjon ved hendelser kan være avgjørende for å beskytte rammede IKT-systemer. Ulike aspekter ved IKT-sikkerhet, i dette tilfellet beskyttelse av informasjon og beskyttelse av systemer, kan dermed komme i konflikt. I den grad ulike etater har særansvar for disse aspektene (for eksempel Datatilsynet og NSM), kan dette skape utfordringer for koordinering og samarbeid. Vi gir derfor denne virkningen middels betydning.

Betydningen av bedre rådgivning på IKT-sikkerhetsområdet vurderes å ha middels samfunnsøkonomisk betydning. Det trekkes frem blant informantene at det er viktig for IKT-sikkerheten at myndighetene gir råd, særlig til enkeltpersoner og små- og mellomstore bedrifter. Selv om vi vurderer at rådgivningen har mindre betydning for store aktører i samfunnet, vurderer vi at rådgivningsfunksjonen er så viktig for de mindre aktørene at betydningen er middels.

Flere av utfordringene som er beskrevet i IKT-sikkerhetsutvalgets rapport, samt beskrevet av Oslo Economics' informanter, knytter seg til tverrsektoriell styring, koordinering og samarbeid. Både koordineringen av offentlige virksomheter, samt samarbeidet mellom de offentlige etatene med IKT-sikkerhetsansvar, vurderes å ha middels samfunnsøkonomisk betydning i analysene.

Tabell 6-1: Betydning av virkninger

Virkning	Betydning
Reduserte interessekonflikter	Middels
Bedre rådgivning	Middels
Bedre koordinering	Middels
Bedre samarbeid i offentlig sektor	Middels

Tydeligere lederskap fra Justis- og beredskapsdepartementet kan redusere potensielle interessekonflikter i offentlig sektor. Hvis det for eksempel er slik at enkelte offentlige virksomheter i større grad fremmer fordelene ved digitaliseringen uten å fremme sikkerhetsutfordringene, kan Justis- og beredskapsdepartementet skape mer forenlighet i insentivene ved å ta tydeligere lederskap. Med sitt tverrsektorielle styringsansvar kan JD sørge for at etatene også internaliserer sikkerhetsutfordringene. Basert på informasjonsgrunnlaget, vurderer Oslo Economics at tydeligere JD-lederskap kan ha lite, positivt virkningsomfang, slik at prediksjonen er at virkningen har en liten positiv konsekvens (+).

Hvis JD lykkes med å ta tydeligere tverrsektorielt lederskap på IKT-sikkerhetsområdet, er det ikke usannsynlig at det kan føre til bedre rådgivning. Rådene fra myndighetsetatene som går på IKT-sikkerhet er beskrevet av informantene å være fragmentert og lite enhetlige, så hvis JD lykkes med å koordinere rådgivningen, vil dette kunne ha hensiktsmessige effekter på IKT-sikkerheten. Som man

kan se i Tabell 6-1 vurderes rådgivning å ha middels betydning for IKT-sikkerheten, og med et forventet lite, positivt virkningsomfang, er prediksjonen at tydeligere lederskap fra JD kan føre til en liten positiv konsekvens (+).

Fordi tydeligere lederskap fra JD er ment å skape både bedre koordinering og bedre samarbeid i offentlig sektor, vurderer Oslo Economics at dersom JD lykkes med å oppnå tydeligere lederskap, vil det ha en middels positiv konsekvens for både koordineringen og samarbeidet (++). Denne vurderingen stammer fra en antakelse om at de to virkningene har middels samfunnsøkonomisk betydning, mens de begge har middels positivt omfang. Det er dermed en antakelse om at tydeligere JD-lederskap vil ha en viss positiv effekt på koordineringen og samarbeidet i offentlig sektor, men at man sannsynligvis også må iverksette andre tiltak, for eksempel skape samordningsarenaer, for å kunne ha størst mulig positiv effekt på koordineringen og samarbeidet.

Tabell 6-2: Omfang av virkninger

Virkning	Omfang
Reduserte interessekonflikter	Lite positivt
Bedre rådgivning	Lite positivt
Bedre koordinering	Middels positivt
Bedre samarbeid i offentlig sektor	Middels positivt

Tabell 6-3: Konsekvens av virkninger

Virkning	Tydeligere JD-lederskap
Bedre forebygging:	
Reduserte interessekonflikter	+
Bedre håndtering:	
Bedre rådgivning	+
Bedre koordinering	++
Bedre samarbeid i offentlig sektor	++

6.6 Vurdering av usikkerhet

En mulig utfordring er at Justis- og beredskapsdepartementet ikke kan være en synlig stemme i samfunnet. Hvis departementet for eksempel skal uttale seg i media, er det gjennom statsråden. Noen av informantene ser behovet for en nasjonal stemme, men mener at et IKT-sikkerhetssenter bør ta den rollen snarere enn et departement.

Justis- og beredskapsdepartementet har i dag et begrenset hjemmelsgrunnlag, og det kan derfor være vanskelig for departementet å stille krav. I motsetning til forsvarssektoren, der en general kan stille krav, vil ikke en tilsvarende tilnærming fungere i sivil sektor. JD kan ikke kreve overfor for eksempel kommunene, så det er usikkerhet knyttet til selve muligheten til å ta tydeligere lederskap.

Det er begrenset hvor mye teknisk IKT-sikkerhetskompetanse som kan tas inn i Justis- og beredskapsdepartementet, og det er derfor usikkert i hvilken grad de kan ta en lederrolle i det tekniske aspektet ved IKT-sikkerheten.

En usikkerhet som trekkes frem blant informantene er i hvilken grad JD bør ta lederskap, ettersom sektor- og nærhetsprinsippet vurderes å være viktig. Blant disse informantene argumenteres det med at det å flytte kompetanse oppover, ikke vil være hensiktsmessig for å forbedre IKT-sikkerheten.

Et relevant spørsmål er også på hvilket område det er ønske om å skape bedre lederskap. Enkelte av intervjuobjektene trekker frem at det ikke bare er koordinering for eksempel mellom NSM og DSB som er viktig på cyberområdet, men også koordineringen mellom NSM og politiet.

6.7 Vurdering av samfunnsøkonomisk lønnsomhet

Det er sannsynlig at tydeligere lederskap fra Justis- og beredskapsdepartementet, gitt at det fører til tydeligere styring og bedre koordinering, vil være samfunnsøkonomisk lønnsomt. Dersom kostnadene i hovedsak dreier seg om en omdisponering av interne ressurser, vil kostnadene være begrensede, og tiltaket kan da bare bli ulønnsomt dersom nyttevirkningene ikke blir realisert.

6.8 Samlet vurdering og anbefaling

IKT-sikkerhetsområdet er tverrsektorielt av natur, og det er uklart hvor stor rolle Justis- og beredskapsdepartementet skal ha i enkelte sektorer. Forsvarsdepartementet har ansvar for

IKT-sikkerheten på militær side, og sektormyndighetene har også betydelige ansvarsområder, så det usikkert hvor store rom det er for JD til å være en leder. Dette forsterkes ytterligere av at NSM har fått oppgaven om å gi råd og anbefalinger om IKT-sikkerhet.

Ettersom det fremdeles vil være deling av ansvar på IKT-sikkerhetsområdet, og fordi et foreslått IKT-sikkerhetssenter også er planlagt å ta en rolle som skal initiere samarbeid og koordinering, er det uklart i hvilken grad Justis- og beredskapsdepartement bør utvise lederskap. Hvis JD imidlertid tar tydeligere lederskap klart innenfor det de har rom for som koordineringsdepartement, så er det positivt og støttes av våre vurderinger.

7. Tiltak 4 – Opprette et IKT-sikkerhetssenter

IKT-sikkerhetsutvalget foreslår å etablere et IKT-sikkerhetssenter. Utvalget mener at dette kan bidra til å styrke koordinering og samarbeid på etatsnivå, og styrke samfunnets evne til å avdekke og håndtere uønskede digitale hendelser. Senteret bør ivareta en rekke oppgaver på IKT-sikkerhets-området – både koordinering av råd og veiledning samt å avdekke og håndtere digitale hendelser.

7.1 Nullalternativet

Nullalternativet vil være å ikke etablere et IKT-sikkerhetssenter. I dag håndteres cyber-angrep mot samfunnskritisk infrastruktur og informasjon av NorCERT, den operative delen av NSM. Videre er det sektorvise respons-miljøer som håndterer de sektorspesifikke hendelsene som ikke er samfunnskritiske. NSM er i dag det nasjonale fagmiljøet for IKT-sikkerhet, og driver også med noe råd og veiledning.

Kripos har startet etableringen av Nasjonalt cyberkrimsenter (NC3), som skal fungere som et nasjonalt ekspertorgan som håndterer cyberkriminalitet. Senteret skal bygges opp over 3–4 år. Etter planen skal senteret etter hvert ha 200 ansatte – både ingeniører, jurister og politiutdannede. Oslo Economics' informanter nevner at NC3 legger til rette for et internasjonalt samarbeid via Europols EC3 (European Cybercrime Centre). Også Sverige og Danmark har tilsvarende nasjonale cyberkrimsenter.

Det investeres om lag 500 millioner kroner i NorCERTs sensorer, som skal støtte både militær og sivil sektor. Dette skal forbedre hendelseshåndteringen via bedre varslingssystemer og bedre deteksjonsevne. De nye sensorene vil være en del av et nytt IKT-sikkerhetssenter, men investeringen er uavhengig av opprettelsen av senteret.

7.2 Mål

Et IKT-sikkerhetssenter skal ha som formål å være en tydelig koordineringsmekanisme og et sentralt kontaktpunkt, samt å operasjon-alisere rammer og føringer fra styrende etater. Et overordnet mål kan være, som ved senteret i Storbritannia, at det strategiske arbeidet skal jobbe mot at landet skal være tryggest i verden for virksomheter på nett.

Rent konkret vil vi ved vurderingen av dette tiltaket, i likhet med de foregående, dele opp målene på IKT-sikkerhetsområdet i to:

- Bedre forebygging av IKT-sikkerhetshendelser
- Bedre håndtering av IKT-sikkerhetshendelser

Det er en rekke effektmål man kan relatere til opprettelsen av et IKT-sikkerhetssenter. Disse konkretiserer og bidrar til oppnåelse av de overordnede målene. Vi vurderer senterets betydning for følgende effektmål:

- Bedre koordinering
- Økt kompetanse på IKT-sikkerhet
- Bedre offentlig-privat samarbeid
- Økt bevissthet
- Mer forskning

En viktig målsetning ved å etablere et IKT-sikkerhetssenter er at aktører får en arena der de kan samarbeide og dele informasjon, slik at koordineringen mulig blir bedre. På den måten kan man potensielt angripe koordineringsproblemene beskrevet i 4.1.4. Videre vil en opprettelse av senteret potensielt rette seg mot både insentivproblemene og kompetansebehovet drøftet i henholdsvis 4.1.1 og 4.1.2.

7.3 Beskrivelse av tiltaket

IKT-sikkerhetssenteret skal være utformet slik at den nasjonale responsfunksjonen skal legges til senteret. Det skal videre samle aktører på ett sted, og dermed være en møteplass slik at kompetanse kan styrkes, samt at man kan styrke koordinering og samarbeid på etatsnivå.

Kjernen i senteret vil basere seg på det som i dag er NSM NorCERT og NSMs rådgivningsmiljø, i tillegg til representanter for sentrale private og offentlige aktører. Dette er tenkt gjennomført gjennom en liaison-ordning. Utvalget mener at senterets målgruppe bør være i spennet fra små og mellomstore bedrifter, til store konsern og offentlige virksomheter.

IKT-sikkerhetssenteret skal ha følgende oppgaver:

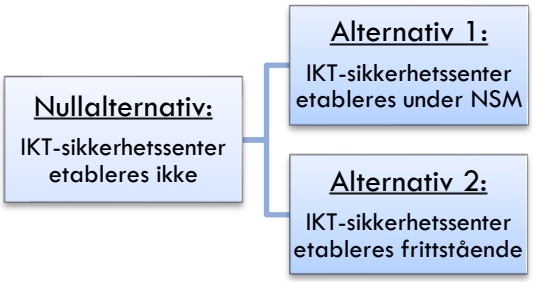
- Gi råd og veiledning, og koordinere andre myndighetsaktørers råd og veiledning
- Ha nasjonal hendelseshåndteringsfunksjon
- Drive varslingssystem for digital infrastruktur eller tilby andre sårbarhetsreduserende tiltak som for eksempel skanningstjenester som Alvis NOR
- Ha en tilknytning til EOS-tjenestene
- Ansvar for å utarbeide risiko- og sårbarhetsvurderinger og publikasjoner som «Helhetlig IKT-sikkerhetsbilde»
- Dele trussel- og sårbarhetsbildet bredt
- Tilby samlokalisering til sektorvise responsmiljøer
- Huse liaisoner fra relevante aktører
- Drifte en hospitantordning for næringsliv, akademia og offentlige virksomheter

Et viktig perspektiv ved utforming av tiltaket gjelder hvem som skal ha myndighetsansvaret for senteret. Utvalget foreslår ulike ordninger, men treffer ingen tydelig konklusjon. De nevner blant annet at NSM kan huse senteret, at det kan legges inn i DSB, eller at det legges direkte under Justis- og beredskapsdepartementet. Vi anser det som mest hensiktsmessig for denne analysen å sette opp to alternative organiseringer:

1. Senter underlagt NSM
2. Frittstående senter i sivil sektor

Vi bruker en slik inndeling fordi vi mener at det som er avgjørende for de samfunnsøkonomiske vurderingene er hvorvidt senteret er forankret i militær eller sivil sektor. Alternativ 2 inkluderer da både et senter under DSB og et senter direkte underlagt Justis- og beredskapsdepartementet.

Figur 7-1: Ordninger for nytt IKT-sikkerhetssenter



7.4 Identifisering av virkninger

7.4.1 Kostnader

Kostnadene ved å etablere IKT-sikkerhetssenter er på nåværende tidspunkt ikke utredet. Det er likevel mulig å gjøre noen vurderinger, basert på konseptnotatet for NSMs planlagte cybersikkerhetssenter. Det er anslått at et sted mellom 60 til 75 prosent av NSMs budsjett skal legges inn under deres foreslåtte IKT-sikkerhetssenter, og at man vil omplassere mellom 150 og 200 ansatte. Dersom et frittstående senter innebærer et lignende kostnadsbilde, vil forskjellen bestå i kostnader knyttet til utstyrsinvesteringer, samt kostnader ved kjøp, leie eller konstruksjon av lokaler utenfor NSM.

I tillegg til de direkte kostnadene ved selve senteret, er det sannsynlig at et frittstående senter innebærer å enten beholde eller bygge opp igjen deler av det nåværende kompetansemiljøet ved NSM, fordi NSM fortsatt vil ha et kompetansebehov på IKT-sikkerhet selv om en del av oppgavene flyttes til et frittstående senter.

Etter det vi forstår er det i praksis ikke noe nytt som skal opprettes i NSMs foreslåtte cybersikkerhetssenter. Det dreier seg egentlig om intern omdisponering av ressurser. Alle funksjonene til IKT-sikkerhetssenteret ligger allerede i NSMs mandat, og at det derfor er begrenset behov for friske midler. Det vil imidlertid oppstå nye kostnader knyttet til etableringen av en møteplass for sivil sektor på Langkaia, som er en del av NSMs konsept for et cybersikkerhetssenter.

Det vil også kunne oppstå kostnader for de offentlige og private virksomhetene som skal ta del i liaisonordningen. Ansatte som bruker

deler av arbeidstiden på å sitte i cybersikkerhetssenteret vil ha mindre tid til andre oppgaver. Det er også mulig at enkelte virksomheter blir nødt til å opprette nye stillinger som skal opprettholde tilknytningen til senteret.

7.4.2 Nyttevirkninger

Det er beskrevet at IKT-sikkerhetssenteret kan ha effekter på tvers av offentlige myndigheter, blant annet ved å sikre tverrsektoriell legitimitet og myndighetsforankring. Et senter kan også ideelt sett bidra til at man unngår dublerende kompetansebehov. Ved å etablere et senter vil man kunne skape en møteplass for ulike aktører, som har blitt beskrevet som vellykket i Storbritannia. Det offentlig-private samarbeidet trekkes frem som særlig viktig i den forbindelse, blant annet fordi informasjonsdelingen er essensiell for både håndtering av truslene samt forståelsen av dem.

Et IKT-sikkerhetssenter vil kunne skape bedre beslutningsgrunnlag og mer forskning på cybersikkerhet. Ved å sentralisere informasjonen kan man forstå det løpende trusselbildet bedre, og det fremkommer nettopp i tidligere forskning anbefalinger om at selskaper bør rapportere sine cyberovervåkningssaker samt kommunisere ut potensiell svindel og andre hendelser som påvirker deres IKT-systemer (Moore, 2010).

Et IKT-sikkerhetssenter vil også via sin forskning kunne kartlegge hva slags saker som er spesielt alvorlige og som må prioriteres.

Basert på diskusjonen ovenfor trekker vi frem følgende virkninger som skal vurderes:

- Økt kompetanse
- Økt bevissthet
- Mer forskning
- Bedre informasjonsdeling
- Bedre rådgivning
- Bedre koordinering
- Bedre samarbeid i offentlig sektor
- Styrket offentlig-privat samarbeid
- Tilgang på etterretningsinformasjon

7.5 Vurdering av virkninger

7.5.1 Kostnader

Hensikten med denne gjennomgangen av kostnadene er å gi et inntrykk av forskjellene i kostnader ved de to alternativene, og ikke å gi et komplett bilde av kostnadene ved å etablere et IKT-sikkerhetssenter. Til det har vi for lite detaljert informasjon. De ulike alternativene for senteret vil ha ulik kostnadsstruktur, som kan ses i Tabell 7-1. Som man kan se i tabellen, vil noen av kostnadene kun påløpe en av de to organiseringene.

Tabell 7-1: Kostnader

Kostnadspost	Senter underlagt NSM	Frittstående senter
Kostnader til lokaler	7–11 mill.	11–19 mill.
Gjenoppbygging av teknisk kapasitet i militær sektor	0	> 0
Gjenoppbygging av kompetanse i militær sektor	0	18–24 mill.
Totale kostnader per år	7–11 mill.	> 29–43 mill.

Senter underlagt NSM

Som en kan se av Tabell 7-1 vil NSMs planlagte senter trolig være det minst kostbare alternativet, ettersom det i hovedsak er en intern omdisponering av deres ressurser. IKT-sikkerhetssenteret skal etter forslaget til utvalget huse liaisoner i egne lokaler, og det vil derfor påløpe kostnader ved å åpne og drifte tilrettelagte lokaler. Det fremgår ikke av utvalgets rapport hvor mange liaisoner som skal inviteres til senteret. For å gi en pekepinn på kostnadene ved en slik ordning legger vi til grunn en antagelse om at 50 liaisoner skal samlokaliseres i senteret til enhver tid.[6] Med 25 kvadratmeter per person i gjennomsnitt, og en kvadratmeterpris på 2000–3000 kr i året, kommer de totale kostnadene til lokaler på rundt 3–4 millioner

[6] Dette er halvparten så mange som ved IKT-sikkerhetssenteret i Storbritannia.

kroner i året.[7,8] Dette er antagelig et konservativt estimat, som er basert på behov for kontorlokaler til en typisk virksomhet. IKT-sikkerhetssenteret kan ha behov utover dette som vil medføre ytterligere kostnader. Dette kan for eksempel være kostnader knyttet til sikring av lokalene.

Det fremgår ikke av NSMs konseptnotat om Nasjonalt cybersikkerhetssenter om de har behov for nye lokaler til selve senteret, eller om det kan lokaliseres i samme bygg som NorCERT sitter i dag. Utvalget har heller ikke konkrete forslag til den fysiske lokaliseringen. Vi legger til grunn at det vil påløpe kostnader til lokaler også dersom senteret legges under NSM. Vi tallfester disse kostnadene til halvparten av kostnadene til lokaler for et senter utenfor NSM, til mellom 4 og 7 millioner kroner årlig. Totalt kommer da kostnader til lokaler på mellom 7 og 11 millioner kroner årlig.

Det kan også være personalkostnader for virksomhetene som skal huse sine liaisoner i senteret. Vi legger til grunn en antagelse om at liaisonene er ansatte som allerede jobber med IKT-sikkerhet i sine virksomheter, og at disse kostnadene derfor er neglisjerbare.

Frittstående senter

I likhet med et IKT-sikkerhetssenter underlagt NSM, vil det påløpe kostnader til lokaler for husing av liaisoner også for et frittstående senter. Det er uklart om disse liaisonene skal sitte i selve senteret eller et annet sted. Disse kostnadene anslås til rundt 3–4 millioner kroner årlig. Vi legger til grunn samme kalkyle som ovenfor i anslaget på kostnader til lokaler. Med 150–200 fast ansatte i senteret som skal ha 25 kvadratmeter hver, og en pris på mellom 2000 og 3000 kroner per kvadratmeter, anslår vi de årlige kostnadene til lokaler til rundt 8–15 millioner kroner. Totale kostnader til lokaler kommer da på mellom 11 og 19 millioner kroner.

Vi kan tenke på et frittstående senter som en *ekstern* omdisponering av ressurser fra NSM og NorCERT. Dermed vil det ikke påløpe direkte kostnader til nye årsverk. Likevel vil et IKT-sikkerhetssenter utenfor NSM bli noe mer kostbart, ettersom man vil være nødt til å opprettholde en viss IKT-sikkerhets-kompetanse i forsvarssektoren, gitt NSMs mandat om å beskytte kritisk infrastruktur. Det vil dermed bli behov for nyansettelser innenfor militær IKT-sikkerhet.[9] Vi legger til grunn at det blir behov for å beholde eller gjenoppbygge 20 % av de 150-200 ansatte som er nødvendig for å drive et IKT-sikkerhetssenter. Med en årsverkskostnad på 600 000 kroner blir kostnadene ved dette mellom 18 og 24 millioner kroner årlig.

Videre, hvis det skal flyttes teknisk utstyr fra NSM til et nytt senter, må antagelig den militære sektoren gjenoppbygge deler av denne tekniske kapasiteten. Vi har ikke nok informasjon til å tallfeste disse kostnadene, og de er derfor angitt som større enn null («>0») i Tabell 7-1.

7.5.2 Øvrige virkninger

I vurderingen av nyttevirkningene er det relevant å vurdere hvorvidt et IKT-sikkerhetssenter kan skape merverdi for samfunnet sammenlignet med nullalternativet. Det er derfor verdt å merke seg at i nullalternativet finnes allerede NorCERT, NC3 og de nye sensorene fra forsvarsbudsjettet, så spørsmålet er hvorvidt et nytt IKT-sikkerhetssenter kan gi ytterligere gevinster.

Gitt at det skal etableres et senter, vil de to alternative utformingene av senteret kunne ha ulike nyttevirkninger. Det er derfor nødvendig å gå igjennom hvert av alternativene.

Senter underlagt NSM

I NSMs eget konseptnotat kommer det frem at deres IKT-sikkerhetssenter skal levere følgende:

- Anbefalinger til offentlige myndigheter og næringsliv
- Nasjonal deteksjon og hendelseshåndtering

[7] Regjeringens rundskriv om normer for energi- og arealbruk for statlige bygg oppgir 23 kvadratmeter per ansatt som et minstemål. Vi setter et kvadratmeterbehov litt over dette minstemålet. Rundskrivet er tilgjengelig på https://www.regjeringen.no/no/dokumenter/rundskriv-om-normer-for-energi--og-arealbruk-for-statlige-bygg/id2474498/

[8] Intervallet for kvadratmeterpris er hentet fra OPAKs prisstigningsrapport for 2017, tilgjengelig på https://www.opak.no/wp-content/uploads/2014/11/Prisstigningsrapport-01-2017-Eiendomsmarkedet.pdf

[9] Alternativt vil en del av den eksisterende kompetansen bli værende i militær sektor, og IKT-sikkerhetssenteret må da hente inn deler av kompetansen fra andre steder.

- Nasjonale tekniske sikkerhetstjenester
- Samlet nasjonal kompetanse, der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse i felles lokaler og over nett

Ettersom mange av IKT-sikkerhetssenterets funksjoner allerede dekkes av NSM i dag, må man i en vurdering av nyttevirkninger vurdere de potensielle gevinstene som skjer utover den eksisterende gevinstoppnåelsen i NSM. Ifølge informantene vil nyttevirkningen hovedsakelig være relatert til at man får samlet en del av aktørene som tidligere har ønsket samarbeid med NSM i selve senteret. Gevinstene relatert til dette drøftes i 7.5.3.

Frittstående senter

Det blir av flere av informantene trukket frem at det er ønskelig å organisere senteret som en del av sivil sektor for å oppnå gevinstene. Mange av IKT-problemstillingene er sivile, for eksempel sedelighetssaker, narkotikasaker, økonomisk bedrageri, bedriftsspionasje osv., og det stilles spørsmål ved om NSM med sin forankring i forsvarssektoren vil være den best egnede aktøren til å gi råd om og håndtere slike saker.

Et sivilt senter vil ha samme funksjoner som senteret i regi av NSM, og vil derfor også kunne ha mange av de samme nytte-virkningene. Særlig viktige er koordinerings-effektene. Styrken på effektene av de ulike alternativene drøftes i avsnitt 7.5.3 under.

7.5.3 Vurdering av virkninger

Som tidligere påpekt avhenger vurderingen av de ikke-prissatte virkningene både av virkningens betydning og omfang. Vi har derfor samlet de potensielle ikke-prissatte virkningene av opprettelsen av et IKT-sikkerhetssenter i Tabell 7-2, der virkningene klassifiseres å enten ha liten, middels eller stor betydning for IKT-sikkerheten.

Kompetansebehovet oppleves å være stort for samtlige intervjuobjekter Oslo Economics har snakket med, og å imøtekomme dette behovet vurderes derfor å ha stor betydning for IKT-sikkerheten. Mange av intervju-objektene trekker frem at økt kompetanse ute i virksomhetene vil kunne ha en stor forebyggende effekt.

Økt bevissthet vurderes å ha middels betydning for den nasjonale IKT-sikkerheten. Fordi informasjonsgrunnlaget for analysen tyder på at det er en økt samfunnsbevissthet om IKT-sikkerhetstrusler allerede, spørs det om enda større bevissthet vil ha den største betydningen. Det er derfor av vårt skjønn mest rimelig å angi virkningens betydning til å være middels.

IKT-sikkerhet er av stor betydning inter-nasjonalt, og det kan derfor argumenteres for at det er forskningen på global skala som har den største virkningen. Det er imidlertid argumenter for at ytterligere forskning nasjonalt vil kunne ha hensiktsmessige effekter, som også Lysneutvalget pekte på. Vi vurderer derfor at den samfunns-økonomiske betydningen av mer forskning vil være middels.

Både utvalget og Oslo Economics' interessenter trekker frem behovet for informasjonsdeling som sentralt. Fordi gode beslutninger om IKT-sikkerhetstrusler avhenger av at man har informerte aktører, er det viktig at informasjonsflyten er tilstrek-kelig friksjonsløs, og dette erkjennes av flere av informasjonskildene. Bedre informasjons-deling vurderes derfor å ha middels samfunnsøkonomisk betydning.

Rådgivning fra myndighetene vurderes å ha middels betydning. Private virksomheter vil ved å følge sin egeninteresse samle inn informasjonen som kan hjelpe dem å maksi-mere profitt, så det er et spørsmål om hvor stor rekkevidde råd fra myndigheter vil ha. Vi vurderer imidlertid at rådene vil ha mid-dels betydning for IKT-sikkerheten ettersom rådene vil kunne være nyttige for enkelt-personer, samt små og mellomstore virk-somheter med lav IKT-sikkerhetskompetanse.

Flere av utfordringene som er beskrevet i IKT-sikkerhetsutvalgets rapport knytter seg til tverrsektoriell styring, koordinering og samarbeid. Koordineringen av offentlige virksomheter, samt samarbeidet i offentlig sektor, vurderes derfor å ha middels samfunnsøkonomisk betydning. Det privat-offentlige samarbeidet vurderes å ha stor samfunnsøkonomisk betydning i analysene. Disse vurderingene understøttes i stor grad av innspillene fra intervjuobjektene Oslo Economics har vært i kontakt med.

Vi vurderer at tilgang på etterretnings-informasjon har stor samfunnsøkonomisk betydning. Dette bekreftes av flere av intervjuobjektene. Forsvarssektoren har informasjon som er viktig for IKT-sikkerheten, og denne informasjonen er også viktig for sivil side. Den militære sektorens informasjon om trusler og hendelser vil for eksempel også påvirke privat næringsliv eller den offentlige forvaltningen.

Tabell 7-2: Betydning av virkninger

Virkning	Betydning
Økt kompetanse	Stor
Økt bevissthet	Middels
Mer forskning	Middels
Bedre informasjonsdeling	Middels
Bedre rådgivning	Middels
Bedre koordinering	Middels
Bedre samarbeid i offentlig sektor	Middels
Styrket offentlig-privat samarbeid	Stor
Tilgang på etterretningsinformasjon	Stor

Senter underlagt NSM

Ved å opprette et IKT-sikkerhetssenter kan man samle IKT-sikkerhetskompetanse på ett sted, og man kan tenke seg at den følgende kunnskaps- og informasjonsutvekslingen kan ha en positiv effekt på kompetansen i samfunnet. Det er ved etableringen av senteret tenkt at man skal samle både offentlige og private aktører, så tiltaket kan være med på å redusere kompetanse-behovet både i privat og offentlig sektor. Som man kan se i Tabell 7-2 over, har kompetansen stor samfunnsøkonomisk betydning, og forventningen er at det å samle kompetansen i et senter kan ha et virkningsomfang som er lite positivt for både offentlig og privat sektor. Konsekvensen er dermed vurdert å være middels positiv, både offentlig og privat (++).

Å skape økt bevissthet om IKT-sikkerhet er en av målsetningene ved å etablere et IKT-sikkerhetssenter, og overordnet er denne virkningen vurdert å ha en middels betydning for IKT-sikkerheten. Basert på informasjonen Oslo Economics har samlet inn, er det gradvis økt samfunnsmessig bevissthet om IKT-sikkerhetstrusler allerede, men hvis NSMs IKT-sikkerhetssenter kan være en synlig stemme, er det tenkelig at de kan bidra til ytterligere bevissthet, men dog i begrenset grad. Forventningen er derfor at NSMs foreslåtte IKT-sikkerhetssenter kan ha en liten positiv konsekvens for IKT-sikkerhetsbevisstheten (+).

Et av målene ved opprettelsen av Nasjonalt cybersikkerhetssenter underlagt NSM er å samle nasjonal kompetanse der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse. Ved å utveksle kunnskap og informasjon, som kan skape økt kompetanse, vil det også kunne ha positiv effekt på forskningen på området. IKT-sikkerhets-senteret skal også, i tillegg til å invitere de relevante aktørene fra privat og offentlig sektor, invitere inn aktører fra akademia, så Oslo Economics vurderer at et senter kan ha middels positivt virkningsomfang på forskningen. Fordi forskning er vurdert å ha middels betydning for IKT-sikkerheten totalt sett, er den samlede forventede konsekvensen middels positiv (++).

Informasjonsdelingen er av middels samfunns-økonomisk betydning, og NSMs cyber-sikkerhetssenter er ment å skape ytterligere forbedring på dette området. Det skjer en del informasjonsdeling mellom private og offentlige aktører i dag, blant annet gjennom sensorene i NorCERT, men tanken er at et IKT-sikkerhetssenter skal legge ytterligere til rette for at informasjonsdeling kan skje. Vi vurderer at virkningsomfanget av NSMs opprettelse av cybersikkerhetssenteret vil være lite og positivt, delvis basert på ytrede spørsmål om NSMs militære forankring skaper noen friksjoner. NSM baserer seg også på privatrettslige avtalegrunnlag, så selv om de oppretter et IKT-sikkerhetssenter og legger til rette for bedre informasjons-deling, kan hendelser fremdeles inntreffe steder der man ikke har slike avtaler. En vurdering er også sporingen og silingen av informasjonen, hvem informasjonen skal deles med, en beslutning som i dag foretas i Felles Cyberkoordineringssenter (FCKS).[10]

[10] Det er uklart hvilken plan man har for FCKS ved en eventuell opprettelse av et IKT-sikkerhetssenter under NSM. Ett argument er uansett at politiet eller NC3 bør foreta sporingen og silingen, slik at de kan avgjøre om det er kriminelle forhold.

Konsekvensen av å etablere et nasjonalt cybersikkerhetssenter under NSM for informasjonsdelingsvirkningen er forventet å være liten og positiv (+).

I NSMs konseptnotat fremkommer det at IKT-sikkerhetssenteret skal være en felles kilde til rådgiving både innenfor og utenfor sikkerhetsloven. Videre oppgis det at senteret skal levere anbefalinger til offentlige myndigheter og næringsliv. Oslo Economics vurderer at dersom NSMs IKT-sikkerhetssenter kan tilrettelegge for at rådgivningen blir mer enhetlig, kan dette ha et lite positivt virkningsomfang. Forventningen er derfor at tiltaket vil ha en liten positiv konsekvens (+).

NSM trekker frem én særlig mulighet senteret skaper som kan føre til ny gevinstrealisering – at det skapes en samhandlingsarena for relevante IKT-sikkerhetsaktører. Det er tenkelig at dette kan føre til bedre koordinering på området. På tross av argumentene om at den militære forankringen i senteret vil kunne stå i veien for bedre koordinering og samarbeid, et poeng som diskuteres mer under, vil en samhandlingsarena trolig kunne skape bedring. Dette er under forutsetning av at IKT-sikkerhetssenteret inviterer de aktørene som faktisk er omfattet av koordineringsutfordringene. Fordi koordinering og samarbeid i offentlig sektor er vurdert til å ha middels betydning, vil et forventet middels, positivt virkningsomfang gi en forventet konsekvens som er middels positiv på begge variablene (++).

Flere av informantene Oslo Economics har vært i kontakt med trekker frem det privat-offentlige samarbeidet som viktig, og kilder beskriver det som «nøkkelen til suksess». Med dagens ordning, der NorCERT har avtaler med aktører i privat næringsliv blant annet om sensorene, har en del offentlig-privat samarbeid forekommet, men en forbedring på området etterspørres likevel blant interessentene. Det planlagte cybersikkerhetssenteret skal derfor sørge for at deler av NSM fysisk samlokaliseres med representanter også fra privat næringsliv, og Oslo Economics vurderer at dette vil ha et middels, positivt virkningsomfang. Vi vurderer derfor at cybersikkerhetssenteret i regi av NSM vil kunne skape en stor positiv konsekvens på dette området (+++).

Frittstående senter

En viktig oppgave i vår analyse er å peke på om det kan være kvalitative forskjeller i virkningene dersom senteret organiseres på en alternativ måte. Vi vurderer det derfor som hensiktsmessig å belyse noen potensielle avvik som kan oppstå i effektene ved en annen organisering.

Hvis senteret etableres uten forankring i forsvarssektoren, påpeker noen av informantene at senteret vil kunne være mer åpent og imøtekommende for aktørene på sivil side. På den måten kan man unngå potensialet for at det skjer det en informant kaller et «graderingsspøkelse». Dette vil igjen kunne gjøre at koordineringen og samarbeidet kan bli bedre med et senter organisert i sivil sektor. Hvis dette er tilfellet, vil en indirekte effekt være at kunnskapsutvekslingen kan bli bedre koordinert, og derfor at reduksjonen i kompetansebehovet i offentlig sektor mulig blir noe kraftigere. Vi vurderer imidlertid at konsekvensen på kompetansebehovet er det samme for et sivilt senter som et senter underlagt NSM.

Det stilles spørsmål blant informantene om et Nasjonalt cybersikkerhetssenter underlagt NSM bør drive med rådgivning til eksempelvis individer og små- og mellomstore bedrifter, som i dag i stor grad gjøres av andre etater og virksomheter.[11] Et spørsmål som stilles er om forsvarssektoren skal gi råd i saker som åpenbart er sivile. Store deler av IKT-sikkerhetsområdet har ikke mye å gjøre med statssikkerheten, for eksempel cyberkriminalitet rettet mot mindre samfunnsaktører. Det stilles i det hele tatt spørsmål ved om statssikkerhetsfokuset i NSM vil gjøre at cybersikkerhetssenteret vil ha mindre rekkevidde for rådgivning i den delen av sivil sektor som ikke omfattes av sikkerhetsloven. Vi vurderer derfor at virkningsomfanget på rådgivningen vil være middels snarere enn lite, og at konsekvensene på rådgivningen derfor vil være middels positivt for et sivilt cybersikkerhetssenter (++).

[11] For eksempel driver NorSIS og NSR med rådgivning til små- og mellomstore bedrifter, samt at politietatene også gir forebyggende råd om cyberkriminalitet.

Det er ikke åpenbart at en intern omdisponering av ressurser i NSM vil føre til bedre samarbeid og koordinering på det tverrsektorielle IKT-sikkerhetsarbeidet. Det erkjennes blant informantene at en del av utfordringene vil kunne løses av at senteret underlagt NSM vil huse liaisoner for private og offentlige aktører, men det er likevel en oppfatning om at den militære forankringen begrenser omfanget av koordinerings- og samarbeidsforbedringer. Ved å flytte senteret ut av militær sektor, er det derfor mulig at både samarbeidet på tvers av offentlige etater og mot det private næringslivet kan bli enda bedre. Fordi mange av utfordringene på IKT-sikkerhets-området er av sivil art, er det sannsynlig at bedre koordinering på sivil side er det som vil ha størst virkning på IKT-sikkerheten.

I motsetning til cybersikkerhetssenteret under NSM, som er forventet å ha et middels, positivt virkningsomfang på henholdsvis koordineringen, samarbeidet og det offentlig-private samarbeidet, vurderer vi at et sivilt IKT-sikkerhetssenter vil kunne føre ha stort, positivt virkningsomfang på hver av disse. Forventingen er derfor at et IKT-sikkerhetssenter som er sivilt organisert vil ha stor positiv konsekvens på samarbeidet og koordineringen (+++), mens det vil ha en meget stor positiv konsekvens for det offentlig-private samarbeidet (++++).

Forsvarssektoren har store ressurser på cybersikkerhetsområdet, og det investeres betydelig på militær side. Det trekkes også frem som et potensielt problem ved et sivilt senter at tilgangen på etterretningen i forsvaret blir begrenset. Likevel, samarbeidet om informasjonsdelingen via NorCERTs sensorer skjer i dag i Felles Cyber-koordineringssenter (FCKS), og hva som skjer med FCKS ved en senteretablering under NSM er uklart. Det er argumenter begge veier på dette punktet, men Oslo Economics vurderer at det er sannsynlig at hvis man skal ha et sivilt cybersikkerhetssenter uten å involvere den militære delen av NSM, så kan man miste noe av etterretningsinformasjonen fra militær side. Omfanget av denne virkningen vurderes derfor å være middels og negativ. Fordi tilgangen på etterretningsinformasjon har stor samfunnsøkonomisk betydning, er forventningen derfor at alternativet vil ha stor negativ konsekvens (÷÷÷).

Tabell 7-3: Omfang av virkninger

Virkning	Senter underlagt NSM	Frittstående senter
Økt kompetanse	Lite positivt	Lite positivt
Økt bevissthet	Lite positivt	Lite positivt
Mer forskning	Middels positivt	Middels positivt
Bedre informasjonsdeling	Lite positivt	Lite positivt
Bedre rådgivning	Lite positivt	Middels positivt
Bedre koordinering	Middels positivt	Stort positivt
Bedre samarbeid i offentlig sektor	Middels positivt	Stort positivt
Styrket offentlig-privat samarbeid	Middels positivt	Stort positivt
Tilgang på etterretningsinformasjon	Intet	Middels negativt

Tabell 7-4: Konsekvens av virkninger

Virkning	Senter underlagt NSM	Frittstående senter
Bedre forebygging:		
Økt kompetanse	++	++
Økt bevissthet	+	+
Mer forskning	++	++
Bedre håndtering:		
Bedre informasjonsdeling	+	+
Bedre rådgivning	+	++
Bedre koordinering	++	+++
Bedre samarbeid i offentlig sektor	++	+++
Styrket offentlig-privat samarbeid	+++	++++
Tilgang på etterretningsinformasjon	0	÷÷÷

7.6 Vurdering av usikkerhet

Vi vil trekke fram to sentrale usikkerhetsfaktorer i vurderingen av IKT-sikkerhetssenteret. Disse alene gir grunnlag for å si at tiltaket må utredes nærmere. Den første usikkerhetsfaktoren oppstår mellom alternativ 1 og alternativ 2, og handler om i hvilken grad et rent sivilt senter kan tilegne seg like god informasjon som et senter som er delvis militært forankret. Den andre gjelder grensedragningene mellom IKT-sikkerhetssenteret og politiets cyberkrimsenter NC3, og er relevant for begge alternativene.

7.6.1 Militær etterretning

Det er sannsynlig at den militære etterretningsinformasjonen er nyttig for den nasjonale IKT-sikkerheten som helhet. Hvis IKT-sikkerhetssenteret skal skilles fra forsvarssektoren så kan man miste viktig kompetanse og tilgang på informasjon. Det er uklart i hvilken grad slik etterretning er avgjørende for at senteret skal kunne utføre sitt samfunnsoppdrag på en god måte, men det er liten tvil om at militær etterretning har en viss verdi for IKT-sikkerheten.

Det trekkes frem blant noen av informantene at det potensielt er store synergier mellom militær og sivil sektor på IKT-sikkerhetsområdet, og at distinksjonen mellom dem kanskje er unødvendig. Dersom IKT-sikkerhetssenteret etableres utenfor NSM, må de etableres nye informasjonslinjer til militær sektor, og det er uklart om dette vil kunne erstatte tilgangen som NSM har til denne etterretningen i dag.

7.6.2 Grensedragningene til NC3

Det er i dag allerede etablert et cyberkrimsenter under Kripos, NC3. En betydelig usikkerhet som fremmes blant informantene er grensedragningene mellom et nytt nasjonalt cybersikkerhetssenter og NC3. Enkelte peker på at det kan være overlappende funksjoner mellom de to sentrene, og det er ulike meninger om hvorvidt det er nødvendig å ha to sentre for IKT-rådgivende miljøer i Norge.

Videre hevdes det at NSM ikke alltid bør dele sensor-informasjon med politiet, fordi det vil skape etterforskningsplikt. Motargumentet er at denne plikten ikke er absolutt, og dermed ikke vil skape problemer for hendelseshåndteringen. Informantene trekker frem at politiet for eksempel ikke lar etterforskningsplikten stå i veien for ambulansepersonell under håndtering av trafikkulykker, selv om det er fare for at spor kan gå tapt.

Noen informanter mener videre at det er politiet som har de beste forutsetningene for å ta imot informasjon og å finne ut hva som har skjedd, og at NSM derfor ikke bør stå for silingen av informasjon. Det kan også hevdes at det er unaturlig at forsvarssektoren skal ha en rolle i alle cyberrelaterte saker som er sivile. Her er det behov for en avklaring rundt hvilke saker som skal håndteres i et IKT-sikkerhetssenter, og hvordan arbeidsfordelingen vil være overfor NC3.

Når det kommer til privat næringsliv er det imidlertid et relevant spørsmål om hva de er opptatte av. En av Oslo Economics' informanter mener at private virksomheter er mer bekymret for at de blir svindlet for penger, eller at systemene krasjer og driften stoppes, enn å fokusere på hendelser relatert til nasjonal sikkerhet.

Grensedragningene mellom NC3 og Nasjonalt Cybersikkerhetssenter er relatert til spørsmålene om koordineringen i offentlig sektor, og videre hvilke lover som følges. Grensedragningene mellom straffeloven og sikkerhetsloven er derfor en relatert diskusjon. Fordi det er stor usikkerhet i grenseflatene mellom sentrene, spesielt fordi informasjonen som foreligger om NSMs planlagte senter er knapp, vil det være betydelig usikkerhet i det forventede virkningsomfanget. Det er også usikkerhet om i hvilken grad NSM, som er sterkt forankret i forsvarssektoren, vil evne å gi hensiktsmessige råd på sivil side.

Informasjonen fra NSMs varslingssystemer koordineres i dag i FCKS, og Kripos har siden 2017 blitt omfattet av dette samarbeidet. I det planlagte IKT-sikkerhetssenteret skal det tilrettelegges for samarbeid mellom senteret og FCKS, men det er usikkert per i dag hvordan dette vil gjøres.

7.7 Vurdering av samfunnsøkonomisk lønnsomhet

Vi mener det er sannsynlig at et IKT-sikkerhetssenter vil være samfunnsøkonomisk lønnsomt, uavhengig av hvilket alternativ man velger. Kostnadene er begrenset ved begge alternativer, mens de positive virkningene er betydelige.

Det er antagelig lavere kostnader ved å opprette et senter innenfor NSM enn å etablere et frittstående senter. Samtidig vurderer vi at virkninger knyttet til rådgivning, koordinasjon og samarbeid vil oppstå i et større omfang ved et frittstående senter. Ulempen med et frittstående senter er at man mister direkte tilgang på militær etterretning. Vi vurderer denne etterretningen som så viktig at et IKT-sikkerhetssenter under NSM kommer best ut av de to alternativene, ut fra forventet samfunnsøkonomisk lønnsomhet.

7.8 Internasjonale erfaringer

Internasjonalt er det ulike løsninger for organisering og regulering innenfor IKT-sikkerhet. Begge de foreslåtte organiseringene i 7.3 kan finnes igjen i implementeringer av IKT-sikkerhetssentre i andre land. For eksempel har man i Sverige og Nederland et justisdepartement med ansvar for IKT-sikkerheten, mens det i Danmark er forsvarsdepartementet som har ansvaret. I Finland er det finansdepartementet som har ansvaret.

I sin datainnsamling har Oslo Economics intervjuet det britiske National Cyber Security Centre (NCSC). Senteret er en del av Government Communications Headquarters (GCHQ), som er den britiske etaten for signaletterretning. På tross av forankringen i etterretningstjenesten, er et av hovedmålene til NCSC å legge til rette for samhandling med allmennheten – både det private næringslivet, andre offentlige etater og befolkningen for øvrig.

NCSC trekker frem noen hovedutfordringer ved måten senteret er organisert på. Som en del av etterretningstjenesten har de vært nødt til å venne seg til en mer offentlig tilnærming til problemstillinger, og kravet til kommunikasjon ut til offentligheten gjorde at de måtte tilegne seg ny kompetanse og ferdigheter. NCSC har kontorer i London og har en bevisst strategi om å være tilgjengelig for allmennheten. NCSC peker også på kommunikasjonsarbeidet sitt som en viktig grunn til at senteret nyter stor tillit i næringslivet og øvrig befolkning. At NCSC trekker frem kommunikasjon til allmennheten som så viktig, kan være et relevant innspill dersom man setter et norsk IKT-sikkerhetssenter under etterretningstjenesten.

En annen utfordring NCSC peker på er forholdet de har til politimyndighetene. Det oppleves som en utfordring å skille mellom hva som er kriminell aktivitet og ikke. NCSC trekker frem at tillitsforholdet til potensielle cyberangreprammede kan være bedre om aktørene er trygge på at det ikke blir politietterforskning. NCSC jobber imidlertid tett med politimyndighetene om problematikken, og de påpeker at det er en svært viktig utfordring.

NCSC beskriver sin etterretningstilknytning som mindre problematisk for tillit og samarbeid med de som er rammet av cyberangrep, enn det samarbeidet med politimyndighetene er. Dette kan være et relevant innspill i lys av påstander om at et IKT-sikkerhetssenter underlagt etterretningstjenesten kan ha problemer med å skape samarbeid med private aktører. NCSC erkjenner at tillitsforholdet til aktører på sivil side var et tema ved etablering, men fordelene ved å ha nærhet til trusselbildet og å være nærme viktige beslutningstakere ble vurdert å være viktigere i et kost-nytte-perspektiv. I dag beskriver NCSC kommunikasjonsutfordringene som i stor grad løst, og de vurderer at forholdet til allmennheten er en av de viktige forutsetningene for at de skal kunne lykkes med det de gjør.

7.9 Samlet vurdering og anbefaling

I lys av diskusjonen i kapittel 7.6, 7.7 og 7.8, mener vi at et IKT-sikkerhetssenter antagelig er samfunnsøkonomisk lønnsomt, men at det bør gjennomføres en mer grundig utredning for å finne ut nøyaktig hvilket behov samfunnet har for et IKT-sikkerhetssenter utover det som eksisterer i form av NorCERT og NC3. Når dette behovet er kartlagt, er det avgjørende å få klarhet i hvordan samarbeidet mellom IKT-sikkerhetssenteret og NC3 bør være. Dette er viktig for å unngå overlapp i ansvarsområder og for å sikre god koordinering ved hendelser som berører begge sentrenes ansvarsområder. Hvem som skal gi råd til hvem er også et spørsmål som må besvares.

Videre mener vi at spørsmålet om tilgang på militær etterretning må utredes; hvor viktig er denne etterretningen for god forebygging og hendelseshåndtering, og hva er konsekvensen av å eventuelt flytte senteret ut av NSM? Er fordelene med et IKT-sikkerhetssenter i sivil sektor verdt dårligere tilgang på militær etterretning? Vår anbefaling innebærer også at planene om et cybersikkerhetssenter hos NSM ikke iverksettes før disse aspektene er nærmere utredet.

8. Tiltak 5 – Tydeligere ansvar og regulering av tilkoblede produkter og tjenester

IKT-sikkerhetsutvalget mener at det må bli tydeligere myndighetsansvar på tilkoblede produkter og tjenester. Det bør videre sørges for at importører, forhandlere og norske produsenter av tilkoblede produkter får bedre veiledning og verktøy. Videre mener utvalget at man trenger en gjennomgang i produktansvarsregelverket, samt at Norge skal være en pådriver på området i EU og internasjonale fora.

8.1 Nullalternativet

Individer legger i dag ut frivillig person-opplysninger i sosiale medier, og benytter produkter som samler inn mye privat informasjon. Det er derfor et relevant spørsmål i hvilken grad vanlige mennesker bryr seg om risikoen i tingenes internett. En hypotese er at de kjenner til risikoen i de tilkoblede produktene og tjenestene, men ikke oppfatter risikoen som stor nok til å kjøpe produkter som kanskje er dyrere, men sikrere. En annen potensiell hypotese er at forbrukere, enten det er snakk om enkeltindivider eller virksomheter, ikke kjenner til risikoen i produktene de anskaffer.

Ifølge Oslo Economics' informanter, er det en mangel på sikkerhetsforståelse om tilkoblede produkter og tjenester. Det beskrives også at trusselen er betydelig i dag, men også sterkt voksende. Det er ifølge blant en informant en brått akselererende konsekvens, og veksten i konsekvens er potensielt større enn veksten i sikkerhetsrådgivning på området.

Det trekkes frem blant Oslo Economics' informanter at tingenes internett mulig har en ny type eksternalitet ved seg; gjenstandene som eies av en enkeltperson eller virksomhet kan benyttes til å angripe en tredjepart. Dette kan gi et insentivproblem ettersom de som har mulighet til å forebygge truslene i tilkoblede produkter og tjenester, kanskje ikke bærer den fulle kostnaden ved et angrep. I et slikt tilfelle kan man stå overfor et «moral hazard»-problem, fordi man mulig tar ekstra risiko ettersom risikoen delvis legges på andre. Det problematiseres derfor blant informantene i hvilken grad sikkerhetsaspektene er en del av den kommersielle etterspørselen.

Det er to viktige hensyn relatert til manglende IKT-sikkerhet i tilkoblede produkter og tjenester:

i. Insentivproblemer ved at aktører ikke bryr seg om risikoen i produktene (og potensiell «moral hazard»)
ii. Kompetansebehov ved at aktørene har ikke tilstrekkelig informasjon om truslene

Som en skal se i det følgende, er tiltakene foreslått av IKT-sikkerhetsutvalget både rettet mot kompetanse- og insentivproblemet.

8.2 Mål

Med et overordnet samfunnsmål om å skape bedre IKT-sikkerhet, er formålet ved dette tiltaket å forebygge at produkter med dårlig IKT-sikkerhet skaper økt sårbarhet i samfunnet.

Det er sannsynlig at mange ikke er tilstrekkelig bevisste på at produktene de kjøper er sårbare for cyberangrep. Et effektmål er derfor å skape økt bevissthet i samfunnet om IoT-sikkerhet (IoT – «Internet of Things»). Relatert til dette vil det også være et effektmål om å skape økt IKT-sikkerhetskompetanse blant aktørene. Ved potensielle gjennomgang av regelverk, vil også insentivproblemene være relevante.

8.3 Beskrivelse av tiltaket

IKT-sikkerhetsutvalget mener det er mangel på IKT-sikkerhet i tingenes internett i dag. Stadig flere gjenstander og redskap man omgir seg med er koblet til internett, samtidig som at antallet enheter i omløp er i sterk vekst. Dette kan skape sårbarhetsutfordringer. Utvalget mener derfor at ansvaret for IKT-sikkerhet i større grad bør flyttes fra forbruker og over på produsentene.

Det bør gjøres tydeligere hvem som har myndighetsansvar på tingenes internett. Det er

viktig at DSB som produktsikkerhetsmyndighet holder seg oppdatert på utviklingen, og utvalget mener det er DSB som bør ta en tydeligere rolle. Importører, forhandlere og norske produsenter av tilkoblede produkter må få et forbedret tilbud om veiledning og verktøy fra myndighetene i samarbeid med bransjeaktører.

Utvalget mener det det er bedre om Norge bidrar til et oppdatert regelverk på EU-nivå enn at Norge unilateralt etablerer en ny lov på feltet. Det foreslås også at Norge bør være en pådriver i internasjonale fora. Likevel mener utvalget at det bør foretas en gjennomgang av produktansvarsregelverket for å vurdere om krav til IKT-sikkerhet i produkter er tilstrekkelig ivaretatt.

8.4 Identifisering av virkninger

8.4.1 Kostnader

Vi anser forslaget som for lite konkret til å gjøre vurderinger av kostnadene. Selv om en tydeliggjøring av myndighetsansvaret og innføring av regelverk potensielt har samfunnsøkonomiske kostnader, foreligger det ikke nok informasjon om tiltaket til at vi kan identifisere slike kostnadsvirkninger.

8.4.2 Nyttevirkninger

Informantene mener det vil være positivt med en tydeliggjøring av myndighetsansvar på tilkoblede produkter og tjenester. Noen av informantene beskriver at DSB er fraværende på området, og at det ville vært ønskelig at de tok mer ansvar.

Redusert kompetansebehov trekkes frem som særlig viktig på problemstillingene knyttet til tilkoblede produkter og tjenester. Det trekkes fem at det kan ha positive effekter om man hever kompetansen i offentlig sektor, ettersom de utgjør en betydelig kjøpermasse i den norske økonomien. Derfor, hvis det stilles krav relatert til IoT i offentlige anskaffelser, tror informantene at sikkerhetsstandarden fra det offentlige kan bli sett hen til også i privat sektor.

En gjennomgang av produktansvarsregelverket for å vurdere om krav til IKT-sikkerhet i produkter er tilstrekkelig ivaretatt, vil kunne ha nyttevirkninger. Dette er relatert til det potensielle «moral hazard»-problemet, fordi man vil potensielt i større grad gjøre aktørene ansvarlig. Hvilken aktør som har erstatningsansvar ved potensielle IKT-sikkerhetsbrudd, med andre ord hvem som bærer kostnadene ved cyberangrep, vil være sentralt i atferden i markedet.

8.5 Vurdering av virkninger

8.5.1 Kostnader

Vi anser forslaget som for lite konkret til å gi anslag på kostnadene.

8.5.2 Øvrige virkninger

Det er identifisert fire virkninger av dette tiltaket, og disse har samfunnsøkonomisk betydning beskrevet i Tabell 8-1.

Som nevnt tidligere i rapporten, er kompetansebehovet vurdert å ha stor samfunnsøkonomisk betydning for IKT-sikkerheten. Dette er basert på vurderinger i tidligere utredninger på IKT-sikkerhetsområdet, samt innspillene fra både Oslo Economics' og IKT-sikkerhetsutvalgets informasjonskilder. Kompetansebehovet vil også være relatert til tingenes internett, fordi det kan stilles spørsmål ved om samfunnsaktørene kjenner til risikoen i tilkoblede produkter og tjenester.

Insentivproblemene i privat sektor er også vurdert å ha stor betydning, som forklart over. Dette er også forventet å være relatert til problematikken knyttet til tingenes internett, ettersom leverandører og kjøpere av tilkoblede produkter og tjenester kanskje ikke internaliserer IKT-sikkerhetskostnadene.

Som også forklart i de foregående kapitlene, vurderes økt bevissthet og bedre rådgivning til å ha middels betydning. Disse virkningene vil trolig også være relaterte til tingenes internett, for det er ifølge informantene behov for å belyse temaet i større grad.

Tabell 8-1: Betydning av virkninger

Virkning	Betydning
Økt kompetanse	Stor
Reduserte insentivproblemer, privat	Stor
Økt bevissthet	Middels
Bedre rådgivning	Middels

Tabell 8-2: Omfang av virkninger

Virkning	Omfang
Økt kompetanse	Lite positivt
Reduserte insentivproblemer, privat	Stort positivt
Økt bevissthet	Middels positivt
Bedre rådgivning	Lite positivt

Tabell 8-3: Konsekvens av virkninger

	Tydeligere ansvar og regulering på IoT
Bedre håndtering:	
Økt kompetanse	++
Reduserte insentivproblemer, privat	++++
Økt bevissthet	++
Bedre håndtering:	
Bedre rådgivning	+

Hvis man lykkes med å regulere IoT, med andre ord om man gjennomgår produktansvarsregelverket og klarer å formulere regelverk som fører til at markedsaktørene internaliserer IKT-sikkerhetskostnadene, vil det kunne føre til et skift i insentivene i det private næringslivet, som kan skape bedre IKT-sikkerhet. Hvis det er slik at sikkerheten er lavere i produktene fordi deler av sikkerhetsrisikoen bæres av andre enn de to partene i en transaksjon, kan reguleringer føre til at produsentene eller innkjøperne har sterkere insentiver til å internalisere denne risikoen ved å investere i sikkerhet. Dette vil kunne gi sikrere produkter, som videre vil kunne føre til bedre IKT-sikkerhet. Ettersom insentivproblemene i privat sektor generelt vurderes å ha stor betydning for IKT-sikkerheten, og en hensiktsmessig lovregulering av produktene forventes å ha et stort positivt virkningsomfang, er forventningen en meget stor positiv konsekvens (++++).

Hvis myndighetsansvaret på tingenes internett tydeliggjøres, er en mulig indirekte effekt at det kan føre til mer kompetanse på området. En myndighetsaktør kan skape økt bevissthet om sikkerhetsaspektene ved de tilkoblede produktene og tjenestene, som gjør at man får mer kunnskap om truslene og sårbarhetene i produktene. Fordi kompetansebehovet har stor betydning for IKT-sikkerheten, vil et lite, positivt virkningsomfang føre til en middels positiv konsekvens for IKT-sikkerheten (++).

Tydeligere myndighetsansvar vurderes for øvrig å ha et middels, positivt virkningsomfang også på bevisstheten rundt IoT, og konsekvensen vurderes derfor å kunne være middels positiv (++). Det er videre en forventning om at tydeligere myndighetsansvar kan gi bedre rådgivning, i et omfang som vurderes å være lite og positivt, så her er konsekvensen estimert til å være liten positiv.

8.6 Vurdering av usikkerhet

Enkelte informanter er usikre på om det er hensiktsmessig at DSB tar tydeligere rolle på IoT-området. Det beskrives at DSB ikke er aktive på IKT-sikkerhetsområdet generelt, og det sås derfor tvil om de har kompetansen til å ta en tydeligere rolle på tilkoblede produkter og tjenester.

Det er usikkert hvor godt regelverk på tingenes internett vil treffe. Produktene og tjenestene som omfattes i IoT er i stor grad bevegelige mål, og kan ha mange underleverandører, noe som kan gjøre regulering vanskelig. Derfor, hvis man skal ha et teknisk regelverk på dette området, er det en fare for at man alltid vil henge etter. Noen av informantene mener at det istedenfor regulering av spesifikke produkter kan være at man trenger en mer generell tilnærming.

Det oppfattes stort sett om en god idé å merke produkter i et sertifiseringssystem lignende CE-merking. Det er imidlertid en viss usikkerhet knytte til effektene av dette også, ettersom den teknologiske utviklingen skjer raskt. Det er derfor viktig at regimene som gir ut disse merkingene tar innover seg livsløpsvurderinger. En sikkerhetsmessig sertifisering basert på

«point of time» kan derfor i mange tilfeller ha begrenset verdi.

8.7 Vurdering av samfunnsøkonomisk lønnsomhet

En tydeliggjøring av myndighetsansvaret på tingenes internett kan vanskelig vurderes å være ulønnsomt. Under forutsetningen om at det ikke vil påløpe betydelige kostnader ved et slikt initiativ, vil dette forslaget være samfunnsøkonomisk lønnsomt.

Ved gjennomgangen av produktansvarsregelverket er det nødvendig å vurdere hvilke potensielle kostnader som kan oppstå ved økning i reguleringsomfanget. Dette henger sammen med argumentene relatert til å etablere en tverrsektoriell IKT-sikkerhetslov, ettersom økt regulering vil føre til at virksomheter må legge inn ressurser i håndteringen av regelverket.

8.8 Samlet vurdering og anbefaling

Oslo Economics støtter vurderingen om at myndighetsansvaret på tingenes internett må bli tydeligere. Likevel, usikkerheten om kompetansen i DSB, og dermed hvorvidt de er det egnede organet for å ha myndighetsansvaret, kan gjøre at man bør utrede nærmere hvem som bør ha ansvaret, eller hvordan DSB skal erverve denne kompetansen.

En gjennomgang av produktansvarsregelverket er også noe som støttes av Oslo Economics. Det er ikke klart i hvilken grad markedsaktører internaliserer kostnadene ved potensielt usikre tilkoblede produkter og tjenester, så en gjennomgang og ytterligere utredning vil derfor kunne være hensiktsmessig.

9. Referanser

Anderson, R. & Fuloria, S., 2010. Security Economics and Critical National Infrastructure. I: T. Moore, D. Pym & C. Ioannidis, red. *Economics of Information Security and Privacy*. Boston, MA: Springer, pp. 55-66.

DFØ, 2018. *Veileder i samfunnsøkonomiske analyser*. Oslo: Direktoratet for økonomistyring.

Difi, 2018. *Arbeidet med informasjonssikkerhet i statsforvaltningen,* Oslo: Difi-rapport 2018:4.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, Z., 2015. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, januar, pp. 24-30.

Gordon, L. & Loeb, M., 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, pp. 438-457.

Meld. St. 38, 2016-2017. *IKT-sikkerhet — Et felles ansvar*. s.l., Regjeringen.

Moore, T., 2010. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, desember, pp. 103-117.

NIFU, 2017. *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud,* Oslo: Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU), Rapport 2017:32.

NOU, 2015:13. *Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden,* Oslo: Justis- og beredskapsdepartementet.

Næringslivets Sikkerhetsråd, 2018. *Mørketallsundersøkelsen 2018,* Oslo: Opinion AS for Næringslivets Sikkerhetsråd.

OPAK, 2017. *OPAKs prisstigningsrapport,* s.l.: s.n.

Vedlegg A

A.1 Bakgrunn

IKT-sikkerhetsutvalget skal utrede ulike tiltak for å øke IKT-sikkerheten i Norge. Utvalget skal blant annet vurdere om dagens regulering er hensiktsmessig, om det er behov for å endre fordeling og organisering av ansvar på etatsnivå, samt vurdere regulatoriske og organisatoriske grep for å styrke IKT-sikkerheten.

I sitt arbeid har utvalget utarbeidet noen foreløpige anbefalinger:

- Etablere et nasjonalt IKT-sikkerhetssenter
- Vurdere å styrke hjemmelsgrunnlaget for hendelseshåndtering
- Tydeligere ansvars- og reguleringsforhold på tilkoblede produkter og tjenester
- Justis- og beredskapsdepartementet (JD) må ta større lederskap
- Innføre krav om grunnsikring av IKT-systemer i en tverrsektoriell lov
- IKT-sikkerhetskrav i anskaffelser og til leverandører

Utvalget har engasjert Oslo Economics for å vurdere de samfunnsøkonomiske konsekvensene av anbefalingene. En viktig informasjonskilde til disse vurderingene er å gjennomføre intervjuer med ulike interessenter, som ventelig vil kunne ha informasjon eller synspunkter som har betydning for vurderingen. Som et utgangspunkt for samtalen har vi listet opp noen spørsmål. Intervjuet er imidlertid fleksibelt, og det legges opp til at vi også kan diskutere eventuelle forhold av betydning som ikke er dekket av spørsmålene. Det er også slik at spørsmålene vil ha ulik grad av relevans for de forskjellige virksomhetene som intervjues.

A.2 Spørsmål

A.2.1 Overordnede spørsmål

1. Kan du kort beskrive din virksomhet, og hvordan myndighetenes IKT-sikkerhetsarbeid er relevant for dere?
2. Mener du at virksomheter i Norge forstår behovet for IKT-sikkerhet?
    a. På hvilke områder mener du virksomhetene eventuelt ikke forstår behovene?
3. Hvordan vurderer du myndighetenes arbeid med IKT-sikkerhet?
4. Er det områder innenfor IKT-sikkerhet som ikke er tilstrekkelig regulert?
    a. Er det spesifikke regelverk som bør utvides eller erstattes?
5. Opplever din virksomhet utfordringer med at det er flere myndighetsorganer som har ansvar for å følge opp IKT-sikkerheten?
6. Hvordan kan det offentlig-private samarbeidet på IKT-sikkerhetsområdet bli bedre?
7. Er informasjonsdelingen på IKT-sikkerhetsområdet tilstrekkelig for å håndtere hendelser?
8. I hvilken grad prioriteres svært kostbare og lite sannsynlige trusler på IKT-sikkerhetsområdet?
9. Er det en god koordinering på IKT-sikkerhetsområdet mellom offentlige etater?
    a. Er det koordineringsproblemer knyttet til grensedragningene mellom DSB og NSM eller andre etater?
10. Er det internasjonale samarbeidet godt nok?
11. Er det behov for å gjennomføre tiltakene som ligger i utvalgets foreløpige anbefalinger?

A.2.2 IKT-sikkerhetssenter

NSM er i gang med å planlegge etableringen av et nasjonalt cybersikkerhetssenter. Utvalget er i utgangspunktet støttende til dette initiativet, men foreløpig finnes det ikke mye informasjon om hvordan innretningen på et slikt senter vil være. Utvalget mener at senteret bør bidra til å beskytte nasjonal kritisk infrastruktur mot cyberangrep, koordinere innsatsen for å håndtere større digitale angrep, og sørge for rådgivning til både innbyggere og store og små virksomheter i Norge.

1. Er det behov for et IKT-sikkerhetssenter i Norge?
2. Hvilke funksjoner bør et IKT-sikkerhetssenter ha, slik at det best mulig kan bedre IKT-sikkerheten i Norge?
    a. Bør senteret drive med veiledning og/eller tilsyn etter en eventuell tverrsektoriell IKT-sikkerhetslov?
3. Hvem vil dra størst nytte av et IKT-sikkerhetssenter – privat eller offentlig sektor?
4. Hvilket departement bør ha ansvar for senteret, og hvorfor?
    a. Forsvarsdepartementet
    b. Justis- og beredskapsdepartementet
    c. Andre
5. Bør senteret være frittstående, som en del av NSM, som en del av DSB, som en del av NKOM, eller andre?
6. Dersom det etableres et senter, hvordan vurderer du at ressursbehovet vil være på:
    a. Kompetanse?
    b. Antall ansatte?
    c. Teknisk utstyr?
    d. Budsjett?
7. Vil din virksomhet dra nytte av et IKT-sikkerhetssenter? Hvis ja, på hvilken måte?

A.2.3 Vurdere å styrke hjemmelsgrunnlaget for hendelseshåndtering

Hjemmelsgrunnlaget for hendelseshåndtering bør muligens styrkes, og de prinsippene som følges i dag bør formaliseres. Videre behøver man et sterkere rettslig fundament for deling av informasjon, deriblant personopplysninger. Dette vil være relevant for forebygging, oppdaging og håndtering av IKT-sikkerhetshendelser, og kan deles mellom berørte aktører. Respondentene kan legge til grunn at NIS-direktivet vil bli innført i Norge.

1. Er det et behov for at prinsippene som følges i dag forankres i lov og forskrift?
2. Trenger man et sterkere rettslig fundament for deling av informasjon?
3. Vil en styrking av hjemmelsgrunnlaget på området påvirke beslutningsprosessene i din virksomhet?
4. Vil hendelseshåndteringen bli mer effektiv hvis man styrker hjemmelsgrunnlaget?
5. Vil det ha noen konsekvenser for din virksomhet at det f.eks. stilles krav til logging eller andre krav som kan bidra til en mer effektiv hendelseshåndtering fra myndighetenes side?

A.2.4 Tydeligere ansvars- og reguleringsforhold på tilkoblede produkter og tjenester

Utvalget mener det er manglende IKT-sikkerhet på tilkoblede produkter og tjenester («internet of things» – tingenes internett). Stadig flere gjenstander og redskap vi omgir oss med i hverdagen er koblet til internett, og dette skaper sårbarhetsutfordringer. Det bør derfor gjøres tydeligere hvem som har myndighetsansvar på området. Det vurderes også om det må stilles krav til sikkerhet i produkter og tjenester.

1. Hvordan vurderer du trusselen i tingenes internett?
2. Vurderer du at det er manglende IKT-sikkerhet på tilkoblede produkter og tjenester?
3. Mener du at det bør stilles IKT-sikkerhetskrav til leverandører av tilkoblede produkter og tjenester?
4. Mener du at det bør stilles IKT-sikkerhetskrav til tilkoblede produkter og tjenester?
5. Hvilke kostnader eller besparelser vil det medføre om det stilles IKT-sikkerhetskrav til tilkoblede produkter og tjenester eller til leverandørene?
6. På hvilken måte vil en tydeliggjøring av myndighetsansvaret være hensiktsmessig for å sikre bedre IKT-sikkerhet på området?

A.2.5 Justis- og beredskapsdepartementet må ta større lederskap

Justis- og beredskapsdepartementet (JD) har det nasjonale ansvaret for å utforme politikk på IKT-sikkerhet i sivil sektor, herunder å etablere nasjonale krav og anbefalinger for både offentlige og private virksomheter. Mange av utfordringene utvalget har identifisert knytter seg til tverrsektoriell

styring, koordinering og samarbeid, det vil si JDs ansvar. For å skape bedring på IKT-sikkerhetsområdet, mener utvalget at JD bør ta større lederskap.

1. Hvordan vurderer du JDs synlighet og lederskap på IKT-sikkerhetsområdet i dag?
2. Kan du peke på områder hvor det er særlig behov for tydeligere lederskap fra JD?
3. Har JD tilstrekkelig kompetanse til å utføre sine oppgaver på IKT-sikkerhetsområdet?
4. Hva er deres vurdering om at NSM som fagmiljø i større grad skal understøtte JD i deres arbeid med IKT-sikkerhet?
5. Vurderer du at et større lederskap fra JD vil føre til bedre IKT-sikkerhet, eventuelt hvordan?
6. Vil det kreve en forsterket ressursinnsats (f.eks. kompetanseheving, ansettelser eller investeringer) for at JD skal kunne utøve sitt ansvar på IKT-sikkerhet på en tilfredsstillende måte?

A.2.6 Innføre krav om grunnsikring av IKT-systemer i tverrsektoriell lov

Det er mange ulike regelverk som er med på å regulere IKT-sikkerhet i Norge, men ingen dekker samtlige elementer. Utvalget mener at man i dag har uforholdsmessig stort fokus på å sikre informasjonen i systemene, fremfor å beskytte systemene og tjenestene som en verdi i seg selv. Videre mener utvalget at det bør diskuteres om det er hensiktsmessig å innføre krav om grunnsikring av IKT-systemer, i form av tekniske og organisatoriske krav, i tverrsektoriell lov. Eksempler på tekniske krav er antivirus, brannmur, redundans, kryptering og sikkerhetslogging. Organisatoriske krav kan være krav til administrasjon, styringssystemer og personell.

1. Er det behov for tverrsektorielle krav til IKT-sikkerhet? Hvorfor, eventuelt hvorfor ikke?
2. Er du enig i utvalgets oppfatning om at man trenger lovpålagte tekniske og organisatoriske krav for grunnsikring av IKT-systemer?
3. Bør krav om grunnsikring gjelde alle offentlige og private virksomheter i Norge?
4. Hva vil konsekvensene for din virksomhet være av at det innføres krav om grunnsikring av IKT-systemer?
5. Er krav om grunnsikring et hensiktsmessig virkemiddel for å bedre IKT-sikkerheten i din virksomhet?
6. Hva skal til for at man i større grad prioriterer å beskytte systemene og tjenestene i tillegg til informasjonen?

A.2.7 IKT-sikkerhetskrav i anskaffelser og til leverandører

Utvalget mener et virkemiddel som kan brukes for å oppnå forsvarlig IKT-sikkerhet er å stille krav til anskaffelser. Utvalget ser på flere ulike grep. Deriblant at det bør kreves at alle departementer etterspør rapporter om virksomhetenes arbeid med IKT-sikkerhet. At det gjøres en risikoanalyse av IKT-sikkerheten før det gjøres en anskaffelse. Forslaget innebærer at det stilles krav om IKT-sikkerhet i anskaffelsesregelverket og at Statens Standardavtaler oppdateres slik at de stiller krav til grunnsikring av IKT-sikkerhet.

1. Er du enig i at det bør stilles IKT-sikkerhetskrav i anskaffelser og til leverandører?
2. Bør man benytte anskaffelsesregelverket for offentlige anskaffelser for å sette krav om IKT-sikkerhet, eller bør man heller benytte annet regelverk?
    a. Hvorfor/hvorfor ikke er dette regelverket egnet?
3. Vil det innebære noen konsekvenser å stille krav om IKT-sikkerhet i anskaffelsesregelverket?
    a. Dyrere offentlige anskaffelser?
    b. Færre tilbydere og mindre konkurranse i anbudene?
4. Utvalget mener at risikoanalyser før anskaffelser ikke vil ha «den største økonomiske utgiften». Er du enig i den vurderingen?
5. Hvor ressurskrevende vil krav om risikoanalyser være?
6. I hvilken grad har innkjøpere tilstrekkelig bestillerkompetanse til å gjennomføre risikoanalyser?
7. Hvor ressurskrevende vil et krav om rapportering være?

8. Er det behov for at Statens standardavtaler oppdateres til å stille krav til IKT-sikkerheten?
9. Hvordan skal innkjøper sikre at tilbydere oppfyller kravene? Har innkjøpere tilstrekkelig kompetanse og ressurser til å vurdere dette selv?
10. Er det hensiktsmessig å pålegge tilbydere å innføre grunnsikring gjennom Statens standardavtaler, eller bør dette gjøres på andre måter?
11. Hvordan vil et slikt tiltak påvirke beslutningsprosessene i din virksomhet?

oslo economics
www.osloeconomics.no

post@osloeconomics.no
Tel: +47 21 99 28 00
Fax: +47 96 63 00 90

Besøksadresse:
Kronprinsesse Märthas plass 1
0160 Oslo

Postadresse:
Postboks 1562
Vika
0118 Oslo