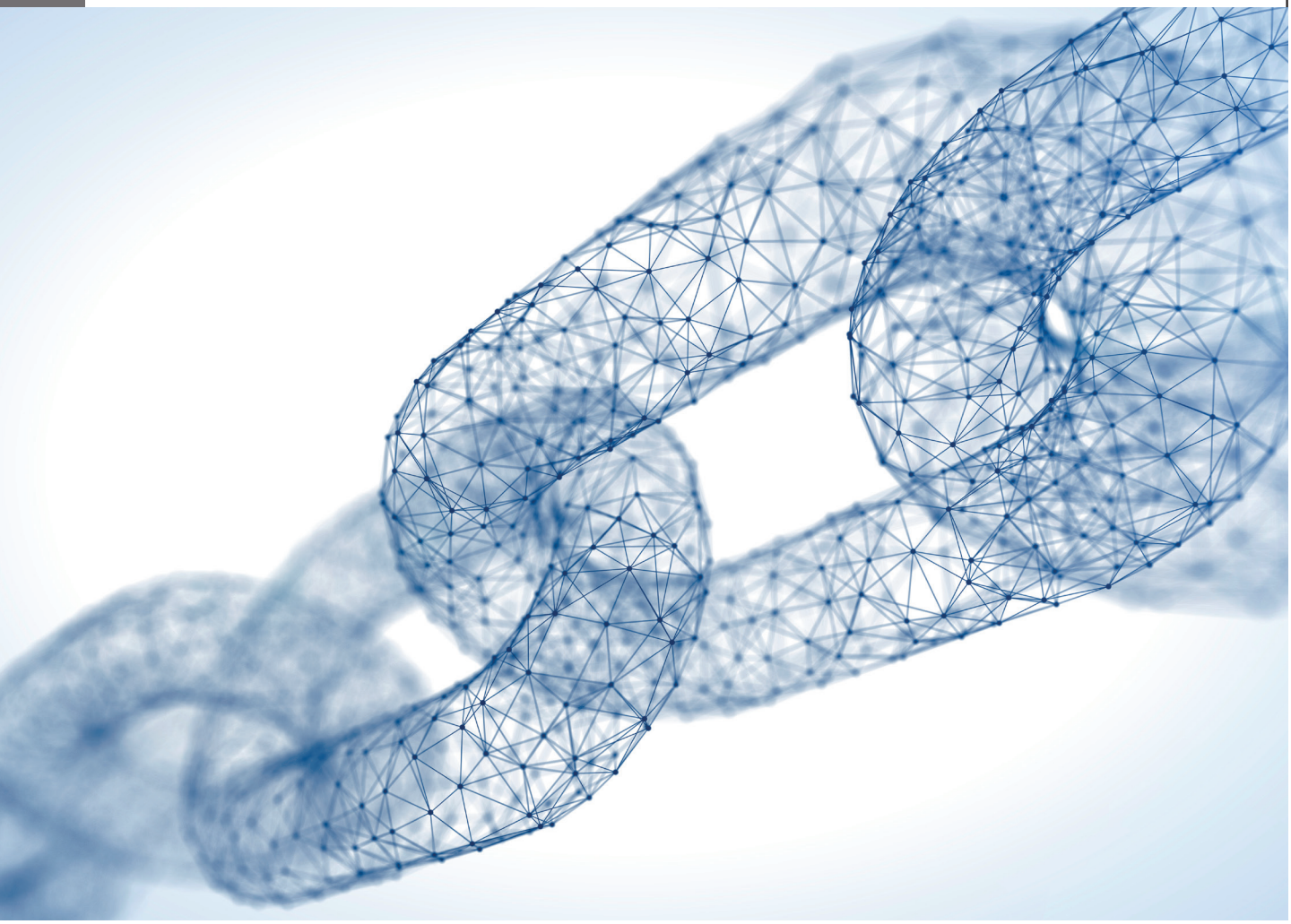
NOU Norges offentlige utredninger 2018: 14

IKT-sikkerhet i alle ledd

Organisering og regulering av nasjonal IKT-sikkerhet



Norges offentlige utredninger 2018

Seriens redaksjon:
Departementenes sikkerhets- og serviceorganisasjon
Teknisk redaksjon

---

1. Markeder for finansielle instrumenter
   Finansdepartementet
2. Fremtidige kompetansebehov I
   Kunnskapsdepartementet
3. Krisehåndtering i forsikrings- og pensjonssektoren
   Finansdepartementet
4. Sjøveien videre
   Samferdselsdepartementet
5. Kapital i omstillingens tid
   Nærings- og fiskeridepartementet
6. Varsling – verdier og vern
   Arbeids- og sosialdepartementet
7. Ny lov om offisiell statistikk og Statistisk sentralbyrå
   Finansdepartementet
8. Grunnlaget for inntektsoppgjørene 2018
   Arbeids- og sosialdepartementet
9. Regnskapsførerloven
   Finansdepartementet
10. Nye prospektregler
    Finansdepartementet
11. Ny fjellov
    Landbruks- og matdepartementet
12. Energiaksjer i Statens pensjonsfond utland
    Finansdepartementet
13. Voksne i grunnskole- og videregående opplæring
    Kunnskapsdepartementet
14. IKT-sikkerhet i alle ledd
    Justis- og beredskapsdepartementet

NOU Norges offentlige utredninger **2018: 14**

IKT-sikkerhet i alle ledd

Organisering og regulering av nasjonal IKT-sikkerhet

Utredning fra utvalg oppnevnt ved kongelig resolusjon 15. september 2017
Avgitt til Justis- og beredskapsdepartementet 3. desember 2018

Departementenes sikkerhets- og serviceorganisasjon
Teknisk redaksjon

Oslo 2018

ISSN 0333-2306
ISBN 978-82-583-1373-8

07 Media AS

Til Justis- og beredskapsdepartementet

Utvalget om organisering og regulering av nasjonal IKT-sikkerhet ble oppnevnt ved kongelig resolusjon 15. september 2017. Utvalget gir med dette sin utredning.

Oslo 3. desember 2018

Hans Christian Holte
Leder

Terje Wold	Håkon Grimstad	Lillian Røstad
Torgeir A. Waterhouse	Marie Moe	Lee A. Bygrave
Therese Steen		

Roger Kolbotn og
Sveinung Torgersen
Sekretariatsleder

Christian Frederik
Mathiessen

Ola Hermansen

Harald Fardal

Anniken Grønli Foss

Anders Bjønnes

Klaus Søreide

Innhold

Digitalt vedlegg:

Oslo Economics, Samfunnsøkonomisk vurdering av anbefalinger fra IKT-sikkerhetsutvalget, OE rapport 2018:37

Del I
Innledning

Kapittel 1
Sammendrag

Liv og helse, demokrati og rettssikkerhet, økonomisk velferd og nasjonens suverenitet er viktige verdier som må beskyttes for å kunne opprettholde et trygt, fritt og velfungerende samfunn. Mange sider ved den teknologiske utviklingen kan styrke og bygge opp under disse verdiene. Teknologi kan for eksempel benyttes til å utvide helsetilbudet, bidra til effektivisering av virksomheter og gi nye måter for enkeltindivider å uttrykke seg på i sosiale medier.

Den teknologiske utviklingen gjør at det norske samfunnet i stadig større grad kobles sammen, og avhengighetene mellom virksomheter og mellom sektorer blir stadig sterkere. Norsk næringsliv og forvaltning har i tillegg stadig tettere bindinger til andre land. IKT-infrastrukturen representerer en stor og fortsatt økende samfunnsmessig verdi. Stadig mer informasjon lagres, transporteres og behandles digitalt, og nye tjenester, prosesser og produkter utvikles fortløpende. Den teknologiske utviklingen skaper nye og endrede risikoer og utfordringer som må håndteres.

Utvalget er gitt i oppdrag å vurdere om dagens regulering av IKT-sikkerhet er hensiktsmessig gitt de samfunnsutfordringene Norge står overfor. Utvalget er også bedt om å vurdere organiseringen av tverrsektorielt ansvar på IKT-sikkerhetsområdet. Ansvar, roller og oppgaver må være hensiktsmessig fordelt mellom etatene.

Utvalget legger tre overordnede prinsipper til grunn for sine anbefalinger. Arbeidet med IKT-sikkerhet må ha en risikobasert tilnærming som innebærer at vesentlig risiko prioriteres. Videre må IKT-sikkerhet balanseres opp mot brukervennlighet, økonomi og grunnleggende menneskerettigheter. En slik balanse innebærer at noe risiko må aksepteres for å oppnå økonomiske og sosiale mål. Til slutt krever arbeidet med IKT-sikkerhet en fleksibilitet i reguleringen og organiseringen slik at man kan tilpasse seg nye trusler, sårbarheter, teknologier og forretningsmodeller.

Nedenfor følger et sammendrag av utvalgets anbefalinger for å styrke den nasjonale IKT-sikkerheten. Utvalget står samlet bak anbefalingene.

1.1 Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Digitaliseringen av samfunnet gjør at virksomheter står overfor et stadig mer komplekst IKT-risikobilde. For at et digitalt samfunn som Norge skal fungere, er det nødvendig å minimere risikoen for at utilsiktede og tilsiktede hendelser rammer IKT-systemer. Til tross for potensielt betydelige økonomiske, sikkerhetsmessige og omdømmemessige konsekvenser har virksomheter ikke alltid tilstrekkelige insentiver til å beskytte seg mot digitale trusler.

Etter utvalgets vurdering håndteres ikke utfordringene på en hensiktsmessig måte i gjeldende regulering. En rekke lover og forskrifter stiller krav om IKT-sikkerhet. Det stilles imidlertid ikke alltid hensiktsmessige krav om sikring av IKT-systemer som understøtter virksomheters produksjon av varer og tjenester.

Gitt det gjeldende IKT-risikobildet mener utvalget at det må utarbeides en ny lov hvor det stilles krav om forsvarlig IKT-sikkerhet til alle samfunnskritiske virksomheter og offentlig forvaltning. Den nye loven skal også gjennomføre NIS-direktivet i norsk rett. Kravene som følger av loven, må konkretiseres i forskrift og veiledning.

Utvalget mener at det ikke er nødvendig å sanere og harmonisere eksisterende regelverk før vedtakelse av loven. Det er viktigere å sørge for at det i fremtiden blir enhetlig begrepsbruk i lover og forskrifter som stiller krav om IKT-sikkerhet.

Selv om samfunnskritiske virksomheter og offentlig forvaltning har forsvarlig IKT-sikkerhet, gjenstår mange digitale sårbarheter. De fleste virksomheter er avhengige av lange og komplekse digitale verdikjeder. I prinsippet kan alle IKT-systemer bli benyttet som mellomledd i angrep mot andre egentlige mål, for eksempel samfunnskritiske virksomheter. Også tilkoblede produkter kan inngå i angrepsnettverk som kan

skade samfunnskritiske funksjoner. Dette er risiko som i liten grad reduseres ved at det stilles krav om forsvarlig IKT-sikkerhet til samfunnskritiske virksomheter og offentlig forvaltning.

Utvalget har vurdert muligheten for å underlegge alle virksomheter krav om IKT-sikkerhet i lov, ikke bare samfunnskritiske virksomheter og offentlig forvaltning. Krav i lov kan være inngripende og ressurskrevende. Utvalget mangler konkrete holdepunkter for å si hvor stort det gjenstående behovet er for å styrke IKT-sikkerheten i alle norske virksomheter. Dersom behovet er stort, taler det for å stille krav i lov til alle norske virksomheter. Utvalget anbefaler derfor at det nedsettes et eget lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter.

1.2 Krav om IKT-sikkerhet ved anskaffelser

Anskaffelser av IKT-tjenester kan, og vil i mange tilfeller, gi bedre trygghet og mer stabile og tilgjengelige tjenester. Med andre ord kan anskaffelser av IKT-tjenester være et fornuftig IKT-sikkerhetstiltak.

Anskaffelser av slike tjenester er imidlertid ikke risikofritt. Det er utvalgets oppfatning at den største utfordringen med anskaffelser er manglende bevissthet om risikoen. For å kunne iverksette hensiktsmessige sikkerhetstiltak, er det avgjørende at virksomhetene vurderer risikoen ved alle anskaffelser. Virksomheter som blir omfattet av utvalgets forslag til ny lov om IKT-sikkerhet plikter å vurdere slik risiko.

Utvalget mener at det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Anskaffelsesregelverket bør endres slik at oppdragsgiveren får en slik plikt.

Statens standardavtaler (SSA) brukes av en rekke private virksomheter, i tillegg til offentlig sektor. Utvalget anbefaler at SSAene endres slik at IKT-sikkerhet blir tydeligere ivaretatt.

Det er et stort behov for kompetanse og veiledning om IKT-sikkerhet ved anskaffelser. Utvalget mener det er viktig at den eksisterende veiledningen på anskaffelsesområdet videreutvikles til å inkludere IKT-sikkerhet i større grad. Veiledningen om anskaffelser og SSAer bør samkjøres med annen veiledning om IKT-sikkerhet.

1.3 Etablere et nasjonalt IKT-sikkerhetssenter

Mange virksomheter opplever at råd og veiledning fra myndighetene er for lite koordinert mellom etatene. De er usikre på hvor de skal henvende seg når de har spørsmål om IKT-sikkerhet. Det er også utfordringer med koordinering og informasjonsdeling når uønskede digitale hendelser skal håndteres. Det er mange som etterlyser mer offentlig-privat samarbeid og en styrket innovasjonsevne innenfor IKT-sikkerhet. Det er behov for å samle kompetanse, skape synergier på tvers av sektorer og miljøer og gjøre samarbeidslinjene kortere og mer effektive.

Utvalget mener at etablering av et nasjonalt IKT-sikkerhetssenter er et godt grep for å møte dette behovet. Et senter kan være en pådriver for koordinering og samordning mellom sektorer og mellom offentlige og private aktører. Det kan være et sentralt kontaktpunkt for råd og veiledning til virksomheter, det kan koordinere håndtering av uønskede digitale hendelser og dele informasjon om trusler og sårbarheter.

Et IKT-sikkerhetssenter kan også tillegges oppgaver som ingen etater har ansvar for i dag, for eksempel å motta og offentliggjøre informasjon om digitale sårbarheter («Coordinated Vulnerability Disclosure»). Senteret må dessuten stimulere til mer forskning, utvikling og innovasjon.

Et nasjonalt IKT-sikkerhetssenter må ha en tydelig forankring i sivile myndigheter. Behovet for styrket IKT-sikkerhet er først og fremst knyttet opp mot sivile samfunnsfunksjoner og kritisk infrastruktur, både i offentlig og privat regi. Samtidig har forsvarssektoren en sentral rolle knyttet til statssikkerhet, og sivil og militær IKT-infrastruktur blir i økende grad integrert. Godt sivilt – militært samarbeid er derfor en viktig oppgave for senteret. Det er også nødvendig at et slikt senter har et tydelig grensesnitt mot nasjonalt cyberkrimsenter, som er under etablering i Kripos.

Parallelt med utvalgets utredning er det startet et arbeid med å etablere et nasjonalt cybersikkerhetssenter som del av NSM. Utvalget mener at det må ligge et godt beslutningsgrunnlag til grunn før det etableres et nasjonalt IKT-sikkerhetssenter i Norge. Justis- og beredskapsdepartementet, i samarbeid med Forsvarsdepartementet, må sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse. En slik analyse må baseres på en bred involvering av potensielle interessenter i privat og offentlig sektor. Behovsanalysen må avklare IKT-sikkerhetssenterets

myndighetsforankring og kobling til NSM, og grensedragninger mot det planlagte nasjonale cyberkrimsenteret.

1.4 Tydelig regulering og ansvar for tilkoblede produkter og tjenester

Antallet produkter og tjenester som er koblet til internett er stort og i sterk økning. Manglende IKT-sikkerhet i slike produkter og tjenester kan utgjøre en trussel for forbrukere, virksomheter og samfunnssikkerheten.

Ansvaret for IKT-sikkerhet på dette området bør i større grad flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester.

Norge må videreføre sitt internasjonale samarbeid, særlig opp mot EU. Fordi mange tilkoblede produkter og tjenester brukes på tvers av landegrenser, er det viktig å ha et harmonisert regelverk internasjonalt. På denne bakgrunn mener utvalget at det er bedre å bidra til et oppdatert regelverk på EU-nivå enn at Norge unilateralt endrer regelverket på feltet.

Utvalget mener videre at det må være et tett samarbeid mellom tilsynsmyndigheter som Datatilsynet, Forbrukertilsynet, DSB og Nkom når det gjelder tilkoblede produkter og tjenester. Myndighetene må gi bedre råd og veiledning til importører, forhandlere og norske produsenter på dette området. Utarbeidelse av råd og veiledning må gjøres i samarbeid med bransjeaktørene. Målsettingen bør være å forebygge at produkter uten tilfredsstillende IKT-sikkerhet lanseres på det norske markedet, og å håndtere avdekkede sikkerhetshull på en god måte.

Myndighetene må også sørge for at produkter uten tilstrekkelig IKT-sikkerhet kan oppdages, varsles om og tilbakekalles. Forbrukerne må kunne heve kjøp av produkter og tjenester som ikke har tilstrekkelig IKT-sikkerhet.

Utvalget mener at myndighetsansvaret for IKT-sikkerheten i tilkoblede produkter og tjenester må tydeliggjøres. Det er viktig at DSB som produktsikkerhetsmyndighet holder seg oppdatert på utviklingen, og utvalget mener DSB bør få en tydelig rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

1.5 Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

IKT-sikkerhet griper inn i alle sektorer og virksomheter i samfunnet. Denne kompleksiteten utfordrer styringen og samordningen av nasjonal IKT-sikkerhet.

Det foreligger ingen enkel oppskrift på hvordan myndighetene best mulig skal organisere seg for å møte disse utfordringene. Utvalgets informasjonsinnhenting har ikke avdekket noe åpenbart behov for å gjøre større endringer i ansvar, roller eller oppgaver til etatene. Det er imidlertid viktig at ansvarsforholdene er tydelig definert der det er tilgrensende områder, og at det er et godt og koordinert samarbeid på tvers av sektorer og etater.

Utvalget mener at Justis- og beredskapsdepartementet i større grad må være en synlig aktør som tar initiativ, løser opp i uklarheter, definerer mål, koordinerer og samordner arbeidet med nasjonal IKT-sikkerhet. Det er et politikkområde som bør løftes systematisk inn i styringsprosesser og i samfunnsdebatten. Etablering av et nasjonalt IKT-sikkerhetssenter og en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning vil styrke departementets evne til å utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.

Justis- og beredskapsdepartementet må ha en mer samordnet styring av underliggende etater når det gjelder IKT-sikkerhetsoppgaver. Utvalget mener også at Justis- og beredskapsdepartementet må være en tydelig pådriver for å samordne departementenes styringssignaler om IKT-sikkerhet.

Justis- og beredskapsdepartementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre, og at tilsyn med teknisk IKT-sikkerhet gis økt oppmerksomhet. Utvalget mener at samarbeidet som har funnet sted mellom en rekke etater og departementer innen HMS-tilsyn, er et godt eksempel på hvordan IKT-sikkerhetstilsyn kan koordineres.

NSM har en sentral rolle som Justis- og beredskapsdepartementets fagmiljø innenfor IKT-sikkerhet på sivil side. De understøtter også Forsvarsdepartementet i deres ansvar på IKT-sikkerhetsområdet i forsvarssektoren. Utvalget mener at Justis- og beredskapsdepartementet og Forsvarsdepartementet må gjennomgå modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes.

Kapittel 2
Mandat, sammensetning og arbeidsmåte

Mandatet for utvalgets arbeid fremgår av dette kapittelet, sammen med utvalgets mandatsforståelse. Det gis en beskrivelse av utvalgssammensetningen og hvordan det har arbeidet. Til slutt gis en kort beskrivelse av strukturen og innholdet i utredningen.

2.1 Mandat

Digitalisering er en avgjørende faktor for økonomisk vekst og sysselsetting. Den driver innovasjon, og bidrar til effektivisering av næringslivet og offentlig sektor. Digitalisering har ført til nye forretningsmodeller og nye næringsveier, samtidig som gamle, analoge løsninger fases ut. Den økte digitaliseringen av samfunnet har samtidig medført at samfunnets risikobilde har endret seg. Ingen virksomheter, sektorer eller nasjoner kan i dag kontrollere sin digitale sårbarhet alene.

Behovet for forsvarlig IKT-sikkerhet i samfunnet har økt i takt med digitaliseringen. Et viktig aspekt er befolkningens trygghet, som inkluderer både kriminalitetsbekjempelse og beskyttelse av personvernet. Et annet aspekt er det teknologiske, der spesielt funksjonaliteten til samfunnskritiske infrastrukturer og tjenester står i fokus. Et tredje aspekt er at forsvarlig IKT-sikkerhet generelt i samfunnet vil bidra til et mer robust samfunn og dermed ha positive virkninger for nasjonal sikkerhet. Et fjerde aspekt er digitaliseringens betydning for økonomisk vekst og utvikling. For å høste gevinster av digitaliseringen er det viktig at virksomheter, offentlig forvaltning, og samfunnet som helhet har tillit til at de digitale tjenestene fungerer som forutsatt, er tilgjengelig når de trengs der de trengs og har et forsvarlig sikkerhetsnivå.

I NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* ble våre digitale sårbarheter kartlagt. Som ledd i oppfølgingen av rapporten, mener regjeringen det er behov for å utrede rettslig regulering på IKT-sikkerhetsområdet og organisering av tverrsektorielt ansvar. Det vises også til Meld. St. 10 (2016–2017) om samfunnssikkerhet og Meld. St. 38 (2016–2017) om IKT-sikkerhet for ytterligere beskrivelser av utfordringer og regjeringens politikk på IKT-sikkerhetsområdet.

Problemstilling 1 – er dagens regulering hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet?

Norske virksomheter må forholde seg til flere ulike regelverk innenfor IKT-sikkerhet. Regelverkene har til dels ulike formål, og benytter ofte ulike begrep og metoder. Utvalget skal:

- kartlegge relevant sektorspesifikt og tverrsektorielt regelverk om IKT-sikkerhet
- vurdere hvorvidt det eksisterende regelverket er hensiktsmessig innrettet, og om dette ivaretar de nye digitale samfunnsutfordringene
- vurdere om det er behov for harmonisering av eksisterende regelverk
- vurdere om det er behov for tverrsektoriell IKT-sikkerhetslovgivning utover det som følger av gjeldende rett

Problemstilling 2 – har vi en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet?

Digitaliseringen har medført større grad av avhengighet og sammenknytning mellom offentlig og privat, sivilt og militært og mellom ulike samfunnssektorer. Trussel- og sårbarhetsbildet endrer seg raskt samtidig som vi får et stadig mer komplekst samfunn. Dette skaper flere utfordringer for myndighetene, blant annet når det gjelder kompetanse og ressurser. Utvalget skal:

- vurdere om ansvar, roller og oppgaver er hensiktsmessig fordelt og organisert mellom etater med tverrsektorielt ansvar på IKT-sikkerhetsområdet
- vurdere hvordan det best kan legges til rette for samspill og samarbeid mellom etater med tverrsektorielt ansvar og relevante sektormyndigheter

- se på muligheter for koordinering, samarbeid og synergieffekter mellom offentlig og privat sektor slik at nasjonal IKT-sikkerhet ivaretas og styrkes
- med utgangspunkt i at Norge skal gjennomføre NIS-direktivet, vurdere en hensiktsmessig fordeling av de oppgaver som følger av direktivet

Utvalget skal ikke se på organiseringen på departementsnivå, men kan komme med forslag om fag- og ansvarsområder som bør sees i sammenheng også på dette nivået.

Problemstilling 3 – hvilke regulatoriske og organisatoriske grep bør gjøres for å styrke nasjonal IKT-sikkerhet?

Hvis utvalget konkluderer med at det er behov for endringer for problemstilling 1 eller 2, skal utvalget foreslå konkrete rettslige og organisatoriske tiltak.

Utvalget står fritt til å foreslå rettslige og organisatoriske tiltak som kan forbedre arbeidet med og styrke nasjonal IKT-sikkerhet. Forslagene kan innebære mindre endringer i oppgaveporteføljer og harmonisering av eksisterende regelverk, sammenslåing av etater, opprettelse av nye etater og utarbeidelse av nytt regelverk. Utvalget må vurdere hvilke virkemidler som vil få best effekt.

Generelt om utvalgets arbeid

Utvalget skal innhente innspill fra, og ha dialog med, berørte aktører både i privat og offentlig sektor og andre med interesse for arbeidet. Utvalget skal i sitt arbeid se til andre sammenlignbare land for hvordan nasjonal IKT-sikkerhet ivaretas gjennom rettslig regulering og fordeling av tverrsektorielt ansvar mellom myndigheter på etatsnivå.

Det skal etableres en referansegruppe med deltakelse fra Justis- og beredskapsdepartementet, Forsvarsdepartementet, Kommunal- og moderniseringsdepartementet, Samferdselsdepartementet, Nærings- og fiskeridepartementet og Statsministerens kontor.

Utredningen skal være avgrenset mot bestemmelser, organisering og myndighet som følger av sikkerhetsloven og forslag til ny sikkerhetslov (Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet).

Utvalget må se hen til EUs NIS-direktiv og Norges arbeid med gjennomføring av direktivet. Utvalget skal legge til grunn at Norge kommer til å gjennomføre direktivet slik det er utformet. Det innebærer at alle forpliktelser som følger av direktivet skal gjelde for Norge. Justis- og beredskapsdepartementet skal orientere utvalget om utviklingen i arbeidet med gjennomføring av direktivet i Norge. Utvalget må også se hen til gjeldende personvernregelverk, samt EUs nye regelverk om personvern (GDPR), inkludert Norges arbeid med gjennomføring av dette.

Utvalget skal utforme eventuelle lovforslag i samsvar med anbefalingene fra Justis- og beredskapsdepartementet i veilederen «Lovteknikk og lovforberedelse». Utvalget skal fremme forslag til endringer i andre lover og forskrifter som er en følge av utvalgets øvrige forslag. Det må vurderes hva som bør reguleres i lov og hva som eventuelt bør reguleres i forskrift eller retningslinjer.

Utredningen skal gjennomføres i samsvar med kravene i utredningsinstruksen, fastsatt ved kongelig resolusjon 19. februar 2016.

Dersom det er behov for avklaringer av eller å gjøre mindre endringer i mandatet så skal utvalget ta dette opp med Justis- og beredskapsdepartementet som kan beslutte disse.

Utvalget skal levere sin utredning i form av en NOU innen 1. desember 2018.

2.2 Utvalgets mandatforståelse

Det er utarbeidet et omfattende kunnskapsgrunnlag på IKT-sikkerhetsområdet de siste årene, blant annet knyttet til digitale sårbarheter og hvilke trusler vi står overfor. Utvalget har tatt utgangspunkt i dette kunnskapsgrunnlaget i sitt arbeid. I tillegg har utvalget innhentet egne data spesielt knyttet til organisering og regulering. Se punkt 2.3 om utvalgets arbeid.

2.2.1 Begrepet IKT-sikkerhet

Begrepet IKT-sikkerhet har ikke en entydig definisjon. Det har grenseflater mot, eller oppfattes som synonymt med, informasjonssikkerhet, cybersikkerhet og digital sikkerhet. Innholdet i disse varierer og glir i noen grad over i hverandre. I noen dokumenter benyttes begrepene helt eller delvis synonymt, i andre tillegges de ulikt innhold. Innholdet i begrepet IKT-sikkerhet har endret seg noe over tid. Tradisjonelt har beskyttelse av nettverk og systemer vært vektlagt. I dag omfatter begrepet i større grad informasjonen som behandles i systemene og nettverkene samt tjenestene som systemene leverer.

IKT-sikkerhet forstås i denne utredningen som beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av

systemene, eller informasjon som behandles i systemene. Sikkerhetsmålene for IKT-sikkerhet er

- tilgjengelighet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene er tilgjengelig der og når det trengs for brukerne
- integritet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene ikke endres utilsiktet eller uautorisert
- konfidensialitet, dvs. at IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene kun er tilgjengelige for dem som rettmessig skal ha tilgang

Den enkelte virksomhet vil vekte sikkerhetsmålene ulikt ut fra hvilket formål den har eller skal understøtte, og hvilke krav og hvilket risikobilde den må forholde seg til. Basert på disse målene og vektingen av dem vil beskyttelsen omfatte teknologiske, menneskelige og organisatoriske barrierer, som skal motvirke uønskede digitale hendelser, evne til å oppdage slike hendelser og påfølgende reaksjon for å gjenopprette en sikker tilstand for IKT-systemene.

2.2.2 Forsvarlig nasjonal IKT-sikkerhet

Forsvarlig nasjonal IKT-sikkerhet er en overordnet målsetting i mandatet. Utvalget legger til grunn at bruken av ordet *nasjonal* innebærer IKT-sikkerhet som har betydning for samfunnet som helhet.

Med ordet *forsvarlig* forstår utvalget at det skal være et minimumsnivå på sikkerheten. Hva som må til for å oppnå et minimumsnivå, er imidlertid ikke entydig. Utvalget legger til grunn at forsvarlig IKT-sikkerhet kommer godt til uttrykk i NSMs grunnprinsipper for IKT-sikkerhet.[1] Disse bygger på anerkjente standarder og rammeverk i Norge og internasjonalt, og beskriver hva en virksomhet bør gjøre for å sikre sine IKT-systemer. En virksomhet som etterlever disse prinsippene, vil ha forsvarlig IKT-sikkerhet. Hovedpunktene i prinsippene er:[2]

1. Identifisere og kartlegge – gjør risikovurdering
2. Beskytte – sikre verdiene dine
3. Opprettholde og oppdage – vær bevisst
4. Håndtere og gjenopprette – lær av utfordringene dine

Hvert grunnprinsipp har underliggende teknologiske og organisatoriske sikringstiltak som beskriver hva som bør gjøres.

2.2.3 Regulering

Første del av mandatet omfatter å vurdere om dagens regulering er hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet.

Utgangspunktet for utvalget er at en regulering anses å stille krav om IKT-sikkerhet hvis den inneholder bestemmelser om beskyttelse av IKT-systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene.

Med begrepet *tverrsektorielt regelverk* forstås regelverk som stiller krav til offentlige og/eller private virksomheter i to eller flere samfunnssektorer. Utvalget har lagt til grunn at begrepet *regelverk* omfatter lov, forskrift og instrukser, mens begrepet *regulering* også omfatter *soft law* (standarder, bransjepraksis og veiledere). Eksempler her er NSMs grunnprinsipper, Difis og Datatilsynets veiledere om informasjonssikkerhet, og Normen i helsesektoren.[3]

2.2.4 Organisering

Andre del av mandatet innebærer å vurdere om Norge har en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet.

Utvalget legger til grunn at etater med tverrsektorielt ansvar har oppgaver som berører mer enn én statsråds sektoransvar, og har særlig vurdert følgende etater med tverrsektorielt ansvar på IKT-sikkerhetsområdet:

- Nasjonal sikkerhetsmyndighet (NSM)
- Direktoratet for samfunnssikkerhet og beredskap (DSB)
- Direktoratet for forvaltning og IKT (Difi)
- Nasjonal kommunikasjonsmyndighet (Nkom)
- Datatilsynet

NSM, DSB og Difi er de som tydeligst har tverrsektorielt ansvar.

Nkom er i utgangspunktet en sektormyndighet, men det elektroniske kommunikasjonsnettet (ekomnett) er en integrert del av den nasjonale

[1] Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for IKT-sikkerhet*.

[2] Hovedpunktene i grunnprinsippene samsvarer med hovedpunktene i veiledningen til NIS-direktivet som det britiske cybersikkerhetssenteret har utarbeidet, National Cyber Security Center (2018) *NIS Guidance Collection*.

[3] Normen i helsesektoren er et omforent sett av krav til informasjonssikkerhet basert på regelverket.

IKT-infrastrukturen. For de fleste virksomheter er ekomnett og -tjenester også en integrert del av egne IKT-systemer. I et slikt perspektiv er Nkoms ansvarsområde tverrsektorielt, noe som også kommer til uttrykk i det utstrakte samarbeidet etaten har på sikkerhetsområdet med blant andre NSM og DSB.

Datatilsynets oppgaver og kompetansefelt er tverrsektorielt i og med at personvernlovgivningen er allmenn og griper inn i alle sektorer. Datatilsynet skiller seg likevel fra de andre ved at det er et mer uavhengig organ som ikke instrueres av et departement. I vår tid er personvern uløselig knyttet til IKT-sikkerhet, og Datatilsynet er derfor en sentral aktør på dette området.

2.2.5 Øvrige avgrensninger

Det følger av mandatet at utredningen er avgrenset mot eksisterende sikkerhetslov og forslaget til ny sikkerhetslov. Med det mener utvalget at det ikke skal foreslås endringer i denne loven. Grensesnitt mellom sikkerhetsloven og regelverk på IKT-sikkerhetsområdet utenfor sikkerhetsloven er imidlertid beskrevet.

Utvalget har ikke vurdert organisering i politietaten eller Forsvaret. Følgende grensesnitt er i noen grad behandlet:

- mellom sivil sektor og forsvarssektor, herunder den gjensidige avhengigheten
- mellom politiet og relevante aktører når det gjelder IKT-kriminalitet
- mellom kommunalt og statlig nivå knyttet til IKT-sikkerhet

2.3 Sammensetning og utvalgets arbeid

Utvalget har hatt åtte medlemmer:

- leder: skattedirektør Hans Christian Holte, Oslo
- direktør for cybersikkerhet Terje Wold, Tromsø
- administrerende direktør Håkon Grimstad, Trondheim
- Head of Cyber Security Advisory Lillian Røstad, Nesodden
- direktør internett og nye medier Torgeir A. Waterhouse, Oslo
- forskningsleder Marie Moe, Trondheim
- professor Lee A. Bygrave, Oslo
- lagdommer Therese Steen, Oslo

Utvalget har vært støttet av et sekretariat. Sekretariatslederfunksjonen har vært delt mellom Roger Kolbotn og Sveinung Torgersen fra Justis- og beredskapsdepartementet. I tillegg har sekretariatet bestått av Christian Frederik Mathiessen og Ola Hermansen fra Justis- og beredskapsdepartementet, Anniken Grønli Foss fra Difi, Harald Fardal fra DSB, og Klaus Søreide og Anders Bjønnes fra NSM. Sekretariatsmedlemmene har hatt ulike prosentstillinger.

Utvalget har avholdt 13 møter fra oktober 2017 til november 2018. Enkelte møter har hatt to dagers varighet. I samme periode har det vært gjennomført to møter med referansegruppen, der utvalgsleder og sekretariatsleder har deltatt.

Utvalgets arbeid er basert på ulike metoder og datagrunnlag. Det har vært gjennomført samtaler med en rekke virksomheter der formålet har vært å få belyst de største utfordringene og de viktigste tiltakene knyttet til organisering og regulering av nasjonal IKT-sikkerhet. I tillegg har enkelte fagpersoner og forskere holdt innlegg om ulike temaer på området. Hos Felles cyberkoordineringssenter fikk utvalget og sekretariatet en oppdatert og sikkerhetsgradert vurdering fra Etterretningstjenesten, PST, NSM og Kripos om de viktigste truslene og sårbarhetene vi som samfunn står overfor når det gjelder IKT-sikkerhet.

Representanter fra sekretariatet har deltatt på utenlandsreiser til Storbritannia, Sverige og Danmark. I tillegg har sekretariatet fått relevante reiserapporter fra Estland og Nederland. Hensikten med utlandsbesøkene har vært å få bedre kjennskap til hvordan andre land arbeider med nasjonal IKT-sikkerhet. Utover dette har informasjon om andre lands organisering og regulering blitt skaffet til veie gjennom de respektive landenes offisielle nettsider og strategidokumenter.

Sekretariatet hadde innledningsvis i arbeidet egne møter med Difi, DSB, NSM, Datatilsynet og Nkom. Hensikten var å møte saksbehandlere og fagpersoner i virksomhetene som jobber med tverrsektorielle oppgaver innen IKT-sikkerhet, og få høre om deres oppgaver og syn på nasjonale utfordringer. I tillegg ønsket sekretariatet å gjennomføre samtalene som en forundersøkelse, slik at den øvrige informasjonsinnhentingen ble mer spisset.

Utvalget ba om skriftlige innspill fra 186 virksomheter i offentlig og privat sektor. Virksomhetene ble identifisert gjennom en interessentanalyse, og de representerer departementer, direktorater og statlige etater, ulike virksomheter i det private næringslivet, fagforeninger, interesseorganisasjoner, utvalgte kommuner og fylkeskommu-

ner og relevante ikke-statlige organisasjoner. Det var åpne spørsmål uten svaralternativer, og respondentene ble bedt om å begrunne svarene. Spørsmålene var særlig knyttet til utfordringer med dagens regulering og myndighetenes organisering av arbeidet med nasjonal IKT-sikkerhet, og hvilke tiltak som kan iverksettes for å styrke IKT-sikkerheten i samfunnet. Undersøkelsen ble utført i perioden fra januar til mars 2018, og det kom svar fra ca. 90 virksomheter.

Det er noen utfordringer med å behandle data fra et spørreskjema med åpne spørsmål. Det kan være krevende å formulere spørsmål som er tilstrekkelig åpne og nøytrale, og det kan være vanskelig å svare tilfredsstillende på komplekse spørsmål i en skriftlig tilbakemelding. Kvaliteten på svarene som utvalget fikk varierte også noe. Spørsmålene ble sendt til virksomhetene, og det kan være litt tilfeldig hvem som har svart. Enkelte ganger har det vært sikkerhetslederen, andre ganger IT-ansvarlig, juridisk direktør eller andre. Utvalget kan ikke se bort fra målefeil, avhengig av hvem som har svart. Det kan også tenkes at utvalget i enkelte tilfeller ville fått et annet svar hvis en annen person i samme virksomheten hadde svart på samme spørsmål. Dette kan svekke reliabiliteten noe. På noen spørsmål kan det se ut som manglende kompetanse og kunnskap preger svarene. Det er allikevel ikke grunn til å tro at undersøkelsen har systematiske målefeil, og samlet sett gir svarene et rimelig bilde av hvordan sentrale virksomheter ser på utfordringer og mulige tiltak.

Utvalget har gjennomgått eksisterende lover, forskrifter og instrukser basert på tekstsøk i Lovdata. Ved å bruke ulike søkeord har utvalget kartlagt og gjennomgått relevante lover, forskrifter og instrukser. Utvalget har vurdert relevansen av disse opp mot eksisterende litteratur på området samt tilbakemeldingene om relevant regelverk fra virksomheter som har svart på utvalgets spørreskjema.

Utvalget arrangerte en workshop blant Norsk informasjonssikkerhetsforums (ISF) medlemmer. På møtet deltok 75 personer fra 55 virksomheter, i hovedsak fra det private. Deltakerne var personer som har særlig interesse av eller kunnskap om IKT-sikkerhet i sine virksomheter, og det var relevant for utvalget å få informasjon om deres syn på nasjonal IKT-sikkerhet. Deltakerne ble bedt om å diskutere de største utfordringene med dagens organisering og regulering av IKT-sikkerhet og relevante tiltak.

Som en del av utredningen har Oslo Economics gjennomført en samfunnsøkonomisk analyse med grunnlag i utvalgets anbefalinger (se digitalt vedlegg). Analysen ble utført parallelt med at utvalget utarbeidet sine anbefalinger. Teknologirådet har i tillegg bidratt til teksten om teknologitrender og sikkerhetsutfordringer i kapittel 4.

I tillegg har utvalget og sekretariatet gjennomført dokumentstudier av evalueringer og forskningsrapporter, stortingsdokumenter, NOU-er, tildelings- og iverksettingsbrev, årsrapporter og annen relevant litteratur. Se vedlegg 4 for nærmere beskrivelse av datagrunnlaget.

2.4 Struktur og innhold

Utredningen er delt inn i seks deler. I del I inngår sammendraget, mandatet og utvalgets mandatforståelse. I del II beskrives noen grunnleggende utviklingstrekk i samfunnet som har betydning for organisering og regulering innenfor IKT-sikkerhet. Utfordringsbildet knyttet til organisering og regulering innenfor IKT-sikkerhet er drøftet i del III etterfulgt av utvalgets tiltak og anbefalinger i del IV. Økonomiske og administrative konsekvenser knyttet til utvalgets anbefalinger beskrives i del V. Til slutt følger utredningens vedlegg.

Del II
Situasjonsbeskrivelse

Kapittel 3
IKT-risikobildet

Dette kapitlet beskriver samfunnets verdier, sårbarheter knyttet til verdiene og trusler som kan ramme verdiene.

3.1 Verdier

Utvalget legger til grunn den samme forståelsen av hva som er grunnleggende samfunnsverdier, som i NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*:[1]

> Våre grunnleggende samfunnsverdier kommer til utrykk både i nasjonal og i internasjonal rett. Grunnloven og rettssystemet vårt bygger på rettsstatsprinsipper som legalitetsprinsippet, rettssikkerhetshensyn, demokratihensyn og menneskerettigheter, herunder personvern, ytringsfrihet og forsamlingsfrihet.

Disse verdiene gir uttrykk for både hva som er enkeltindividets rettigheter og friheter, og hva som skal til for at de kan realiseres. Verdiene er også «fundamentet for reguleringen av det innbyrdes forholdet mellom statsmaktene ved maktfordelingsprinsippet og forholdet mellom staten og befolkningen».[2]

Arbeidet med samfunnssikkerhet er en viktig brikke i ivaretakelsen av de grunnleggende samfunnsverdiene. Samfunnssikkerhet handler om[3]

> [s]amfunnets evne til å verne seg mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger.

Det overordnede målet med samfunnssikkerheten er altså å ivareta grunnleggende samfunnsverdier. Samlet sett er det en rekke funksjoner i samfunnet som er kritiske for å ivareta disse verdiene.[4] Disse funksjonene ivaretas av private og offentlige virksomheter. Svikt i eller bortfall av leveransene til slike virksomheter kan få konsekvenser utover deres egen virksomhet, og med betydelige negative følger for samfunnet. Det er derfor viktig at samfunnskritiske virksomheter sikres godt. Fordi samfunnssikkerhet også er et myndighetsansvar, har myndighetene behov for å ha en viss kontroll og styring med sikkerheten i disse virksomhetene.

Verdiene som trekkes frem i mandatet, må ses i denne konteksten. Der vises det til befolkningens trygghet, samfunnskritisk infrastruktur, nasjonal sikkerhet og økonomisk vekst og utvikling. Disse verdiene griper inn i og er avhengige av hverandre, og må beskyttes for å opprettholde et trygt, fritt og velfungerende samfunn.

3.2 Sårbarheter

Digitalisering er et globalt fenomen. Den digitale utviklingen er avgjørende for verdiskaping og vekst, men fører også til nye sårbarheter og dilemmaer. Stadig flere systemer og enheter kobles sammen, slik at den samfunnsmessige sårbarheten utvides. Dette gjør systemer, infrastrukturer og verdikjeder utsatt for hendelser som kan få negative konsekvenser for enkeltindivider, for den enkelte virksomhet og for samfunnet som helhet.[5]

Utviklingen der «alt henger sammen med alt», utgjør en strukturell sårbarhet i samfunnet på flere måter. De fleste virksomheter er avhengige av digitale tjenester som er levert av andre, for egen produksjon eller aktivitet. Sårbarheter og feil

---

1 NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*, kapittel 3.

2 Ibid.

3 Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*

4 Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner*. Se mer informasjon i boks 15.1.

5 Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018.*

forplanter seg raskt mellom leddene i verdikjeden og kan få uante konsekvenser. Tjenester, systemer, virksomheter og infrastrukturer arver sårbarheter fra hverandre.

Lysne-utvalget skrev i sin utredning at på grunn av de digitale verdikjedene er det ingen virksomheter som har full oversikt over egne sårbarheter.[6] Verdikjedene er sårbare for alle typer hendelser, både de som skyldes bevisste handlinger, og de som skyldes feil eller ulykker. For en enkeltperson kan en feil i ett ledd i verdikjeden føre til bortfall av en viktig digital tjeneste, for eksempel nettbanken. Gjensidige avhengigheter og sårbarheter i digitale verdikjeder kan i ytterste konsekvens påvirke samfunns- og statssikkerheten.

Økende globalisering innebærer sårbarhet overfor uønskede hendelser som har sin opprinnelse utenfor landegrensene og dermed utenfor norsk kontroll. Ekomsektoren er et godt eksempel på dette. I Lysne-utvalgets rapport fremgår det at det er en av de mest kritiske sektorene i et digitalisert samfunn.[7] Nkom skriver i sin årlige risikovurdering at forringelse av nasjonal kontroll over kritisk tjenesteproduksjon og et uforutsigbart sikkerhetspolitisk bilde utgjør en økende risiko innen elektronisk kommunikasjon.[8]

Produksjon av norske elektroniske kommunikasjonsløsninger avhenger i stor grad av fysisk infrastruktur og innsatsfaktorer fra leverandører utenfor Norge. Tilgang til profesjonelle og mer effektive tjenester som gir større forutsigbarhet, stabilitet og bedre finansieringsmodeller, gjør at flere IKT-funksjoner settes ut til en tredjepart, også til lavkostland. Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, i tillegg til lavere og mer forutsigbare kostnader. Samtidig kan det føre til økt risiko på grunn av redusert kontroll over stadig mer komplekse verdikjeder.

Stadig flere enheter, prosesser og tjenester kobles til internett. Internett har utviklet seg til å bli verdens kanskje viktigste infrastruktur og utgjør ryggraden i den globale flyten av varer, tjenester og informasjon. Fremveksten av tingenes internett og andre teknologitrender kan skape nye sikkerhetsutfordringer. Noen utvalgte trender behandles nærmere i kapittel 4.

Internasjonal cyberpolitikk er fremdeles i støpeskjeen. Det finnes ingen overordnet aktør som styrer infrastrukturen globalt. Det er få mellomstatlige arenaer for å utvikle kjøreregler for statlig oppførsel i det digitale rommet og få internasjonale konvensjoner som spesifikt regulerer det.

Utviklingen av internett og digitale produkter og tjenester foregår i all hovedsak gjennom private selskaper og i forsknings- og utviklingsmiljøer. Viktige beslutninger om utvikling og sikkerhet i det digitale rommet og i digitale produkter og tjenester blir i stor grad fattet av kommersielle aktører med begrenset påvirkning fra myndigheter. Disse aktørene befinner seg i all hovedsak utenfor Norges grenser.

Utformingen av normer, konvensjoner og reguleringer som får direkte betydning for Norge, foregår også i stor grad internasjonalt. Mange store IKT-sikkerhetsutfordringer er grenseoverskridende, og de kan best løses i fellesskap. EUs arbeid med digital sikkerhet påvirker for eksempel direkte Norges evne til å sikre nasjonale nettverk. NIS-direktivet som skal bidra til et felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU, er et godt eksempel på dette, i tillegg til personvernforordningen (General Data Protection Regulation (GDPR)) og Cybersecurity Act.[9] NATOs krav om at medlemslandene skal ha robuste sivile elektroniske kommunikasjonsnett, er et annet eksempel på en internasjonal forpliktelse som Norge må forholde seg til.[10]

Tilgang til IKT-sikkerhetskompetanse fremstår som en av de største utfordringene på IKT-sikkerhetsområdet. En rekke dokumenter peker på dette som en økende utfordring.[11] I 2030 vil det ifølge estimatene være et underskudd på 4100 personer med slik kompetanse i det norske samfunnet.[12] På globalt nivå er det estimert at det i år 2022 vil være et underskudd på 1 800 000 personer med IKT-sikkerhetskompetanse.[13] Manglende kompetanse er en utfordring ikke bare for enkeltindividet, men også for virksomheter og samfunnet. Kompetansesituasjonen påvirker

6 NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.*

7 Ibid.

8 Nasjonal kommunikasjonsmyndighet (2017) *EkomROS 2017.*

9 NIS-direktivet og Cybersecurity Act er omtalt i vedlegg 2.

10 NATO Commitment to enhance resilience, erklæring fra NATO-toppmøtet 8.-9. juli 2016.

11 Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*, Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*, NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* NIFU (2017). *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud.* I tillegg utvalgets informasjonsinnhenting.

12 NIFU (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud.*

13 Frost, & Sullivan. (2017) *Global Information Security Workforce Study.*

utviklingen av IKT-systemer og programvare, driften av systemene og hvordan lover og forskrifter, råd, veiledere, rutiner og styringssystemer er uformet og fulgt opp. IKT-personell må ha kompetanse til å implementere tilstrekkelig sikkerhet, og det er behov for spesialisert sikkerhetskompetanse, for eksempel innenfor kryptografi. God evne til å avdekke og håndtere uønskede digitale hendelser krever også spesialistkompetanse på flere områder. NSM vurderer det økende gapet mellom tilgjengelighet og behov for sikkerhetskompetanse som en nasjonal sårbarhet.[14]

Sikkerhetsarbeidet i en virksomhet er et lederansvar. Erfaringer fra tilsyn gjennomført av NSM viser imidlertid at sikkerhetsarbeidet fortsatt i for liten grad inngår som et naturlig ledd i den totale ledelsen av virksomheten. Dette får konsekvenser i form av manglende kunnskap og bevissthet om risiko og egne tiltak, svak organisering, manglende prioriteringer og utilfredsstillende ressurstildeling. Svakheter som er avdekket gjennom tilsyn, lar seg ofte tilbakeføre til ledelsesutfordringer. Det registreres imidlertid økt etterspørsel etter informasjon, råd og veiledning fra ledernivåer.[15]

3.3 Trusler

Etterretningstjenesten, NSM og PST utgir årlige nasjonale vurderinger som viser hvilke trusler Norge som samfunn står overfor.[16] I tillegg bidrar forskningsinstitusjoner og offentlige og private virksomheter til å synliggjøre sikkerhetsutfordringer som både enkeltpersoner og samfunnet for øvrig må forholde seg til. En stor andel av uønskede hendelser er utilsiktet. Feil og utfall i IKT-systemer og -tjenester skjer på grunn av menneskelige feil, programvarefeil, utstyrsfeil, naturhendelser, eller en kombinasjon av disse. Nkom viser blant annet til at Norge i 2016 hadde tre tilfeller av ekstremvær som forårsaket skader på infrastruktur som ga utfall av kraft og elektronisk kommunikasjon.[17]

Tilsiktede uønskede digitale hendelser er et økende problem. Dette er aktiviteter som kan være krevende å kartlegge, og som i ytterste konsekvens kan utgjøre en alvorlig trussel mot norske interesser og privatpersoner. Målet til angriperne kan være å skade en motpart ved å påvirke, redusere eller ødelegge funksjonaliteten i produksjonssystemer. Det kan også være å stjele privat informasjon fra enkeltpersoner eller skaffe seg informasjon om stats- og forretningshemmeligheter, forskningsresultater eller teknologiske nyvinninger fra kommersielle bedrifter. Man ser også handlinger som retter seg mot grunnleggende verdier og demokratiske funksjoner i samfunnet, for eksempel gjennom desinformasjon og påvirkningskampanjer.

I *Helhetlig IKT-risikobilde* trekker NSM frem at underleverandører og kontraktører i økende grad blir utsatt for målrettede operasjoner.[18] I tillegg er også tilfeldige systemer i tiltakende grad utsatt for kompromittering ved at de kan bli utnyttet for videre nettverksoperasjoner mot andre mål. Dette kan i prinsippet være et hvilket som helst IKT-system, som ikke er et mål i seg selv, men som fungerer som mellomledd mellom en angriper og det egentlige målet.

Når det gjelder hvilke metoder som brukes i dag, slår NSM fast at mange digitale angrep innledes med bruk av ulike varianter av skadevare distribuert via e-post. Innhold og utforming fremstår som relevant og legitimt for mottakeren, men lenker og vedlegg inneholder skadelig kode som aktiveres ved at man klikker på lenken eller åpner vedlegget. NSM trekker også frem krypteringsvirus og innsidere som særlig aktuelle trusler.

---

14 Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018,* s. 10.

15 Ibid.

16 Etterretningstjenesten (2018) *Fokus 2018*, Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018* og Politiets sikkerhetstjeneste (2018) *Trusselvurdering 2018.*

17 Nasjonal kommunikasjonsmyndighet (2017) *EkomROS 2017.*

18 Nasjonal sikkerhetsmyndighet (2016) *Helhetlig IKT-risikobilde 2016.*

Kapittel 4
Teknologitrender og sikkerhetsutfordringer

Teknologien utvikler seg i høyt tempo, og nye produkter, tjenester og tekniske løsninger introduseres fortløpende. Utviklingen innebærer at samfunnet er i endring, og at oppgaver og funksjoner som for få år siden var manuelle og analoge, nå digitaliseres i et raskt tempo.

Teknologiutviklingen bidrar til økt sikkerhet. For eksempel kan systemer for førerstøtte og annen ny teknologi i bil redusere risikoen for ulykker og begrense skadeomfanget. Utviklingen introduserer også nye sårbarheter. Det gjør det krevende å vite hvor sårbarhetene er, og om verdiene er tilstrekkelig sikret mot uønskede digitale hendelser.

I dette kapittelet trekkes det frem noen eksempler på teknologitrender som kan føre til nye sikkerhetsutfordringer for samfunnet. Disse trendene er kunstig intelligens og maskinlæring, tingenes internett og 5G.

4.1 Kunstig intelligens og maskinlæring

Maskinlæring er den mest brukte tilnærmingen innen kunstig intelligens.[1] Teknikkene har hatt betydelige fremskritt de siste årene og er i alminnelig bruk på flere områder, som internettsøk, navigering, oversettelse, talekommandoer, filtrering av epost og virtuelle assistenter (for eksempel chatbots). Bakgrunnen for denne utviklingen er tilgang til store mengder data, kraftige og rimelige regneressurser, fremskritt i algoritmer og utviklingen av nevrale nett.[2]

Maskinlæring kan brukes med ondsinnede hensikter. Smarte algoritmer kan skaleres raskt og rimelig og dermed spres bredt. Teknologien har derfor potensial for stor utbredelse. Enkelte oppgaver kan maskiner gjøre mer effektivt og bedre enn mennesker, men det blir vanskelig å ha god oversikt over oppgaver som blir utført av autonome systemer. Dette kan svekke tilliten til oppgaveløsningen. En algoritme kan misbrukes på ulike måter som et ledd i et digitalt angrep.

Ondsinnet bruk av kunstig intelligens kan true innbyggere, organisasjoner og stater på spesielt tre områder:[3]

For det første kan kunstig intelligens automatisere oppgaver knyttet til digitale angrep. Tidligere arbeidsintensive angrep som utsendelse av epost kan gjøres både mer målrettet og bredere. Angrep kan også utnytte svakheter i systemer for kunstig intelligens, som å bruke bilder som bevisst lurer systemet med en slags optisk illusjon.[4]

For det andre kan kunstig intelligens automatisere oppgaver knyttet til angrep med droner eller andre fysiske systemer. Autonome systemer utstyrt med våpen krever ikke at mennesker er fysisk til stede. Kunstig intelligens muliggjør også nye typer angrep, for eksempel svermer med tusenvis av mikrodroner.

For det tredje kan kunstig intelligens automatisere oppgaver knyttet til overvåkning (som å analysere masseinnsamlede bilder), overtalelse (som å lage psykologisk målrettet propaganda) og bedrageri (som å manipulere videoer). Desinformasjon og falske nyheter kan utarbeides mer troverdig og spres mer persontilpasset, noe som kan forsterke truslene knyttet til både personvern og sosial manipulering.

---

1 Kunstig intelligens er drevet frem av et ønske om å gjøre maskiner i stand til å løse både fysiske og kognitive oppgaver som tidligere var forbeholdt mennesker, og oppgaver som mennesker ikke er i stand til å løse eller utføre.

2 Nevrale nett er i denne sammenheng en datadrevet tilnærming til maskinlæring som er inspirert av strukturen og funksjonen til biologiske nevrale nettverk i hjernen. Nevrale nett kan lære noe vi ikke visste fra før, eller noe som ikke er mulig for mennesker å lære. Denne tilnærmingen driver kunstig intelligens fremover nå. Se mer om nevrale nett i Teknologirådet (2018) *Kunstig intelligens – muligheter, utfordringer og en plan for Norge.*

3 Future of Humanity Institute et al. (2018) *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Februar 2018.

4 OpenAI (2017) *Attacking Machine Learning with Adversarial Examples.*

Etter hvert som kunstig intelligens blir mer avansert og presis, blir også angrepene mer sofistikerte, og dermed også vanskeligere å forsvare seg mot. En annen utfordring med kunstig intelligens-drevne systemer er at de kan være vanskelige å forstå og dermed kontrollere for mennesker. Systemlogikkens manglende transparens og forståelighet kan svekke menneskers evne til å oppdage systemfeil med sikkerhetsmessige konsekvenser.

For IKT-sikkerheten kan derfor kunstig intelligens utgjøre en trussel, men også innebære en mulighet for sterkere forsvar. For eksempel kan maskinlæring brukes for å oppdage og motarbeide avanserte angrep, som å lete etter tegn til unormal nettverkstrafikk som indikerer at en angriper er inne i systemene. Utviklingen innebærer at eventuelle reguleringer både må kunne beskytte mot kunstig intelligens-drevne angrep og tillate tilsvarende forsvar.

4.2 Tingenes internett

Tingenes internett (Internet of Things (IoT)) viser til en utvikling hvor stadig flere gjenstander som vi omgir oss med i hverdagen, blir koblet til internett. Ved hjelp av små innebygde sensorer og datamaskiner blir tingene dermed i stand til å samle inn data og dele dem med andre enheter over digitale nettverk. Alt fra smartklokker og telefoner til strømmålere, biler og avansert fabrikkutstyr registrerer og prosesserer nå helt nye typer data om omgivelsene. Det kan være eierens fysiske aktivitet, husholdningens strømforbruk, bilens kjøremønster eller maskiners produksjonsprosesser.

Drivkreftene bak utviklingen er mindre og billigere sensor- og kommunikasjonsteknologi som kan integreres i tingene. I tillegg er enklere overføring og skylagring av de store datamengdene dette produserer, også en viktig faktor. Dette har åpnet for nye datadrevne forretningsmodeller basert på automatisert analyse av sanntidsdata, optimering og tilbakemelding. Et eksempel er når en smartklokke gir eieren beskjed om at hun bør gå en kort tur for å nå dagens aktivitetsmål. Et annet eksempel er når en bil løpende sender data tilbake til fabrikken, slik at de kan lære og forbedre bilene de lager.

I dag anslås det at det er flere gjenstander koblet til internett enn det er mennesker på jorda.[5] Det er også forventet at veksten vil øke vesentlig i årene som kommer. Mye av denne veksten er knyttet til brede trender, som utviklingen av smarte byer, smarte hjem og digitale helsetjenester. Industri- og næringsliv vil fortsatt være viktige drivere, men tingenes internett er i økende grad på vei inn i privatliv og husholdninger.

Boks 4.1 Tingenes internett

«Ovens are computers that makes things hot; refrigerators are computers that keep things cold. These computers – from home thermostats to chemical plants – are all on-line. The Internet, once a virtual abstraction, can now sense and touch the physical world. Cutting-edge digital attackers can crash your car, your pacemaker and the nation's power grid.»[1]

[1] Schneier, Bruce (2018) *Click Here to Kill Everybody.* New York: W.W. Norton and Company.

Tilkoblede produkter uten tilstrekkelig IKT-sikkerhet kan benyttes i angrep mot samfunnsviktige institusjoner eller funksjoner. Slike angrep kan for eksempel skje ved at noen kobler sammen flere millioner ulike tilkoblede produkter (en mobiltelefon, en smart-TV, et nettkamera, et kjøleskap) og lager et gigantisk nettverk av små datamaskiner som kan brukes til å forstyrre eller sette nettsider og tjenester ut av drift (se boks 4.2).

Tingenes internett bringer risikoen knyttet til usikrede nettverk inn i bedrifter, men også inn i privatliv og husholdninger. Informasjon kan komme på avveie, både gjennom målrettede dataangrep og feil.

Smart teknologi i offentlige rom kan registrere persondata uten at folk vet eller godkjenner det. Personlige produkter, som treningsarmbånd, produserer persondata som kan brukes på måter som eieren ikke er klar over eller kan forvente. Data om brukerens aktivitetsmønster kan havne hos tredjeparter og brukes til markedsføring eller vurdering av forsikringspremier.

Alle tilkoblede enheter kan potensielt hackes, utsettes for datakrasj eller bli utilgjengelige på grunn av nettfeil eller mangel på dekning. Dette kan medføre trusler mot liv og helse. Det har vist seg mulig å overta kontrollen over biler i fart. Den økende bruken av hjemmesensorer og velferdsteknologi, for eksempel i eldreomsorgen, utgjør også en sårbarhetsutfordring.

[5] Gartner (2017) *Gartner Says 8.4 Billion Connected «things» Will be in use in 2017.*

Boks 4.2 Eksempel på botnett som benytter tilkoblede produkter

Mirai er navnet på en skadevare som infiserer en rekke tilkoblede produkter, og som kan bruke disse til å angripe nettsider og nettleverandører. Skadevaren benytter forhåndsdefinerte administrasjonspassord for å få administratortilgang til produktene og dermed ta kontroll over enheten. Mirai-botnettet skal ha bestått av hele 500 000 enheter, blant annet nettkameraer og opptakere. Dette botnettet ble benyttet i 2016 i et stort tjenestenektangrep rettet mot en sentral leverandør av DNS-tjenester. Angrepet fikk konsekvenser for en rekke amerikanske nettjenester, inkludert Twitter, Amazon, Tumblr, Reddit, Spotify, Netflix og flere spillservere. Angrepene fikk ringvirkninger også i Norge.

4.3 5G

Neste generasjons mobilnett kalles 5G.[6] Arbeidet med å standardisere teknologien er i gang, og internasjonal godkjenning forventes i 2020.[7] 5G tilbyr stor dataoverføringshastighet. Særlig innenfor maskin-til-maskin-kommunikasjon får 5G en helt annen kapasitet enn dagens mobilnett har. I tillegg til å gjøre det samme som 4G, bare bedre og raskere, defineres det to typer maskin-til-maskin-kommunikasjon i 5G – massiv og kritisk.

Massiv maskin-til-maskin-kommunikasjon vil tilby stabil dekning for mange enheter samtidig – inntil en million enheter innenfor en kvadratkilometer. Enhetene som kan kobles på, er enkle IoT-enheter som må ha en batterikapasitet på minst ti år. Det betyr at de må være energieffektive, og mulighetene for å implementere avanserte sikkerhetsalgoritmer er små fordi dette er energikrevende. Gitt dagens sikkerhetsprotokoller peker dette seg ut som et område med store sikkerhetsutfordringer.

Kritisk maskin-til-maskin-kommunikasjon er innrettet mot kommunikasjon som krever høy pålitelighet og lav responstid. For eksempel trenger autonome kjøretøyer dette for å operere sikkert. Denne delen av 5G-standarden er også ment å håndtere nødetaters og andre kritiske tjenesters behov.

I 5G er virtualisering av nettverksfunksjoner en viktig bestanddel. Det betyr at slike funksjoner i fremtiden kommer til å kjøre som programvare på standard maskinvare, i motsetning til i dag der hver funksjon har en egen dedikert maskinpark. Følgene av dette er at ekommarkedet i stor grad kommer til å globaliseres, og at få, men store driftssentre verden rundt står for driften av ekominfrastrukturen. Dette vil utfordre måten virksomhetene tenker sikkerhet på, og kreve høy spesialistkompetanse innenfor virtualisering.

Universitetet i Surrey i Storbritannia peker på at mangfoldet av tjenester og applikasjoner i 5G gir sikkerhetsutfordringer.[8] Ulike tjenester og applikasjoner vil ha forskjellig sikkerhetsbehov, og en utfordring blir å dele nettverkene i segmenter som kan kjøres uavhengig av hverandre for å ivareta de ulike behovene.

6 Se nærmere Bentstuen, Ole Ingar; Farsund, Bodil Hvesser; Øverlier, Lasse; Køien, Geir (2017). *Sikkerhetsutfordringer i fremtidens EKOM-tjenester.* FFI-rapport 17/17047.

7 Telenor (2018) *Hva er 5G?*

8 University of Surrey (2017) *5G Whitepaper: 5G Security Overview.*

Kapittel 5
Myndighetenes arbeid med IKT-sikkerhet

En rekke offentlige myndigheter har roller og ansvar innenfor IKT-sikkerhet. Noen av de mest sentrale er omtalt nedenfor. I tillegg har private aktører en viktig rolle knyttet til digitaliseringen av Norge, og gjennom dette et stort ansvar for å ivareta IKT-sikkerhet. Private aktører forvalter i stor utstrekning samfunnets kritiske IKT-infrastruktur, for eksempel ekomnettene og styrings- og kontrollsystemer for en rekke andre viktige funksjoner i samfunnet. Flere private virksomheter arbeider også for å fremme IKT-sikkerhet.[1] I tillegg til de tverrsektorielle etatene og departementenes oppgaver som er beskrevet under, er det en rekke sektormyndigheter som har ansvar for oppgaver innad i sin sektor. Det kan være tilsyn, råd, veiledning og øvelser. Det er også forventet at de skal ha en viss evne til å håndtere hendelser.

5.1 Statens målsettinger med IKT-sikkerheten

En hovedprioritering for myndighetene er å legge til rette for at både offentlige og private virksomheter skal ta i bruk nye digitale løsninger. En forutsetning for en vellykket digitalisering er at det skjer innenfor rammer hvor også IKT-sikkerheten ivaretas. Statens arbeid med IKT-sikkerhet knyttes derfor gjerne opp mot både samfunnssikkerhet og statssikkerhet.[2] Det vil si å beskytte samfunnet mot trusler og sårbarheter som kan ramme liv og helse, samfunnets funksjonalitet, demokrati og rettssikkerhet, økonomiske verdier og nasjonens suverenitet.

I stortingsmeldingen om IKT-sikkerhet fra juni 2017 fremheves det at ingen aktør eller myndighet kan løse IKT-sikkerhetsutfordringene alene.[3] Offentlig–privat, sivilt–militært og internasjonalt samarbeid er avgjørende for å lykkes. I tillegg er de overordnede prinsippene for arbeidet med samfunnssikkerhet – ansvar, nærhet, likhet og samvirke – også førende for IKT-sikkerheten.

Myndighetene legger i stortingsmeldingen vekt på fire områder som er av særlig betydning for nasjonal IKT-sikkerhet:
- forebyggende IKT-sikkerhet
- avdekke og håndtere digitale angrep
- IKT-sikkerhetskompetanse
- kritisk IKT-infrastruktur

Disse fire områdene har vært mer eller mindre uforandret i flere år og er omtalt i stortingsmeldinger, nasjonale strategier og stortingsproposisjoner.[4] Regjeringen jobber med en ny nasjonal strategi med handlingsplan for digital sikkerhet som er ventet i begynnelsen av 2019.

5.2 Sentrale departementer og etater

Norge er organisert i tre forvaltningsnivåer: kommunen, fylkeskommunen og staten. Staten er inndelt i flere departementer som har én eller flere statsråder. Statsråden er ansvarlig for at Stortingets beslutninger blir fulgt og implementert innenfor sin sektor. Ansvaret og oppgavene til departementet kan fordeles til andre enheter. Dette kan for eksempel være statseide selskaper, statsforetak, etater eller stiftelser. Enhetene er ulike når det gjelder hvor tett de kan bli politisk styrt, og hvor stor instruksjonsrett statsråden har over dem.

Begrepet etat brukes som en samlebetegnelse på «[…] et landsdekkende myndighetsorgan

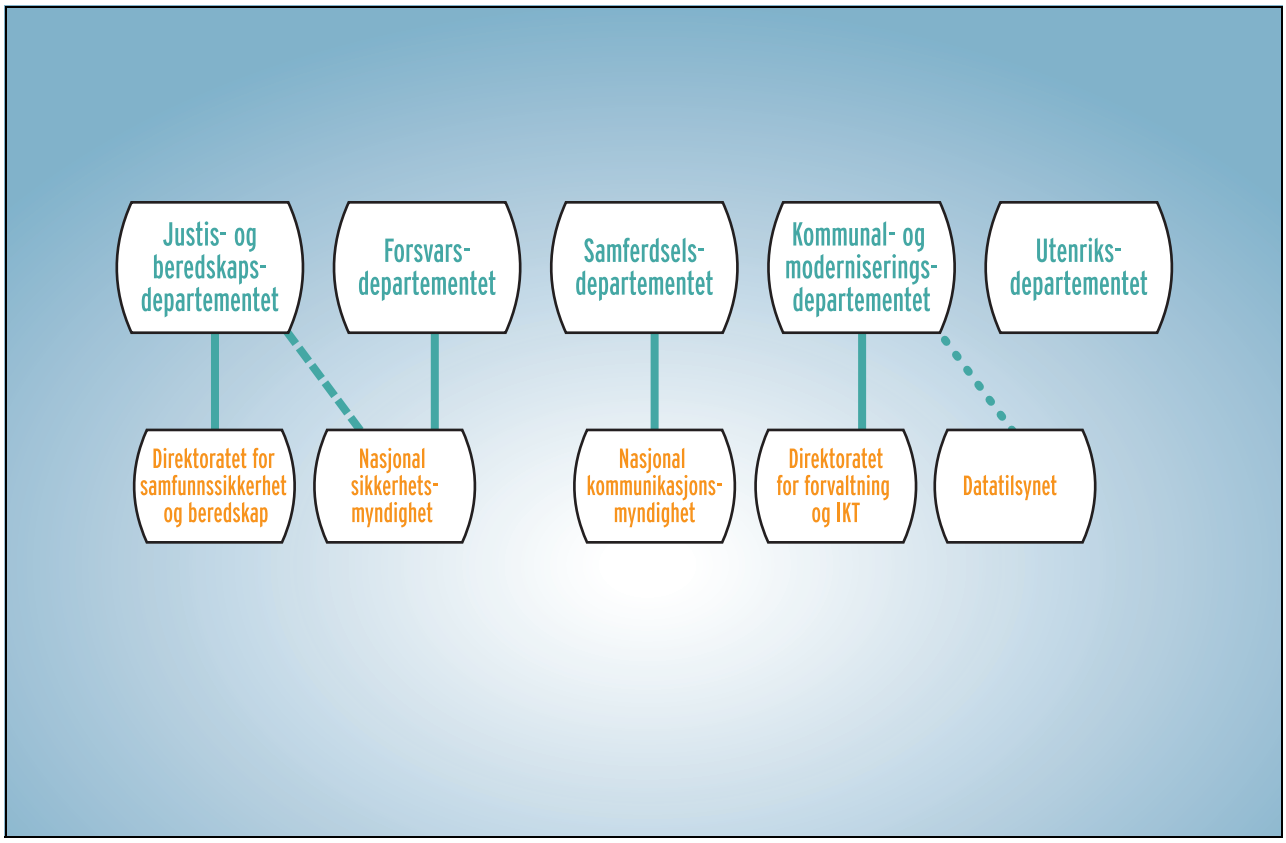
---

1 Se for eksempel NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*. Kap. 8.

2 Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*, Prop. 151 S (2015–2016) *Kampkraft og bærekraft*, Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*.

3 Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar.*

4 Blant annet Fornyings-, administrasjon- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet med handlingsplan*, Meld. St. 27 (2015–2016) *Digital agenda for Norge,* Prop. 151 S (2015–2016) *Kampkraft og bærekraft,* Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*



Figur 5.1 Organisasjonskart over sentrale departementer og etater

underlagt et departement. Oppgaven(e) til etatene er å avlaste departementene når det gjelder faglig arbeid og gjennomføring av tiltak».[5] Noen etater har ansvar for oppgaver som ikke bare berører én statsråds sektoransvar. Dette kan kalles etater med tverrsektorielt ansvar. Disse etatene er i stor grad avhengige av at andre etater og virksomheter bidrar til måloppnåelsen etaten har ansvaret for. Etater med tverrsektorielt ansvar følger vanlige regler for etatsstyring, rapportering og mål- og resultatstyring i staten, men oppgavene de skal løse, griper over flere sektorer.

Justis- og beredskapsdepartementet har samordningsansvaret for IKT-sikkerhet i sivil sektor. Departementet skal utforme regjeringens politikk for IKT-sikkerhet, herunder etablere nasjonale krav og anbefalinger på IKT-sikkerhetsområdet for både offentlige og private virksomheter.

Forsvarsdepartementet har ansvaret for IKT-sikkerhet i forsvarssektoren. Justis- og beredskapsdepartementet skal involvere Forsvarsdepartementet i saker innenfor sivil IKT-sikkerhet som berører forsvarssektoren. De to departementene skal sammen bidra til at sivil–militære utfordringer og behov sees i sammenheng.

Kommunal- og moderniseringsdepartementet har samordningsansvaret for regjeringens IKT-politikk. Departementet har i tillegg et ansvar for å arbeide med IKT-sikkerhet i statsforvaltningen. Digitaliseringsarbeidet i statsforvaltningen og i offentlig sektor som helhet skal følge opp de føringene som følger av den nasjonale IKT-sikkerhetspolitikken. Departementet skal i samråd med Justis- og beredskapsdepartementet legge til rette for at digitaliseringen i offentlig forvaltning og samfunnet for øvrig skjer på en forsvarlig måte.

Samferdselsdepartementet har ansvar for IKT-sikkerheten knyttet til elektroniske kommunikasjonsnett og -tjenester, herunder internett.

Utenriksdepartementet har overordnet ansvar for norsk utenriks- og sikkerhetspolitikk, herunder å koordinere Norges innsats og posisjoner på internasjonale arenaer hvor globale utfordringer i det digitale rommet diskuteres. Justis- og beredskapsdepartementet skal sammen med Utenriksdepartementet bidra til at internasjonalt arbeid på IKT-sikkerhetsområdet blir håndtert godt på tvers av departementsområder i sivil sektor.

[5] Kommunal- og moderniseringsdepartementet (2015). *Hva er statsforvaltningen?*

Organiseringen av tverrsektorielle oppgaver innen IKT-sikkerhet i Norge er fordelt mellom flere etater. Sentrale virksomheter er NSM, Difi, Nkom, DSB og Datatilsynet.

Nasjonal sikkerhetsmyndighet (NSM) er et direktorat for forebyggende sikkerhet. Det er administrativt underlagt Forsvarsdepartementet, men rapporterer med en faglig ansvarslinje til Justis- og beredskapsdepartementet i sivile saker. Direktoratets ansvar og oppgaver følger av «Instruks for sjef NSM», gitt 5. desember 2014 av Forsvarsdepartementet i samråd med Justis- og beredskapsdepartementet, og av iverksettingsbrevet for langtidsplanen for forsvarssektoren.

NSM fyller rollen som nasjonal sikkerhetsmyndighet i henhold til sikkerhetsloven (1998).[6] Dette omfatter blant annet å gi informasjon, råd og veiledning til og føre tilsyn med IKT-sikkerheten i virksomheter underlagt loven, og gjennomføre inntrengningstesting av og godkjenne sikkerhetsgraderte IKT-systemer. Oppgavene blir utvidet som følge av den nye loven om nasjonal sikkerhet.[7] Direktoratet driver også den frivillige sertifiseringsordningen for IKT-sikkerhet i produkter og systemer (SERTIT).

NSM er nasjonalt fagmiljø for IKT-sikkerhet til støtte for Forsvarsdepartementets og Justis- og beredskapsdepartementets ansvar på IKT-sikkerhetsområdet. Som del av dette ansvaret skal NSM blant annet etablere og vedlikeholde et nasjonalt IKT-risikobilde og foreslå tiltak og følge opp med informasjon og rådgivning.

De drifter det nasjonale varslingssystemet for digital infrastruktur (VDI) og koordinerer den nasjonale håndteringen av alvorlige IKT-angrep mot viktige samfunnsfunksjoner (NSM NorCERT).[8] Sjef NSM skal ved behov iverksette nødvendige beredskapsmessige tiltak innenfor gitte fullmakter, herunder i Nasjonalt beredskapssystem.[9] NSM leder arbeidet i Felles cyberkoordineringssenter, hvor også Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos inngår (se punkt 5.4).

NSM fører årlig tilsyn med om lag 50 virksomheter i sivil og militær sektor etter sikkerhetsloven. De fører systemrettet tilsyn understøttet av fagrevisjoner. Tilsynet blir gjennomført med gjennomgang av dokumentasjon, intervjuer og stedlige kontroller.

I iverksettingsbrevet for 2017 fremgår det at NSM skal samarbeide med andre aktører, blant annet gjennom å etablere en arena for erfaringsoverføring knyttet til råd og veiledning sammen med Difi. Videre skal NSM sammen med DSB og relevante sektortilsyn utrede og etablere en arena for informasjonsutveksling og kompetanseoverføring for de ulike sektorenes tilsynsmyndigheter. NSMs iverksettingsbrev har en annen form og struktur enn tildelingsbrevene til de øvrige tverrsektorielle etatene.

I mars 2018 uttalte Forsvarsdepartementet at NSM NorCERTs funksjon og rolle skal tydeliggjøres, og at navnet skal endres til «Nasjonalt cybersikkerhetssenter». Dette for å styrke samarbeidet mellom offentlige og private nasjonale aktører som arbeider med IKT-sikkerhet. NSM har senere utarbeidet et konseptnotat hvor senterets formål utvides til også å omfatte rådgivning og tilgjengeliggjøring av tekniske tjenester. Senteret er nærmere omtalt i kapittel 17.

Direktoratet for forvaltning og IKT (Difi) skal modernisere og omstille offentlig sektor. Difi er underlagt Kommunal- og moderniseringsdepartementet og Nærings- og fiskeridepartementet i fellesskap på fagområdene ledelse, organisering, offentlige anskaffelser og digitalisering. Difi har siden 2013 vært statsforvaltningens kompetansemiljø og fagorgan for informasjonssikkerhet. De skal bidra i utformingen av nasjonale strategier og handlingsplaner, legge til rette for å realisere disse og arbeide for en helhetlig tilnærming til informasjonssikkerhet i forvaltningen. De bidrar særskilt til at alle statlige virksomheter har styring og kontroll med informasjonssikkerheten.

Difi har siden 2014 vært utpekt av Kommunal- og moderniseringsdepartementet til å gi råd og veiledning i henhold til eforvaltningsforskriften § 15.[10] Det omfatter å gi råd og veiledning om styring og kontroll med informasjonssikkerhet til statlige virksomheter og kommuner.

Difi gir veiledning til hele offentlig sektor om blant annet internkontroll, planlegging og gjennomføring av IKT-øvelser, kompetanse- og kulturutvikling innen informasjonssikkerhet og veiledning i risikovurdering av elektronisk kommunika-

---

6 Sikkerhetsloven (1998) (lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste).

7 Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*.

8 VDI er et nasjonalt sensorsystem for deteksjon og verifikasjon av angrep mot kritisk IKT-infrastruktur. Sensorene er plassert på internettforbindelsen til en rekke offentlige og private virksomheter. Systemet er et offentlig–privat samarbeid hvor den enkelte virksomheten bekoster sin egen sensor.

9 For beskrivelse av Nasjonalt beredskapssystem, se Forsvarsdepartementet og Justis- og beredskapsdepartementet (2018) *Støtte og samarbeid*.

10 Eforvaltningsforskriften. Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen.

sjon. De arrangerer også Nettverk for informasjonssikkerhet, som deler erfaringer innen arbeid med informasjonssikkerhet på tvers av offentlige virksomheter.

Difi forvalter kravspesifikasjonen for PKI (Public Key Infrastructure) i offentlig sektor.[11] Den skal brukes ved anskaffelser av PKI-baserte e-ID-løsninger i staten. Difi forvalter også rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. De forvalter dessuten noen fellesløsninger for forvaltningen, blant annet ID-porten som felles innloggingsløsning for offentlig sektor. Difi jobber med IKT-sikkerhet i alle fellesløsningene som de tilbyr forvaltningen.

Difi har også ansvaret for Statens standardavtaler (SSA). De utformer krav om informasjonssikkerhet i disse og veileder i bruk av avtalene. Blant annet veileder Difi offentlig sektor i kjøp av skytjenester, og de har utredet muligheten for å tilby en markedsplass for skytjenester for hele offentlig sektor.[12] De fører også tilsyn med universell utforming av IKT.

Difis tildelingsbrev skisserer fire hovedprioriteringer for 2018. En av disse er å «styrke arbeidet med informasjonssikkerhet». De blir bedt spesifikt om å samarbeide med fagmyndigheter som NSM, Nkom og Datatilsynet for å sørge for felles forståelse av utfordringene i forvaltningen, og se til at tiltakene overfor forvaltningen er koordinerte, risikobaserte og kostnadseffektive. I tillegg skal Difi delta i utformingen av en ny handlingsplan for informasjonssikkerhet i statsforvaltningen.

Nasjonal kommunikasjonsmyndighet (Nkom) er underlagt Samferdselsdepartementet, og skal bidra til å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester. De har et særskilt ansvar knyttet til sikkerhet og beredskap i ekomnett og -tjenester. EkomCERT ble etablert hos Nkom 1. juli 2017.

Nkom skal utarbeide krav om sikkerhet og robusthet og forvalte tilskuddsmidler til sikkerhet og beredskap, samt veilede om dette. De har også ansvar for å innhente, sammenstille og analysere informasjon om hendelser, og de veileder i sikkerhetsarbeid og person- og kommunikasjonsvern. Nkom, Norsk senter for informasjonssikring (NorSIS) og NSM samarbeider blant annet om nettstedet nettvett.no. Nkom deltar i øvingsvirksomhet og har et tett samarbeid med DSB.

Nkom fører risikobaserte tilsyn etter en rekke lover.[13] Tilsyn velges ut basert på en risiko- og sårbarhetsanalyse, og det åpnes tilsyn der det er størst risiko for avvik.

Nkom fører tilsyn med at tilbyderne oppfyller sine forpliktelser i regelverket. Tilsynet skal bidra til at ekomnettene er best mulig sikret og kan stå imot både digitale hendelser og belastninger fra for eksempel ekstremvær.

I tildelingsbrevet til Nkom i 2018 ber Samferdselsdepartementet om at de skal «videreutvikle samarbeidet med NSM innen forebyggende arbeid med informasjonssikkerhet». Utover dette er omtalen av IKT-sikkerhet i tildelingsbrevet knyttet til sikkerhet i kommunikasjonsnettet og videreutvikling av etatens evne til hendelseshåndtering.

Direktoratet for samfunnssikkerhet og beredskap (DSB) er underlagt Justis- og beredskapsdepartementet og skal ha oversikt over risiko og sårbarhet i samfunnet. IKT-sikkerhet inngår i flere av DSBs analyser og utredninger. DSB har en koordineringsrolle innenfor samfunnssikkerhet og beredskap.[14] Det skal legge grunnlaget for et godt og helhetlig forebyggende arbeid og gode beredskapsforberedelser innenfor offentlig forvaltning og samfunnskritisk virksomhet. Direktoratet har en samordningsrolle på etatsnivå på vegne av Justis- og beredskapsdepartementet. De skal også være en pådriver for å forebygge ulykker, kriser og andre uønskede hendelser, herunder sørge for god beredskap og effektiv ulykkes- og krisehåndtering.

DSB fører tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid. IKT-sikkerhet har inngått i enkelte av tilsynene. Direktoratet arrangerer også store nasjonale øvelser som inkluderer IKT-sikkerhetshendelser. De eier og forvalter Nødnett, etter en virksomhetsoverdragelse av Direktoratet for nødkommunikasjon våren 2017.

DSBs tildelingsbrev for 2018 er mer detaljert enn de andre, og to krav angår IKT-sikkerhet.

---

[11] PKI – Public Key Infrastructure i offentlig sektor er en overordnet, funksjonell kravspesifikasjon for anskaffelse av tjenester som bruker eID/e-signatur til bruk i elektronisk kommunikasjon mellom offentlige virksomheter og med innbyggere/næringsliv.

[12] Direktoratet for forvaltning og IKT (2018) *Innkjøpsordning/markedsplass for skytjenester* 2018: 6.

[13] Lov om elektroniske tillitstjenester (lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked). Ekomloven (lov 4. juni 2003 nr. 83 om elektronisk kommunikasjon). Postloven (lov 4. september 2015 nr. 91 om posttjenester).

[14] Justis- og beredskapsdepartementet (2017) *Instruks for departementenes arbeid med samfunnssikkerhet* 1. september 2017.

DSB skal «bistå JD i vurderinger av behov for en felles arena for IKT-sikkerhet på lokalt og regionalt nivå» og «bistå JD i vurderinger av kommunenes og fylkesmannens rolle i responsmiljøene og i nasjonalt rammeverk for digital hendelseshåndtering».

Datatilsynet er et uavhengig forvaltningsorgan som administrativt er underlagt Kommunal- og moderniseringsdepartementet. Datatilsynet er både tilsyn og ombud, og kan ikke instrueres av forvaltningen. Datatilsynet skal føre kontroll med at personvernregelverket etterleves, og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Datatilsynet forvalter personopplysningsloven, som blant annet stiller krav om IKT-sikkerhet.[15] De fører normalt tilsyn med 50–70 private og offentlige virksomheter hvert år. De gir veiledning innenfor sine områder til forvaltningen, bedrifter og privatpersoner. Tildelingsbrevet er på et overordnet nivå. Det er ingen pålegg om samarbeid eller beskrivelser av oppdrag innenfor IKT-sikkerhet.

5.3 Lokalt og regionalt nivå

Kommunene har et generelt og grunnleggende ansvar for å ivareta befolkningens sikkerhet og trygghet innenfor sitt geografiske område. Gjennom sivilbeskyttelsesloven er kommunene blant annet pålagt et ansvar for å gjennomføre en helhetlig risiko- og sårbarhetsanalyse, herunder kartlegge, systematisere og vurdere sannsynligheten for uønskede hendelser som kan inntreffe i kommunen, og hvordan disse kan påvirke kommunen.[16] Kommunene har også plikt til å være forberedt på å håndtere uønskede hendelser, og skal med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen utarbeide en overordnet beredskapsplan. Den skal samordne og integrere øvrige beredskapsplaner i kommunen.[17]

Det kommunale folkestyret innebærer at den enkelte kommunen har et selvstendig ansvar for digitaliseringstiltak og IKT-sikkerhet i egen kommune. Dette har ført til at mange kommuner har ulike digitale løsninger og ulik kompetanse om IKT-sikkerhet. Statsforvaltningen har ingen generell instruksjonsmyndighet overfor kommunene, og den kan bare gripe styrende inn overfor kommunene med grunnlag i lov eller budsjett vedtatt av Stortinget.[18]

Rundt 300 kommuner, fylkeskommuner og interkommunale selskaper er medlem av foreningen Kommunal Informasjonssikkerhet (KINS). Foreningen ble stiftet i 2003 med formål om å øke informasjonssikkerheten i kommuner og fylkeskommuner. Foreningen arrangerer seminarer og konferanser for medlemmene.

KS er kommunesektorens interesse- og arbeidsgiverorganisasjon i Norge. Alle landets kommuner og fylkeskommuner er medlemmer i KS, i tillegg til mer enn 500 bedrifter. KS har vedtatt en digitaliseringsstrategi som blant annet omhandler informasjonssikkerhet, personvern og dokumentasjonsforvaltning. Gjennom dette mandatet jobber KS for å bedre kommunenes rammevilkår og mulighet for å oppå målene i digitaliseringsstrategien.[19]

Fylkesmannen er statens representant i fylket og har ansvar for å følge opp vedtak, mål og retningslinjer fra Stortinget og regjeringen. Embetene utfører ulike forvaltningsoppgaver på vegne av flere departementer.[20] De er dessuten et viktig bindeledd mellom kommunene og sentrale myndigheter. Fylkesmannen har ansvar for å samordne, holde oversikt over og informere om samfunnssikkerhet og beredskap i fylket.[21] Det innebærer blant annet en plikt til å ha oversikt over risiko og sårbarhet i fylket, noe som inkluderer IKT-sikkerhet. I tillegg skal fylkesmannen ha oversikt over og samordne myndighetenes krav og forventninger til kommunenes samfunnssikkerhets- og beredskapsarbeid. Fylkesmannen fører også tilsyn med dette arbeidet samt oppfølging av sivilbestkyttelsesloven og rapporterer til DSB på området. Dette omfatter også kommunenes arbeid med IKT-sikkerhet som en del av samfunnssikkerheten.

---

15 Personopplysningsloven (lov 15. juni 2018 nr. 38 om behandling av personopplysninger).

16 Sivilbeskyttelsesloven (lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret).

17 NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.*

18 Direktoratet for forvaltning og IKT (2015) *Statens styring av kommunene.* 2015: 19.

19 KS (2017) *Digitaliseringsstrategi for kommuner og fylkeskommuner 2017–2020.*

20 Kommunal- og moderniseringsdepartementet (2018) *Virksomhets- og økonomiinstruks for Fylkesmannen* av 13.09.2018.

21 I henhold til instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering fastsatt i kgl.res. 19. juni 2015.

5.4 Nasjonale samordningsarenaer

Myndigheter med ansvar innenfor IKT-sikkerhet samarbeider i det daglige. I tillegg er det samarbeid mellom myndigheter og private aktører. Slikt samarbeid har gjerne oppstått fordi partene har en egeninteresse i det, og det kan være regulert gjennom avtaler inngått mellom dem. Samarbeidet kan omfatte alt fra langsiktig kompetansebygging til informasjonsutveksling knyttet til konkrete saker.

Det er etablert flere tverrsektorielle samordningsarenaer hvor IKT-sikkerhet er hovedtemaet eller inngår blant flere temaer.

Nettverk for nasjonal IKT-sikkerhet skal sikre at strategiske spørsmål knyttet til nasjonal IKT-sikkerhet og internasjonalt samarbeid relatert til dette, blir diskutert og koordinert mellom departementene. Nettverket er en arena for Justis- og beredskapsdepartementets samordningsansvar for IKT-sikkerhet i sivil sektor, for Forsvarsdepartementet i sivile–militære spørsmål knyttet til IKT-sikkerhet, og for Utenriksdepartementet i deres koordinerende rolle for norske posisjoner i internasjonal cyberpolitikk. Alle departementer skal være representert i nettverket som ledes av Justis- og beredskapsdepartementet.

Regjeringen etablerte i 2018 *Forum for nasjonal IKT-sikkerhet*. Det skal sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid blir diskutert mellom private aktører og myndighetene. Forumet består av representanter fra myndigheter, næringslivet, interesse- og bransjeorganisasjoner og akademia. På samme måte som Nettverk for nasjonal IKT-sikkerhet skal forumet være et verktøy for Justis- og beredskapsdepartementet, Forsvarsdepartementet og Utenriksdepartementet i deres særlige samordnings- og koordineringsansvar for IKT-sikkerhet. I tillegg skal det være et verktøy for Nærings- og fiskeridepartementet som tilrettelegger for politikk og rammevilkår for næringslivet. Forumet skal benyttes som referansegruppe for nasjonale strategier og handlingsplaner.

Sentralt totalforsvarsforum er et eksempel på en sektorovergripende arena for forsvars-, sikkerhets- og beredskapsspørsmål hvor IKT-sikkerhet også kan være et tema. Forumet består som sivilt–militært samarbeidsorgan av representanter fra Forsvaret og en rekke sivile etater med ansvar innenfor totalforsvar og samfunnssikkerhet. Det skal bidra til at det er god gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunnet i hele krisespekteret fra fred til sikkerhetspolitisk krise og krig. Sjefen for Forsvarets operative hovedkvarter og direktøren for DSB veksler på å lede forumet.

Ved de mest alvorlige IKT-angrepene, hvor trusselaktøren kan være, eller ha tilknytning til, en fremmed stat, vil det på nasjonalt nivå være en egen koordinering mellom NSM, Etterretningstjenesten, PST og Kripos. Denne koordineringen skjer i Felles cyberkoordineringssenter hvor de fire etatene er til stede med eget personell under ledelse av NSM.

På oppdrag fra Justis- og beredskapsdepartementet opprettet NSM våren 2018 en samhandlingsarena for styrket IKT-tilsyn. Formålet med arenaen er blant annet å bidra til enhetlige tilsyn med mest mulig felles tilsynsmetodikk, kompetanseheving og kunnskapsoverføring mellom tilsynsmyndighetene. Arenaen vil i første omgang omfatte de sektortilsynene som blir utpekt av departementene til å føre tilsyn etter den nye sikkerhetsloven.[22]

I Meld. St. 38 (2016–2017) *IKT-sikkerhet* fremkommer det at NSM skal etablere en arena for erfaringsoverføring, slik at offentlige og private virksomheter i større grad skal få koordinert, tilrettelagt og hensiktsmessig rådgivning og veiledning på IKT-sikkerhetsområdet. Arenaen er etablert med deltagere fra Difi, Datatilsynet og NSM. De møtes fire ganger i året og rapporterer til sine departementer en gang i året.

Difi har tatt initiativ til å etablere et faglig nettverk for statlige veiledningsaktører innenfor styring og kontroll, inkludert IKT-sikkerhet. Datatilsynet, Arbeidstilsynet, DSB, Direktoratet for økonomistyring, Direktoratet for e-helse og NSM er med i nettverket. Formålet er å bidra til mer helhetlig styring og kontroll i de virksomhetene aktørene veileder.

I tillegg til sektorovergripende fora og arenaer finnes en rekke sektorspesifikke arenaer for sikkerhet og beredskapsarbeid som i hovedsak er innrettet mot IKT-sikkerhet eller hvor IKT-sikkerhet inkluderes i en bredere ramme. Eksempler på slike fora er Ekomsikkerhetsforum, som ledes av Nkom, og Luftfartens sikkerhetsråd, som ledes av Luftfartstilsynet.

5.5 Internasjonalt samarbeid

Regjeringen lanserte i 2017 en internasjonal cyberstrategi hvor Norges styrende prinsipper og strategiske prioriteringer innenfor internasjo-

[22] Sikkerhetsloven (lov 1. juni 2018 nr. 24 om nasjonal sikkerhet).

nal cyberpolitikk ble presentert. Om styrende prinsipper står det blant annet at «Norge arbeider for et digitalt rom som fremmer innovasjon og internasjonal handel, som bidrar til internasjonal stabilitet og sikkerhet, og som ivaretar demokratiske verdier og universelle menneskerettigheter. Det gjør vi i samarbeid med andre stater og internasjonale organisasjoner, men også med partnere fra ikke-statlige aktører som akademia og forskningsmiljø, næringslivet og sivilsamfunnet».[23]

For å trygge nasjonale interesser deltar Norge i utformingen av NATOs politikk innenfor IKT-sikkerhet med tanke på forebygging og hendelseshåndtering. Norge og NATO har en samarbeidsavtale om beskyttelse mot digitale trusler som sikrer informasjonsdeling mellom partene. Også innenfor de enkelte samfunnssektorer foregår det internasjonal koordinering av regelverksutvikling av betydning for IKT-sikkerhet.

EUs arbeid med politikk for IKT-sikkerhet har stor betydning også for Norge gjennom EØS-tilknytningen. Norge deltar på en rekke arenaer i EU og i Europarådet. Norge er med i ENISA (European Network and Information Security Agency) og bidrar på flere områder for å videreutvikle evnen til å forebygge, oppdage, varsle og håndtere alvorlige IKT-sikkerhetshendelser på tvers av landegrensene i EU/EØS-området.

Internasjonalt samarbeid om IKT-sikkerhet foregår også i andre internasjonale fora – for eksempel i mellomstatlige organisasjoner som OECD og FN, i regionale konstellasjoner som mellom nordiske land og bilateralt med enkeltland. Næringslivet og akademia har også et selvstendig og utstrakt internasjonalt samarbeid innenfor fagfeltet.

[23] Utenriksdepartementet (2017) *Internasjonal cyberstrategi for Norge.*

Kapittel 6
Regulering av IKT-sikkerhet

I dette kapittelet gis det en oversikt over eksisterende regelverk på IKT-sikkerhetsområdet. I tillegg beskrives ny lovregulering som legger rammer for utvalgets arbeid.

6.1 Eksisterende regelverk

Utvalget har kartlagt at det er omtrent 150 lover og forskrifter som potensielt angår IKT-sikkerhet på nasjonalt plan. Kun et mindretall av disse stiller eksplisitte IKT-sikkerhetskrav. En sammenstilling av utvalgets kartlegging fremgår av vedlegg 1. Kartleggingen viser stor variasjon når det gjelder i hvilken grad lovene og forskriftene stiller krav om IKT-sikkerhet. Enkelte lover og forskrifter – for eksempel sikkerhetsloven og IKT-forskriften for finanssektoren – har omfattende og eksplisitte bestemmelser om IKT-sikkerhet.[1] Andre lover og forskrifter inneholder generelle krav om sikring – for eksempel krav om internkontroll, produktsikkerhet og taushetsplikt – som indirekte regulerer IKT-sikkerhet.

Det er få eksempler på tverrsektorielle lover som inneholder krav om IKT-sikkerhet. Disse er primært sikkerhetsloven, personopplysningsloven, lov om elektroniske tillitstjenester og forvaltningsloven.[2] Disse stiller på ulik måte krav om IKT-sikkerhet.

De fleste sektorer har regelverk som inneholder krav om IKT-sikkerhet, men det er stor variasjon mellom de sektorvise lovene og forskriftene (se boks 6.1). Utgangspunktet for de fleste av dagens lover og forskrifter som stiller krav om IKT-sikkerhet, har vært et behov for sikring av informasjon, og da primært informasjonens konfidensialitet. Mange lover og forskrifter bygger på kravene til sikring av informasjon (informasjonssikkerhet) fra den gamle personopplysningsloven med tilhørende forskrift.[3] Disse kravene kommer til anvendelse kun ved behandling av personopplysninger.

I tillegg til nasjonale lover og forskrifter er det også en mengde internasjonale avtaler, lover og standarder som regulerer IKT-sikkerhet, som norske virksomheter i ulik grad er forpliktet til å følge, eller som kan legge føringer for regelverk i Norge. Eksempler er NIS-direktivet og GDPR, samt sektorspesifikke regelverk som EUs energimarkedsdirektiv og EUs direktiv om banktjenester.

Virksomheter benytter ofte andre kilder enn lov og forskrift for å finne beskrivelser av krav og nivå på IKT-sikkerhet, herunder ulike standarder, veiledere, anbefalinger og retningslinjer. I utvalgets informasjonsinnhenting trakk en rekke virksomheter frem at de har interne rutiner som bygger på ISO 27000-serien. Flere viste til at de også benytter offentlige myndigheters veiledningsmateriell, blant annet fra Datatilsynet, Difi, NorSIS og NSM. Flere virksomheter trekker dessuten frem bransjenormer, for eksempel Norm for informasjonssikkerhet i helsesektoren.

IKT-sikkerhet kan også være regulert gjennom anskaffelsesregulering. Mange virksomheter, også de som ikke er forpliktet til å følge det offentlige anskaffelsesregelverket, benytter seg av SSAer (se punkt 12.1). De inneholder i liten grad krav om sikkerhet utover sikring av informasjon.

I utvalgets informasjonsinnhenting fremgår det at mange begreper kan innbefatte krav om IKT-sikkerhet. Ulike begreper brukes for å beskrive det samme, og det samme begrepet brukes til å beskrive ulike krav. For eksempel er begrepet informasjonssikkerhet definert på forskjellige måter i regelverkene. Figur 6.1 viser de mest brukte meningsbærende ordene i et utdrag av lover og forskrifter som omhandler IKT-sikkerhet.

Tilbakemeldingene fra respondentene i utvalgets informasjonsinnhenting ga uttrykk for at regelverkene oppleves som vanskelige å etterleve. I tillegg er det flere offentlige organer og tilsyns-

[1] IKT-forskriften. Forskrift 21. mai 2003 nr. 603 om bruk av informasjons- og kommunikasjonsteknologi i banker mv.

[2] Forvaltningsloven (lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker).

[3] Personopplysningsloven (2000) (lov 14. april 2000 nr. 31 om behandling av personopplysninger).

Boks 6.1 Eksempler på regelverk i sektorer

I *helsesektoren* er det en rekke regelverk som stiller krav om informasjonssikkerhet, men det stilles i liten grad krav om beskyttelse av systemer og tjenester utover det som kreves for å sikre visse typer informasjon. NAV-loven stiller kun krav om generell beredskap i etaten og utarbeidelse av en plan for blant annet driftssikkerhet.[1] Drikkevannsforskriften, som ble revidert i 2016, har derimot fått en bestemmelse om sikkerhet, hvor det også stilles krav om sikring av styringssystemer mot uautorisert tilgang og bruk.[2]

Finanssektoren har sin egen IKT-forskrift. Den inneholder blant annet krav om planlegging og organisering, risikoanalyse, utvikling og anskaffelse, systemvedlikehold, drift, avviks- og endringshåndtering, driftsavbrudd, kriseberedskap, utkontraktering og dokumentasjon.

Innenfor *ekomsektoren* er IKT-sikkerhet regulert i flere ulike regelverk. Mye av detaljstyringen gjøres gjennom veiledning, tilsyn og enkeltvedtak fattet av Nkom.

For *veitransportsektoren* er det få formelle krav om IKT-sikkerhet, men virksomhetene blir gjennom nasjonal transportplan oppfordret til å sørge for IKT-sikkerhet.

To ytterliggående eksempler på variasjonen i tilnærming til regulering av IKT-sikkerhet er regelverkene for henholdsvis *petroleumssektoren* og *kraftsektoren*. Kravene om IKT-sikkerhet i disse regelverket er ulikt utformet.

På den ene side har olje- og gassindustrien et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet. Petroleumsloven stiller krav om sikkerhet og forsvarlig petroleumsvirksomhet, men regelverket har lagt til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak.[3] Dette gjøres gjennom risiko- og beredskapsanalyser i de enkelte selskapene. Næringen har selv utarbeidet spesifikke retningslinjer for IKT-sikkerhet i prosesskontroll-, sikkerhets- og støttesystemer som legges til grunn for arbeidet basert på ISO 27000-serien.

På den andre siden stiller NVEs revidert forskrift for beredskap i kraftforsyningen relativt omfattende krav om sikring av alle digitale informasjonssystemer hos virksomheter som er underlagt forskriften.[4] Den digitale grunnsikringen innebærer at virksomheter plikter å sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Grunnsikringen skal være i henhold til anerkjente standarder og normer, deriblant å identifisere og dokumentere, sikre og oppdage, håndtere og gjenopprette. I tillegg er det krav om risiko- og sårbarhetsanalyse og sikkerhetskrav ved tjenesteutsetting i forskriften.

1 NAV-loven (lov 16. juni 2006 nr. 20 om arbeids- og velferdsforvaltningen).
2 Drikkevannsforskriften. Forskrift 22. desember 2016 nr. 1868 om vannforsyning og drikkevann.
3 Petroleumsloven (lov 29. november 1996 nr. 72 om petroleumsvirksomhet).
4 Endring i beredskapsforskriften. Forskrift 1. november 2018 nr. 1641 om endring i forskrift om forebyggende sikkerhet og beredskap i energiforsyningen.

myndigheter som gir råd og veiledning eller fører tilsyn med IKT-sikkerheten. For en virksomhet som faller inn under flere regelverk, skaper dette utfordringer med etterlevelsen.[4]

6.2 Ny lovregulering

Implementeringen av en ny personopplysningslov og en ny sikkerhetslov samt gjennomføringen av NIS-direktivet legger rammer for utvalgets vurderinger av dagens regulering på IKT-sikkerhetsområdet. I tillegg arbeider EU med ny regulering for sikkerhetssertifisering av IKT-produkter og -tjenester. Nedenfor følger en kort redegjørelse om regelverkene. Se nærmere beskrivelse av disse i vedlegg 1 og 2.

Ny personopplysningslov

Den nye personopplysningsloven trådte i kraft 20. juli 2018. Formålet med loven er å sikre behandlingen av personopplysninger. Nivået på sikkerhetskravene er stort sett de samme som i den tidligere personopplysningsloven. Det nye er at det

4 Dette samsvarer med funnene i Furuseth, Helge Rager (2013) *Etterlevelse av regelverk for informasjonssikkerhet,* Masteroppgave ved Avdeling for forvaltningsinformatikk, UiO, Våren 2013.

Figur 6.1 Ordsky over de mest brukte meningsbærende ordene i bestemmelser som omhandler IKT-sikkerhet i et utdrag av lover og forskrifter

nå er spesifikke krav om tekniske og organisatoriske løsninger, krav om innebygd personopplysningsvern og krav til utforming av informasjonssystemer og -arkitektur. Det stilles mer detaljerte sikkerhetskrav til databehandleren som behandler personopplysninger på vegne av den behandlingsansvarlige.

Ny sikkerhetslov

Den nye sikkerhetsloven skal tre i kraft 1. januar 2019 med et bredere virkeområde enn dagens lov. For å opprettholde grunnleggende nasjonale funksjoner stiller loven krav om sikring av skjermingsverdig informasjon, informasjonssystem, objekt og infrastruktur. Loven regulerer også departementers, nasjonale og sektorvise sikkerhetsmyndigheters ansvar og roller og til dels forholdet mellom de ulike myndighetene. Med hjemmel i loven utarbeides det forskrifter om myndighetenes ansvar, virksomhetenes ansvar og klarering av leverandører og personell. Utover at loven fortsatt vil gjelde for forvaltningen, er det foreløpig ikke fastsatt nøyaktig hvilket nedslagsfelt loven vil få, da hvert enkelt departement er gitt kompetanse til å fastsette dette nærmere. Loven kommer til å gjelde et relativt sett lite antall private virksomheter.

Den nye sikkerhetsloven fastslår at det fortsatt er behov for et sentralt og tverrsektorielt element som kan se alt arbeidet med forebyggende nasjonal sikkerhet i sammenheng, men at sektorene også hver for seg besitter unik kompetanse som må utnyttes så godt som mulig. Med den nye sikkerhetsloven søkes det å balansere ansvarsprinsippet og samvirkeprinsippet. At ansvarsprinsippet på denne måten lovfestes, innebærer stor grad av sektorautonomi, men også stor grad av ansvarliggjøring av hver enkelt sektor. Sentrale myndigheter, her med NSM som utøvende organ, blir tillagt en rekke samordnings- og koordineringsoppgaver, for eksempel å legge til rette for informasjonsdeling og å utarbeide tilsynsmetodikk.

Gjennomføring av NIS-direktivet

EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) trådte i kraft i EU i august 2016. Det er foreløpig uklart om, eller når, direktivet blir bindende for Norge gjennom EØS-avtalen. Imidlertid følger det av utvalgets mandat

at det skal legge til grunn at NIS-direktivet skal gjennomføres i norsk rett. Det vil utvide omfanget av den tverrsektorielle reguleringen av IKT-sikkerhet. Mange av virksomhetene som omfattes av sikkerhetsloven, vil også omfattes av NIS-direktivet, men direktivet omfatter flere private virksomheter enn sikkerhetsloven.

I NIS-direktivet stilles det krav om en risikobasert tilnærming til IKT-sikkerhet og varsling av alvorlige hendelser. Det stilles også krav til nasjonale myndigheter om etablering av ett eller flere miljøer for å håndtere digitale hendelser, en eller flere nasjonale kompetente myndigheter og ett nasjonalt kontaktpunkt.

Justis- og beredskapsdepartementet har utarbeidet et forslag til høringsnotat med utkast til lov som gjennomfører direktivet i Norge. Slik utvalget forstår høringsnotatet, er man i departementet åpne for å kunne foreslå denne loven uavhengig av den videre EØS-prosessen.[5]

EU Cybersecurity Act

EU arbeider med en ny forordning om sikkerhetssertifisering av IKT-produkter og -tjenester. Bakgrunnen for dette er blant annet at trusselbildet og økningen av IKT-kriminalitet har fremtvunget ulike nasjonale sertifiseringsordninger. Dette har igjen medført fragmenterte og lite hensiktsmessige ordninger mellom medlemslandene.

Formålet med forordningen er å sikre et velfungerende indre marked med et høyt nivå av IKT-sikkerhet, motstandsdyktighet og tillit i EU. En felles regulering for EU kan også redusere sertifiseringskostnadene. Initiativet gir virksomheter som er omfattet av NIS-direktivet et verktøy for å påvise etterlevelse overfor hele EU. Forslaget etablerer et rammeverk for utarbeidelse av spesifikke europeiske sertifiseringsordninger for IKT-produkter og -tjenester. En sertifiseringsordning for cybersikkerhet vil i henhold til forslaget attestere at IKT-produktene og -tjenestene som er sertifisert i overensstemmelse med ordningen, oppfyller fastsatte sikkerhetskrav.

Forslaget til ny forordning innebærer også at EUs European Network and Information Security Agency (ENISA) skal få et permanent og styrket mandat. ENISAs navn foreslås endret til EUs cybersikkerhetsbyrå (EU Cybersecurity Agency).

Det foreslås ulike sertifiseringsordninger for ulike kategorier av produkter og tjenester: kritiske- og høyrisikoapplikasjoner (for eksempel biler), mye brukte digitale tjenester, nettverk og systemer (for eksempel rutere til e-post), og masseproduserte tilkoblede produkter som utgjør tingenes internett (for eksempel nettkameraer). Det skal være frivillig å benytte seg av sertifiseringsregelverket.

[5] Høringsnotatet er pr. 20. november 2018 ikke sendt på høring.

Kapittel 7
Virkemidler i staten

Offentlige myndigheter kan bruke en rekke virkemidler for å bidra til å løse et samfunnsproblem.[1] Statens styringsvirkemidler iverksettes for å påvirke adferden til privatpersoner, bedrifter eller organisasjoner. Det finnes mange ulike inndelinger av virkemiddelbruk, men det er vanlig å skille mellom juridiske, økonomiske, pedagogiske og organisatoriske styringsvirkemidler (se boks 7.1).[2]

Det er kombinasjonen av virkemidler som skaper og setter rammene for påvirkningen og måloppnåelsen innen et politikkområde. Utvalgets mandat handler om juridiske og organisatoriske virkemidler. I det følgende presenteres disse to virkemidlene nærmere.

7.1 Juridiske virkemidler

Juridiske virkemidler er som regel utformet i form av ulike påbud eller forbud, kombinert med en adgang til å kunne gi tillatelser, rettigheter og plikter eller fritak knyttet til disse.

Den overordnede målsettingen for lover og forskrifter er at budskapet skal nå frem til brukerne på en presis og normativ måte, og med

[1] Se blant annet Direktoratet for økonomistyring (2018) *Veileder i samfunnsøkonomiske analyser* og Direktoratet for forvaltning og IKT (2015) *Statlig styring av kommunene.*2015:19.

[2] Se for eksempel Hood, C.C. og Margetts, H.Z. (2007) *The Tools of Government in the Digital Age.* New York. Palgrace Macmillian.

Boks 7.1 Virkemidler i staten

Juridiske virkemidler er lover, forskrifter, konsesjoner, instrukser og vedtak. Tilsyn og klagebehandling blir noen ganger omtalt som egne styringsvirkemidler, men disse kan best forstås som kontrollmekanismer som skal sørge for at lover og forskrifter blir iverksatt og anvendt på en korrekt måte.[1]

Økonomiske virkemidler omfatter blant annet overføringer over statsbudsjettet, pålegg og bøtelegging, subsidier og konkurranseeksponering.[2] Økonomiske insentiver kan påvirke mottakerens atferd i en bestemt retning, gjennom muligheten til å oppnå økonomiske gevinster.

Pedagogiske virkemidler brukes gjerne som en samlebetegnelse for ulike skriftlige publikasjoner som rundskriv, retningslinjer og veiledere. De er ikke i seg selv juridisk bindende, men tar som oftest utgangspunkt i lover og forskrifter og har som mål å medvirke til at disse blir fulgt. De gir tolkninger og anbefalinger knyttet til lovanvendelse i saksbehandling og praksis i utforming av tjenester. Kunnskapsdatabaser, kompetanseutviklingstiltak, holdningskampanjer, muntlig rådgivning og andre tiltak som kan være til hjelp for mottakeren ved oppgaveløsning, betegnes også som pedagogiske virkemidler.

Organisatoriske virkemidler knytter seg til måter å strukturere og organisere staten på. Staten kan velge mellom en rekke ulike tiltak eller virkemidler som påvirker organiseringen av staten, som igjen kan endre for eksempel måloppnåelse og grad av politisk styring på et område. Det kan være selskapsdannelser, fusjonering, endring av tilknytningsform eller organisasjonstype, eierstyring, sentralisering/desentralisering og for eksempel inngåelse av avtaler.

[1] Direktoratet for forvaltning og IKT (2015) *Statlig styring av kommunene*. 2015:19.

[2] Direktoratet for økonomistyring (2018) *Veileder i samfunnsøkonomiske analyser*.

minst mulig omkostninger i form av tid og arbeidsinnsats både for forvaltningen og for den enkelte.[3] Lov og forskrift skal ha språklig klarhet, god meningsmessig sammenheng i reglene og en regelsystematikk det er lett å finne frem i og forholde seg til. Det legges også vekt på at reguleringen må ha lovforankret legitimitet og utøve ansvarlighet på en demokratisk måte. Reguleringen må være tilstrekkelig rettferdig og åpne for demokratisk innflytelse. I tillegg må reguleringen være tuftet på tilstrekkelig kompetanse i form av kunnskap, dyktighet og erfaring. Et siste moment er at reguleringen skal være effektiv.[4]

En oppgave bør ikke forsøkes løst gjennom rettslig regulering uten at det på forhånd er vurdert om den ønskede effekten kan oppnås bedre eller enklere ved bruk av andre virkemidler.[5] Hjemmel i lov er imidlertid nødvendig for tiltak som innebærer inngrep i private forhold (legalitetsprinsippet) der det ikke foreligger andre kompetansegrunnlag.

Pedagogiske virkemidler for påvirkning av handlinger og atferd har grenseflater mot juridiske virkemidler, for eksempel der myndighetene anbefaler eller legger til rette for bruk av internasjonale standarder, bransjestandarder og liknende.

Både nasjonalt og internasjonalt har det de siste par tiårene vært en utvikling av reguleringsregimer der rettsregler i større grad har vært rettet mot styring og formål og i mindre grad mot spesifiserte (tekniske) løsninger eller metoder. Rettsregler rettet mot styring og formål kalles ofte funksjonsbaserte regelverk.[6] Funksjonskrav kan også formuleres som generelle krav rettet mot prosess og ikke resultat, slik det for eksempel er i tilknytning til internkontroll og systematisk HMS-arbeid i virksomheter. Årsaken til økt bruk av funksjonskrav er flere:

- Lover og forskrifter er ikke tilstrekkelig dynamiske til å følge utviklingen av de beste løsningene innen forskjellige fagområder.
- Virksomhetene får handlefrihet og kan utnytte lokal og situasjonsspesifikk kunnskap til å finne egnede løsninger innenfor rammene av lover og forskrifter.
- Funksjonsbaserte regelverk ansvarliggjør i større grad virksomhetene for egen drift og de konkrete løsningene de velger.
- Funksjonsbaserte regelverk kan i større grad bidra til at man unngår kreativ etterlevelse, at hensikten med reglene oppnås, og at virksomhetene også kan strekke seg lenger enn til fastsatte minimumskrav.

Funksjonskrav er ofte utformet som rettslige standarder der innholdet i bestemmelsene utledes av normer utenfor de tradisjonelle juridiske rettskildene, og er knyttet til hva som er ansett som god faglig praksis på området. Det er valgt ulike løsninger i ulike sektorer for hvor konkret disse standardene angis.

I Norge har funksjonskrav i særlig grad vært utviklet innenfor petroleumssektoren, men det er også utbredt innenfor andre reguleringsområder. Hovedtilnærmingen har vært at lover og forskrifter angir overordnede formål som skal ivaretas, med henvisninger til anerkjente normer eller minimumskrav som kan benyttes. Det gis imidlertid anledning til å velge andre løsninger, men virksomheten pålegges da i ulik grad å dokumentere at disse tilfredsstiller de overordnede kravene.

Utvikling og bruk av funksjonsbaserte rettsregler innebærer en rekke avveiinger og dilemmaer. De generelle begrunnelsene – ansvarliggjøring, handlefrihet, fleksibilitet og endringstilpasning – må avveies mot generelle rettssikkerhetshensyn, som klarhet, tydelighet og forutberegnelighet. Funksjonsbaserte regelverk setter også større krav til at virksomhetene har kompetanse og evne til å vurdere hva som ligger innenfor regelverkets krav, og hva som er myndighetenes forventninger.

Fordi regelverket er mer dynamisk, må også virksomhetene kontinuerlig oppdatere seg på hva som er innenfor og utenfor forsvarlig praksis. Blir regelverket for generelt eller vagt, kan det gi stor variasjon i etterlevelsen og håndhevingen. Dersom målgruppens evne og kompetanse på det regulerte feltet varierer mye, vil avveiingen mellom praktiske oppskrifter og funksjonsbaserte rettsregler være særlig utfordrende. Viktige faktorer i denne sammenhengen vil være de regulerte virksomhetenes ressurser, kapasitet, motivasjon og behov (eksempelvis knyttet til tempo i teknologisk utviklingstakt).

---

3 NOU 1992: 32 *Bedre struktur i lovverket*. Lovstrukturutvalgets delutredning II s. 19–20.

4 Baldwin, R., Cave, M. og Lodge, M. (2012) *Understanding Regulation,* Oxford: Oxford University Press, s. 26–27.

5 Justis- og beredskapsdepartementet (2000) *Lovteknikk og lovforberedelse*, s. 13.

6 Begrepet funksjonsbasert regelverk har ikke helt entydig innhold. I St.meld. nr. 17 (2002–2003) *Om statlige tilsyn* legges det vekt på at funksjonsbaserte regelverk i større grad retter seg mot mål og resultater og i mindre grad mot bestemte metoder eller løsninger. I NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* s. 293–295 ble funksjonsbasert regelverk diskutert, teksten er basert på denne diskusjonen.

Avveiinger må også ses i lys av myndighetenes evne og kapasitet til kontinuerlig å vurdere om etterlevelsesmønstre reflekterer kravene til tilstrekkelige og forsvarlige løsninger. Reguleringsmyndigheten må tilby tilstrekkelig veiledning i regelverksforståelse, for eksempel gjennom standardfastsetting, veiledere, implementeringsstøtte og forsvarlighetsnivåer.

Virkemidlene for å sikre etterlevelse trenger ikke nødvendigvis å være regulert i lov. Både i Norge og internasjonalt forskes det mye på hva som gir god etterlevelse. Tradisjonelt har oppfatningen vært at det vesentligste for å sikre etterlevelsen er bruk av makt gjennom kontroll og sanksjoner. Dette omtales som harde virkemidler. Tenkningen har vært i retning av at «anledning gjør tyv», og at det mest effektive for å sikre etterlevelse er virkemidler og tiltak som øker frykten for å bli oppdaget hvis man gjør noe ulovlig.[7] Nyere forskning peker imidlertid i retning av at det ikke er så enkelt. For det første har såkalte myke virkemidler, av typen veiledning og god service, større betydning enn tidligere antatt.[8] For det andre kan harde virkemidler som brukes feil, ha en ødeleggende effekt på viljen til å følge reglene.[9]

Ved bruk av juridiske virkemidler kan det også oppstå en etterlevelsesillusjon.[10] Det betegner en situasjon hvor overholdelsen av reglene i lover og forskrifter helt eller delvis er tilsynelatende. Det kan for eksempel skje ved at reglene etterleves i form snarere enn i innhold. Det skapes et inntrykk av å etterleve regler, men det tas ingen grep for at reglene faktisk etterleves. For eksempel er det dokumentert at dokumentasjonskravene i den gamle personopplysningsloven og personopplysningsforskriften fører til at kommunene gir inntrykk av å være mer lojale og kompetente regelbruker enn hva de i realiteten er.[11] For å avhjelpe etterlevelsesillusjon er det nødvendig med aktivt tilsyn og oppfølgning av de som er underlagt kravene. Kompetanseheving og sertifiseringsordninger kan være andre tiltak for å minimere illusjonen om etterlevelse.

7.2 Organisatoriske virkemidler

Hvilken type organisasjon som er egnet til å utvikle og gjennomføre politikk, avhenger av en rekke forhold. NAV-reformen er et eksempel på hvordan man kan søke å få til endring gjennom å lage en helt ny organisasjonsstruktur. Endring av en eller flere organisasjoner for å oppnå bestemte mål i politikken skjer hele tiden.

Det er imidlertid ikke uproblematisk å bruke organisering som virkemiddel for å nå bestemte mål, for eksempel omorganisering, organisasjonsendring og endring av tilknytningsform. For det første kan kostnadene ved en organisasjonsendring være store, og det må vurderes hvordan kostnadene står seg i forhold til gevinstene. For det andre kan ulike forhold gjøre at effektene av en organisasjonsendring uteblir eller blir annerledes enn det som var tiltenkt.

Organisering er like fullt viktig. Hvem som skal utføre hvilke oppgaver i organisasjonen, kan være bestemt gjennom formelle roller eller posisjoner, for eksempel et personvernombud eller plasseringen av ansvaret for IKT-sikkerhet i eller utenfor ledergruppen. Hvilke underenheter oppgaver og roller er knyttet til, og hvilken større enhet de inngår i, kan påvirke hvordan oppgaven løses. På den måten vil organisering både muliggjøre og vanskeliggjøre bestemte typer handlinger. Jo bedre organisasjonen er tilpasset de problemene den skal løse, jo mer effektiv vil den være som instrument for å få gjennomført politikken på en god måte.[12]

I organisasjoner er det etablerte regler og normer for hvordan ulike typer problemer skal løses. Etablerte organisasjonsformer kan også være til hinder for endring og nytenkning. Organisasjonsendring kan bidra til å endre disse etablerte normene og reglene. Samtidig opphører ikke etablerte normer og regler automatisk ved organisasjonsendringer, og det kan bremse effekten av endringen som var ønsket. Fusjonering av organisasjoner kan bidra til at problemer som bør sees i sammenheng, i større grad gjør det, men større enheter kan også føre til mindre fleksibilitet og nytenkning. Flere mindre enheter som har til dels overlappende oppgaver, kan «konkurrere» og bidra til mer fleksibilitet og nytenkning.[13]

Endringer i en organisasjons tilknytningsform kan også være et organisatorisk virkemiddel. For eksempel er tilknytningsformen bestemmende for

---

7 Holte, Hans Christian (2017) *Harde og myke virkemidler*. Ukeavisen Ledelse 10. februar 2017.

8 Andreoni, J., Erard, B., & Feinstein, J. (1998) *Tax Compliance*. Journal of Economic Literature, 36(2), 818–860.

9 Feld, L.P. and Frey, B.S. (2007) *Tax Compliance as the Result of a Psychological Tax Contract: The Role of Incentives and Responsive Regulation*. Law and Policy, 29, 102–120.

10 Teori om etterlevelsesillusjon er drøftet i Tranvik, Tommy (2012) *Kommunal regeletterlevelse. Illusjoner og realiteter på personvernområdet.* Tidsskrift for samfunnsforskning, nr. 2, s. 131–156. Denne teksten er basert på den artikkelen.

11 Ibid.

12 Direktoratet for forvaltning og IKT (2016) *Nytt veg- og jernbanedirektorat* 2016:3.

13 Ibid.

hvor tett en enhet kan styres, og hvilket styringsprinsipp som er gjeldende. Ordinære forvaltningsorganer styres for eksempel direkte av statsråden, mens et særlovsforetak er eierstyrt. Det har betydning for hvordan staten kan benytte seg av enhetene, og endringer i tilknytningsform kan være et verktøy for å endre dette.

Et annet spørsmål er hvorvidt spredning av ansvar på flere versus samling av oppgaver i én organisasjon gir best grunnlag for politisk styring. Flere virksomheter gjør at politisk ledelse har flere å spille på. Samtidig vil samling av ansvaret gjøre det lettere med enhetlig styring. For store virksomheter vil det da være viktig med sterk sentral styring, slik at det blir en klar og tydelig styringslinje fra politisk ledelse og ut til de utøvende leddene i virksomheten. Erfaringsmessig kan det imidlertid ofte oppstå et informasjonsgap mellom en stor tung etat og en relativt liten departementsavdeling.[14]

[14] Ibid.

Del III
Utfordringsbildet

Kapittel 8
Styrings- og samordningsutfordringer

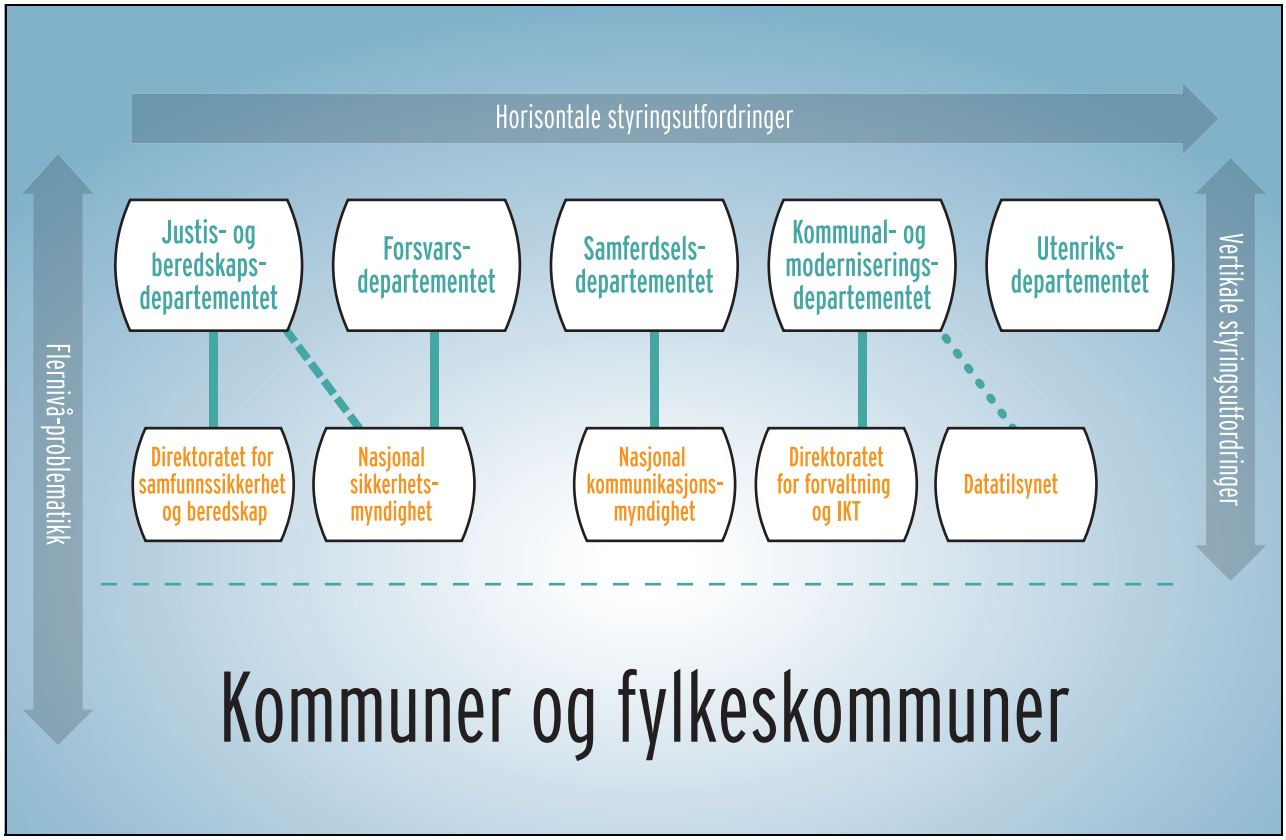
Digitaliseringen av samfunnet skjer i alle sektorer og på alle nivåer. Det gjør IKT-sikkerhet til et tverrsektorielt politikkområde. I forvaltningen har hver enkelt statsråd et overordnet ansvar for å ivareta IKT-sikkerheten i sin egen sektor.[1] Justis- og beredskapsdepartementet har imidlertid et samordningsansvar for IKT-sikkerhet i sivil sektor og skal utforme regjeringens politikk på området.[2] Politiske målsettinger som angir retning og styring på området, kan komme i konflikt med andre målsettinger, både sektorvise og tverrsektorielle.

For departementer med samordningsansvar, som Justis- og beredskapsdepartementet, kan det være utfordrende å utøve rollen som samordningsdepartement innenfor rammen av det konstitusjonelle system med ministeransvar som en grunnleggende forutsetning. Et departement kan ikke uten videre pålegge andre departementer oppgaver, tiltak eller roller. De er likestilte enheter i en flat styringsstruktur. Det fører til en horisontal styringsutfordring mellom departementene (se figur 8.1).

For eksempel kan Kommunal- og moderniseringsdepartementets ansvar for effektive og bru-

1 Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar.*

2 Kongelig resolusjon 10. mars 2017: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet.*



Figur 8.1 Oversikt over sentrale departementer og etater, med markering hvor det er horisontale styringsutfordringer mellom departementene, vertikale styringsutfordringer mellom departementene og etatene og flernivå-problematikk mellom to folkevalgte nivå

kervennlige digitale tjenester ha mål og oppgaver som ikke er i samsvar med Justis- og beredskapsdepartementets målsettinger for nasjonal IKT-sikkerhet.

I utvalgets informasjonsinnhenting peker flere respondenter på at styringen av IKT-sikkerhet i flere sektorer oppleves som sterk, men at samordningen og oversikten på tvers er mangelfull. Blant annet trekkes det frem at samarbeid på tvers av etatene ofte skyldes initiativ fra etatene selv og fra privat sektor, og at det i mindre grad skyldes føringer og krav til samarbeid og koordinering fra departementene. Uklare styringssignaler til underliggende etater og direktorater kan svekke måloppnåelsen. Samlet kan staten oppnå mindre med sine ressurser, enn om styringen var sett i sammenheng.

Informasjonsinnhentingen viser også at de tverrsektorielle etatenes oppgaver i liten grad er samordnet mellom departementene.[3] Dette kan føre til dårligere måloppnåelse ved at etatene kan bli bedt om å gå i ulike retninger og at man ikke prioriterer hva som gagner politikkområdet som helhet. De tverrsektorielle etatene har for eksempel i liten grad felles oppdrag, koordinerte oppdrag eller andre oppgaver hvor målene blir sett i sammenheng med hverandre. Unntaksvis hender det at de blir bedt om å samarbeide med hverandre for å løse ulike oppgaver (se figur 8.1).

I tillegg viser en kartlegging fra Difi at IKT-sikkerhet ikke representerer noen sentral del av etatsstyringsdialogen med statlige etater.[4] Difi påpeker at bedre dialog på dette området kan bidra til å vektlegge styring og kontroll i statsetatene i større grad, og således bedre IKT-sikkerheten i offentlig sektor. IKT-sikkerhet har heller ikke vært en av fellesføringene i tildelingsbrevene de senere årene.[5]

Tildelingsbrevene som sendes fra departementene til underliggende etater er i hovedsak like, bare med noen mindre forskjeller. Iverksettingsbrevet til NSM er imidlertid helt ulikt tildelingsbrevene til andre etater utenfor Forsvarsdepartementets styringssystem. Det er i en rekke utredninger blitt pekt på at det er utfordrende å samarbeide om tildelingsbrev på grunn av ulik styringskultur og praksis.[6] Slike utfordringer er imidlertid basert på departementer som samarbeider innenfor likere styringssystemer enn Forsvarsdepartementet og Justis- og beredskapsdepartementet. Det kan derfor antas at utfordringen med felles styring er større i styringen av NSM.

Kommunene i Norge er selvstendige rettssubjekter og et demokratisk folkevalgt nivå med ansvar for egen IKT-sikkerhet. De må forholde seg til ulike sektorlover og forskrifter, for eksempel innenfor helse og vannforsyning, i tillegg til overordnede lover og forskrifter, som personvernlovgivningen. Dette kommer til utrykk innen helsesektoren, hvor helsestatsråden har et ansvar for hele helsesektoren, men bare styringsmessig kontroll over spesialisthelsetjenesten. Kommunene har ansvar for primærhelsetjenesten, som dermed er utenfor statsrådens direkte styringslinje. Dette fører til at utviklingen av digitale fellesløsninger i hele helsesektoren er utfordrende. På den andre siden har man innenfor helsesektoren utviklet Normen, som også gjelder i kommunal sektor.

Samtidig har staten et overordnet ansvar for ivaretakelsen av samfunnssikkerhet. Spenningen mellom sentralt og lokalt ansvar gir styringsutfordringer, noe som fører til at man må balansere ulike styringsstrategier (se figur 8.1). På den ene side trengs det en sentral ledelse som kan sørge for oversikt, konsistent styring og effektiv allokering av begrensede ressurser. På den andre siden trengs det en desentralisert organisering som sikrer utnyttelse av lokale ressurser, fleksibilitet og evne til å improvisere.[7]

Utvikling av mange digitale tjenester og produkter foregår i private virksomheter og i forsknings- og utviklingsmiljøer. En stor andel av landets kritiske digitale infrastrukturer eies og driftes av private virksomheter. For myndighetene er det en utfordring at de ikke kan styre og påvirke private virksomheter på samme måte som offentlig sektor, og er derfor avhengig av et godt offentlig–privat samarbeid og en hensiktsmessig arbeidsdeling. Statens mulighet for styring av de private virksomhetene er som lovgiver, tilrettelegger og tilsynsmyndighet. For eksempel peker Telenor på avhengigheten mellom offentlig og privat sektor og ønsker et tettere offentlig–privat samarbeid.[8]

---

3 Basert på gjennomgang av de tverrsektorielle etatenes tildelingsbrev for 2018 og samtaler med de ansvarlige departementene. Vi har sett på omtale av oppgaver eller områder som refererer til etatens utadrettede ansvar for IKT-sikkerhet, ikke interne krav om IKT-sikkerhet innad i etatene.

4 Direktoratet for forvaltning og IKT (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen – kunnskapsgrunnlag.* 2018: 4.

5 Felles oppdrag til alle statsetater som er av særlig viktighet for regjeringen og relevans for alle statsetater.

6 Direktoratet for økonomistyring og Direktoratet for forvaltning og IKT (2017) *Departementers styring av samarbeidsoppgaver som gis til underliggende virksomheter.*

7 Rykkja. L. (2017) Håndtering av ekstremvær, flom og skred. I Askim m.fl. (2017) *En smartere stat.* Universitetsforlaget.

8 Telenor (2018) *Sterkere sammen, Digital sikkerhet 2018.*

Kapittel 9
Digitaliseringen av samfunnet utfordrer oppgaveløsning, ansvar og roller

Dagens organisering av tverrsektorielle etater med ansvar for IKT-sikkerhet er historisk og strukturelt betinget.[1] I stor grad har utviklingen skjedd gradvis og som regel uten store eller omfattende organisatoriske endringer. Digitaliseringen av samfunnet fører til at IKT-sikkerhet blir relevant på nye områder hvor det tidligere ikke var av nevneverdig betydning. For eksempel fører fremveksten av intelligente trafikksystemer til at digitale løsninger mellom infrastruktur, trafikant og kjøretøy blir viktig for å ivareta både fremkommelighet og sikkerhet, og IKT-sikkerhet kommer dermed inn som et sentralt element. I mange tilfeller har det betydd at etatene har fått flere oppgaver innenfor IKT-sikkerhet enn de tidligere hadde.

Utfordringen med å avgrense og «ramme inn» IKT-sikkerhet har betydning for hvordan etatene med tverrsektorielt ansvar for IKT-sikkerhet løser sine oppgaver. På enkelte områder har det ført til noe overlapping mellom etatene. Etter hvert som IKT-sikkerhet i stadig større grad har kommet på dagsordenen, har det vært naturlig for flere av de tverrsektorielle etatene å definere arbeidet med nasjonal IKT-sikkerhet som en viktig del av sin rolle og sine oppgaver.

Utviklingen har medført at de tverrsektorielle etatene har fått utvidede oppgaver og beveget seg mot hverandre, tilsynelatende uten at grensedragning mot andre etater har vært tilstrekkelig vurdert. For eksempel fikk Difi i 2013 utvidet mandat til å etablere et kompetansemiljø for informasjonssikkerhet i statsforvaltningen, og dermed beveget Difis oppgaver seg nærmere NSMs oppgaver. Da NSM fikk oppgaver ut over sikkerhetsloven, beveget de seg nærmere DSBs ansvar for samfunnssikkerheten. Samtidig preges innretningen på IKT-sikkerhetsarbeidet naturlig nok av de ulike etatenes kjerneoppgaver. Sett utenfra kan det derfor oppleves som om etatene har sine egne måter å tilnærme seg IKT-sikkerhet på.

I tillegg til at det har utviklet seg slike overlappende områder, har den teknologiske utviklingen ført til konvergens mellom forvaltningsområder. For eksempel blir det stadig vanskeligere å skille mellom el- og ekominstallasjoner fordi mange av dem nå kan være bærere av strømforsyning, styresignaler og kommunikasjon. Når lysbrytere, termostater og sikringer i elektriske installasjoner blir ekomutstyr, men like fullt har en helt avgjørende funksjon i det elektriske anlegget, kan det bli vanskelig å skille forvaltningsområder.[2] Både DSB og Nkom har uttrykt at skillet mellom elektrisk utstyr (som DSB har ansvaret for) og kommunikasjonsutstyr (som Nkom har ansvaret for) blir stadig mindre ved nye teknologiske produkter. Utviklingen berører ansvarsområdene og oppgavene til begge etatene, i tillegg til at den skaper regulatoriske utfordringer som gjelder el-tilsynsloven og ekomloven.[3]

Et annet eksempel er at energiflyt og smarte nett utfordrer grensesnittet mellom DSB som elsikkerhetsmyndighet og NVE (Norges vassdrags- og energidirektorat) som energimyndighet. Installasjoner og nett integreres stadig mer med lokal energiproduksjon, og fører til at det er vanskelig å skille hva som skal reguleres og forvaltes av henholdsvis DSB og NVE.

9.1 Samfunnssikkerhet og statssikkerhet overlapper

DSB har et særskilt ansvar for å ha oversikt over risikoer og sårbarheter som kan ramme samfunnet, og som samfunnet må være forberedt på å håndtere. Tilnærmingen til DSB bygger på en

[1] De tverrsektorielle etatene er definert som NSM, Difi, Nkom, Datatilsynet og DSB. Se mandatforståelse punkt 2.2.

[2] Direktoratet for samfunnssikkerhet og beredskap (2018) *Internt notat om Elektro og ekom konvergerer* av 10.04.2018.

[3] El-tilsynsloven (lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr).

såkalt «all-hazards approach», som innebærer at samfunnets sårbarheter behandles uavhengig av hva som utløser en hendelse. Selv om DSB ikke har et spesifikt og uttalt ansvar for IKT-sikkerhet, må de allikevel ha oversikt over hvilke sårbarheter den digitale utviklingen medfører for samfunnssikkerheten.

I tillegg skal DSB støtte Justis- og beredskapsdepartementet i deres samordningsrolle innenfor samfunnssikkerhet. I kongelig resolusjon fra 2017 sees IKT-sikkerhet som en integrert del av arbeidet med samfunnssikkerhet.[4] Samordning av arbeidet med samfunnssikkerhet vil da kunne innebære at DSB har samordningsansvar også for IKT-sikkerhet.

NSM er nasjonalt fagmiljø for IKT-sikkerhet og skal understøtte Justis- og beredskapsdepartementet innenfor IKT-sikkerhet på sivil side. NSM er i en spesiell situasjon fordi etaten styres av to departementer. De rapporterer til Forsvarsdepartementet for saker i forsvarssektoren og til Justis- og beredskapsdepartementet for saker i sivil sektor. NSM er administrativt underlagt Forsvarsdepartementet, som dermed er det ledende departementet i styringen.

NSM har tradisjonelt jobbet mest innenfor sikkerhetslovens domene. Loven skal motvirke særlig alvorlige tilsiktede handlinger, men sikkerhetstiltakene vil også motvirke menneskelig svikt og tekniske feil. Etter at NSM ble etablert som nasjonalt fagmiljø og fikk oppgaver for Justis- og beredskapsdepartementet innen IKT-sikkerhet fikk etaten et bredere virkefelt. Dette har skapt nye grensesnitt mellom NSM og andre virksomheter, blant annet DSB.

Et uttrykk for NSMs nye rolle er den årlige rapporten *Helhetlig IKT-risikobilde*, hvor ulike typer uønskede digitale hendelser danner grunnlag for risikobildet. I instruksen til sjef NSM fremgår det blant annet at NSM skal koordinere arbeidet mellom myndigheter som har en rolle innenfor forebyggende IKT-sikkerhet, og legge til rette for hensiktsmessig samhandling mellom disse. DSB har i informasjonsinnhentingen til utvalget påpekt at NSM ikke i tilstrekkelig grad er opptatt av utilsiktede hendelser.

Utvidelsen av virkeområdet til den nye sikkerhetsloven er et annet eksempel på potensielle gråsoner mellom NSM og DSB. Evalueringen av gjeldende sikkerhetslov konkluderte med at lovens virkeområde var for snevert, og at det var et sikringsbehov utover det som fulgte av etablert praktisering av begrepet «rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser». Virkeområdet samsvarte ikke med de virksomhetene som er viktige aktører innenfor nasjonal sikkerhet, særlig fordi IKT-sikkerhetsutfordringer er gjennomgripende og tverrsektorielle. Derfor ble det gamle begrepet erstattet med begrepene «nasjonale sikkerhetsinteresser» og «grunnleggende nasjonale funksjoner» i den nye loven. Virkeområdet til den nye sikkerhetsloven beveger seg i større grad enn tidligere inn på samfunnssikkerhetsområdet der DSB har et særlig ansvar.

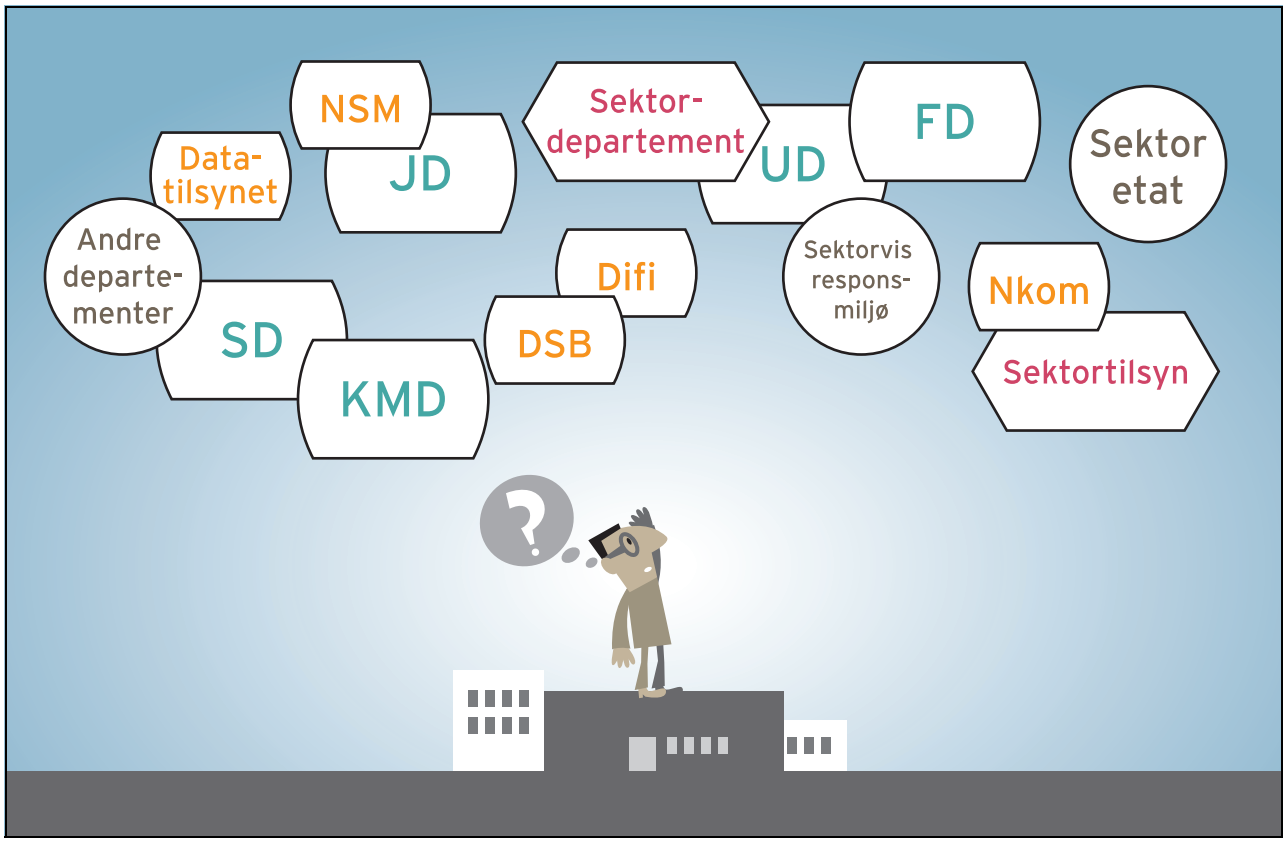
9.2 Råd og veiledning fremstår fragmentert og lite koordinert

Råd og veiledning gis av mange aktører i ulike former. Det fremgår av punkt 5.2 at det særlig er NSM, Nkom, Difi og Datatilsynet som har rådgivning og veiledning om IKT-sikkerhet som en tverrsektoriell oppgave. I tillegg til disse gir NorSIS rådgivning om informasjonssikkerhet til private og offentlige virksomheter. Sektoretatene, for eksempel NVE og Finanstilsynet, gir også råd og veiledning om IKT-sikkerhet innenfor sine sektorer. I tillegg finnes det en rekke private virksomheter som tilbyr rådgivning.

De tverrsektorielle etatene har noe ulike målgrupper for sitt arbeid med råd og veiledning. Utvalget har identifisert noe overlapping mellom disse, særlig når det gjelder veiledning mot stat og kommune. For eksempel har både Datatilsynet og Difi utarbeidet veiledere i internkontroll og informasjonssikkerhet. Begge tar utgangspunkt i ISO 27001-standarden, men innretning og enkelte områder er ulike fordi de har ulikt formål. Et annet eksempel er at både Difi og NSM gir veiledning til statsforvaltningen om tilgrensende områder. Difi gir veiledning om informasjonssikkerhet knyttet til styring og kontroll, og spesifikt til eforvaltningsforskriften § 15. NSM gir veiledning om spesifikke sikkerhetstiltak knyttet til IKT-sikkerhet i henhold til sikkerhetsloven eller mer generelt med utgangspunkt i grunnprinsippene for IKT-sikkerhet og råd i forbindelse med hendelseshåndtering. Også her tar begge virksomhetene utgangspunkt i ISO 27001.

I informasjonen utvalget har hentet inn, kommer det til uttrykk at brukerne er usikre på hvor de skal henvende seg for å få råd og veiledning om IKT-sikkerhet. Dette kan tyde på at det man-

[4] Kongelig resolusjon 10. mars 2017: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*.



Figur 9.1 Fremstilling av hvordan IKT-sikkerhetsverdenen kan oppleves fra et brukerperspektiv

gler en tydelig stemme eller ett kontaktpunkt som brukerne opplever er det rette stedet å henvende seg. Det kan også tyde på at det er uklart for brukerne hva de ulike etatene har ansvaret for. Fra et brukerperspektiv kan det være krevende å forholde seg til mange aktører (se figur 9.1).

I tillegg peker enkelte av respondentene på at veiledningsaktørene ikke har tilstrekkelig kapasitet til å gi veiledning. NSM har uttalt at de ikke har kapasitet til å yte tilstrekkelig oppfølgende rådgivning og kompetansebygging etter tilsyn. De sier også at den økende mengden IKT-sikkerhetshendelser gjør det krevende å skulle gi god nok støtte til de virksomhetene som rammes.[5] Enkelte tilbakemeldinger peker også på at rådene ikke er koordinerte og enhetlige. Dette knytter seg særlig til en-til-en-veiledningen og ikke det skriftlige materialet etatene gir ut.

De tverrsektorielle etatene peker også på at det meste av den skriftlige generiske veiledningen er koordinert mellom dem. En større utfordring er å samordne en-til-en-veiledning og det at brukerne ikke har ett felles kontaktpunkt. I tillegg utarbeider sektormyndigheter veiledning til sine sektorer, noe som også enkelte av respondentene opplever som lite koordinert med de tverrsektorielle etatene.

Kommunene trekker i tillegg frem at de må forholde seg til flere sektorielle og tverrsektorielle lover og forskrifter. Samtidig opplever de at råd og veiledning bidrar til å skape uklarheter om hva det egentlig stilles krav om, og at rådene og veiledningen som gis, til tider er motstridende. Blant annet trekkes det frem at de statlige aktørene i for liten grad involverer eller har som formål å bistå kommunene innen IKT-sikkerhet. I tillegg vises det til at kommuner har mangler når det gjelder generell fagkompetanse, sektorkompetanse og ledelseskompetanse på IKT-området.[6] De har derfor særlig behov for veiledning.

Punkt 6.1 viser at det er variasjon i begrepsbruken i de ulike regelverkene, til dels også i begrepsdefinisjoner og -forståelse. Både etater med tverrsektorielt ansvar og sektoretater gir råd og veiledning i henhold til regelverkene de forvalter. Disse rådene kan være basert på ulike standarder og bransjepraksis eller lover og forskrifter. Det kan medføre at enkelte råd og veiledninger

[5] Nasjonal sikkerhetsmyndighet (2015) *Sikkerhetsfaglig råd.* s. 32.

[6] Dokument 3:6 (2015–2016) *Riksrevisjonens undersøkelse av digitalisering av kommunale tjenester.*

oppleves som lite harmoniserte og i verste fall motstridende, basert på utformingen av selve reguleringen.

Aktører kan være underlagt flere ulike tverrsektorielle og sektorspesifikke lover og forskrifter. Det kan for eksempel tenkes at en virksomhet er omfattet av en sektorlov, som ekomloven, og tverrsektorielle lover, som sikkerhetsloven og personopplysningsloven. Da er det særlig viktig at råd og veiledning knyttet til disse lovene er samordnet og enhetlig.

9.3 Utfordringer med koordinering og informasjonsdeling ved uønskede digitale hendelser

Digitale systemer utsettes kontinuerlig for uønskede hendelser, både tilsiktede og utilsiktede. Det kan utgjøre en trussel mot systemene i seg selv, informasjonen som er i systemene, og tjenestene de bidrar til å levere. Slike hendelser omtales med ulike begreper: hacking, digitale angrep, IKT-sikkerhetshendelser, digitale hendelser med mer. Her brukes *uønskede digitale hendelser*, i tråd med IKT-sikkerhetsmeldingen.[7]

Den enkelte virksomhet har et selvstendig ansvar for å håndtere uønskede digitale hendelser, uavhengig av om virksomheten befinner seg i privat eller offentlig sektor. Samtidig kan det være en utfordring å knytte til seg tilstrekkelig kompetanse for å håndtere slike hendelser. Særlig utfordrende kan det være å ha rett spisskompetanse og kapasitet, for eksempel analysekapasitet. Dette gjelder spesielt små og mellomstore virksomheter.

En rekke offentlige virksomheter kan være involvert i håndteringen av en uønsket digital hendelse. Justis- og beredskapsdepartementet har sammen med Forsvarsdepartementet et overordnet ansvar for å sikre hensiktsmessig koordinering av håndteringen av slike hendelser. NSM har et ansvar på nasjonalt nivå for å varsle og dele informasjon om sårbarheter og IKT-hendelser, koordinere håndtering av hendelser mellom berørte sektorer, bistå med rådgivning og teknisk analyse og oppdatere deteksjonsparametere. I tillegg har sektorene et særlig ansvar innenfor sine respektive ansvarsområder for å bistå i håndteringen.

Utfordringer med koordinering og informasjonsdeling mellom aktører ved hendelseshåndtering har blitt løftet frem i tilbakemeldingene til utvalget. Dette har også vært tema i flere utredninger og stortingsmeldinger.[8] Lysne-utvalget registrerte at mange aktører opplevde at informasjonsdelingen var mangelfull, og at samarbeidet mellom offentlige og private virksomheter kunne vært bedre. Det ble pekt på at utfordringer innen hendelseshåndtering skyldes dårlig samarbeidsklima, og at eksisterende strukturer ikke er godt nok utnyttet.[9] Lysne-utvalget pekte også på at sårbarheten øker når flere gis tilgang til informasjon, noe som kan legge begrensninger for hva som deles og hvem det deles med. Særlig ved uønskede digitale hendelser må slike begrensninger vektes opp mot den enkelte virksomhets behov for informasjon. En annet grunn til mangelfull informasjonsdeling kan være at virksomheter som har vært utsatt for en uønsket digital hendelse, kan mene at detaljer og omfanget av hendelsen er bedriftssensitiv informasjon. Derfor kan de ønske at denne typen informasjon ikke blir delt på en slik måte at virksomheten blir eksponert.

9.3.1 Koordinerings- og informasjonsbehovet

Behovet for koordinering og informasjonsdeling gjør seg gjeldende før, under og etter en uønsket digital hendelse. Virksomheter vil ha et løpende behov for trussel- og sårbarhetsinformasjon for å være best mulig i stand til å forebygge at hendelser inntreffer i virksomheten. Når en hendelse har inntruffet, vil det være et behov for koordinering og informasjon som kan bidra til håndteringen i de berørte virksomhetene. Virksomheter som ikke selv er rammet, kan under en hendelse ha behov for informasjon som gjør at de kan treffe nødvendige tiltak for å hindre at de rammes. I etterkant av en hendelse vil det være behov for å dele informasjon for å evaluere og forbedre virksomhetenes evne til å forebygge og håndtere hendelser.

Ved en uønsket digital hendelse er det behov for å dele teknisk informasjon, som typisk omhandler angrepsmetoder, skadepotensial og annen relevant informasjon som er nødvendig for å forstå den tekniske siden av hendelsen. Denne typen informasjon deles gjerne mellom NSM og sektorvise responsmiljøer, innbyrdes i de sektorvise responsmiljøene, mellom responsmiljøer og virksomheters IKT-avdelinger og mellom ulike

[7] Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar.*

[8] Blant annet NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* kap. 21, Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar* kap. 7.

[9] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.*

virksomheters IKT-avdelinger. Medlemmer av VDI-samarbeidet mottar i henhold til særlig avtale automatisk informasjon fra NSM som angår dem.

Informasjon som deles under en uønsket digital hendelse, kan være sikkerhetsgradert eller ugradert. Behovet for gradering gir begrensninger i informasjonsdelingen. Ikke alle virksomheter har teknisk mulighet til å kommunisere på gradert nivå, og det kan være utfordringer med at personell ikke er sikkerhetsklarert og autorisert. I tillegg kan virksomheter be om begrensninger i distribusjonen av informasjon som de er opphav til.

Informasjon som er relevant for den tekniske forebyggingen og hendelseshåndteringen, kan også inneholde personopplysninger, for eksempel utveksling av IP-adresser, metadata om IKT-trafikk til og fra virksomheter, og logger. Behandling og deling av personopplysninger krever et hjemmelsgrunnlag. Det foreligger i dag ikke noe slikt grunnlag for deling av personopplysninger som dekker hele håndteringskjeden. Virksomheters mulighet for å innhente og dele informasjon har derfor noen begrensninger.

Evalueringen av den nasjonale IKT-øvelsen i 2016 viser at det er behov for deling av andre typer informasjon enn bare den tekniske ved en alvorlig uønsket digital hendelse.[10] NSM NorCERT og de sektorvise responsmiljøene er først og fremst opptatt av den tekniske siden av hendelsen. Etatene på sin side har behov for et bredere situasjonsbilde. Under øvelsen innebar det at det ble etablert doble rapporteringskanaler i enkelte sektorer, hvor både de sektorvise responsmiljøene og etatene rapporterte til departementene. Med to rapporteringslinjer risikerer man å få ulik informasjon. Det blir da problematisk å sette sammen et situasjonsbilde, og det kan gi et unødvendig merarbeid.

En uønsket digital hendelse kan medføre svikt i en eller flere kritiske samfunnsfunksjoner eller på annen måte ha potensial for å gi et konsekvensbilde som krever fysisk håndtering.[11] Konsekvensene for samfunnet kan være store, noe både erfaringene fra den nasjonale IKT-øvelsen i 2016 og reelle uønskede digitale hendelser har vist. DSB peker på dette som en utfordring og mener det ordinære krisehåndteringsapparatet tidlig må kobles på ved uønskede digitale hendelser. De mener det er helt nødvendig for å sikre god håndtering av samfunnskonsekvensene.[12]

[10] DSB (2017) *Tverrsektoriell evaluering av øvelse IKT16.*

[11] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner.*

[12] DSB i møte med utvalget 24.04.2018.

9.3.2 Ulike krav til håndtering av uønskede digitale hendelser

Det er i dag ingen enhetlig regulering av roller og ansvar knyttet til håndtering av uønskede digitale hendelser, herunder informasjonsdeling og rapportering. Eventuelle krav følger av ulike regelverk, og det er ingen krav til at hendelser skal ses i sammenheng. Etableringen av den nasjonale NorCERT-funksjonen i NSM i 2006 og en føring fra 2012 om at det skal etableres sektorvise responsmiljøer, har søkt å kompensere for dette.[13]

I tillegg fastsatte Justis- og beredskapsdepartementet og Forsvarsdepartementet i desember 2017 Rammeverk for håndtering av IKT-sikkerhetshendelser.[14] Det beskriver håndtering av slike hendelser i og på tvers av virksomheter og sektorer. Rammeverket avgrenser myndighetenes ansvar til å bidra til og tilrettelegge for en koordinert og effektiv håndtering av «alvorlige IKT-sikkerhetshendelser», det vil si hendelser rettet mot kritisk infrastruktur og/eller kritiske samfunnsfunksjoner. Det foreligger imidlertid ingen rettslig plikt for sektorer og virksomheter til å implementere krav og tiltak i rammeverket. Se boks 9.1 for en nærmere beskrivelse av rammeverket.

Nedenfor beskrives utfordringer knyttet til informasjonsdeling og koordinering med utgangspunkt i sektorvise responsmiljøer, kommunalt nivå og private virksomheter som ikke er en del av kritiske samfunnsfunksjoner.

9.3.2.1 Sektorvise responsmiljøer

For å bidra til god informasjonsdeling og koordinering mellom relevante aktører har myndighetene besluttet at det skal etableres sektorvise responsmiljøer.[15] Miljøene skal ha oversikt over egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM NorCERT. Miljøene skal i tillegg ha en tydelig styringslinje til sektordepartementet. Slike responsmiljøer er trukket frem som en styrke for hendelseshåndteringen, fordi miljøene kjenner egen sektor, har tillit hos brukerne, og det følger av ansvarsprinsippet at sektorene selv må ta ansvar for store deler av hendelseshåndteringen.

[13] Fornyings-, administrasjon- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet med handlingsplan.*

[14] Brev fra Justis- og beredskapsdepartementet av 14.12.2017.

[15] Fornyings-, administrasjon- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet med handlingsplan*.

Boks 9.1 Rammeverk for håndtering av IKT-sikkerhetshendelser

Justis- og beredskapsdepartementet og Forsvarsdepartementet fastsatte i desember 2017 Rammeverk for håndtering av IKT-sikkerhetshendelser. Dette er sendt ut til departementene for implementering innenfor de respektive forvaltningsområdene.[1] Rammeverket beskriver håndtering av IKT-sikkerhetshendelser i og på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal håndteringsevne innenfor rammen av de etablerte beredskapsprinsippene.

Rammeverk for håndtering av IKT-hendelser stiller krav/forventninger til virksomhetene, sektorvise responsmiljøer og NSM knyttet til 1) planlegging og forberedelse, 2) deteksjon og vurdering av omfang og alvorlighetsgrad, 3) varsling av relevante parter, 4) iverksetting av prosesser og tiltak for å håndtere hendelsen, 5) situasjonsrapportering og 6) tilbakeføring og læring av hendelsen.

Det enkelte departementet har stor fleksibilitet knyttet til å vurdere hvorvidt det er hensiktsmessig med ett eller flere sektorvise responsmiljøer i egen sektor eller mer hensiktsmessig å samarbeide med andre sektorers responsmiljøer eller private leverandører.

For å utnytte tilgjengelig kommersiell kompetanse i arbeidet med hendelseshåndtering etablerte NSM i februar 2016 en kvalitetsordning for private virksomheter for at disse skal kunne gi råd og bistand til andre knyttet til hendelseshåndtering.

[1] Brev fra Justis- og beredskapsdepartementet av 14.12.2017.

Det fremgår av stortingsmeldingen om samfunnssikkerhet at flere sektorer så langt ikke har etablert egne responsmiljøer.[16] I noen tilfeller skyldes dette manglende finansiering eller begrenset tilgang på relevant kompetanse. I andre tilfeller skyldes dette at ikke alle virksomheter har en sterk og naturlig tilhørighet i én sektor, og derfor har etablert løsninger tilpasset egen virksomhet og eget utfordringsbilde.

Status i dag er at de sektorvise responsmiljøene som er etablert, har varierende organisering, roller og myndighetsforankring. For eksempel kan sektorvise responsmiljøer være en del av en etat (slik som EkomCERT) eller privateide (slik som KraftCERT og Nordic Financial CERT).

Det at de sektorvise responsmiljøene er såpass forskjellige, fører til noen utfordringer. Overfor private CERTer har sektormyndighetene liten mulighet for annet enn regulatorisk styring, eventuelt avtaler som regulerer forholdet mellom partene. Videre ser utvalget det som utfordrende at det i enkelte sektorer er uklarhet om hele sektoren er knyttet til CERT-funksjonen, eller bare utvalgte virksomheter gjennom betalt medlemskap eller andre frivillige tilknytningsformer.

De ulike sektorvise responsmiljøene har også forskjellig oppgaveportefølje. EkomCERT har primært en koordinerende rolle, mens HelseCERT også har en operativ rolle i hendelseshåndteringen og bistår virksomheter ved behov. Summen av disse ulikhetene gjør at det etter utvalgets mening er vanskelig å omtale de sektorvise responsmiljøene som en samlet kapasitet innenfor hendelseshåndtering.

Enkelte store private aktører har egne hendelseshåndteringsmiljøer med høy kompetanse, for eksempel innenfor ekom- og finansnæringen. Koblingen til disse miljøene er ment ivaretatt av de sektorvise responsmiljøene, men dette er dårlig beskrevet i den nasjonale strukturen. Det kan ligge et uutnyttet potensial i å involvere private håndteringsmiljøer i større grad.

Med dagens status for de sektorvise responsmiljøene tviler utvalget på om intensjonen med dem fullt ut er oppfylt, og dermed om alle responsmiljøene som går under benevnelsen sektorvist responsmiljø, faktisk er det. Selv om krav til både NSM NorCERT og de sektorvise responsmiljøene er gitt i Rammeverk for håndtering av IKT-sikkerhetshendelser, bidrar ulikhetene mellom de sektorvise responsmiljøene til uklare ansvars- og rolleforhold ved håndtering av hendelser.

9.3.2.2 Kommunalt nivå

Kommunal sektor er ikke en del av et etablert håndteringsregime for uønskede digitale hendelser. Mange kommuner er gjennom avtaler koblet til HelseCERT og/eller KraftCERT for å få bistand til håndtering. Det vil likevel være deler av

[16] Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*

kommunens virksomhet som ikke er knyttet til sektorvise responsmiljøer, og hvor det er uavklart hvordan slike hendelser skal håndteres og varsles videre i systemet.

Kommune-Norge omtales ofte enhetlig som kommunal sektor, men i virkeligheten består kommunene av en rekke sektorer, noe som kanskje bidrar til at det er utfordrende å etablere en egen Kommune-CERT eller et responsmiljø.[17] I kommunal sektor er det ingen aktører som beskriver et samlet situasjonsbilde (trusler, sårbarheter, hendelser og sikkerhetstiltak) for kommunene. Dette er noe av kjernen i utfordringen de står overfor.

Det er heller ingen aktører som i dag har ansvar for varsling og informasjonsdeling mellom alle kommuner, fylkeskommuner og andre håndteringsmiljøer. Noe varsling og deling av informasjon forekommer, primært sentrert rundt eksisterende håndteringsmiljøer og i kommuner som har kompetanse og kapasitet til dette. Videre mangler kommunene et felles ressurs- eller kompetansesenter som kan støtte dem med tekniske analyser, eller yte teknisk og metodisk støtte ved håndtering av uønskede digitale hendelser. Det er heller ikke formalisert et kontaktpunkt for kommunal sektor i den nasjonale CERT-strukturen.

I tillegg er det noe uklart for utvalget hvordan det vanlige håndteringssporet innen samfunnssikkerhet skal kobles på når kommunene i økende grad skal forholde seg til sektorvise responsmiljøer. Når hendelser med samfunnsmessige konsekvenser inntreffer skal kommunen iverksette rapportering på samordningskanal til fylkesmannen, som igjen rapporterer til DSB.[18] En vurdering av alvorlighetsgrad avgjør videre rapportering til Justis- og beredskapsdepartementet ved Krisestøtteenheten og eventuell involvering av andre etater.[19] Kommunen må også rapportere i den relevante fagkanalen, det vil si til sektormyndigheten(e) som har ansvaret for det området hendelsen skjer innenfor.

9.3.2.3 Private virksomheter som ikke er en del av kritiske samfunnsfunksjoner

Målgruppen for rammeverket for håndtering av IKT-sikkerhetshendelser er offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner. Det vil si at virksomheter i privat sektor som ikke er omfattet av denne avgrensningen, faller utenfor rammeverket. De får dermed ikke samme støtte, informasjonsdeling og koordinering som virksomhetene som er en del av rammeverket. De har likevel et selvstendig ansvar for å håndtere uønskede digitale angrep, slik tilfellet er for alle andre virksomheter. De må derfor benytte seg av den generelle veiledningen til NSM, Datatilsynet, Difi eller andre for selv å forebygge og håndtere angrep, eller de kan kjøpe tjenester av andre private virksomheter på dette området.

9.4 Tilsyn med IKT-sikkerhet oppleves som mangelfullt og lite koordinert

Utvalget har identifisert tre forhold knyttet til tilsyn som kan forbedres. For det første fremstår tilsynsetatene som lite koordinert i tid, begrepsbruk og metodikk. For det andre er det mangler og hull i tilsynsvirksomheten, herunder utilstrekkelig kompetanse til å foreta tekniske IKT-tilsyn i sektorene. I tillegg utfordrer uoversiktlige digitale verdikjeder hjemmelsgrunnlaget for tilsyn med underleverandører.

9.4.1 Manglende koordinering av tilsyn

I utvalgets informasjonsinnhenting har det blitt pekt på manglende koordinering og samordning i gjennomføringen av tilsyn. Det kan se ut som dette er en generell problemstilling knyttet til statlig tilsynsvirksomhet og ikke noe spesifikt bare for de tverrsektorielle etatene som gjennomfører tilsyn med IKT-sikkerhet. Det er et relativt beskjedent antall tilsyn som gjennomføres av DSB, NSM og Datatilsynet hvert år, og utvalget antar derfor at denne utfordringen skyldes at respondentene også er gjenstand for sektortilsyn i tillegg til de tre tverrsektorielle tilsynene.

Utvalget har fått tilbakemelding på at tilsyn fra ulike etater kan komme relativt tett i tid. Tilsynene kan be om ganske lik dokumentasjon, for eksempel dokumenter på styringssystemet og internkontroll for å kontrollere etterlevelse av sine regelverk. At mange tilsyn kommer samtidig, eller nært i tid, bryter med forventingen om at til-

[17] NorSIS (2015) *Kommune CSIRT 2015*.

[18] Direktoratet for samfunnssikkerhet og beredskap (2016) *Retningslinjer for varsling og rapportering på samordningskanal*.

[19] Krisestøtteenheten er et sivilt bemannet situasjonssenter med døgnkontinuerlig beredskap. Under en krise bidrar enheten med kompetanse i form av rådgivning og faglig bistand til Kriserådet og lederdepartementet.

syn utført av ulike virksomheter skal være samordnet for å minimere byrden for dem det føres tilsyn med.[20]

Respondentene til utvalget har også pekt på at tilsynsmyndighetene bruker ulike begreper og metodikk. Det er få føringer for hvordan tilsynet skal gjennomføres i de ulike sektorene. For eksempel er det ingen felles krav til tilsynsmetodikk eller hvilke elementer som skal inngå i et IKT-sikkerhetstilsyn. Det er heller ingen enhetlig regulering av tilsynsmyndighetens rettigheter og tilsynsobjektets plikter, og det er varierende sanksjonsmuligheter og ulike måter å finansiere tilsynene på.

For å bidra til bedre informasjonsutveksling og kompetanseoverføring for de ulike sektorenes sentrale tilsynsmyndigheter opprettet NSM våren 2018 en samhandlingsarena for styrket IKT-tilsyn (se punkt 5.4).

9.4.2 Mangler i tilsynsvirksomheten

Utvalget konstaterer at det gjennomføres få tilsyn med teknisk IKT-sikkerhet, og at flere av respondentene i utvalgets undersøkelse etterspør dette. Dette understrekes ytterligere av evalueringen som Difi og Forsvarets forskningsinstitutt har utført på oppdrag fra Justis- og beredskapsdepartementet av DSBs tilsyn med departementene.[21] Den viser blant annet at departementene etterspør inntrengningstesting som en del av, eller et tillegg til, dagens tilsyn.

Tilsyn med IKT-sikkerhet retter seg i dag i første rekke mot de styrings- og kontrollfunksjonene en virksomhet har for å ivareta IKT-sikkerhet. Det er få tilsynsmyndigheter som har kompetanse til å utføre tekniske IKT-tilsyn der en vurderer hvilke sikkerhetsmekanismer som er implementert i IKT-systemene, om systemene er konfigurert på en slik måte at de faktisk sett er sikre, og om de tilfredsstiller de sikkerhetskravene som følger av ulik regulering.[22] Utvalget er imidlertid kjent med at flere tilsyn nå jobber med å styrke kompetansen på dette området.

Lange og uoversiktlige digitale verdikjeder kan også føre til at tilsynet blir mangelfullt gitt en tradisjonell inndeling i tilsynsobjekt og tilsynsutfører. Norges Bank peker på at svikt hos sentrale IKT-leverandører kan sette viktige deler av betalingssystemet og andre sentrale samfunnsfunksjoner ut av spill. Slik konsentrasjonsrisiko kan vanskelig håndteres av den enkelte systemeier. Norges Banks hovedstyre mener derfor det bør utredes hvordan sentrale IKT-leverandører til betalingssystemet best kan underlegges tilsyn.[23] Utfordringer med å føre tilsyn hos underleverandører kan gjelde hos flere samfunnskritiske virksomheter.

---

[20] St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap*.

[21] Direktoratet for forvaltning og IKT (2017) *Evaluering av tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid – tredje tilsynsrunde.* 2017:4.

[22] Nasjonal sikkerhetsmyndighet (2015) *Sikkerhetsfaglig råd* s. 28.

[23] Norges Bank (2018) *Finansiell infrastruktur.*

Kapittel 10
Mangelfull regulering av IKT-sikkerhet

I dette kapittelet vurderes det om gjeldende lover og forskrifter stiller hensiktsmessige krav om forsvarlig IKT-sikkerhet til norske virksomheter. Etter en gjennomgang av regelverk (se vedlegg 1), informasjonsinnhentingen til utvalget og samtaler med en rekke sentrale aktører konstaterer utvalget at det foreligger mangler ved eksisterende rettslige krav om forsvarlig IKT-sikkerhet.

Utvalget har kartlagt at det er mye regelverk som inneholder bestemmelser som kan ha betydning for IKT-sikkerheten. Det er ingen eksisterende lov, forskrift, instruks, legaldefinisjon, enhetlig begrepsbruk eller «norm» som eksplisitt gir uttrykk for hva som er IKT-sikkerhetsregelverk. Utvalgets kartlegging av regelverk viser en uensartet tilnærming til regulering av IKT-sikkerhet, noe som gjenspeiles i ulik regulering i sektorene og uensartet begrepsbruk. Det gjør det krevende å etablere en oversikt over de faktiske krav som ulike regelverk stiller om IKT-sikkerhet.

Utvalget vil nedenfor gå nærmere inn på de største utfordringene med dagens regulering. Det stilles ofte kun krav om sikring av informasjon. Videre er det usikkert om generelle sektorspesifikke krav om sikkerhet inkluderer krav om IKT-sikkerhet. Det er ikke hensiktsmessig regulering av IKT-sikkerhet i offentlig forvaltning, og sikkerhetsloven har begrensninger av betydning.

Det er i tillegg andre utfordringer som har sammenheng med dagens regulering, men som ikke gjennomgås i dette kapittelet. Utfordringer knyttet til digitale verdikjeder og anskaffelser tas opp i kapittel 12, og tilkoblede produkter og tjenester behandles i kapittel 13. Utfordringer med hendelseshåndtering og tilsyn er også relevante, og de drøftes i kapittel 8 og 9.

10.1 Krav om sikring av informasjon er ikke tilstrekkelig

Mange av dagens lover og forskrifter stiller delvis krav om forsvarlig IKT-sikkerhet. I mange tilfeller stilles det imidlertid kun krav om sikring av informasjon. Noe av grunnen til dette kan være at mange regelverk har sin opprinnelse i en analog og papirbasert verden. Senere forsøk på modifikasjon av hensyn til samfunnsutviklingen har i varierende grad vært vellykkete. Et eksempel på dette er krav i arkivloven som ifølge Stortinget «[…] er laget før digitalisering og bruk av data, og loven har av den grunn flere mangler».[1, 2]

Personopplysningsloven er ett eksempel der formålet med sikringen er å beskytte en bestemt type informasjon, nemlig personopplysninger. Lovens krav om IKT-sikkerhet er dermed utformet med dette for øyet. Flere andre lover og forskrifter som regulerer sikring av informasjon, bygger på personopplysningsloven. Den gjelder for bortimot alle virksomheter som behandler personopplysninger.[3] Det følger av loven at alle IKT-systemer som behandler personopplysninger, må sikres. Det vil si at omtrent alle norske virksomheter må forholde seg til kravene om IKT-sikkerhet i loven.

Personopplysningsloven dekker likevel bare deler av behovet utvalget ser for IKT-sikkerhet. Særlig fordi mange virksomheter er avhengige av IKT-systemer som ikke behandler personopplysninger. Personopplysningsloven stiller da ikke krav om sikring av slike IKT-systemer.

---

1 Innst. 14 S (2016–2017) *Innstilling fra familie- og kulturkomiteen om bevilgninger på statsbudsjettet for 2017*, punkt 5.11.

2 Arkivloven (lov 4. desember 1992 nr. 126 om arkiv).

3 Loven og forordningen gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven mv.), jf. § 2 annet ledd bokstav b.

10.2 Varierende krav om IKT-sikkerhet

Sektorspesifikke lover og forskrifter regulerer i all hovedsak gjennomføring av en viss type aktivitet, slik som bankvirksomhet, drikkevannsforsyning og luftfart. I mange tilfeller stilles det krav om sikkerhet i tilknytning til gjennomføringen av aktiviteten, for eksempel for å unngå ulykker og skader på miljøet.

Sektorregelverket har ulik tilnærming til sikkerhet generelt og IKT-sikkerhet spesielt. I noen tilfeller stilles det hensiktsmessige krav om forsvarlig IKT-sikkerhet. I andre tilfeller stilles det ingen krav om IKT-sikkerhet. Videre ser utvalget at det i mange tilfeller er uklart om lover og forskrifter faktisk stiller krav om forsvarlig IKT-sikkerhet.

Slik utvalget vurderer det, er virksomheter i finanssektoren, drikkevannsforsyningen, kraftforsyningen, ekomsektoren og langt på vei jernbanesektoren underlagt krav om forsvarlig IKT-sikkerhet.

For virksomheter i enkelte andre sektorer, som for eksempel vegtransport og drivstofforsyning, gjelder det ingen sektorspesifikke krav om forsvarlig IKT-sikkerhet, verken i lov eller i forskrift.

Flere sektorspesifikke lover og forskrifter stiller mer generelle krav om sikkerhet i tilknytning til en type aktivitet, for eksempel luftfart, havnevirksomhet og skipsfart. Det kan være gode grunner til at IKT-sikkerhet skal tolkes inn i allerede eksisterende lover og forskrifter. Det må imidlertid vurderes konkret om disse regelverkene faktisk stiller krav om forsvarlig IKT-sikkerhet.

For det første er det spørsmål om et krav i lov eller forskrift endrer seg, fordi samfunnsutviklingen gir begrepene som benyttes nytt eller endret innhold. Er for eksempel et krav om risikovurdering det samme i dag som for fem år siden? Kan man si at det påhviler den enkelte virksomheten å forstå at det i sikkerhetssammenheng må tas høyde for digitale elementer i sikkerhetsarbeidet? Dersom lov og forskrift ikke opplyser eksplisitt hva som konkret ligger i begrepet forebyggende sikkerhet, kan det likevel tolkes inn krav om sikkerhetslogging og tilknytning til et hendelseshåndteringsmiljø?

Det kan argumenteres med at jo lengre tid som går uten signaler fra lovgiver, domstoler eller forvaltningspraksis, jo vanskeligere blir det å mene noe bestemt hva som er den «riktige» forståelsen av begrepet (se boks 10.1).

Boks 10.1 Begrepsbruk om sikkerhetslovens virkeområde

Sikkerhetslovens (1998) begreper «rikets sikkerhet» og «andre vitale nasjonale sikkerhetsinteresser» er viktig for forståelsen av lovens virkeområde. Traavik-utvalget kom frem til at det var motstridende synspunkter på det nærmere meningsinnholdet i begrepene. Forarbeidenes henvisning til at overordnede politiske myndigheter til enhver tid skal vurdere og definere innholdet i begrepene, var i liten grad blitt fulgt opp i praksis.[1] Traavik-utvalget uttalte videre at dersom de innarbeidede begrepene skulle videreføres i den nye loven, noe det var flere gode argumenter for å gjøre, så ville det også være en risiko for at usikkerheten knyttet til innholdet ville bli videreført. Konklusjonen ble, blant annet med dette som grunnlag, at en ny sikkerhetslov burde benytte andre begreper.

[1] NOU 2016: 19 *Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* s. 100.

For det andre er det spørsmål om praksis blant aktørene som er underlagt regelverket. Et relevant moment er om disse virksomhetene, har endret atferd. Et annet moment er om tilsynsmyndighetene har endret innhold i sine tilsyn i samsvar med en fornyet forståelse av de rettslige kravene.

Manglende eller uklare sikkerhetskrav betyr ikke nødvendigvis at de enkelte virksomhetene ikke har forsvarlig IKT-sikkerhet. Utvalget mener likevel at gjeldende lover og forskrifter er lite hensiktsmessige for å oppnå forsvarlig nasjonal IKT-sikkerhet. For det første er det utfordrende for virksomheter å etterleve utydelige krav. For det andre er tydelige krav i eller i medhold av lov en forutsetning for å føre tilsyn med IKT-sikkerhet, og for å kunne sanksjonere mangelfull IKT-sikkerhet. For det tredje er det her i vesentlig grad snakk om virksomheter som er særlig viktige for samfunnet. Da har myndighetene behov for å ha en viss styring med gjeldende sikkerhetstilstand.

Regulering på et veldig overordnet nivå kan skape uklarhet knyttet til forståelsen av om loven eller forskriften stiller krav om forsvarlig IKT-sikkerhet, og hvilke krav som stilles. Det er enkelte lover og forskrifter i dag som benytter begreper

som «forsvarlig sikkerhet» og tolker IKT-sikkerhet inn i dette begrepet, for eksempel ekomloven. I praksis vil det imidlertid være vanskelig for brukerne ut fra et så overordnet krav å utlede hva forsvarlighetskravet gjelder, og hvilke tekniske og organisatoriske tiltak som forutsettes implementert. Det stiller krav om høy kompetanse både hos virksomheter og tilsynsmyndigheter.

10.3 Lite hensiktsmessig regulering av IKT-sikkerhet i offentlig forvaltning

Utfordringene som ble påpekt i punkt 10.1 og 10.2 gjelder for mange virksomheter i offentlig forvaltning. Det er videre to relevante lover som gjelder spesifikt for offentlig forvaltning, forvaltningsloven og sivilbeskyttelsesloven.

Forvaltningsloven gjelder for all offentlig forvaltning. Det følger av loven at den gjelder for forvaltningsorganer, som er ethvert organ for stat og kommune. Loven hjemler eforvaltningsforskriften, som også gjelder for forvaltningsorganer. Forskriften stiller krav om «internkontroll på informasjonssikkerhetsområdet». Etter utvalgets syn er det tre grunner til at forskriften ikke stiller tilfredsstillende krav om forsvarlig IKT-sikkerhet.

For det første er det usikkert om forskriften gjelder for alle relevante IKT-systemer i offentlig forvaltning. Forskriften gjelder IKT-systemer som brukes til saksbehandling og til kommunikasjon med og i forvaltningen. Fordi flere forvaltningsorganer produserer tjenester som ikke er tradisjonell saksbehandling, kan det være at IKT-systemer som brukes til tjenesteproduksjon, ikke omfattes av forskriften.

For det andre stilles det for vage sikkerhetskrav. Etter utvalgets syn, som det redegjøres nærmere for i punkt 15.2, er det ikke tilstrekkelig at det kun stilles krav om internkontroll på informasjonssikkerhetsområdet. Det bør gå tydelig frem at kravet om IKT-sikkerhet også gjelder for en virksomhets produksjon av varer eller tjenester. Videre må det stilles krav om at det skal iverksettes tiltak for å forebygge og håndtere hendelser.

For det tredje har eforvaltningsforskriften ikke rettsregler om tilsyn. Etter utvalgets mening er tilsyn et viktig virkemiddel for å få virksomhetene til å etterleve de rettslige kravene.

Riksrevisjonen har påpekt at flere statlige virksomheter har for dårlig styring av informasjonssikkerhet og sikring av IKT-systemer. Ofte er det mangler i grunnleggende sikkerhetstiltak som tilgangsstyring og overvåking av egne systemer.[4] Dette tyder på manglende etterlevelse av eforvaltningsforskriften.

Kommunene har en sentral rolle i arbeidet med samfunnssikkerhet og beredskap. Denne rollen er tydeliggjort gjennom kommunal beredskapsplikt i sivilbeskyttelsesloven. Beredskapsplikten pålegger kommunen å arbeide helhetlig og systematisk med samfunnssikkerhet og beredskap, og loven understreker kommunens viktige rolle som samordner og pådriver i samfunnssikkerhetsarbeidet. I DSBs veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen er cyberangrep og hacking anført som to eksempler på tilsiktede uønskede hendelser som kommunen skal vurdere.[5]

Beredskapsplikten for kommunene kan derfor også omfatte IKT-sikkerhet, men utvalget anser kravet som vagt utformet. Det kan vanskelig konstateres at den kommunale beredskapsplikten omfatter tydelige krav om forsvarlig IKT-sikkerhet. Undersøkelser viser at under halvparten av kommunene har en helhetlig risiko- og sårbarhetsanalyse som oppfyller utvalgte krav.[6] Videre har 1 av 3 kommuner i Norge for dårlig nettsidesikkerhet.[7] I utvalgets informasjonsinnhenting var det også få av respondentene som viste til sivilbeskyttelsesloven som grunnlag for krav om IKT-sikkerhet.

10.4 Begrensninger i sikkerhetsloven

Den nye sikkerhetsloven stiller krav om forsvarlig sikkerhet, inkludert IKT-sikkerhet. Loven gjelder for offentlig forvaltning, for leverandører av varer og tjenester i forbindelse med sikkerhetsgraderte anskaffelser og for virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner. Loven stiller tydelige krav om sikring av IKT-systemer. Mange av virksomhetene som har avgjørende betydning for grunnleggende nasjonale funksjoner, er også samfunnskritiske virksomheter. Det kommer ikke eksplisitt frem i sikkerhetsloven hvilke konkrete virksomheter som inngår i grunnleggende nasjonale funksjoner,

---

4 Dokument 1 (2018–2019) *Riksrevisjonens årlige revisjon og kontroll – budsjettåret 2017*.

5 Direktoratet for samfunnssikkerhet og beredskap (2014) *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*. s. 62.

6 Direktoratet for samfunnssikkerhet og beredskap (2016) *Kommuneundersøkelsen 2016*.

7 Loopia (2018) *1 av 3 kommuner i Norge har for dårlig nettside-sikkerhet.*

men det er grunn til å anta at det vil dreie seg om virksomheter innen for eksempel kraftsektoren, elektronisk kommunikasjon og lignende.

Sikkerhetsloven oppfyller imidlertid kun i begrenset grad det behovet utvalget ser for IKT-sikkerhet i samfunnet. Det er særlig tre grunner til dette. For det første er sikkerhetslovens formål avgrenset til å gjelde forebygging, avdekking og motvirkning av tilsiktede handlinger. Loven stiller derfor ikke krav om at man sikrer seg mot utilsiktede hendelser. For det andre er det antakelig mange private virksomheter, herunder samfunnskritiske virksomheter, som ikke vil bli omfattet av loven. For det tredje stilles det kun krav om å sikre skjermingsverdige IKT-systemer. Det er IKT-systemer som enten behandler sikkerhetsgradert informasjon, eller som har avgjørende betydning for grunnleggende nasjonale funksjoner. Dette utelukker mange IKT-systemer som utvalget mener bør sikres.

Kapittel 11
Manglende insentiver for å investere i IKT-sikkerhet

Til tross for potensielt betydelige økonomiske konsekvenser er det ikke alltid slik at virksomheter har tilstrekkelige insentiver til å beskytte seg mot digitale trusler og sårbarheter. Mørketallsundersøkelsen fra 2018 konkluderer med at norske virksomheter investerer for lite i IKT-sikkerhet.[1] Ifølge undersøkelsen er det kun 24 prosent av norske toppledere som mener at deres virksomhet enten er «svært godt» eller «godt» forberedt på et cyberangrep, og nesten halvparten sier de er for dårlige til å identifisere nye cybertrusler.

Manglende insentiver kan ha en rekke årsaker. I en rapport fra britiske myndigheter trekkes det frem at mange virksomheter mener at de har for lite kunnskap, forståelse eller kjennskap til digitale trusler til å iverksette hensiktsmessige tiltak.[2] Det kommer i tillegg frem at mindre virksomheter tror de er uaktuelle mål for cyberangrep, og at de har lite kjennskap til de mulige negative konsekvensene av slike hendelser. Mange er også usikre på hvem i virksomheten som er ansvarlig. Enkelte mindre virksomheter tror for eksempel det er banken som håndterer slike trusler, mens større virksomheter mener det er IT-avdelingens ansvar.

Virksomhetene har enda mindre insentiver til å gjøre noe med de eksterne virkningene som manglende sikkerhetstiltak har på andre aktører i samfunnet. Som Oslo Economics trekker frem i sin rapport (se digitalt vedlegg), er det en kjent problemstilling i det samfunnsøkonomiske fagfeltet at virksomheter kan ha manglende insentiver som fører til at de underinvesterer i IKT-sikkerhet.

Gordon–Loeb-modellen viser at selskaper som er profittmaksimerende og følger sine egeninteresser, kun burde investere en liten andel av det forventede tapet ved IKT-sikkerhetsbrudd.[3] Dersom man inkluderer de negative virkningene som et IKT-sikkerhetsbrudd har utenfor virksomheten, vil det bedriftsøkonomisk rasjonelle investeringsnivået være for lavt i et samfunnsøkonomisk perspektiv.[4] Den teoretiske prediksjonen er derfor at det investeres for lite i IKT-sikkerhet. En virksomhet kan for eksempel gå konkurs, mens samfunnet blir sittende igjen med hoveddelen av kostnadene ved et alvorlig IKT-sikkerhetsbrudd.

Et annet poeng er at virksomheter kan velge å investere mindre i IKT-sikkerhetstiltak fordi investeringene er synlige som kostnader i regnskapene. Sikkerhetsinvesteringene har derfor normalt negativ innvirkning på lønnsomheten i virksomhetene. Det kan føre til at ledelsen i en virksomhet blir mer opptatt av kortsiktig lønnsomhet enn tiltak for å redusere sikkerhetstrusler.

I tillegg til potensielle insentivproblemer i det private næringslivet kan det også oppstå insentivproblemer i offentlig sektor. Det er for eksempel tenkelig at noen etater har insentiver til først og fremst å drive digitaliseringen fremover med sikte på økt effektivitet, mens andre i første rekke ønsker å ha god IKT-sikkerhet. Dette er en form for målkonflikt som kan føre til insentivproblemer. Et annet eksempel kan være at noen etater ønsker kort lagringstid på logger for å fremme personvern, mens andre etater ønsker lengre lagringstid for å få bedre sikkerhetsinformasjon.

Underinvestering i IKT-sikkerhet hos virksomheter kan ha konsekvenser for større deler av økonomien fordi forbrukere, kunder og andre virksomheter kan bli rammet når det skjer IKT-sikkerhetsbrudd. Myndighetene har derfor en motivasjon og en rolle å spille for å påvirke insentivene, for eksempel gjennom regulering eller gjennom råd og veiledning.

---

1 Næringslivets sikkerhetsråd (NSR) har kartlagt sikkerhetstilstanden hos over 1500 virksomheter i privat og offentlig sektor. Mørketallsundersøkelsen gir et innblikk i norske virksomheters holdninger til digital sikkerhet, kunnskap, forebygging og beredskap.

2 UK Department for Digital, Culture, Media and Sport (2016) *Cyber Security Regulation and Incentives Review.*

3 Gordon, Lawrence; Martin Loeb (November 2002) *The Economics of Information Security Investment.* ACM Transactions on Information and System Security. 5 (4): 438–457.

4 Gordon et al. (2015) *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon–Loeb Model,* Journal of Information Security, 2015, 6, 24–30.

Kapittel 12
Anskaffelser og digitale sårbarheter

Enhver virksomhet, enten den er offentlig eller privat, er avhengig av å kjøpe inn varer og tjenester. Som et samlebegrep på slike kjøp benyttes gjerne anskaffelser. Dette omfatter alt fra innkjøp av kontorrekvisita, mobiltelefoner og printere, til leasing av flymotorer og tjenesteutsetting av IKT-drift og renhold. Ved kjøp av tjenester benyttes som regel begrepet tjenesteutsetting. Hvis tjenesteutsettingen leveres av en aktør utenfor Norge, kalles det gjerne offshoring.

Noen anskaffelser kan utgjøre en kritisk innsatsfaktor for virksomheten. For eksempel er de fleste virksomheter avhengig av at IKT-systemene fungerer som de skal. Virker de ikke, så stopper produksjonen opp. Slik avhengighet utgjør i seg selv en risiko for virksomheten.

Et av hovedfunnene i Lysne-rapporten er at mange virksomheter ikke bare er avhengige av at leverandøren leverer som forutsatt. Underleverandører i flere ledd har ulike avhengigheter, ofte lange og komplekse digitale verdikjeder. En feil langt ute i kjeden kan forplante seg raskt og umiddelbart få konsekvenser for egen virksomhet.

Uavhengig av om anskaffelsen er kritisk for virksomheten eller ikke, kan alle anskaffelser innebære digital risiko for virksomheten. Digitale produkter kan gjøre virksomheten sårbar ved at de kobles både til internett og interne IKT-systemer, for eksempel termostater og overvåkningskameraer. Noen tjenesteleveranser innebærer at eksterne får tilgang til virksomhetens IKT-system. Det kan være aktuelt ved utsetting av IKT-drift og innkjøp av regnskap- og HR-tjenester.

12.1 Mangelfull regulering

Gjeldende lover og forskrifter regulerer IKT-sikkerhet ved anskaffelser i varierende grad. Sikkerhetsloven og personopplysningsloven regulerer det på en tilsynelatende tilfredsstillende måte. Fordi lovenes virkeområde er begrenset, har bestemmelsene likevel begrenset relevans for denne utredningen.

Beredskapsforskriften og IKT-forskriften har tydelige krav til IKT-anskaffelser.[1] Andre anskaffelser er ikke like tydelig regulert. For mange sektorer gjelder det som nevnt i kapittel 10 ingen krav om IKT-sikkerhet, og heller ikke krav om IKT-sikkerhet ved relevante anskaffelser. Andre steder, hvor det stilles krav om IKT-sikkerhet, er det likevel ikke opplagt om det faktisk stilles krav om sikring av alle relevante IKT-systemer. Samlet sett mener utvalget at gjeldende lover og forskrifter ikke er tilfredsstillende på dette området.

12.2 Offentlige anskaffelser

Ifølge tall fra SSB var det samlede innkjøp av varer og tjenester for offentlig sektor over 500 milliarder kroner i 2016. Offentlig sektor investerer årlig flere milliarder kroner i IKT. I *Digital agenda for Norge* blir det anslått at offentlig sektor anskaffet IKT for 16,6 milliarder kroner i 2014.[2]

Anskaffelseslovens formål er å fremme effektiv bruk av samfunnets ressurser, og gjelder når offentlige myndigheter kjøper varer og tjenester over en viss verdi.[3] Oppdragsgiveren kan stille krav knyttet til anskaffelsesprosessen, slik at kontrakten gjennomføres på en måte som fremmer ulike samfunnshensyn, forutsatt at kravene har tilknytning til leveransen. Det kan stilles krav om IKT-sikkerhet ved kjøp av IKT-produkter og -tjenester. Det er imidlertid ikke like opplagt om det kan stilles krav om IKT-sikkerhet i tilknytning til andre anskaffelser. Spørsmålet er ikke diskutert i forarbeidene til loven.

Difi har utarbeidet et sett med standardavtaler (SSAer) for kjøp av IT og konsulenttjenester. Flere av avtalene har generelle krav om informa-

---

1 Beredskapsforskriften. Forskrift 7. desember 2012 nr.1157 om forebyggende sikkerhet og beredskap i energiforsyningen.

2 Meld. St. 27 (2015–2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.*

3 Anskaffelsesloven (lov 17. juni 2016 nr. 73 om offentlige anskaffelser).

sjonssikkerhet og personvern. Kravene handler først og fremst om å sikre konfidensialiteten og integriteten til kundens data. Oppdragsgiveren er henvist til å angi eventuelle nærmere krav om informasjonssikkerhet i bilag til avtalen (se vedlegg 1, punkt 3.3).

12.3 Tjenesteutsetting

Tjenesteutsetting, inkludert bruk av skytjenester, er en betydningsfull trend som følge av digitaliseringen av samfunnet. Ifølge SSB har andelen norske virksomheter med ti eller flere ansatte som kjøper skytjenester, økt fra 40 til 48 prosent fra 2016 til 2017.[4] Økende bruk av tjenesteutsetting gjelder også for virksomheter som understøtter samfunnets kritiske funksjoner.

Formålet med tjenesteutsetting er ofte et ønske om kvalitetsheving, effektivisering og kostnadsreduksjon gjennom tilgang til større og mer profesjonelle leveransemiljøer enn man har i egen organisasjon. På denne måten kan virksomheten i større grad konsentrere seg om sine kjerneaktiviteter.

Det er flere forhold som må tas i betraktning ved en tjenesteutsetting. Det har betydning for hvilken type virksomhet (offentlig eller privat) det gjelder. Videre om anskaffelsen innebærer overføring av personell (virksomhetsoverdragelser) eller nedskalering og/eller endring av personalets arbeidsoppgaver. I hvilken grad anskaffelsen medfører risiko for virksomheten må vurderes. I tillegg må det vurderes om det er egne lover og forskrifter som får anvendelse og kan regulere handlingsrommet.

Den siste tiden har det vært en del debatt i offentligheten rundt tjenesteutsetting av IKT-tjenester generelt og offshoring spesielt. Med utviklingen av skybaserte tjenester, det vil si nett-

[4] I Nasjonal sikkerhetsmyndighet (2018) *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området «Beslutt leveransemodell» i NSMs grunnprinsipper for IKT-sikkerhet.*

Boks 12.1 Tjenesteutsetting og offshoring

Det er mye debatt og mediedekning om mulige sikkerhetsrisikoer ved tjenesteutsetting og spesielt offshoring. Gjennomgående fokuseres det på sikkerhetsrisikoer som, i henhold til fremstillingene, antas å ville oppstå fordi tjenesteutsetting foregår utenfor Norge. Ofte bærer debattene og dekningen også preg av at databehandlingen er sikker eller til og med risikofri om den gjøres i Norge. En slik tilnærming til databehandling og risikovurdering er etter utvalgets syn i seg selv en sikkerhetsrisiko.

Av den offentlige debatten kan det også synes som at det er en utbredt oppfatning at det er forbudt å behandle data utenfor Norge. Et slikt generelt forbud finnes ikke.

Risikobildet varierer fra land til land, men det er ingen automatikk i at risikoene alltid er større utenfor Norge. Risikoen kan også være lavere. I *Helhetlig IKT-risikobilde 2017* skriver NSM at «sårbarheter finnes i nær sagt alle virksomheter, systemer og infrastrukturer, både av teknisk, organisatorisk og menneskelig art». Hvor databehandlingen geografisk skjer er bare ett av flere momenter i den risikovurderingen som må gjøres for å kunne iverksette hensiktsmessige sikkerhetstiltak. Som utgangspunkt eksisterer de samme risikoene alle steder.

Uavhengig av hvilket land en tjeneste leveres fra, må man vurdere de samme forholdene, og gjennomføre mange av de samme tiltakene. Viser vurderingen at det knytter seg forhøyet risiko til enkelte forhold, må det iverksettes tiltak som reduserer risikoen til et akseptabelt nivå. Det må kontinuerlig vurderes om det er mulig å oppnå et akseptabelt sikkerhetsnivå for den gjeldende tjenesteleveransen. Denne risikovurderingen må inngå som en del av en samlet vurdering av fordeler og ulemper som følger av tjenesteutsettingen.

Tilgang på kompetanse er et viktig element når tjenesteutsetting skal vurderes. NSM påpeker at det er et økende gap mellom behov for og tilgang på sikkerhetskompetanse, og at dette utgjør en nasjonal sårbarhet. Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan redusere sårbarheten og bidra til bedre sikring av IKT-systemer og andre verdier.

NSM presiserer at tjenesteutsetting krever gode risikovurderinger og høy bestillerkompetanse. De ser at der sårbarheter lukkes, åpnes ofte nye. Likevel anbefaler NSM tjenesteutsetting, inkludert skytjenester, forutsatt at det gjøres grundige risikovurderinger.

baserte tjenester som er fullautomatiserte, og som kan skaleres opp og ned etter behov, har dette blitt ytterligere aktualisert (se boks 12.1).

Det finnes enkelte virkeområder i samfunnet som er regulert av lover og forskrifter som begrenser muligheten for offshoring (eksempelvis sikkerhetsloven og arkivloven). For øvrig gjelder en grunnleggende forutsetning om at den som skal gjennomføre en tjenesteutsetting, gjør en grundig risikovurdering knyttet til tiltaket og sikrer at uakseptabel risiko håndteres gjennom relevante avbøtende tiltak. NSM har utarbeidet en egen rapport om hvordan denne risikoen kan håndteres når det gjelder tjenesteutsetting til utlandet.[5] Dersom en tjeneste skal leveres fra utlandet, anbefaler NSM at virksomheten vurderer landets statlige styringsindikatorer, IKT-sikkerhetstilstanden, IKT-infrastruktur og kompetanse samt forretningsstabilitet.

Sikkerhet kan også være en driver for tjenesteutsetting, særlig med fremveksten av skytjenester fra store, anerkjente IT-selskaper. Gitt at virksomheten har vurdert risiko og gjennomført tiltak for å bøte på risiko, vil tilgangen til store, profesjonelle sikkerhetsmiljø hos driftsleverandøren erfaringsmessig gi bedre sikkerhet, fordi kompetansen er større, sikringstiltakene er flere, og tjenester og løsninger i bruk er oppdatert til siste versjoner. I tillegg kommer det at denne typen tjenester baserer seg på standardisert teknologi, hvor leverandøren alltid sørger for løpende oppdatering.

Samtidig medfører tjenesteutsetting et endret risikobilde for virksomheten. Tjenesteutsetting kan føre til mindre kontroll over de tjenestene som kjøpes, og det stiller krav til effektiv leverandørstyring. Digitale verdikjeder, som det er vanskelig for en virksomhet å ha oversikt over, kan bli enda mer komplekse.

---

5 Nasjonal sikkerhetsmyndighet (2018) *Anbefaling om landvurdering ved tjenesteutsetting*. Må ses i sammenheng med rapporten Nasjonal sikkerhetsmyndighet (2018) *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* og NSM grunnprinsipper for IKT-sikkerhet.

Kapittel 13
Utfordringer med IKT-sikkerhet i tilkoblede produkter og tjenester

Fordeling av ansvar, roller og oppgaver mellom de tverrsektorielle etatene blir stadig utfordret av den teknologiske utviklingen. Digitaliseringen av samfunnet fører til at IKT-sikkerhet blir relevant på nye områder hvor det tidligere ikke var av nevneverdig betydning. Særlig er det en utfordring når det gjelder IKT-sikkerhet i tilkoblede produkter og tjenester (se kapittel 4). Det er forventet en sterk vekst i tingenes internett de neste årene, særlig innenfor bil- og transportbransjen, helsevesenet, detaljhandelen, finans og offentlige myndigheter.[1]

Forbrukerrådet påpeker i sine innspill til utvalget at manglende IKT-sikkerhet i tilkoblede produkter og tjenester kan medføre problemer som identitetstyveri, manipulasjon og svindel. Tjenester og produkter som er utilstrekkelig sikret, kan også utgjøre en trussel mot samfunnssikkerheten.

Myndighetene i Storbritannia har nylig utgitt en rapport hvor de vektlegger de samme utfordringene: Forbrukerens sikkerhet og personvern undergraves av sårbarheten til produkter som er knyttet opp mot internett, og hele økonomien står overfor en økende trussel om større cyberangrep lansert fra store mengder usikre enheter som er tilkoblet internett.[2]

Nkom skriver i sin årlige risikovurdering av ekomsektoren for 2017 at «[d]en forventede massive økningen i IoT vil skape mange nye utfordringer i nettene i årene som kommer. Stor vekst av billig utstyr av dårlig kvalitet, samt tilgang til og effekt av jammeutstyr, vil øke risikoen for forstyrrelser i kritisk trådløs kommunikasjon».[3]

I tillegg til sårbarheter og trusler påpeker EUs IKT-sikkerhetsorgan ENISA at den raske utviklingen av tilkoblede produkter åpner opp for en rekke nye politiske og regulatoriske utfordringer som foreløpig er uløste.[4] En konsekvens av dette er at det finnes få retningslinjer, og at selskaper og produsenter velger sine egne tilnærminger og løsninger i utviklingen av tilkoblede produkter og tjenester som igjen fører til ulike IKT-sikkerhetsutfordringer. Et eksempel er trygghetsalarmer eller GPS-sporing av demente, der digitale løsninger fører til økt sikkerhet for den enkelte. Samtidig er det en fare for at man gjør seg avhengig av teknologien i en slik grad at sikkerheten svekkes om trygghetsalarmen eller GPS-sporingen er utilgjengelig, eller dersom man ikke kan stole på at GPS-koordinatene som kommuniseres er riktige.

13.1 Mangelfull regulering

Det er krevende å regulere IKT-sikkerhet i tilkoblede produkter og tjenester. Forbrukerorganisasjoner som BEUC (den europeiske paraplyorganisasjonen for forbrukerorganisasjoner) og ANEC (europeisk organisasjon som forsvarer forbrukerinteresser i standardiseringsarbeid) hevder at det europeiske produktsikkerhetsregelverket ikke er tilstrekkelig oppdatert eller egnet til å møte sikkerhetsutfordringene med tilkoblede produkter.[5]

Utvalget finner heller ingen hjemler i det norske regelverket som gjør at myndighetene i dag kan tilbakekalle produkter som følge av manglende IKT-sikkerhet, slik for eksempel DSB kan tilbakekalle produkter på grunn av brannfare. I tillegg er det uklart om en forbruker kan kreve å heve et kjøp dersom produktet ikke har tilstrekkelig IKT-sikkerhet. I sum kan det se ut til at dagens regelverk gir svake insentiver for å produsere og

---

1 Consumers International (2016) *Connection and protection in the digital age. The Internet of Things and challenges for consumer protection*.

2 UK Department for Digital, Culture, Media & Sport *(2018) Secure by Design: Improving the cyber security of consumer Internet of Things – Report*, 7 March 2018.

3 Nasjonal kommunikasjonsmyndighet (2017) *EkomROS 2017*.

4 ENISA (2017) *Baseline Security Recommendation for Internet of Things in the context of critical information infrastructure*, November 20, 2017.

5 BEUC/ANEC (2018) *Cybersecurity for connected products.* Position Paper, 2018.

selge forbrukerprodukter med tilstrekkelig IKT-sikkerhet.

13.2 Uklart myndighetsansvar

Det kan synes uklart hvem som har myndighetsansvar for IKT-sikkerhet i tilkoblede produkter. DSB er fag-, forvaltnings- og tilsynsmyndighet for sikkerhet ved produkter og forbrukertjenester etter produktkontrolloven, el-tilsynsloven og brann- og eksplosjonsvernloven.[6] Produktkontrolloven stiller krav om at produkter skal være sikre og ikke utgjøre en uakseptabel risiko for helse- eller miljøskade, og den gjelder alle produkttyper dersom de ikke er underlagt særskilt sektorregelverk.

El-tilsynsloven, som regulerer de fleste elektriske produkter, har tilsvarende målsetting (sikkerhet for liv, helse og materielle verdier). Elektriske produkter tilkoblet internett som ikke er omfattet av særregelverk, som leketøy og elektromedisinsk utstyr, reguleres av ekomloven som forvaltes av Nkom. Tilkoblede produkters behandling av personopplysninger er imidlertid regulert i personopplysningsloven som forvaltes av Datatilsynet.

NSM er sertifiseringsmyndighet for IKT-sikkerhet i produkter og systemer (SERTIT). Dette kan omfatte tilkoblede produkter. Ordningen er imidlertid frivillig, noe som tilsier at det må være et ønske om sertifisering fra den som skal anskaffe produktet, eller fra produsenten eller leverandøren. Sertifisering kan også skje med utgangspunkt i at det stilles krav om dette i regelverk. Ordningen, som er del av et internasjonalt arrangement for sertifisering, benyttes i liten grad av norske aktører. Utenom sikkerhetsloven har det i liten grad vært stilt krav om sertifisering av IKT-produkter og -systemer i norsk regelverk.

Det er vanskelig å vite til hvem og hvordan man skal varsle dersom man oppdager alvorlige IKT-sikkerhetshull i slike produkter. Det kan også være en utfordring at forskjellige regelverk og tilsynsmyndigheter ofte er relevante for ett og samme tilkoblede produkt. Dette kan føre til at ingen myndigheter tar tak i saker der produkter mangler IKT-sikkerhet, eller at saker blir en kasteball mellom flere myndigheter. I 2016 erfarte for eksempel Forbrukerrådet at ingen tilsyn tok tak i klager på manglende sikkerhet i lekene Cayla og I-que, til tross for kontakt med DSB, Forbrukerombudet, Nkom og Datatilsynet.[7]

Ifølge Forbrukerrådets innspill til utvalget etterspør importører og forhandlere råd og veiledning for å forebygge at tilkoblede produkter uten tilstrekkelig IKT-sikkerhet kommer på det norske forbrukermarkedet. Det er uavklart hvilken rolle det offentlige skal ha i dette, og hvilken myndighet som eventuelt skal ha et tydelig ansvar.

Mens det foreligger varslingssystem for giftige produkter, slik at myndighetene på tvers av landegrenser kan ta tak i denne typen produkter i sitt marked, er det uklart om det finnes eller planlegges noe tilsvarende varslingssystem for produkter med store IKT-sikkerhetsmangler.[8] Ifølge Forbrukerrådet virker håndheving på tvers av landegrenser lite effektivt. Hvert lands tilsyn må gjøre egne tid- og ressurskrevende vurderinger for å kunne handle på enkeltklager.

13.3 Offentliggjøring av digitale sårbarheter

En annen utfordring er knyttet til i hvilken grad og hvor koordinert man skal offentliggjøre digitale sårbarheter i forskjellige informasjonssystemer, programvarer eller andre IKT-produkter. Alle IKT-produkter og all programvare har sårbarheter. En forutsetning for å redusere og rette opp slike sårbarheter er at de er kjent. Videre må leverandørene sørge for å gjøre sikkerhetsoppdateringene sine tilgjengelige, slik at forbrukere og offentligheten kan ta sine forholdsregler.

Det er imidlertid mange ulike hensyn som må veies opp mot hverandre. Fullstendig åpenhet om digitale sårbarheter i et produkt eller en tjeneste kan bety åpenbare sikkerhetsutfordringer. Produsenter eller selgere ønsker kanskje ikke å vise offentlig frem svakheter ved sine produkter, selv om de i utgangspunktet ønsker å rette opp sårbarhetene. På grunn av lange digitale verdikjeder er det heller ikke alltid mulig å finne ut hvor sårbarhetene ligger, og hvem som er ansvarlig for dem.

---

6 Produktkontrolloven (lov 11. juni 1976 nr. 79 om kontroll med produkter og forbrukertjenester). Brann- og eksplosjonsvernloven (lov 14. juni 2002 nr. 20 om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver).

7 Forbrukerrådet (2016) *Cayla og i_que bryter flere norske lover.* Se også ISO/IEC 29147:2014 *Information technology – Security techniques – Vulnerability disclosure.*

8 European Commission *Rapid Alert System for Dangerous non-food Products.*

I flere land har man imidlertid begynt å utarbeide retningslinjer for hvordan man skal få til en mer styrt tilnærming til å ta imot varsler og offentliggjøre digitale sårbarheter. Nederland er et eksempel der de har etablert et system med ansvarlig offentliggjøring (såkalt «Responsible Vulnerability Disclosure Guidelines»).[9] I Norge mangler vi en slik tilnærming, og det er uklart hvilken myndighet som er ansvarlig for å ta tak i problemstillingene.

---

9 National Cyber Security Centrum (2018) *Coordinated Vulnerability Disclosure: the Guideline*.

Del IV
Tiltak og anbefalinger

Kapittel 14
Innledning

IKT-sikkerhet som en samfunnsutfordring er omtalt i både stortingsmeldinger og proposisjoner de siste årene. En overordnet problemstilling som trekkes opp, er at digitaliseringen gir et komplekst samfunn, der digitale verdikjeder går på tvers av både sektorer og landegrenser. Trusler og sårbarheter kan vanskelig knyttes til enkelte sektorer, og det er mange private aktører som eier og drifter kritisk IKT-infrastruktur. Kompleksiteten gjør det utfordrende å ivareta IKT-sikkerheten i samfunnet.

Samtidig er teknologien i kontinuerlig endring. Man kan si at det er en systematisk forsinkelse mellom teknologiutvikling på den ene siden og organisasjonsutvikling og regelverksutvikling på den andre.

Teknologiutviklingen og digitaliseringen av samfunnet synliggjør nye sårbarheter og gir et endret trusselbilde. Like fullt er våre grunnleggende samfunnsverdier, som befolkningens trygghet, nasjonal sikkerhet og økonomisk vekst og utvikling, de samme.

Utvalget ønsker gjennom anbefalingene som fremmes nedenfor, å bidra til forsvarlig nasjonal IKT-sikkerhet. En overordnet målsetting er at Norge som samfunn må sørge for å videreutvikle vår evne til å forebygge og håndtere uønskede digitale hendelser.

Utvalget legger tre overordnede prinsipper til grunn for sine anbefalinger. Disse omfatter hvordan myndighetens arbeid med IKT-sikkerhet bør være, noe som igjen gir retning og støtte for en hensiktsmessig organisering og regulering på IKT-sikkerhetsområdet.

For det første må arbeidet med IKT-sikkerhet ha en *risikobasert tilnærming*. Det betyr at både regulering og organisering må innrettes slik at vesentlig risiko på IKT-sikkerhetsområdet prioriteres. Risikobildet på området vil være i endring over tid, og både regulering og organisering må jevnlig evalueres opp mot hvordan de ivaretar de alvorligste risikoene i det rådende risikobildet.

For det andre må arbeidet med IKT-sikkerhet *balansere sikkerhet* opp mot brukervennlighet, økonomi og grunnleggende menneskerettigheter. Sikkerhet må ikke gis forrang for enhver pris og skal heller ikke i urimelig grad forstyrre brukeropplevelsen og effektiviteten til en digital tjeneste. IKT-sikkerhet må tilpasses behovene, og både organisering og regulering må være proporsjonal med den aktuelle trusselen. Kostnader og ulemper ved risikoreduserende tiltak må sees i sammenheng med effekt og nytte. En slik balanse vil innebære at noe risiko må aksepteres for å oppnå økonomiske og sosiale mål.

For det tredje krever arbeidet med IKT-sikkerhet en *fleksibilitet* i reguleringen og organiseringen. Kompleksiteten og de tverrsektorielle utfordringene ved IKT-sikkerhet gjør det vanskelig med et for statisk regelverk eller en for fastlåst organisering av etater. Både organisering og regulering må være fleksibel og kunne tilpasses nye trusler, sårbarheter, teknologier og forretningsmodeller.

Utvalget vil i denne delen vurdere og drøfte fem hovedanbefalinger som bidrar til forsvarlig nasjonal IKT-sikkerhet i Norge:

- Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
- Krav om IKT-sikkerhet ved anskaffelser
- Etablere et nasjonalt IKT-sikkerhetssenter
- Tydelig regulering og ansvar for tilkoblede produkter og tjenester
- Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Utvalget er i mandatet bedt om å se på virkemidlene regulering og organisering. I anbefalingene kommer utvalget også inn på pedagogiske virkemidler ettersom rådgivning og veiledning til virksomheter inngår som et sentralt element i alle anbefalingene.

Kapittel 15
Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Digitalisering av samfunnet gjør at virksomheter står overfor et stadig mer komplekst IKT-risikobilde. For at et digitalt samfunn som det norske skal fungere, er det nødvendig å minimere risikoen for at utilsiktede og tilsiktede hendelser rammer IKT-systemer. Til tross for potensielt alvorlige konsekvenser for en virksomhets økonomi, sikkerhet og omdømme, har virksomheter ikke alltid tilstrekkelige insentiver til å beskytte seg selv mot digitale trusler. Etter utvalgets vurdering har Norge en mangelfull regulering av IKT-sikkerhet. Dette er drøftet i kapittel 10.

Utvalget foreslår i dette kapittelet en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning. Nedenfor diskuterer utvalget virkeområdet for loven og sikkerhets- og varslingskrav. Utvalget diskuterer også hvordan man kan sikre etterlevelse av den nye loven og forholdet til eksisterende lover og forskrifter.

Utvalget mener at det er behov for å styrke IKT-sikkerheten også for virksomheter som ikke vil omfattes av den nye loven, noe som drøftes nærmere i punkt 15.6. Hvorvidt rettslige krav om forsvarlig IKT-sikkerhet er et hensiktsmessig virkemiddel også for disse virksomhetene drøftes et stykke på vei.

Utvalget har følgende anbefalinger:

- Utarbeide ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning.
  - Den nye loven skal gjennomføre NIS-direktivet i norsk rett.
  - Den nye loven skal gjelde for samfunnskritiske virksomheter, offentlig forvaltning og virksomheter som omfattes av NIS-direktivet.
  - Den nye loven skal stille krav om forsvarlig IKT-sikkerhet. Kravene bør konkretiseres i forskrift og veiledning.
  - Den nye loven skal stille krav om varsling av uønskede digitale hendelser.
  - Det skal føres tilsyn med etterlevelsen av den nye loven.
  - Justis- og beredskapsdepartementet må sørge for koordinert veiledning til loven, herunder vurdere en sertifiseringsordning.
  - Fremtidige regelverk må harmoniseres med kravene i den nye loven.
- Sette ned et lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter.

15.1 Virkeområde

15.1.1 Relevante lover

Mange tverrsektorielle og sektorvise lover og forskrifter regulerer deler av det som inngår i forsvarlig IKT-sikkerhet. Det er særlig den nye sikkerhetsloven og personopplysningsloven som bidrar til å oppfylle behovet for en tverrsektoriell regulering av IKT-sikkerhet. Som drøftet i kapittel 10 er det noen mangler ved begge de to lovene, som gjør at behovet ikke er dekket fullt ut.

Justis- og beredskapsdepartementets utkast til NIS-lov er også relevant i denne sammenheng. Loven skal gjennomføre NIS-direktivet i norsk rett. Lovutkastet retter seg mot virksomheter som leverer tjenester som er viktige for et velfungerende samfunn og næringsliv.[1] Loven skal gjelde for to kategorier virksomheter. Den første kategorien er «tilbydere av samfunnsviktige tjenester» innenfor sektorene energi (elektrisitet, olje og gass), transport (luft, jernbane, sjø og vei), helse (helsetjenester), bank, finansmarkedsinfrastruktur, drikkevannsforsyning- og distribusjon og digital infrastruktur. Den andre kategorien er «tilbydere av digitale tjenester», nærmere bestemt nett-

[1] Justis- og beredskapsdepartementet *(2018) Utkast til høringsnotat om NIS-lov.*

baserte markedsplasser, nettbaserte søkemotorer og skytjenester.

I utkastet til NIS-lov er det tre vilkår som må oppfylles for at en virksomhet skal anses som tilbyder av en samfunnsviktig tjeneste: Virksomheten må tilby en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter, tjenesteleveransen må være avhengig av nettverk og informasjonssystemer, og en hendelse i virksomhetens nettverk og informasjonssystemer må få vesentlig forstyrrende virkning på leveransen av den samfunnsviktige tjenesten. Hvilke konkrete virksomheter som i Norge vil inngå i denne kategorien, er ikke fastsatt på det nåværende tidspunkt.

Justis- og beredskapsdepartementet skriver i utkast til høringsnotat om NIS-lov at det endelige virkeområdet skal fastlegges gjennom en identifiseringsprosess. Departementet har gitt NSM i oppdrag å utarbeide mer konkrete kriterier for hvilke virksomheter som skal omfattes. Der det er mulig, skal det utarbeides terskelverdier innenfor hver enkelt sektor. Berørte sektormyndigheter og andre aktuelle aktører skal involveres i arbeidet. Justis- og beredskapsdepartementet ser for seg at en slik liste tas inn i en forskrift til den foreslåtte loven.[2] For tilbydere av digitale tjenester skal det ikke gjennomføres en tilsvarende identifikasjonsprosess.[3]

[2] Ibid.

[3] Se nærmere om hvem som er i denne kategorien i European Commission (2017) *COM (2017) 476 final/2, Making the most of NIS – towards the effective implementation of Directive* og den svenske Myndigheten för samhällsskydd och beredskap (2018) *Redovisning av vissa vidtagna åtgärder för att förbereda genomförandet av NIS-direktivet.*

15.1.2 Utvalgets vurdering

Det fremgår ikke av NIS-direktivet, Justis- og beredskapsdepartementets utkast til NIS-lov eller sikkerhetsloven hvilke konkrete virksomheter som skal omfattes av regelsettene. I stedet vises det til ulike prosesser for å identifisere og peke ut virksomheter. Ingen av disse prosessene er foreløpig ferdige. På bakgrunn av dette har ikke utvalget et tilstrekkelig grunnlag for å identifisere hvilke konkrete virksomheter som må ha forsvarlig IKT-sikkerhet.

Utvalget drøfter i det videre hvilke typer virksomheter som bør omfattes av en ny lov om IKT-sikkerhet.

15.1.2.1 Samfunnskritiske virksomheter

Noen virksomheter leverer tjenester som har særlig betydning for opprettholdelsen av et velfungerende og trygt samfunn. Dette er tjenester som andre deler av samfunnet er avhengig av. Det er vanlig å bruke begrepet kritisk når avhengigheten er så stor at det kan få alvorlige konsekvenser for samfunnet om tjenesten faller bort. Hvilke virksomheter som er kritiske for samfunnet, beror på en vurdering av kritikaliteten og funksjonaliteten til den tjenesten som virksomheten leverer.

DSB utarbeidet i 2016 på oppdrag fra Justis- og beredskapsdepartementet en rapport med oversikt over samfunnets kritiske funksjoner (se boks 15.1). Regjeringen benytter blant annet oversikten når den fordeler ansvar mellom departementene for tverrsektorielle områder i samfunnssikkerhetsarbeidet.[4] Samme oversikt benyttes også i

Boks 15.1 DSBs rapport om samfunnets kritiske funksjoner[1]

DSBs rapport om samfunnets kritiske funksjoner gir en oversikt over hvilke funksjoner som er kritiske for samfunnssikkerheten, og beskriver hvilken funksjonsevne det må planlegges for å opprettholde uansett hva som måtte inntreffe. Hensikten med oversikten er å legge til rette for et mer målrettet samfunnssikkerhetsarbeid. Målgruppen for rapporten er virksomheter som har ansvar for de funksjonene som er kritiske for samfunnssikkerheten.

Til sammen defineres 14 kritiske samfunnsfunksjoner: Kraftforsyning, transport, finansielle tjenester, forsyningssikkerhet, elektroniske kommunikasjonstjenester, vann og avløp, satellittbaserte tjenester, styring og kriseledelse, forsvar, lov og orden, helse og omsorg, redningstjenester, IKT-sikkerhet samt natur og miljø.

I rapporten er samfunnsfunksjonene gruppert etter hvordan de bidrar til å ivareta befolkningens sikkerhet og trygghet. Innenfor hver samfunnsfunksjon er det definert «kapabiliteter» som beskriver den funksjonsevnen samfunnet må være i stand til å opprettholde til enhver tid.

[1] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner.*

Tabell 15.1 Funksjoner som er tatt med i DSBs rapport om samfunnets kritiske funksjoner og i Justis- og beredskapsdepartementets utkast til NIS-lov

DSBs rapport om samfunnets kritiske funksjoner	Justis- og beredskapsdepartementets utkast til NIS-lov
Kraftforsyning	Energi
Transport	Transport
Finansielle tjenester	Bank
Forsyningssikkerhet	Finansmarkedsinfrastruktur
Helse og omsorg	Helse
Vann og avløp	Drikkevann
Elektroniske kommunikasjonstjenester	Digital infrastruktur
Satellittbaserte tjenester	Digitale tjenester
Styring og kriseledelse	
Forsvar	
Lov og orden	
Redningstjenester	
IKT-sikkerhet	
Natur og miljø	

ulike stortingsmeldinger, blant annet i siste stortingsmelding om samfunnssikkerhet.[5]

Utvalget mener at DSBs oversikt over samfunnets kritiske funksjoner på en god måte beskriver og begrunner hvilke funksjoner som er kritiske for samfunnet. Med dette som utgangspunkt blir det også kritisk for samfunnet at virksomhetene som har ansvaret for, understøtter eller på annen måte er en del av samfunnskritiske funksjoner, klarer å levere sine tjenester. En samlebetegnelse på disse virksomhetene er *samfunnskritiske virksomheter.*

Utkastet til Justis- og beredskapsdepartementets NIS-lov har langt på vei samme tilnærming til hvilke funksjoner som er særlig viktige for samfunnet. Tabell 15.1 viser hvilke samfunnskritiske funksjoner DSBs rapport fremhever, og hvilke samfunnssektorer som omfattes av utkastet til NIS-lov.

Utvalget har merket seg at EU-kommisjonen, i dokumentet *Making the most of NIS*, foreslår at medlemsstatene selv skal vurdere å inkludere flere samfunnssektorer ved gjennomføringen av direktivet, herunder offentlig forvaltning.[6] Det fremgår også av direktivet at man i nasjonal lovgivning kan ha et bredere virkeområde enn det som følger av direktivet.

Utvalgets gjennomgang av regulering av IKT-sikkerhet i andre land (se vedlegg 3), viser at flere av disse i løpet av de siste årene har utarbeidet regelverk som stiller krav til IKT-sikkerhet i kritiske samfunnsfunksjoner.

Gitt det gjeldende IKT-risikobildet mener utvalget at alle samfunnskritiske virksomheter må ha forsvarlig IKT-sikkerhet. Utvalget mener derfor at det må stilles krav i lov om forsvarlig IKT-sikkerhet til alle samfunnskritiske virksomheter.

15.1.2.2 Offentlig forvaltning

En rekke offentlige virksomheter er samfunnskritiske virksomheter, og de blir gjennom utvalgets anbefaling i punkt 15.1.2.1 underlagt krav om forsvarlig IKT-sikkerhet.

Etter utvalgets syn er det imidlertid flere offentlige virksomheter som har stor samfunnsmessig betydning. Som nevnt i kapittel 10 stilles det per i dag ikke tilfredsstillende krav om sikring av IKT-systemer som understøtter offentlige virksomheters tjenesteleveranser.

Utvalget vil i det følgende vurdere behovet for å stille krav om forsvarlig IKT-sikkerhet til alle offentlige virksomheter. I sin veiledning til NIS-direktivet uttaler EU-kommisjonen at det vil være fornuftig å vurdere å inkludere hele den offentlige forvaltning ved utarbeidelsen av et nasjonalt regelverk som skal gjennomføre direktivet. Kommisjonen viser til at:[7]

4 Prop. 1 S (2017–2018) *Justis- og beredskapsdepartementet*, s. 42–43.

5 Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*

6 European Commission (2017) *COM (2017) 476 final/2, Making the most of NIS – towards the effective implementation of Directive*. s. 23.

7 Ibid.

> Public administrations are responsible for the proper delivery of public services provided by governmental bodies, regional and local authorities, agencies and associated enterprises. These services often imply the creation and management of personal and corporate data about individuals and organisations, which can be shared and made available to multiple public entities. More broadly, a high level of security of network and information systems used by public administrations is an important interest for the society and economy as a whole.

Utvalget mener det er flere gode grunner for å inkludere offentlig forvaltning i den nye loven om IKT-sikkerhet.

For det første tilbyr forvaltningen viktige tjenester til befolkningen. For å levere disse tjenestene er forvaltningen i stor grad avhengig av at IKT-systemene som understøtter tilbudet til befolkningen virker. Hvis disse ikke er tilstrekkelig sikret vil det medføre en risiko for at befolkningen ikke får tjenestene de trenger. Utvalget mener dette alene er en god grunn for å stille krav om forsvarlig IKT-sikkerhet til offentlig forvaltning.

For det andre har forvaltningen en sentral og viktig rolle i digitaliseringen av samfunnet. Utvalget mener krav om forsvarlig IKT-sikkerhet for hele forvaltningen kan sees i sammenheng med regjeringens politikk slik den kommer til uttrykk i *Digital agenda for Norge*.[8] Alle deler av offentlig sektor må ha tilstrekkelig IKT-sikkerhet for at digitale løsninger skal fungere. Befolkningen må kunne stole på at den digitale forvaltningen er trygg. Etter utvalgets syn, er det å sikre digitale tjenester en nøkkelfaktor for å skape nødvendig tillit. Befolkningens tillit til det offentlige er videre sentralt for å sikre en vellykket digitalisering av samfunnet, som igjen bidrar til økonomisk vekst.[9] Utvalget mener derfor at forsvarlig IKT-sikkerhet er en forutsetning for en vellykket digitalisering av offentlig sektor. En felles tilnærming til IKT-sikkerhet er nødvendig for økt digital samhandling i offentlig sektor og med brukere av offentlige tjenester.[10]

For det tredje mener utvalget at det å underlegge offentlig forvaltning den nye loven vil føre til bedre etterlevelse av kravene om IKT-sikkerhet. Når lov, forskrift og veiledere er koordinerte vil det bli tydeligere hvilke krav som gjelder. Den nye loven vil også ha hjemler for å kunne kontrollere etterlevelsen med kravene om IKT-sikkerhet. Tilsyn og sanksjoner, sammen med veiledning og rådgiving, kan bidra til mindre grad av etterlevelsesillusjon i offentlig forvaltning og bedre faktisk IKT-sikkerhet (se punkt 7.1).

Når det gjelder konsekvensene av å innlemme hele offentlige forvaltning i den nye loven er det flere usikkerhetsfaktorer. Som vist i kapittel 10 stiller gjeldende lover og forskrifter i varierende grad krav om IKT-sikkerhet. Det er imidlertid vanskelig å anslå hvor store endringer et nytt krav om forsvarlig IKT-sikkerhet faktisk vil føre til. Utvalget antar at for store deler av offentlig forvaltning vil det å bli underlagt kravene i den nye loven medføre en opprydding i eksisterende lovgiving, snarere enn et ytterligere krav.

Samlet sett mener utvalget at offentlig forvaltning derfor bør inkluderes i den nye loven om IKT-sikkerhet.

15.2 Sikkerhetskrav

15.2.1 Sikkerhetskrav i utkastet til NIS-lov

Det følger av Justis- og beredskapsdepartementets utkast til NIS-lov at virksomheten plikter å gjennomføre en risikovurdering av de IKT-systemene som benyttes for å levere den samfunnsviktige tjenesten. Dette betyr at virksomheten må foreta en vurdering av hvilke IKT-systemer den er avhengig av for å levere sine tjenester. Dermed kan det være at bare noen IKT-systemer må sikres.

Med utgangspunkt i risikovurderingen skal virksomheten iverksette hensiktsmessige og proporsjonale sikkerhetstiltak for å redusere risikoen. Videre skal det iverksettes tiltak som er egnet til å forebygge, avdekke og redusere konsekvensene av hendelser.[11]

Kravene i utkastet til NIS-lov er funksjonsbaserte og overordnede. For å forstå nærmere hva som skal til for å være i samsvar med kravene er det behov for nærmere presisering. Det er ingen nærmere beskrivelse av sikkerhetskravene i høringsnotatet, utover at det konstateres at det er samsvar mellom kravene i NIS-direktivet og utkastet til NIS-lov. Departementet uttaler imidler-

---

8 Meld. St. 27 (2015–2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.*

9 Meld. St. 39 (2012–2013) *Mangfold av vinnere.*

10 Kommunal- og moderniseringsdepartementet (2015) *Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015–2017*, s. 11.

11 En veiledning til sikkerhetskravene som følger av NIS-direktivet, er under utarbeidelse av NIS Cooperation Group.

tid at NSMs grunnprinsipper for IKT-sikkerhet gir god veiledning i grunnleggende IKT-sikkerhet, og at veiledningen er et godt utgangspunkt for å ha tilstrekkelig god digital sikkerhet i virksomheten. Departementet peker også på at det er viktig å se IKT-sikkerhet i sammenheng med virksomhetens mer generelle sikkerhetsstyringssystem og virksomhetens overordnede styringssystem.

15.2.2 Utvalgets vurdering

Utvalget mener det er hensiktsmessig å ta utgangspunkt i sikkerhetskravene som følger av Justis- og beredskapsdepartementets utkast til NIS-lov.

Utvalget har vurdert hvilke systemer som skal underlegges sikkerhetskrav. Det har deretter vurdert innholdet og detaljeringsgraden i sikkerhetskravene. Utvalget kommer også med betraktninger om behovet for forskrifter og veiledning.

15.2.2.1 IKT-systemer som skal sikres

I henhold til utkastet til NIS-lov skal det gjennomføres risikovurdering av de nettverkene og informasjonssystemene som benyttes for å levere en samfunnskritisk tjeneste. Med andre ord vil høyst sannsynlig ikke alle IKT-systemer omfattes av utkastet til lov. For eksempel vil IKT-systemer som brukes til trafikkavvikling på en flyplass, måtte sikres. IKT-systemene som brukes til å behandle lønn trenger det ikke.

Det følger av NSMs grunnprinsipper at man skal ha kontroll på egen IKT-infrastruktur, ikke bare «viktige» systemer. Man må kjenne til alle sammenkoblinger og hvilke systemer som har tilgang hvor. Store mengder informasjon er lagret i administrative systemer, databaser og andre tilknyttede IKT-systemer. Dette er informasjon som er viktig for driften av virksomhetene. Den kan være nyttig for uvedkommende, som kan bruke den til å komme seg videre inn til de viktige systemene.

Administrative støttesystemer kan være fysisk koblet sammen med industrikontrollsystemer, men separert logisk. Ulik praksis og kompetanse hos virksomhetene og deres leverandører gjør at virksomhetene i ulik grad er eksponert for digitale trusler.[12] Videre vil kompleksiteten i dagens IKT-strukturer kunne medføre at hendelser i mindre kritiske IKT-systemer raskt kan spre seg til mer kritiske systemer. Dersom alle IKT-systemene til virksomheten er underlagt de samme kravene til forsvarlig IKT-sikkerhet, kan det gjøre arbeidet med IKT-sikkerhet mer oversiktlig. Dette taler for at alle virksomhetens IKT-systemer bør sikres forsvarlig.

Utvalget har imidlertid ikke hatt mulighet til å vurdere konsekvensen av å stille et slikt omfattende krav, og det må derfor utredes før det eventuelt inngår i den nye loven om IKT-sikkerhet.

15.2.2.2 Innholdet og detaljeringsgrad i sikkerhetskravene

I Justis- og beredskapsdepartementets utkast til NIS-lov er det krav om at virksomheten skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak for å redusere sin risiko. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et passende sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen. For å opprettholde tjenesteleveransen skal virksomheten iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser.

For å avklare hva som er innholdet i kravene har utvalget sett på andre lands veiledere til NIS-direktivet. Blant annet har IKT-sikkerhetssenteret i Storbritannia utarbeidet en veiledning til NIS-direktivet. Utvalget har vurdert at den har de samme hovedpunktene som NSMs grunnprinsipper for IKT-sikkerhet:[13]

1. Identifisere og kartlegge – gjør risikovurdering
2. Beskytte – sikre verdiene dine
3. Opprettholde og oppdage – vær bevisst
4. Håndtere og gjenopprette – lær av utfordringene dine

Utvalget mener at det kan legges til grunn at sikkerhetskravene som følger av utkastet til NIS-lov er en hensiktsmessig regulering av forsvarlig IKT-sikkerhet.

Å stille krav om forsvarlig IKT-sikkerhet i en lov kan virke klargjørende for mange virksomheter. Mange aktører har uttrykt at det er vanskelig å vite hvilke krav de skal forholde seg til, fordi dagens regelverk oppfattes som omfattende og fragmentert, og det er for få presise krav til IKT-sikkerheten. Detaljerte rettslige krav om forsvarlig IKT-sikkerhet, som omfatter de ulike elementene ved

[12] Norges vassdrags- og energidirektorat (2017) *Regulering av IKT-sikkerhet* 2017/26 s. 119.

[13] IKT-sikkerhetssenteret i Storbritannias veiledning til GDPR har de samme fire hovedpunktene. National Cyber Security Center (2018) *GDPR Security Outcomes.*

IKT-sikkerheten, kan bidra til økt bevissthet og forenkle implementeringen i virksomhetene. Det vil gi et bedre beslutningsgrunnlag for lederne av virksomhetene og være til hjelp for dem som skal sette opp systemene og tjenestene.

Utfordringen med detaljerte krav om forsvarlig IKT-sikkerhet er at det kan bli veldig omfattende, fordi det skal dekke mange ulike forhold. Kravene til forsvarlig IKT-sikkerhet skal i minst mulig grad sette begrensninger for en virksomhets bruk av ny teknologi. En mulig løsning er da, slik det er gjort i utkastet til NIS-lov, at loven kun angir hovedpunktene i sikkerhetskravene.

På den annen side har flere respondenter i utvalgets informasjonsinnhenting spilt inn at et funksjonsbasert regelverk er vanskelig å etterleve. Mange har ikke tilstrekkelig kompetanse til å etterleve et slikt regelverk, som gjennomgående innebærer at kravene er overordnede og vage. For vage krav kan medføre dårligere etterlevelse på grunn av usikkerhet rundt hva som kreves for å oppfylle kravet. Utfordringene ved et funksjonsbasert regelverk er nærmere diskutert i punkt 7.1.

Samtidig er det avgjørende i utformingen av sikkerhetskrav at de blir fleksible nok til å møte et IKT-risikobilde i stadig endring. Kompleksiteten og de tverrsektorielle utfordringene ved IKT-sikkerhet tilsier at det ikke er hensiktsmessig med for statiske sikkerhetskrav. De må være fleksible og kunne tilpasses nye trusler, sårbarheter, teknologier og forretningsmodeller. Sikkerhetskravene må være robuste overfor teknologi- og samfunnsutviklingen.

Utvalget mener derfor at sikkerhetskravene må være overordnede og funksjonsbaserte, slik det fremgår av utkastet til NIS-lov. Sikkerhetskravene i utkastet omfatter tiltakene som inngår i NSMs grunnprinsipper. Etter utvalgets oppfatning stiller dermed utkastet til NIS-lov krav om forsvarlig IKT-sikkerhet. Innholdet i utkastets sikkerhetskrav er dermed tilfredsstillende.

For å avhjelpe utfordringene med funksjonelle og overordnede krav anbefaler utvalget at det utarbeides forskrifter som angir hvilke tekniske og organisatoriske tiltak som kan gjøres for å oppfylle funksjonalitetskravene.

Andre tiltak for å bedre forståelsen av hva som ligger i kravet til forsvarlig IKT-sikkerhet, er veiledning, rådgivning eller en form for sertifisering. Utvalget har vurdert dette nærmere i punkt 15.4 om etterlevelse.

Det er verdt å merke seg at sikkerhet i anskaffelser er en viktig del av virksomhetens arbeid med IKT-sikkerhet. Dette fremgår både av NSMs grunnprinsipper for IKT-sikkerhet og av veiledningen fra cybersikkerhetssenteret i Storbritannia. Sikkerhet ved anskaffelser drøftes nærmere i kapittel 16.

15.3 Krav om varsling av hendelser

Justis- og beredskapsdepartementets utkast til NIS-lov pålegger virksomhetene å varsle om hendelser som har betydelig innvirkning på opprettholdelsen av en gitt tjeneste. I denne vurderingen skal det legges vekt på antall brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen. Varselet skal inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser.

Hensikten med varslingen er for det første at virksomheten som varsler skal kunne få bistand til å håndtere hendelsen. For det andre er varsling nødvendig for at sektorvise myndigheter eller responsmiljøer skal kunne ha oversikt over hendelser innenfor sitt ansvarsområde, og om nødvendig varsle videre til andre virksomheter, nasjonale myndigheter og andre land. For det tredje skal varslinger bidra til bedre kunnskap om sikkerhetstilstanden, som er nyttig i myndighetenes mer generelle arbeid med IKT-sikkerhet.

Utvalget mener at dette varslingskravet er hensiktsmessig for alle som omfattes av den nye loven om IKT-sikkerhet. Hvor omfattende varslingsplikten skal være, hvem som skal være mottaker, og hva varselet skal bestå av, er noe utvalget mener bør vurderes nærmere.

15.4 Etterlevelse

For å sikre etterlevelse av den nye loven om IKT-sikkerhet kan virkemidler både i og utenfor loven benyttes. Tilsyn og sanksjoner vurderes først, siden det er bestemmelser om dette i Justis- og beredskapsdepartementets utkast til NIS-lov. Videre vurderes veiledning og sertifisering. Rapporteringskrav drøftes i punkt 15.7.

15.4.1 Tilsyn

Utkastet til NIS-lov legger opp til at det skal utpekes en eller flere tilsynsmyndigheter som skal føre tilsyn med etterlevelsen av loven. Det skal være forskjellige tilsynsregimer for henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Tilsynsregimet for førstnevnte er av tradisjonell karakter, mens det for til-

bydere av digitale tjenester vil føres tilsyn kun etter at det er fremkommet mistanke om brudd på lovens krav.

Utkastet til NIS-lov hjemler at tilsynsmyndigheten etter pålegg får de opplysningene den krever for å utføre oppgavene sine.

Å føre tilsyn med et funksjonsbasert regelverk er krevende for tilsynsmyndighetene. Funksjonskravene må fortolkes for å komme frem til et konkret innhold i rettsreglene, men funksjonskravene gjør også at tilsynsobjektene får større frihet til å finne løsninger som er optimale for virksomheten.[14] Når regelverket er funksjonsbasert, er det viktig at tilsynsmyndighetene er påpasselig med rolleforståelsen for når de fører tilsyn og når de gir veiledning, siden regelverket åpner for frihet for tilsynsobjektene i oppgaveløsningen.

Et av funnene i Lysne-utvalgets arbeid var at det stilles ulike krav om IKT-sikkerhet fra de ulike myndighetsaktørene. De trakk frem at enkelte myndigheter synes å stille detaljerte krav, mens andre stiller mer åpne krav.[15] Økt teknisk kompleksitet på IKT-området øker utfordringene på tilsynsområdet. Regelverk som ikke henger med i den tekniske utviklingen, gjør at tilsynene mangler retningslinjer å føre tilsyn etter. Økt bruk og avhengighet av IKT er med på å skape kompetanseutfordringer for tilsynene, som tradisjonelt har ført tilsyn som i større grad har vært basert på faglige krav og føringer.[16] Uoversiktlige digitale verdikjeder utfordrer hjemmelsgrunnlaget for tilsyn med relevante underleverandører.

Tilsynsmeldingen pekte på at det finnes alternative ordninger til tradisjonelle statlige tilsyn.[17] Eksempler på dette er ulike sertifiserings- og akkrediteringsordninger. Tilsynsmeldingen peker videre på at det i takt med samfunnsutviklingen bør vurderes om det er mulig å deregulere enkelte områder som til nå har vært underlagt statlig tilsyn. Det kan i stedet vurderes å legge opp til at etterlevelse av regelverket, eller iverksetting av politiske mål, kan kobles til for eksempel forsikringsordninger eller utstedelse av tilstandssertifikater.

Utvalget mener at hjemmelen for å føre tilsyn etter Justis- og beredskapsdepartementets utkast til NIS-lov er vid nok til å dekke behovet for tilsyn også når virkeområdet utvides. Utvalget mener imidlertid at det er viktig at den nye loven også gir hjemmel for å føre tilsyn med underleverandører og å føre teknisk IKT-tilsyn. Det bør vurderes nærmere om tilsynshjemmelen slik den er utformet i utkastet til NIS-lov, kan benyttes til disse formålene.

15.4.2 Sanksjoner

Utkastet til NIS-lov gir hjemmel for tilsynsmyndighetene til å ilegge pålegg, tvangsmulkt og overtredelsesgebyr. Det er ikke hjemmel for straff, som bot eller fengsel. Bestemmelsene skiller ikke mellom tilbydere av henholdsvis samfunnsviktige og digitale tjenester.

I NIS-direktivet fremgår det at medlemsstatene skal fastsette krav i lov eller forskrift om sanksjoner ved brudd på de forpliktelsene som følger av nasjonal lovgivning. Sanksjonene skal være virkningsfulle, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Det er et betydelig nasjonalt handlingsrom når det gjelder utformingen av sanksjonsbestemmelsene.[18]

Den nye loven om IKT-sikkerhet vil ha en pedagogisk verdi som i seg selv kan føre til atferdsendring. Videre vil veiledning og tilsyn være viktige komponenter for å få det til. Utvalget mener imidlertid at det også er viktig at den nye loven har tilstrekkelige sanksjoner.

Det er en sentral retningslinje at et mer inngripende virkemiddel ikke bør brukes hvis det samme målet kan nås med mindre inngripende tilgjengelige virkemidler.[19] Dette gjelder både ved valget mellom bruk av sanksjoner og andre tiltak, og ved valget mellom straff og administrative sanksjoner.[20]

Desto mer diffust et rettslig krav er, desto vanskeligere er det å sanksjonere brudd på en streng måte. Derfor mener utvalget at sanksjoner må vurderes på bakgrunn av diskusjonen om detaljeringsgrad i punkt 7.1 og 15.2. For å skape forutsigbarhet for virksomhetene bør det derfor også knyttes sanksjonsmuligheter for overtredelse av kravene i forskrifter som er hjemlet i loven.

Effekten av sanksjoner er etter utvalgets vurdering illustrert ved innføringen av GDPR i norsk rett, som har fått mye oppmerksomhet det siste året. En av grunnene til oppmerksomheten ligger

---

14 Haugland, Anders (2012) «Bruk av funksjonsbasert regelverk og rettslige standarder», i Lindøe, P.H., Kringen, J., Braut G.S. (2012) *Risiko og tilsyn.*

15 NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.* s. 293.

16 Ibid.

17 St.meld. nr. 17 (2002–2003) *Om statlige tilsyn*, s. 28.

18 European Commission (2017) *COM (2017) 476 final/2, Making the most of NIS – towards the effective implementation of Directive*.

19 Prop. 62 L (2015–2016) *Endringer i forvaltningsloven mv. (administrative sanksjoner mv.)*.

20 Ibid. s. 52.

antakelig i muligheten Datatilsynet har fått til å ilegge store gebyrer. Selve sikkerhetskravene i GDPR, som i dag er nedfelt i personopplysningsloven, er ikke stort annerledes enn de kravene som følger av tidligere lovgivning, og virkeområdet er heller ikke nevneverdig forandret.

I Justis- og beredskapsdepartementets utkast til høringsnotat om NIS-lov foreslås det at sanksjonsbestemmelsene i loven ikke angir hvilken størrelse på gebyret som er aktuelt. Det kommer an på hva slags overtredelse det gjelder, om det har skjedd over tid, og om det er tale om gjentakende handlinger. Det må bero på en konkret vurdering i hver enkelt sak hva som er et passende gebyr. Den aktuelle virksomhetens omsetning kan også vektlegges. Det vil dessuten kunne variere over tid hva som er passende beløpsmessige rammer. Blant annet kan dette påvirkes av rettsutviklingen i EU. Justis- og beredskapsdepartementet foreslår derfor at beløpsrammene fastsettes i forskrift.[21]

Utvalget mener at bestemmelsene i Justis- og beredskapsdepartementets utkast til NIS-lov om pålegg, tvangsmulkt og overtredelsesgebyr dekker behovet for sanksjoner også når virkeområdet utvides. Utvalget mener at Justis- og beredskapsdepartementets forslag om å fastsette beløpsrammene i forskrift er fornuftig, og støtter departementet i den vurderingen som er foretatt.

15.4.3 Veiledning og sertifisering

I det daglige er det ofte andre kilder enn loven som benyttes for å tilegne seg kunnskap om hvilke krav som følger av regelverket.[22] En standard, mal eller veileder som indikerer et nivå for hva som er forsvarlig IKT-sikkerhet, er ofte enklere tilgjengelig enn en lovtekst. Forskjellen er at det ikke vil være rettslig bindende å følge en veileder. Den nye loven om IKT-sikkerhet vil ha funksjonsbaserte krav, som gir større frihet for virksomhetene til å fylle kravene med innhold. Gitt kompetansesituasjonen mener utvalget det er nødvendig å utarbeide et hensiktsmessig veiledningsmateriell. Veiledning bør ta utgangspunkt i NSMs grunnprinsipper, men tilpasses virksomheter på ulike nivåer.

Utvalget mener at myndighetene må gi koordinert veiledning om hvordan kravene i loven skal oppfylles. I tillegg mener utvalget at gitt den begrensede tilgangen på IKT-sikkerhetskompetanse bør det legges til rette for at private aktører også kan tilby rådgivning. Det foreslåtte IKT-sikkerhetssenteret kan være en hensiktsmessig arena for å legge til rette for veiledning og rådgiving, se kapittel 17 for nærmere omtale.

Utvalget mener at det også bør vurderes å opprette en form for sertifiseringsordning for IKT-sikkerhet for å verifisere samsvar med lovens krav. Et eksempel på en sertifiseringsordning er Direktoratet for byggekvalitets «sentral godkjenning», som er en generell godkjenning av et foretaks kvalifikasjoner vurdert opp mot kravene i byggesaksforskriften (SAK10) kapittel 9–11.[23] En annen sertifiseringsordning er å gi godkjenning på bakgrunn av kurs i regelverket. Normen i helsesektoren legger opp til kurs- og opplæringsaktivitet. Direktoratet for e-helse tilbyr to typer kurs: Fagkurs i informasjonssikkerhet og personvern for kommuner og kurs i informasjonssikkerhet basert på Normen for medisinsk-teknisk personell.

Utvalget anbefaler at en sertifiseringsordning bør vurderes nærmere.

15.5 Myndigheter

Utvalget skal i henhold til mandatet vurdere en hensiktsmessig fordeling av de oppgaver som følger av NIS-direktivet. I følge direktivet skal medlemsstatene utpeke eller etablere et nasjonalt kontaktpunkt, en eller flere kompetente myndigheter og et eller flere hendelseshåndteringsmiljøer. For en nærmere beskrivelse av disse organene og deres oppgaver vises det til vedlegg 2, punkt 1.2.
Slik som direktivets krav er utformet, står medlemslandene fritt til å organisere seg slik de vil, så lenge de tre funksjonene er på plass. Gitt gjeldende myndighetsstruktur innenfor IKT-sikkerhet i Norge, er det ikke nødvendig å gjøre strukturelle endringer for å oppfylle direktivets krav.

Utvalget mener at det er flere grunner for at fordelingen av oppgaver som følger av NIS-direktivet i størst mulig grad bør bygge på etablerte myndighetsstrukturer. For det første har utvalgets informasjonsinnhenting ikke avdekket noe åpenbart behov for å gjøre større endringer i ansvar, roller eller oppgaver til de etatene som utvalget har sett nærmere på. For det andre leg-

[21] Justis- og beredskapsdepartementet *(2018) Utkast til høringsnotat om NIS-lov*. s. 63.

[22] Tranvik, Tommy (2012) *Kommunal regeletterlevelse. Illusjoner og realiteter på personvernområdet.* Tidsskrift for samfunnsforskning, nr. 2, s. 131–156.

[23] Byggesaksforskriften. Forskrift 26. mars 2010 nr. 48 om byggesak. Direktoratet for byggkvalitet (2016) *Hva er sentral godkjenning.*

ger den nye sikkerhetsloven viktige rammer for organiseringen. For det tredje er NSM nasjonal fagmyndighet for IKT-sikkerhet, de er sikkerhetsmyndighet i henhold til sikkerhetsloven, og de har ansvaret for NSM NorCERT.

Slik som situasjonen er i dag mener utvalget at det er mest naturlig at NSM får rollen som nasjonalt kontaktpunkt. NSM bør fortsatt ha ansvar for et nasjonalt hendelseshåndteringsmiljø, og sørge for at dette oppfyller direktivets krav om dette. Videre bør de enkelte sektormyndigheter få ansvar som kompetente myndigheter innenfor egen sektor. Direktivet forutsetter at den enkelte kompetente myndighet har tilstrekkelige ressurser og kompetanse til å ivareta et slikt ansvar.

Utvalget mener at de samme argumentene må legges til grunn ved vurderingen av hva som er en passende myndighetsstruktur for forvaltning og oppfølging av den foreslåtte loven om IKT-sikkerhet i samfunnskritiske virksomheter og offentlig forvaltning. Avhengig av organisering av og myndighetsforankring for et fremtidig nasjonalt IKT-sikkerhetssenter, kan det bli nødvendig å flytte ansvaret for enkelte oppgaver som per i dag naturlig hører inn under NSMs portefølje.

15.6 Forholdet til eksisterende lover og forskrifter

Den nye loven om IKT-sikkerhet skal bidra til å avhjelpe de påpekte manglene ved gjeldende lover og forskrifter. I dette punktet vurderes om det også bør gjøres endringer i dagens regelverk, slik at det gjennomgående stilles mer hensiktsmessige krav om IKT-sikkerhet.

En gjennomgang av gjeldende lover og forskrifter kan bidra til at dagens regelverk blir mer oversiktlig, hvilket igjen kan føre til økt IKT-sikkerhet. Utvalget antar imidlertid at et slikt arbeid er omfattende og ressurskrevende, da det er snakk om et relativt stort antall lover og forskrifter. De påpekte manglene er dessuten ikke ensartet.

Utvalget ser ikke at nytten av et slikt arbeid kan forsvare ressursbruken. Med et felles sikkerhetskrav i den nye loven om IKT-sikkerhet innføres det en minimumsstandard for samfunnskritiske virksomheter og offentlig forvaltning. Etter utvalgets syn bør man heller prioritere å bruke ressurser på å sørge for at lovkravene blir etterlevd.

Utvalget mener derimot at det vil være fornuftig at fremtidige regelverk harmoniseres med kravene i den nye loven om IKT-sikkerhet. Det kan blant annet oppnås ved at det stilles krav om slik harmonisering i utredningsinstruksen eller i Justis- og beredskapsdepartementets veileder om lovteknikk og lovforberedelse.[24]

15.7 Lovutvalg for å vurdere en IKT-sikkerhetslov for alle virksomheter

Gjeldende lover og forskrifter møter utfordringene som beskrives i IKT-risikobildet et stykke på vei.[25] Den nye loven om IKT-sikkerhet skal bidra til å styrke den nasjonale IKT-sikkerheten ytterligere.

Selv etter innføringen av en slik lov vil det fortsatt være en rekke virksomheter som ikke er underlagt krav om forsvarlig IKT-sikkerhet. Eksempler på slike virksomheter er bedrifter innenfor oppdrett og havbruk, teknologibedrifter innenfor IT og materialteknikk og virksomheter som driver med foredling og bearbeiding av råvarer, samt leverandører til disse bransjene.

Det kan også være flere andre private rettssubjekter, særlig små og mellomstore virksomheter, som ikke vil være omfattet av krav om forsvarlig IKT-sikkerhet. Privatpersoner er i utgangspunktet ikke underlagt krav om IKT-sikkerhet, med mindre de oppnår skattepliktig inntekt gjennom behandlingen av personopplysninger.

Samtlige IKT-systemer, uavhengig av hvem som eier dem, kan bli utsatt for eller kan benyttes som ledd i uønskede digitale hendelser. I et gjennomdigitalisert samfunn som vårt vil det fortsatt være en betydelig restrisiko selv om samfunnskritiske virksomheter og offentlig forvaltning må etterleve krav om forsvarlig IKT-sikkerhet. Deres avhengighet av lange og komplekse digitale verdikjeder er eksempel på én risiko som lovforslaget og gjeldende rett ikke vil bøte på i tilstrekkelig grad. Selv om en samfunnskritisk virksomhet gjør alt riktig overfor underleverandørene sine, er det fare for at virksomheten ikke kan påvirke risikobildet lenger ute i en lang og kompleks verdikjede. Et digitalt angrep langt ute i verdikjeden kan imidlertid få konsekvenser for den samfunnskritiske virksomheten. Ifølge en undersøkelse utført av Ponemon Institute skjedde så mye som 56 prosent av alle datainnbrudd i 2017 gjennom tredjepartsangrep.[26]

---

[24] Justis- og beredskapsdepartementets lovavdeling (2000) *Lovteknikk og lovforberedelse.*

[25] Se kapittel 3 for nærmere beskrivelse av IKT-risikobildet.

[26] Ponemon (2017) *Third Party Data Risk Study Your Organization Can't Afford to Ignore.*

Ikke bare er det vanskelig for en virksomhet å styre risikoen i en slik verdikjede, det er også utfordrende å kartlegge verdikjeden. Når det skal vurderes hvordan disse utfordringene kan møtes, er det vanskelig å avgrense hvem som må ha bedre IKT-sikkerhet.

Etter utvalgets oppfatning kan disse utfordringene derfor kun møtes ved at alle IKT-systemer er forsvarlig sikret. Det vil imidlertid kreve et omfattende utrednings- og lovarbeid for å finne svar på hvorvidt det er mulig og ønskelig å utarbeide en allmenn, tverrsektoriell IKT-sikkerhetslov som vil gjelde for alle, og hvilke minimumskrav om IKT-sikkerhet den i så fall skal stille.

Det må for det første kartlegges hvor stor restrisikoen for samfunnet faktisk er når omfanget av en ny sikkerhetslov, personopplysningsloven og den nye loven om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning er avklart. Det må også ses hen til virkningene av ulike tiltak myndighetene har iverksatt som følge av blant annet IKT-sikkerhetsmeldingen og nasjonal strategi for digital sikkerhet.

Det knytter seg også noen sikkerhetsutfordringer til privatpersoners bruk av IKT. EUs Cybersecurity Act vil et stykke på vei møte utfordringene med tilkoblede produkter. I tillegg mener utvalget prinsipielt at ansvaret for IKT-sikkerhet i tilkoblede produkter og tjenester i større grad bør flyttes fra forbrukeren til produsentene og leverandørene (se kapittel 18).

For det andre må det tas stilling til hvilke minimumskrav om IKT-sikkerhet som vil ha den nødvendige effekten og hvordan kravene skal utformes. Det er på det rene at det overfor mindre virksomheter, for eksempel enkeltpersonforetak, kun kan stilles begrensede og konkrete krav, som det ikke er for krevende å etterleve.

For det tredje må det vurderes om det totalt sett vil være samfunnsøkonomisk lønnsomt å stille slike krav. Det må legges til grunn at krav om IKT-sikkerhet i lov vil ha en kostnadsside for både virksomheter og offentlige myndigheter. Krav om IKT-sikkerhet til alle virksomheter i Norge kan imidlertid være et konkurransefortrinn. Sammen med god tilgang til elektrisitet og vann, høy tillit i befolkningen og høyt utdannende innbyggere, kan god IKT-sikkerhet i hele næringslivet bidra til å gjøre det attraktivt å investere i Norge, og å samarbeide med norske virksomheter.

Utvalget mener det særlig bør vurderes å stille krav om forsvarlig IKT-sikkerhet til virksomheter med stor betydning for norsk økonomi. Traavik-utvalget mente landets økonomiske trygghet og velferd var en grunnleggende forutsetning for Norges evne til å ivareta egen sikkerhet. Utvalget argumenterte med at et anslag som rammer virksomheter som har en helt sentral rolle for ivaretakelsen av landets økonomiske trygghet og velferd, ikke bare vil ha stor symbolverdi. Det vil i ytterste konsekvens kunne ha en vesentlig negativ innvirkning på nasjonens evne til å opprettholde økonomisk trygghet og velferd.[27] Utvalget mener at dette er relevante momenter også ved vurderingen av behovet for å stille krav om forsvarlig IKT-sikkerhet.

Utvalget anbefaler at det settes ned et lovutvalg som skal utrede behovet for og eventuelt utarbeide forslag til en lov som stiller krav om forsvarlig IKT-sikkerhet til alle norske virksomheter.

15.8 Rapporteringskrav

Rapporteringskrav til private og offentlige virksomheter ble omtalt i NOU 2015: 13.[28] Lysneutvalget anbefalte at ivaretakelse av IKT-sikkerhet bør inngå i private og offentlige virksomheters årsmelding. Dette for at arbeidet med IKT-sikkerhet skulle bli prioritert høyere hos den øverste ledelsen i virksomhetene. I stortingsmelding om IKT-sikkerhet fremgår det at høringsinstansene var delte i synet på dette tiltaket.[29]

Kritikere har påpekt at rapportering av såkalte ikke-finansielle temaer gjennomgående følges for dårlig opp. Det er en fare for at kravene kun medfører ekstra papirarbeid for bedriftene. Det er også en risiko for misbruk i markedsføringsøyemed.[30] Solberg-regjeringen fremmet i 2017 forslag om å oppheve plikten til å utarbeide årsberetning for små virksomheter. I den forbindelse uttalte Finansdepartementet at krav til omtale av et forhold synes å ha liten effekt på hvordan forholdet faktisk følges opp i foretakene.[31] Departementet viste til Regnskapslovutvalget, som mente at utarbeidelse av årsberetning for små foretak i stor grad var en plikt-

---

[27] NOU 2016: 19 *Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*, s. 115.

[28] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn,* s. 295.

[29] Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*. s. 79.

[30] Sjåfjell, Beate, *CSR-rapporteringsplikt for store selskaper. Lov om endringer i regnskapsloven og enkelte andre lover* (NIP-2013-2-29), s. 29.

[31] Prop. 160 L (2016–2017) *Endringer i regnskapsloven mv. (forenklinger),* s. 29.

øvelse, og at kostnaden ved utarbeidelsen var større enn informasjonsnytten.[32]

Difi har i en rapport om arbeidet med informasjonssikkerhet i statsforvaltningen konkludert med at arbeidet med styring og kontroll av informasjonssikkerhet i virksomhetene må styrkes.[33] Difi mener bedre rapportering vil gjøre det lettere å sammenligne status på tvers av virksomheter og sektorer og å se endringer over tid.[34] Difi anbefaler at departementene stiller krav om at virksomhetene rapporterer om sikkerhetstilstanden i egen virksomhet, og at statusen på arbeidet med styring og kontroll av informasjonssikkerhet tas inn i årsrapporten.

Utvalget mener det er usikkert om rapporteringskrav er en effektiv måte å få ledelsen til å vie oppmerksomhet til IKT-sikkerhet. Utvalget mener at dette må utredes nærmere av lovutvalget som skal vurdere en IKT-sikkerhetslov for alle virksomheter.

---

32 NOU 2015: 10 *Lov om regnskapsplikt*, s. 318.

33 Direktoratet for forvaltning og IKT (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen.* 2018:4.

34 Ibid.

Kapittel 16
Krav om IKT-sikkerhet ved anskaffelser

Utvalget mener at anskaffelser av IKT-tjenester i mange tilfeller gir bedre trygghet og mer stabile og tilgjengelige tjenester. Med andre ord kan anskaffelser av IKT-tjenester være et fornuftig IKT-sikkerhetstiltak.

Anskaffelser av slike tjenester er imidlertid ikke risikofritt. Som påpekt i kapittel 12 er det ikke bare anskaffelser av IKT-tjenester som kan medføre økt digital risiko for en virksomhet. Anskaffelser av andre tjenester som i utgangspunktet ikke har noe med IKT å gjøre, kan innebære at leverandøren allikevel får tilgang til virksomhetens IKT-systemer. Med slik tilgang følger risiko for bevisst eller ubevisst kompromittering av konfidensialitet, integritet og tilgjengelighet. Et digitalt angrep mot tjenesteleverandøren kan ramme oppdragsgiverens virksomhet.

Det er utvalgets oppfatning at den største utfordringen med anskaffelser er manglende bevissthet om risikoen. For å kunne iverksette hensiktsmessige sikkerhetstiltak, er det avgjørende at virksomhetene vurderer risikoen ved alle anskaffelser. Krav om slike risikovurderinger og å iverksette hensiktsmessige sikkerhetstiltak er en del av kravet om forsvarlig IKT-sikkerhet, som behandles i punkt 15.2. Det vil følge av ny lov om IKT-sikkerhet at alle virksomheter som omfattes av loven skal gjennomføre risikovurderinger ved anskaffelser.

Vurderingen av hvilken risiko som knytter seg til den enkelte anskaffelsen legger viktige føringer for gjennomføring av anskaffelsen og hvilke krav som må stilles til leverandøren. Nedenfor redegjør utvalget for krav om IKT-sikkerhet i anskaffelsesregelverket og SSAer, samt behov for veiledning om anskaffelser og IKT-sikkerhet.

Utvalget har følgende anbefalinger:

- Det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Anskaffelsesregelverket bør endres slik at oppdragsgiveren får en slik plikt.
- IKT-sikkerhet må ivaretas bedre i Statens standardavtaler
- Veiledning om IKT-sikkerhet ved anskaffelser må videreutvikles

16.1 Krav om IKT-sikkerhet i anskaffelsesregelverket og Statens standardavtaler

Utvalget påpeker i IKT-risikobildet (kapittel 3) og i kapitlet om anskaffelser og digitale sårbarheter (kapittel 12) at det kan knytte seg digital risiko til alle anskaffelser. Utvalget mener derfor at det må stilles krav om IKT-sikkerhet ved alle anskaffelser.

Utvalget har vurdert om det er behov for å endre regelverket om offentlige anskaffelser for å ivareta krav om sikkerhet. Anskaffelsesregelverket forutsetter at offentlige virksomheter stiller krav som leverandørene må oppfylle, og at det brukes tildelingskriterier for å skille ut hvilket tilbud som er best. Dette regelverket gjelder for alle typer anskaffelser og inneholder ikke spesifikke krav om for eksempel IKT-anskaffelser.

Utvalget legger til grunn at det innenfor rammene av anskaffelsesregelverket er fullt mulig å stille krav om IKT-sikkerhet ved anskaffelse av IKT-produkter og -tjenester. For utvalget er det ikke like tydelig om det er anledning til å stille krav om IKT-sikkerhet ved anskaffelse av andre produkter og tjenester som ikke like intuitivt kan innebære en digital risiko.

Utvalget mener at det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Anskaffelsesregelverket bør endres slik at oppdragsgiveren får en slik plikt.

SSAene brukes av en rekke virksomheter, også ut over offentlig sektor. De har en del generelle krav om sikkerhet og personvern. I tillegg til de generelle avtaletekstene skal det fylles ut bilag med kravspesifikasjoner fra kunden og løsningsbeskrivelser fra leverandøren. Det må gjøres konkrete vurderinger av krav om sikkerhet ved hver

anskaffelse, og de relevante kravene må beskrives i kravspesifikasjonene og bilagene til avtalen.

Utvalget mener det er behov for en helhetlig tilnærming til IKT-sikkerhet i standardavtalene. For eksempel bør det stilles krav om at leverandører som får tilgang til oppdragsgivers IKT-systemer, har forsvarlig IKT-sikkerhet i egen virksomhet. Det er klausuler om informasjonssikkerhet i flere av standardkontraktene. De ser imidlertid ikke ut til å dekke behovet for IKT-sikkerhet ved anskaffelser fullt ut.

Utvalget anbefaler at det vurderes om SSAene bør endres slik at IKT-sikkerhet blir tydeligere ivaretatt.

16.2 Bedre veiledning om anskaffelsesregelverket og Statens standardavtaler

Det er stort behov for kompetanse og veiledning om krav om IKT-sikkerhet ved anskaffelser. Dette omfatter blant annet hva virksomhetene må vurdere når det gjelder sikkerhet ved anskaffelser, og hvordan dette bør gjenspeiles i kravene som stilles i konkurransedokumentene og kontraktene. Difi har noe veiledning om dette på sine hjemmesider og på portalen anskaffelser.no. Det er viktig at veiledningen videreutvikles.

I tillegg bør også veiledningen til standardavtalene videreutvikles ved at det for eksempel gis bistand til å fylle ut bilag. Dette bør vurderes samkjørt med annen veiledning om IKT-sikkerhet. En mulighet er at et IKT-sikkerhetssenter (se kapittel 17) kan sørge for å koordinere slik veiledning.

Kapittel 17
Etablere et nasjonalt IKT-sikkerhetssenter

Flere land har de siste årene etablert egne IKT-sikkerhetssentre. Formålet har blant annet vært å skape en tydelig koordineringsmekanisme for å håndtere alvorlige uønskede digitale hendelser, og å etablere et nasjonalt kontaktpunkt for IKT-sikkerhet og en arena for offentlig–privat samarbeid. Utvalget er kjent med at det planlegges et tilsvarende nasjonalt senter også i Norge.

Utvalget mener at et IKT-sikkerhetssenter kan bidra til å styrke den nasjonale IKT-sikkerheten. Det kan legge til rette for bedre oppgaveløsning og sørge for et mer effektivt samarbeid mellom etater med tverrsektorielt ansvar for nasjonal IKT-sikkerhet og mellom disse og sektormyndighetene. Et senter kan også bidra til et mer hensiktsmessig samarbeid mellom offentlige myndigheter, private infrastruktureiere og næringslivet for øvrig.

Det er imidlertid nødvendig å gjennomføre en grundig behovs- og kostnadsanalyse før et nasjonalt IKT-sikkerhetssenter etableres.

Utvalget har følgende anbefalinger:

- Det må etableres et nasjonalt IKT-sikkerhetssenter for å styrke koordinering og samordning mellom sektorer og mellom offentlige og private aktører.
- Justis- og beredskapsdepartementet må, i samarbeid med Forsvarsdepartementet, sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse før et nasjonalt IKT-sikkerhetssenter etableres.
  - Behovs- og kostnadsanalysen må baseres på en bred involvering av potensielle interessenter i privat og offentlig sektor.
  - Behovs- og kostnadsanalysen må avklare IKT-sikkerhetssenterets myndighetsforankring og kobling til NSM.
- Følgende oppgaver bør vurderes lagt til IKT-sikkerhetssenteret:
  - Koordinere myndighetenes råd og veiledning.
  - Være nasjonalt responsmiljø (NSM Nor-CERT).
  - Være sentralt kontaktpunkt for råd- og veiledning og ved uønskede digitale hendelser.
  - Tilgjengeliggjøre oppdatert informasjon om trusler og sårbarheter.
  - Motta rapportering og offentliggjøre informasjon om digitale sårbarheter i IKT-systemer («Coordinated Vulnerability Disclosure»).
  - Være pådriver for offentlig-privat samarbeid.
  - Stimulere til mer forskning, utvikling og innovasjon.

17.1 Oppgaver og innretning

Utvalget mener at flere av de utfordringene som drøftes i del III av utredningen, kan møtes ved å etablere et nasjonalt IKT-sikkerhetssenter. Særlig gjelder det utformingen av enhetlig rådgivning og veiledning fra myndighetene og bedre informasjonsdeling og koordinering ved uønskede digitale hendelser. Utvalget mener det er behov for å samle kompetanse, skape synergier på tvers av sektorer og miljøer og gjøre samarbeidslinjene kortere og mer effektive. Det er også behov for å styrke offentlig-privat samarbeid og å bedre innovasjonsevnen innenfor IKT-sikkerhet. Etablering av et nasjonalt IKT-sikkerhetssenter kan bidra til å oppnå dette. Utvalget har i vurderingen av et nasjonalt IKT-sikkerhetssenter blant annet hentet inspirasjon fra Danmark, Nederland og Storbritannia (se boks 17.1).

17.1.1 Oppgaver som kan inngå i et IKT-sikkerhetssenter

Gjennom utvalgets informasjonsinnhenting kommer det frem at flere virksomheter er usikre på hvem de skal kontakte når de trenger rådgivning, enten det gjelder å håndtere en hendelse eller andre typer henvendelser. Utvalget mener at et IKT-sikkerhetssenter bør fungere som nasjonalt

Boks 17.1 Oppgaver og innretning av IKT-sikkerhetssentre i andre land[1]

I 2012 ble Center for Cybersikkerhed opprettet i Danmark som en del av Forsvarets Efterretningstjeneste. Senteret er den nasjonale IKT-sikkerhetsmyndigheten i Danmark, og fungerer som nasjonalt kompetansesenter for IKT-sikkerhet. I rollen som nasjonal IKT-sikkerhetsmyndighet driver senteret rådgivning, godkjenner sikkerhetsgraderte IKT-systemer og fører tilsyn. Hovedformålet med senteret er å styrke beskyttelsen av Danmarks digitale infrastruktur og å bedre evnen til å møte alvorlige cyberangrep. Selv om senteret er en del av etterretningstjenesten, er det organisatorisk atskilt og har sitt eget lovgrunnlag. Senteret får tilgang til etterretningsbasert informasjon og ivaretar den danske nasjonale CERT-funksjonen. Senteret har også ansvar innenfor beredskap på ekomområdet. Det innebærer at senteret fører tilsyn med IKT-sikkerheten og beredskapen i telesektoren og gir råd og veiledning til virksomheter i sektoren.

Også i Nederland ivaretar cybersikkerhetssenteret den nasjonale CERT-funksjonen. I tillegg er råd og veiledning og samarbeid med relevante aktører, både offentlige og private, blant senterets viktigste oppgaver. Selv om virksomheter med ansvar for kritiske samfunnsfunksjoner eller kritisk infrastruktur vies ekstra oppmerksomhet, søker senteret å nå bredt med råd og veiledning. Offentlig–privat samarbeid anses som helt essensielt for å bedre den digitale sikkerheten i Nederland. I motsetning til i Danmark har dette senteret ingen typiske myndighetsoppgaver som tilsyn eller annen regelverksforvaltning. Senteret ligger under justis- og sikkerhetsministerens ansvarsområde.

I Storbritannia, som i Danmark, er cybersikkerhetssenteret en del av en etterretningstjeneste med sikkerhetsoppgaver (Government Communications Headquarters). Senterets oppgaver og ansvar er imidlertid mer likt det i Nederland. Det britiske senteret gir råd og veiledning, avdekker og håndterer uønskede digitale hendelser, jobber med kompetansehevende tiltak i næringslivet og akademia, og bistår i sikring av offentlige og private nettverk. Visjonen senteret jobber mot, er at Storbritannia skal være det tryggeste landet for virksomheter «online». Det innebærer at senteret har store deler av Storbritannia som målgruppe, og senteret er tydelige på at visjonen bare kan nås med utstrakt offentlig–privat samarbeid.

[1] Se vedlegg 3 for mer informasjon.

kontaktpunkt for alle typer IKT-sikkerhetshenvendelser (se figur 17.1). Senteret skal kunne svare på henvendelser selv, eller sørge for at brukerne får kontakt med rett virksomhet som kan bistå. Virksomhetene må enkelt kunne skaffe seg oversikt over de samlede råd og veiledninger som myndighetene gir. Et godt eksempel er det svenske nettstedet informationssakerhet.se, som er et samarbeid mellom svenske myndigheters viktigste rådgivnings- og veiledningsaktører. Her finner man lenker til relevant lovgivning og sentrale veiledningsdokumenter om teknisk sikkerhet og om metoder for å systematisere arbeidet med IKT-sikkerhet. Et tilsvarende nettsted er nylig opprettet i Danmark – sikkerdigital.dk.

Også i Storbritannia er myndighetenes råd og veiledning samlet på ett sted. IKT-sikkerhetssenteret utarbeider mye rådgivnings- og veiledningsmateriell selv. På områder som andre har ansvaret for, lenkes brukeren videre til rett myndighet som kan bidra med riktig informasjon. Senteret fungerer således som selvstendig rådgivnings- og veiledningsaktør og som et knutepunkt som leder brukerne til rett informasjon. Utvalget mener det er behov for en tilsvarende løsning også i Norge, og det er naturlig at senteret har ansvaret for dette.

Det er også nødvendig at myndighetenes råd- og veiledningsmateriell er tilpasset teknologiutviklingen og aktuelle temaer. For eksempel er det uklart hvilken etat som har ansvaret for å gi råd og veiledning når det gjelder IKT-sikkerhet i tilkoblede produkter og tjenester. For brukerne kan det være vanskelig å vite hvor de skal henvende seg. Her vil senteret kunne være en sentral veiledningsaktør.

Senteret må legge vekt på forebygging, men samtidig ha evne til å avdekke og håndtere alvorlige uønskede hendelser. I andre land som utvalget har sett nærmere på, er den nasjonale responsfunksjonen lagt til IKT-sikkerhetssentre. Slik utvalget ser det, er det en sterk kobling mellom en nasjonal responsfunksjons ansvar og opp-

gaver og de øvrige forebyggende oppgavene senteret bør ha.

Utvalget mener derfor at den nasjonale responsfunksjonen, NSM NorCERT, må legges til et IKT-sikkerhetssenter. I tillegg mener utvalget at senteret ved behov må ha kapasitet til midlertidig å huse representanter eller liaisoner fra de sektorvise responsmiljøene. Det er visse utfordringer knyttet til disse responsmiljøenes ulikheter, som deres heterogene struktur, ansvar og oppgaveportefølje. Det å knytte miljøene tettere sammen med IKT-sikkerhetssenteret, for eksempel gjennom liaisonordninger, kan bidra til å løse disse utfordringene. Utvalget vil imidlertid understreke at de sektorvise responsmiljøene først og fremst må prioritere nærhet til egen sektor, sin egen ledelse og egne IKT-systemer, fremfor å være fysisk samlokalisert permanent i senteret. Ved behov (for eksempel ved en hendelse) bør senteret ha kapasitet til å huse også andre relevante aktører, som eiere av kritisk infrastruktur og sentrale myndigheter. Fleksibilitet bør være et kjennetegn ved senteret.

Videre mener utvalget at et IKT-sikkerhetssenter må holde seg oppdatert på gjeldende trusler og sårbarheter. Denne informasjonen må på et tilpasset nivå gjøres tilgjengelig for alle, med unntak av sikkerhetsgradert informasjon. Senteret i Storbritannia utarbeider for eksempel ukentlige trusselrapporter som publiseres på senterets nettsider. Utvalget mener dette er et tiltak som fører til åpenhet om aktuelle trusler, og det gir virksomhetene mulighet til å sikre seg innen rimelig tid. Trusselrapportene fra senteret i Storbritannia er et eksempel til etterfølgelse, og tilsvarende bør være en oppgave for et IKT-sikkerhetssenter i Norge også.

I Nederland har man utarbeidet retningslinjer for hvordan man skal ta imot varsler om og offentliggjøre digitale sårbarheter ved ulike produkter, tjenester og IKT-systemer. Tanken bak dette er at informasjon om en sårbarhet nettopp er den informasjonen som trengs for å redusere den samme sårbarheten. Fordelen med en slik offentliggjøring er at den gjør det mulig for alle å vite om sårbarheten, og tredjeparter kan for eksempel bestemme at kun oppdaterte produkter fra den aktuelle leverandøren får tilgang til nett og nettsider. Ulempen er at det gir mulighet for å utnytte sårbarheter før eventuelle oppdateringer gjøres.

Utvalget anbefaler at det igangsettes et arbeid i Norge for å finne ut hvordan informasjon om digitale sårbarheter i IKT-systemer mer systematisk skal offentliggjøres, og hva man bør gjøre for å håndtere dem. Det må utarbeides retningslinjer, og det må tilbys råd og veiledning på dette området. Utvalget mener det er mye å lære av andre land som har kommet lenger, blant annet Nederland. Et IKT-sikkerhetssenter kan etter mønster fra Nederland gis ansvar for å motta og koordinere oppfølgingen av informasjon om digitale sårbarheter.

Utvalget mener at konkrete tiltak for å styrke offentlig–privat samarbeid må legges inn i et IKT-sikkerhetssenter. Erfaringer fra andre land, særlig Nederland og Storbritannia, viser at det er mange tiltak som kan gjøres på dette området. Storbritannia fremhever spesielt et program de har kalt «100-secondees». Det innebærer at det til enhver tid skal være 100 hospitanter fra offentlige og private virksomheter i IKT-sikkerhetssenteret, herunder akademia. De jobber i senteret to til tre dager i uken i en periode på inntil et år. Ordningen innebærer en kompetanseheving for hospitantene og dermed for virksomhetene de representerer, samtidig som senteret får verdifull sektorkompetanse. Utvalget mener at hospitantordningen i Storbritannia er et eksempel til etterfølgelse, og at en tilsvarende ordning tilpasset norske forhold bør etableres i tilknytning til IKT-sikkerhetssenteret.

IKT-sikkerhetssenteret må unngå å komme i konkurranseforhold til kommersielle aktører. Ved etablering av nye tiltak for offentlig–privat samarbeid må senteret sørge for at tiltakene ikke kan oppfattes som konkurransevridende ut fra hvem som deltar og i hvilket omfang.

IKT-sikkerhetskompetanse er en knapp ressurs i Norge. Utvalget mener at det å bringe sammen kompetanse fra ulike miljøer kan ha positive synergieffekter. Særlig med tanke på å utnytte samfunnets IKT-sikkerhetskompetanse på en hensiktsmessig måte. Til en viss grad forventer utvalget at samarbeidet innenfor rammene av et IKT-sikkerhetssenter i seg selv bidrar til et kompetanseløft for aktørene.

Samtidig må IKT-sikkerhetssenteret være initiativtaker og pådriver for kompetansehevende tiltak i samarbeid med offentlige og private virksomheter, utdanningssektoren og akademia for øvrig. I Storbritannia samarbeider senteret med utdanningsmyndighetene om et program som kalles CyberFirst. Programmet retter seg mot barn helt ned i 11-årsalderen og videre oppover hele utdanningsløpet. Overfor de yngste er formålet å skape interesse og dermed et rekrutteringsgrunnlag for høyere utdanning innenfor IKT-sikkerhet. I arbeidet mot universiteter og høyskoler bistår senteret med kvalitetssikring av utdanningsprogrammer og sertifiserer både bachelor- og masterutdanninger.

Figur 17.1 Et IKT-sikkerhetssenter som nasjonalt kontaktpunkt

Videre støtter senteret ph.d.-kandidater og oppretelsen av Centres of Excellence innenfor IKT-sikkerhetsforskning. I samarbeid med næringslivet arbeider senteret blant annet med å bistå oppstartsbedrifter og andre med å videreutvikle IKT-sikkerhetsinnovasjoner gjennom programmet Cyber Accelerator. Liknende kompetanse- og innovasjonsfremmende oppgaver mener utvalget bør tillegges et IKT-sikkerhetssenter i Norge.

17.1.2 Organisering og myndighetsforankring

En av suksessfaktorene ved IKT-sikkerhetssentrene i Storbritannia og Nederland er at de har etablert sentrene som møteplasser for ulike aktører. Utvalget tror at å samle flere aktører under samme tak kan bidra til bedre koordinering, mer samarbeid, mer informasjonsdeling og mer innovasjon. Ved at flere virksomheter har en slik møteplass kan noen av utfordringene med overlappende ansvar og roller mellom etatene realiseres uten krevende organisasjonsendringer.

I tillegg mener utvalget at det er helt avgjørende at et IKT-sikkerhetssenter legger tillit og åpenhet til grunn for samhandlingen med andre. Trussel- og risikovurderinger, samt råd om tiltak, må ut til dem som skal forebygge eller håndtere uønskede digitale hendelser. Det krever betydelig samhandling med både offentlige og private aktører, og nettopp åpenhet og tillit fremheves av sentrene i Nederland og Storbritannia som viktige faktorer for å oppnå dette.

Utvalget mener at et nasjonalt IKT-sikkerhetssenter må ha en tydelig forankring i sivile myndigheter. Arbeidet med IKT-sikkerhet i kritiske samfunnsfunksjoner og kritisk infrastruktur foregår i all hovedsak på sivil side, både i offentlig og privat regi. Råd og veiledning fra et IKT-sikkerhetssenter vil først og fremst være til nytte for det sivile samfunn. Samtidig har forsvarssektoren en sentral rolle knyttet til statssikkerhet, og sivil og militær IKT-infrastruktur blir i økende grad integrert.

I rapporten fra Oslo Economics er vurderingen at tilgang på etterretningsinformasjon har stor samfunnsøkonomisk betydning. Denne informasjonen er også viktig for det sivile samfunnet. Forsvarssektorens informasjon om og vurderinger av trusler vil i mange tilfeller ha betydning for privat næringsliv og andre deler av offentlig forvaltning. Det vil også være informasjon om og vurderinger av trusler i det sivile samfunn som vil være nyttig og relevant for forsvarssektoren. Det

er derfor nødvendig at IKT-sikkerhetssenteret også har en kobling til forsvarssektoren.

I løpet av 2018 har Kripos begynt arbeidet med å opprette nasjonalt cyberkrimsenter. I løpet av tre til fire år skal det ha rundt 200 ansatte. Ifølge Politidirektoratet skal nasjonalt cyberkrimsenteret ha kapasiteter som kan benyttes mot både kriminalitet som retter seg mot IKT-systemer og teknologi, og kriminalitet der teknologi er et vesentlig element eller verktøy i gjennomføringen av den kriminelle handlingen. I tillegg skal senteret ha avanserte kapasiteter innenfor datatekniske undersøkelser for spor- og bevissikring, uavhengig av kriminalitetsform. Etableringen av nasjonalt cyberkrimsenteret skal sette politiet i stand til å bli den koordinerende og sentrale ressursen på datakrimområdet.

Det er nødvendig at et IKT-sikkerhetssenter har et tydelig grensesnitt mot nasjonalt cyberkrimsenter. Tilsvarende cyberkrimsentre finnes i Sverige, Storbritannia, Danmark og i en rekke andre land. Utvalget har ikke kjennskap til land hvor cyberkrimsenteret og IKT-sikkerhetssenteret er en og samme enhet, men det er tett samarbeid mellom dem. Slik utvalget oppfatter det, er nasjonalt cyberkrimsenters formål etterforsking og påtale av straffbare handlinger, mens et IKT-sikkerhetssenter vil ha som formål å legge forholdene til rette for forsvarlig nasjonal IKT-sikkerhet. Det er allikevel ikke opplagt hvor grensene går mellom to slike sentre, blant annet når det gjelder arbeidet med å avdekke og håndtere digitale angrep. Det er derfor nødvendig at de detaljerte ansvarsforholdene mellom de to sentrene avklares, og at de har et godt samarbeid.

17.2 Behovs- og kostnadsanalyse

Utvalget er kjent med at NSM arbeider med å etablere et IKT-sikkerhetssenter i Norge.[1] I et konseptnotat fra NSM, datert 24. august 2018, betegner de et slikt senter som et «Nasjonalt cybersikkerhetssenter». Det fremgår av notatet at senteret vil være et nasjonalt kontaktpunkt og et nav for IKT-sikkerhet i Norge. Det vektlegges at samarbeid mellom sentrale aktører, også private, skal ligge til grunn for aktivitetene. NSM NorCERT skal inngå som en del av senteret. I konseptnotatet beskrives det at aktivitetene innledningsvis vil vektlegge tre hovedleveranser:

- Utvikling og tilgjengeliggjøring av tiltak og anbefalinger, herunder rådgivning
- Forbedret nasjonal responsevne, med deteksjon og hendelseshåndtering
- Videreutvikling av nasjonale tekniske sikkerhetstjenester, herunder skanningstjenester og Sikret offentlig nett[2]

I følge konseptnotatet skal det samles bred nasjonal kompetanse i senteret, der ulike offentlige og private aktører samarbeider ut fra et felles risikobilde og felles situasjonsforståelse i samme lokale (fysisk samlokalisering eller tilstedeværelse) og over nettet (virtuelt). Det er planlagt at sektorvise responsmiljøer, andre myndigheter, næringsliv og akademia etter nærmere kriterier vil bli invitert inn, helt eller delvis, i senterets lokaler sammen med ekspertise fra NSM. De enkelte virksomhetene deltar på eget rettsgrunnlag.

Det vil også bli utviklet verktøy for informasjonsdeling med aktører som ikke er fysisk samlokalisert. Nasjonalt cyberkrimsenter i Kripos og Felles cyberkoordineringssenter vil ikke være en integrert del av senteret, men man vil i det videre arbeidet se på hvordan et tettest mulig samarbeid mellom senteret og disse skal etableres.[3]

Utvalget mener det kan stilles spørsmål om NSMs cybersikkerhetssenter vil favne bredt nok med tanke på de oppgavene som bør ivaretas, og de eksterne deltakerne som bør være med i et slikt senter. Konseptnotatet gir en for generell beskrivelse av senteret. Utvalget er ikke kjent med at det foreligger dokumentasjon og planer for hvordan senteret skal organiseres, hvilke kostnader som er forbundet med en slik etablering, hvordan offentlig–privat samarbeid skal styrkes gjennom senteret eller hvordan ulike fagmiljøer skal inkluderes. Langt på vei forstår utvalget det slik at cybersikkerhetssenterets oppgaver samsvarer med de oppgavene NSM allerede har i dag.

Utvalget mener det må ligge et godt beslutningsgrunnlag til grunn før det etableres et nasjonalt IKT-sikkerhetssenter. Det må gjøres en grundig behovsanalyse, herunder vurderinger av kostnader knyttet til etablering og drift av et slikt senter. Utvalget mener det er viktig at interessenter, for eksempel andre tverrsektorielle etater eller relevante aktører fra privat næringsliv, får anledning til å mene noe om behovet og oppgavene til

[1] Prop. 1 S (2018–2019) Forsvarsdepartementet, s. 112. Prop. 1 S (2018–2019) Justis- og beredskapsdepartementet, s. 159.

[2] Sikret offentlig nett (SON) gir mulighet til å koble nettet fra internett og fremdeles kommunisere mellom aktørene. For mer informasjon om SON, se omtale i Nasjonal sikkerhetsmyndighet (2015) *sikkerhetsfaglige råd*. s. 40.

[3] Nasjonal sikkerhetsmyndighet (2018) *Konseptnotat, Nasjonalt cybersikkerhetssenter – en del av NSM*. 24. august 2018.

et slikt senter. Et senter basert på samarbeid krever avklaringer om hvilke aktører som kan inngå i senteret, hva de skal bidra med, og hva de skal få ut av samarbeidet. For alle aktører innebærer deltakelse i senteret en viss ressursinnsats, særlig i form av personell. Behovsanalysen må gi avklaringer om aktørenes villighet og mulighet til å knytte seg til senteret.

Videre er det utvalgets oppfatning at sentrale oppgaver i et IKT-sikkerhetssenter, for eksempel samordning av råd og veiledning, koordinering og informasjonsdeling, først og fremst dekker sivile behov. Samtidig er forsvarssektoren opptatt av at digitale angrep kan utgjøre en trussel mot statssikkerheten dersom kritiske samfunnsfunksjoner settes ut av spill. Dessuten er forsvarssektoren i økende grad avhengig av sivil IKT-infrastruktur og -tjenester. Gjennom en behovsanalyse er det viktig å avklare hvilke behov i sivil sektor og i forsvarssektoren senteret skal bidra til å løse.

Som nevnt i kapittel 8 og 9 kan det være enkelte utfordringer med modellen for styring av NSM. Et IKT-sikkerhetssenter som er organisert som en del av NSM, vil bringe med seg disse styringsutfordringene. Utvalget mener det er viktig at myndighetsforankringen til IKT-sikkerhetssenteret drøftes og avklares i behovsanalysen.

Justis- og beredskapsdepartementet må derfor, i samarbeid med Forsvarsdepartementet, sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse før et nasjonalt IKT-sikkerhetssenter etableres. Analysen må ha bred involvering fra potensielle interessenter i både privat og offentlig sektor og den må også avklare senterets myndighetsforankring og kobling til NSM. Som del av analysen bør også det rettslige rammeverket knyttet til informasjonsdeling vurderes. Dette for å fjerne unødvendige hindringer for informasjonsdeling, både mellom sektorvise responsmiljøer og overfor offentligheten. Det er også viktig at grensesnittet mellom et nasjonalt IKT-sikkerhetssenter og Nasjonalt cyberkrimsenter avklares.

Kapittel 18
Tydelig regulering og ansvar for tilkoblede produkter og tjenester

IKT-sikkerheten i tilkoblede produkter og tjenester vil være en sentral problemstilling i årene fremover, etter hvert som stadig nye produkter og tjenester kobles til internett. Utvalget er opptatt av at produkter og tjenester som selges i Norge, skal ha akseptabel IKT-sikkerhet. Manglende IKT-sikkerhet i slike produkter og tjenester kan utgjøre en trussel for den enkelte forbrukeren, for virksomheter og for samfunnssikkerheten.

Utvalget har følgende anbefalinger:

- Ansvaret for IKT-sikkerhet i tilkoblede produkter og tjenester bør i større grad flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester.
- Norge må fortsette sitt internasjonale samarbeid på dette området, særlig opp mot regelverksprosesser i EU.
- Myndighetene må gi bedre råd og veiledning til importører, forhandlere og norske produsenter av tilkoblede produkter og tjenester. Utarbeidelse av råd og veiledning må gjøres i samarbeid mellom myndighetene og bransjeaktørene.
- DSB bør få en tydelig rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

Når det gjelder IKT-sikkerhet i tilkoblede produkter og tjenester, mener utvalget at ansvaret for IKT-sikkerhet i større grad bør flyttes fra forbrukerne til produsentene og leverandørene. Det kan ofte være vanskelig for forbrukere å forstå hva som kreves av dem for å holde et produkt sikkert. Det kan for eksempel være stor usikkerhet på grunn av manglende informasjon fra produsenten eller uklare forventinger til hva brukeren må gjøre for å holde produktet oppdatert. Det kan også være usikkerhet knyttet til hvilke data som blir samlet inn gjennom produktet, og hva som skjer med disse. Denne usikkerheten er ikke bare begrenset til forbrukere. Bedrifter som designer eller utvikler tilkoblede produkter eller løsninger, har ofte vanskeligheter med å få, eller forstå, informasjon om sikkerheten ved de komponentene de skal bruke.

For å flytte mer av dette ansvaret over på produsentene og leverandørene må Norge fortsette sitt internasjonale samarbeid, særlig opp mot EU. Fordi mange tilkoblede produkter og tjenester krysser landegrenser, er det viktig å ha et harmonisert regelverk internasjonalt. På denne bakgrunn mener utvalget at det er bedre å bidra til et oppdatert regelverk på EU-nivå enn at Norge unilateralt endrer regelverket på feltet. Datatilsynet og Forbrukertilsynet bør fortsette å gå foran i europeisk sammenheng ved å samarbeide, dele informasjon og delta i relevante internasjonale sammenhenger gjennom for eksempel Digital Clearinghouse. De kan også arbeide for at det på grunnlag av EUs Cybersecurity Act utarbeides sertifiseringsordninger som ivaretar forbrukere og forbrukerrettigheter (se vedlegg 2, punkt 2.2).[1]

I denne sammenhengen er det også interessant at britiske myndigheter i 2018 tydelig har gitt uttrykk for at de forventer at markedet og produsentene selv sørger for tilstrekkelig IKT-sikkerhet i tilkoblede produkter og tjenester. De har blant annet utarbeidet et forslag til retningslinjer for sikkerhet i produkter og tjenester, som angir praktiske og prinsipielle krav til produsentene.[2] Myndighetene truer imidlertid med å gjøre om anbefa-

[1] European Data Protection Supervisor, *Big Data & Digital Clearinghouse.*Regjeringen (2018) *Cybersecurity Act – foreløpig posisjonsnotat* 5.2.2018.

[2] Retningslinjene inneholder for eksempel krav om ingen universelle passord, krav om en deklarasjon som viser sårbarheter (vulnerability disclosure), krav til oppdateringer, krav til sikker kommunikasjon og systemer for at forbrukeren kan slette persondata.

lingene til lovkrav hvis ikke produsentene innen kort tid følger anbefalingene.[3]

Utvalget mener at importører, forhandlere og norske produsenter av tilkoblede produkter må få bedre veiledning fra myndighetene. Slik veiledning bør utarbeides i samarbeid med bransjeaktører. Målsettingen med bedre veiledning bør være å forebygge at produkter uten tilfredsstillende IKT-sikkerhet lanseres på det norske markedet, og å håndtere varsling om sårbarheter i slike produkter på en god måte. Det bør gis mer veiledning om dagens regelverk, og om hvordan utviklere kan ha innebygd sikkerhet i sine produkter og tjenester. Innebygd sikkerhet («Security by design») vil si at produsenter må tenke på sikkerhet allerede i utviklingen og gjennom hele livsløpet til produktet. De må regelmessig vurdere sikkerhetsrisikoer og implementere tiltak for å imøtekomme disse.[4] Spesielt gjelder det produkter som biler, medisinsk utstyr og velferdsteknologi, hvor konsekvensene av manglende sikkerhet kan være særlig store. Andre høyrisikoprodukter kan være produkter rettet mot barn, smarte-hjemprodukter og ulike sikkerhetsprodukter.

Utvalget registrerer at forskjellig regelverk og forskjellige tilsynsmyndigheter kan være relevante for ett og samme tilkoblede produkt. Dette øker risikoen for at ingen tar tak i saken hvis produkter har mangelfull IKT-sikkerhet, eller at saken blir en kasteball mellom ulike myndigheter. Både Datatilsynet og Nkom undersøkte for eksempel høsten 2017 GPS-klokker for barn. Mens Datatilsynet fant alvorlige brudd på personopplysningsloven ved tre produkter som Forbrukerrådet varslet inn, fant Nkom mangler i etterlevelsen av radioutstyrsdirektivet (knyttet til blant annet CE-merking og dokumentasjon på stråling) i alle produktene som ble undersøkt. Dette viser at det må være tett samarbeid mellom tilsynsmyndigheter som Datatilsynet, Forbrukertilsynet, DSB og Nkom.

Et slikt samarbeid bør ikke bare begrenses til tilsyn. Økt samarbeid mellom relevante etater kan bidra til å avdekke digitale sårbarheter i produkter og forebygge alvorlige uønskede hendelser hvor tilkoblede produkter benyttes i nettverksangrep. Det foreslåtte IKT-sikkerhetssenteret kan være en hensiktsmessig arena for et samarbeid mellom sentrale aktører.

Konkrete målsettinger for et tettere samarbeid bør være at produkter som ikke har tilstrekkelig IKT-sikkerhet, effektivt oppdages, at det kan varsles om svakheter, og at produkter som ikke utbedres, kan tilbakekalles. Det bør også være mulig for forbrukerne å heve kjøp når produkter og tjenester ikke har tilstrekkelig IKT-sikkerhet.

Utvalget mener at myndighetsansvaret for IKT-sikkerheten i tilkoblede produkter og tjenester, må tydeliggjøres. Det er viktig at DSB som produktsikkerhetsmyndighet holder seg oppdatert på utviklingen, og utvalget mener DSB bør få en tydelig rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

---

3 UK Department for Digital, Culture, Media & Sport *(2018) Secure by Design: Improving the cyber security of consumer Internet of Things – Report*, 7 March 2018.

4 Ibid.

Kapittel 19
Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Som det fremgår av utfordringsbildet i del III, er det særlige utfordringer knyttet til hvordan IKT-sikkerhet griper inn i alle sektorer og virksomheter i samfunnet. Denne kompleksiteten utfordrer styringen og samordningen av nasjonal IKT-sikkerhet.

Det foreligger ingen enkel oppskrift på hvordan myndighetene skal organisere seg best mulig for å møte disse utfordringene. Utvalgets undersøkelser viser også at andre land har ulike måter å organisere sitt arbeid med IKT-sikkerhet.

Utvalgets informasjonsinnhenting har ikke avdekket noe åpenbart behov for å gjøre større endringer i ansvar, roller eller oppgaver til etatene. Det er imidlertid viktig at ansvarsforholdene er tydelig definert der det er tilgrensende områder, og at det er et godt og koordinert samarbeid på tvers av sektorer og etater (se punkt 7.2).

Justis- og beredskapsdepartementet har et overordnet ansvar for flere av disse utfordringene. Utvalget ser ikke behov for å endre eller utvide departementets ansvar innenfor nasjonal IKT-sikkerhet. Dette er godt definert i ulike kongelige resolusjoner og instrukser.[1] Utvalget mener imidlertid at departementet må utvise et tydeligere lederskap for det samordningsansvaret de allerede har for IKT-sikkerhet i sivil sektor.

Det er grunn til å utvise en viss grad av nøkternhet når det gjelder mulighetene Justis- og beredskapsdepartementet har til å håndtere sektorovergripende oppgaver og utfordringer på nye og bedre måter innenfor regjeringsapparatet. Med vårt konstitusjonelle system med ministeransvar som en grunnleggende forutsetning, vil det alltid være utfordrende å være et samordningsdepartement på et sektorovergripende område som nasjonal IKT-sikkerhet.

Utvalget har følgende anbefalinger:

- Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.
  - Etablering av et nasjonalt IKT-sikkerhetssenter og den nye loven om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning vil styrke departementets evne til å utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.
  - Justis- og beredskapsdepartementet og Forsvarsdepartementet må gjennomgå modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes.
- Justis- og beredskapsdepartementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre, og at tilsyn med teknisk IKT-sikkerhet gis økt oppmerksomhet.

19.1 Justis- og beredskapsdepartementet må være tydeligere i sitt lederskap på IKT-sikkerhetsområdet

På flere områder har Justis- og beredskapsdepartementet tatt et tydeligere lederskap de siste årene. I 2017 ble for eksempel den første stortingsmeldingen om IKT-sikkerhet lagt frem for Stortinget.[2] Meldingen peker på satsingsområder og gir en strategisk retning i arbeidet med nasjonal IKT-sikkerhet fremover. Et annet eksempel er departementets arbeid med en ny nasjonal stra-

[1] Kongelig resolusjon 22. mars 2013: *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*. Kongelig resolusjon 10. mars 2017: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet. Instruks for departementenes arbeid med samfunnssikkerhet*, fastsatt av Justis- og beredskapsdepartementet 1. september 2017.

[2] Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*.

tegi for digital sikkerhet som er forventet i begynnelsen av 2019. I dette arbeidet har Justis- og beredskapsdepartementet tatt initiativ til et samarbeid med næringslivet, akademia og andre virksomheter, og gjennom dette vært pådriver for å få til et tettere samarbeid mellom private og offentlige aktører.

Utvalget mener at å etablere et nasjonalt IKT-sikkerhetssenter (se kapittel 17) og å utarbeide og forvalte en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning (se kapittel 15) vil styrke departementets evne til utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.

Justis- og beredskapsdepartementet må også i større grad være en synlig aktør som tar initiativ, løser opp i uklarheter, definerer mål, koordinerer og samordner arbeidet på dette området. Samordning kan dreie seg om organisering og styring av oppgaver og prosesser, men det kan også handle om å avveie og prioritere ulike verdier og formål som kan være motstridende eller stå i ressursmessig konkurranseforhold til hverandre. Det betyr at Justis- og beredskapsdepartementet må bidra til mer aktiv samordning med andre departementer som har ansvar for tilgrensende områder innenfor IKT-sikkerhet.

Særlig viktig er det at Justis- og beredskapsdepartementet og Forsvarsdepartementet har et godt og velfungerende samarbeid når det gjelder å avklare prioriteringene og målsettingene til NSM. De skal understøtte Justis- og beredskapsdepartementet og Forsvarsdepartementet i deres ansvar på IKT-sikkerhetsområdet i sivil sektor og i forsvarssektoren.[3] Selv om det er tette koblinger mellom sivil sektor og forsvarssektoren innenfor IKT-sikkerhet, er dette en krevende styringsmodell. Det gjelder ikke bare den administrative styringen av etaten, men også hvilke prioriteringer, veivalg og målsettinger som skal gjelde for det strategiske arbeidet med nasjonal IKT-sikkerhet.

Utvalget anbefaler at Justis- og beredskapsdepartementet og Forsvarsdepartementet gjennomgår modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes.

I den forbindelse bør det også vurderes hvordan NSM i større grad kan bidra til politikkutforming på området. NSM har selv pekt på at både Forsvarsdepartementet og Justis- og beredskapsdepartementet har behov for substansielle bidrag til støtte for sin politikkutforming innenfor samfunnssikkerhet og beredskap. Behovet er større enn det NSM er i stand til å etterkomme.[4] Et NSM som i større grad sørger for substansielle bidrag innenfor IKT-sikkerhet vil styrke Justis og beredskapsdepartementets evne til å utøve tydeligere lederskap på området.

Det må være godt kjent at Justis- og beredskapsdepartementet sørger for å ivareta helhet, sammenheng og forvaltningspolitisk styring av IKT-sikkerhetsområdet. Departementet må bidra til mer langsiktig og strategisk tekning på tvers av sektorer. Nasjonal IKT-sikkerhet er et politikkområde på linje med andre store tverrsektorielle samfunnsutfordringer som miljø, arbeidslivkriminalitet og ruspolitikk. Det er mulig å løfte dette området og gjøre det mer synlig som politikkområde, både i samfunnsdebatten og i regjeringen.

Statsrådene spiller hovedrollene for å oppnå helhet, sammenheng og samordning i statens virksomhet, i deres egenskap av å være sjef i eget departement og i rollen som medlem i regjeringskollegiet. Det kan i større grad legges sterkere politiske føringer og krav til samarbeid og koordinering på tvers av departementene. Statssekretærutvalg, enten permanente eller situasjonsoppnevnte, kan med fordel benyttes i større grad for styrke arbeidet med nasjonal IKT-sikkerhet. Ved det unngår man også at mindre saker må behandles i samlet regjering. Det er derfor viktig å finne gode koordineringsmekanismer som kan settes i verk på tidligere stadier i beslutningsprosessen.

Det kan også gjøres mer for å styrke samordningen og samarbeidet på tvers av sektorer uten at departementsnivået blir belastet. I tildelingsbrev og i styringsdialogen kan det for eksempel gis større mulighet for, og oppmuntres til, å finne løsninger i direkte kontakt mellom underliggende etater og organer. Dette kan for eksempel gjøres ved at etatsjefer får et bredere handlingsrom og at de gis i oppdrag aktivt å samarbeide med andre etater når det er behov for det. I mange tilfeller vil etatene med tverrsektorielt ansvar for IKT-sikkerhet selv ta ansvar for å koordinere seg. I tilfeller hvor det ikke skjer, bør Justis- og beredskaps-

[3] Se side 75–76 i iverksettingsbrevet for langtidsplanen 2017–2020. (Iverksettingsbrevet for langtidsplanen formaliserer Forsvarsdepartementets oppdrag til etatene for gjennomføringen av langtidsplanen for 2017–2020, basert på Stortingets behandling av Innst. 62 S (2016–2017), jf. Prop. 151 S (2015–2016) *Kampkraft og bærekraft*.

[4] Nasjonal sikkerhetsmyndighet (2015) *Sikkerhetsfaglig råd,* s. 51.

departementet i større grad tilrettelegge for og bidra til et hensiktsmessig samarbeid mellom etatene.

Justis- og beredskapsdepartementet må legge bedre til rette for å koordinere råd og veiledning. Utvalgets informasjonsinnhenting viste at råd og veiledning oppleves som fragmentert og lite koordinert (se punkt 9.2). Utvalget anbefaler at departementet tar initiativ til å etablere en samordningsarena for etater som driver med råd og veiledning innenfor IKT-sikkerhet. Formålet med arenaen bør være at brukerne opplever myndighetene som mer koordinerte og enhetlige. Justis- og beredskapsdepartementet bør se hen til og eventuelt ta utgangspunkt i allerede etablerte arenaer, for eksempel NSMs nylig etablerte arena med Difi og Datatilsynet (se punkt 5.4). Det vil være naturlig at arenaen blir en del av oppgavene til et IKT-sikkerhetssenter, som nevnt i kapittel 17. Utvalget mener imidlertid at etablering av samordningsarenaen ikke bør avvente etablering av senteret.

19.2 Tilsyn må koordineres bedre

Selv om utvalget har fått mange positive tilbakemeldinger på gjennomførte IKT-sikkerhetstilsyn, kommer det også frem at det kan være manglende koordinering og samordning av tilsyn. Det er også uklarheter knyttet til begrepsbruk og metodikk. Utvalget mener Justis- og beredskapsdepartementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre.

Utvalget vil trekke frem måten dette er løst på for HMS-regelverket. Sju ulike departementer, og flere etater, har under ledelse av Arbeidstilsynet gått sammen om en felles tilnærming til tilsyn.[5] Formålet med samarbeidet mellom tilsynsmyndighetene er at arbeidslivet blir behandlet på en enhetlig måte, og at virksomhetene møter et samordnet tilsyn fra myndighetenes side. Samarbeidet skal bidra til at myndighetene fremstår med en felles statlig tilsynsprofil, og at tilsynsressursene blir utnyttet effektivt. Tilsynsmyndighetene skal ha et felles rammeverk for hvordan tilsyn skal gjennomføres og samordnes, slik at de blir enhetlige og koordinert.

Utvalget mener at noe lignende kan gjennomføres for tilsyn innenfor IKT-sikkerhet. På denne måten kan IKT-sikkerhetstilsyn foregå på en mest mulig enhetlig og koordinert måte. På samme måte som Arbeidstilsynet har koordineringsrollen ved HMS-tilsyn, kan NSM ha koordineringsrollen ved IKT-sikkerhetstilsyn. Utvalget mener et samordnet tilsyn innen IKT-sikkerhet bør legge vekt på brukernes behov, både når det gjelder veiledning og koordinering.

Koordineringen av tilsyn kan også bedres gjennom etableringen av en felles tilsynskalender og arenaen for IKT-tilsyn som NSM har etablert.[6] Den vil i første omgang bli videreutviklet til å omfatte de sektortilsynene som blir utpekt etter den nye sikkerhetsloven. Utvalget ser det som viktig at man i koordineringsarbeidet ikke avgrenser seg til de tilsynene som vil bli utpekt som sektortilsyn etter sikkerhetsloven, men anlegger en bredere tilnærming.

Det bør unngås at flere tilsynsorgan fører tilsyn som skal ivareta samme formål. I den grad det skjer, må det være tilstrekkelig koordinering av de aktuelle tilsynene.[7] I den nye sikkerhetsloven er det lagt opp til at sektortilsynene skal kunne føre tilsyn med IKT-sikkerheten i egen sektor. Da vil koordineringen med andre tilsyn være særlig viktig. NSMs rolle blir å sikre en helhetlig, samordnet og tverrsektoriell tilnærming. De vil føre tilsyn med de utpekte sektortilsynene, men også med virksomheter i sektorer med utpekte sektortilsyn der det er «tvingende nødvendig».[8] NSM har i den forbindelse allerede fått et sterkt samordningsmandat for tilsyn, og dette mener utvalget det bør bygges på i den utvidede samordning av IKT-sikkerhetstilsynene.

En felles tilsynskalender er et verktøy for tilsynsmyndighetene som bidrar til å koordinere varslede og planlagte tilsyn i tid. Det skal sikre at brukerne ikke opplever at tilsynene belaster det samme tilsynsobjektet i unødvendig grad. En tilsynskalender kan være offentlig, som fylkesmannens felles tilsynskalender, eller den kan være skjermet for andre enn tilsynsførerne. For at en tilsynskalender skal fungere, er det viktig at de ulike tilsynsførerne gir en oversikt over alle planlagte tilsyn de skal utføre det neste året, og at dette skjer på samme tidspunkt i alle virksomhetene som omfattes av kalenderen. Deretter er det viktig at den som koordinerer tilsynskalenderen, finner hensiktsmessige tiltak hvis det blir avdekket at to etater vil åpne tilsyn med samme objekt nært i tid.

---

5 Arbeidstilsynet, Direktoratet for samfunnssikkerhet og beredskap, Mattilsynet, Miljødirektoratet, Næringslivets sikkerhetsorganisasjon, Petroleumstilsynet, Statens helsetilsyn og Statens strålevern (2014) *Tilsynsmyndighetenes retningslinje for samordnet tilsyn og felles tilsynsprofil.*

6 Se kap. 5.4 for nærmere beskrivelse av arenaen.

7 St.meld. nr. 17 (2002–2003) *Om statlige tilsyn.*

8 Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)* s. 67.

Utvalget mener at tilsyn med teknisk IKT-sikkerhet må gis økt oppmerksomhet. Dette er nødvendig for å kunne kontrollere at aktuelle sikringstiltak faktisk er implementert, og at de fungerer etter hensikten. Den nye loven om IKT-sikkerhet vil være et verktøy for å gi økt oppmerksomhet. Det er imidlertid få tilsynsmyndigheter som har nødvendig kompetanse til å føre slikt tilsyn. De ulike tilsynsorganene bør derfor styrke egen kompetanse på dette området. Utvalget peker i den forbindelse på den ovenfor nevnte arenaen som er etablert i regi av NSM, og på arbeidet de gjør for å etablere en sentral kapasitet med IKT-sikkerhetskompetanse som kan benyttes som ressurs for tilsynsmyndighetene. Dette arbeidet skal være sluttført i 2018. Utvalget er også kjent med at NSM har etablert et utviklingsprosjekt for automatisering av tilsyn med tekniske IKT-sikkerhetstiltak med sluttleveranse i løpet av 2019. Slik utvalget ser det, vil disse tiltakene kunne avhjelpe kompetanseutfordringen.

Del V
Økonomiske og administrative konsekvenser

Kapittel 20
Økonomiske og administrative konsekvenser

I dette kapittelet vurderer utvalget de økonomiske og administrative konsekvensene av anbefalingene i del IV. Utvalget vil understreke at utredningen ikke har gitt grunnlag for å fange opp den fulle bredden av konsekvensene av anbefalingene. En nærmere utforming av anbefalingene vil ha betydning for nytte- og kostnadsvirkningene, og disse bør utredes nærmere ved videre oppfølging.

Oslo Economics har på oppdrag fra utvalget bistått med samfunnsøkonomiske vurderinger av anbefalingene. Rapporten fra Oslo Economics følger som digitalt vedlegg.

Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Utvalget anbefaler at det utarbeides en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning. Den nye loven skal gjennomføre NIS-direktivet i norsk rett. Den skal gjelde for samfunnskritiske virksomheter og offentlig forvaltning, i tillegg til virksomheter som ellers omfattes av NIS-direktivet.

Oslo Economics trekker i sin rapport frem flere usikkerhetsmomenter når det gjelder de samfunnsøkonomiske konsekvensene ved innføring av en slik lov. Blant annet oppfatter Oslo Economics at det er usikkerhet knyttet til virkeområdene til eksisterende lover og forskrifter, og setter derfor spørsmålstegn ved om det er behov for en ny lov. Det pekes på at et alternativ til en ny lov er at man presiserer og avgrenser eksisterende regelverk.

Det er krevende å tallfeste de samfunnsøkonomiske kostnadene ved å innføre en ny lov. Det vil påløpe administrative kostnader i arbeidet med å utforme en ny lov. Det kan også tenkes at en ny lov om IKT-sikkerhet 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 ny lov. Videre er samfunnskritiske virksomheter en lite presis størrelse. Særlig når det gjelder utfordringer knyttet til IKT-sikkerhet, er det ikke enkelt å avgrense hvilke konkrete virksomheter loven skal gjelde for. Dette gjør det krevende å tallfeste de samfunnsøkonomiske kostnadene.

Utvalget har særlig vurdert insentivproblematikken i forkant av anbefaling av en ny lov. Selv om bedriftsøkonomiske kostnader ved IKT-sikkerhetsbrudd i noen tilfeller kan være relativt små, kan kostnadene for samfunnet være betydelige. Utvalget vurderer det slik at en ny lov vil påvirke insentivene til å prioritere IKT-sikkerhet, slik at den enkeltes beslutninger blir mer i samsvar med hva som er ønskelig sett fra samfunnets ståsted. Utvalget mener at de kravene som foreslås i en ny lov er et minimum av hva man kan forvente av samfunnskritiske virksomheter og offentlig forvaltning når det gjelder å sikre seg mot IKT-sikkerhetsbrudd.

Utvalget vurderer samlet sett at dersom man klarer å utforme en god lov vil mest sannsynlig de samfunnsøkonomiske nyttevirkningene av en ny lov overstige kostnadene.

Utvalget foreslår at det vurderes nærmere om det skal stilles krav om IKT-sikkerhet i lov til alle norske virksomheter. Det vil si virksomheter som ikke treffes av sikkerhetsloven og utvalgets forslag til lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning. En slik utredning må omfatte økonomiske og administrative konsekvenser.

Krav om IKT-sikkerhet ved anskaffelser

Utvalget anbefaler at det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser. Videre må IKT-sikkerhet bedre ivaretas i SSAene, og veiledning om IKT-sikkerhet ved anskaffelser må videreutvikles.

Det er ikke enkelt å tallfeste kostnadene ved eventuelle IKT-sikkerhetskrav i offentlige anskaffelser, selv om de kvalitativt lar seg identifisere. Hvis det er slik at noen leverandører får konkur-

ransefortrinn og større markedsmakt, kan det føre til at de tar høyere priser slik at det potensielt oppstår samfunnsmessige effektivitetstap.

Det kan allikevel være samfunnsøkonomiske nyttevirkninger av et slikt tiltak. Det er hovedsakelig fordi krav i anskaffelser kan endre adferden til både innkjøpere og tilbydere, slik at nødvendig sikkerhet prioriteres. Det kan også forventes at krav om IKT-sikkerhet i anskaffelser vil øke bevisstheten både hos de som kjøper og de som tilbyr tjenester.

Et krav vil medføre kostnader for de som lyser ut anbud, og også for tilbydere som må dokumentere sikkerheten i anskaffelsesprosessen. Som argumentert for i rapporten fra Oslo Economics kan forslaget derfor medføre samfunnsøkonomiske kostnader. Krav kan svekke konkurransen i noen markeder hvis de er for kostbare til å kunne innfris blant noen aktører. Formuleringene av kravene må derfor være veloverveide, slik at de stiller hensiktsmessige krav i lys av en samfunnsøkonomisk kost/nytte-vurdering.

Etablere et nasjonalt IKT-sikkerhetssenter

Utvalget mener det må etableres et nasjonalt IKT-sikkerhetssenter. Et slikt senter kan bidra til å styrke koordinering og samordning mellom sektorer og mellom offentlige og private aktører. Det vil være et sentralt kontaktpunkt som gir råd og veiledning til virksomheter, bidrar til å koordinere håndtering av uønskede digitale hendelser og sørger for å dele informasjon om trusler og sårbarheter.

Utvalget legger vekt på å organisere senteret med en tydelig forankring i sivile myndigheter. Senterets myndighetsforankring og kobling til NSM, og grensedragninger mot det planlagte nasjonale cyberkrimsenteret må avklares.

Parallelt med utvalgets arbeid er det kommet forslag fra myndighetene om å opprette et nasjonalt cybersikkerhetssenter som del av NSM. I den forbindelse har NSM utarbeidet et konseptnotat for senteret. Utvalget forstår forslaget i hovedsak som en intern omdisponering av ressurser i NSM. De fleste funksjonene til senteret slik det fremkommer i konseptnotatet ligger allerede i NSM sitt mandat.

Kostnadene ved å etablere et nasjonalt IKT-sikkerhetssenter er på nåværende tidspunkt ikke utredet.[1] Utvalget mener at det må gjøres ytterligere vurderinger knyttet til samfunnets behov for et IKT-sikkerhetssenter og kostnader ved dette. Dette er fordi det kan ha positive effekter å organisere senteret på en annen måte som ikke er vurdert.

Utvalget anbefaler at Justis- og beredskapsdepartementet, i samarbeid med Forsvarsdepartementet, må sørge for at det gjennomføres en uavhengig behovs- og kostnadsanalyse før et slik senter etableres. Som del av analysen bør også det rettslige rammeverket knyttet til informasjonsdeling vurderes, slik at det ikke er unødvendige hindringer for informasjonsdeling, både mellom miljøer og overfor offentligheten. Utvalget legger vekt på at behovsanalysen må gjøres av en uavhengig part. Det vil komme utgifter i forbindelse med innkjøp av tjenester for å gjennomføre en uavhengig behovsanalyse.

Tydelig regulering og ansvar for tilkoblede produkter og tjenester

Et viktig samfunnsøkonomisk spørsmål er hvem som bærer kostnadene ved potensielle IKT-sikkerhetsbrudd i tilkoblede produkter og tjenester. Hvis aktører har anledning til å skyve noe av kostnadene over på andre, kan dette føre til at sikkerheten i produktene nedprioriteres, og at det oppstår underinvestering i IKT-sikkerhet på dette området.

Utvalget mener at ansvaret for IKT-sikkerhet i tilkoblede produkter og tjenester i større grad bør flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjeneste. Norge må fortsette sitt internasjonale samarbeid på dette område, særlig opp mot regelverksprosesser i EU. Myndighetene må gi bedre råd og veiledning til importører, forhandlere og norske produsenter av tilkoblede produkter og tjenester. Videre bør DSB få en tydelig rolle når det gjelder varsling, rapportering, tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

Den viktigste nyttevirkningen av tiltaket kan være at man får reduserte insentivproblemer. Et tydeligere ansvar gjør det vanskeligere for produsenter og brukere å benytte utstyr med betydelig risiko for andre. Det antas videre at forslaget vil øke kompetansen, øke bevisstheten rundt IKT-sikkerhet i tilkoblede produkter og tjenester samt gjøre myndigheter og andre bedre i stand til å gi rådgivning til produsenter og forhandlere.

---

[1] For vurderinger av økonomiske kostnader knyttet til forslaget i konseptnotatet til NSM, se rapport fra Oslo Economics (digitalt vedlegg).

Forslaget må imidlertid utredes nærmere før man endelig kan fastslå de økonomiske og administrative konsekvensene.

Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Utvalget mener Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet. Etablering av et nasjonalt IKT-sikkerhetssenter og den nye loven om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning vil styrke departementets evne til å utøve et tydeligere lederskap for nasjonal IKT-sikkerhet. I tillegg anbefaler utvalget at Justis- og beredskapsdepartementet og Forsvarsdepartementet gjennomgår modellen for styring av NSM for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt, samtidig som koblingen mellom sivil sektor og forsvarssektoren beholdes. Videre mener utvalget at departementet må tilrettelegge for at tilsyn på IKT-sikkerhetsområdet koordineres bedre, og at tilsyn med teknisk IKT-sikkerhet gis økt oppmerksomhet.

Anbefalingene om at Justis- og beredskapsdepartementet må ta tydeligere lederskap har ingen klar økonomisk konsekvens, men det kan innebære noen mindre kostnader.

Bedre og tydeligere samordning av fagmiljøene på IKT-sikkerhetsområdet kan føre til bedre forebygging og håndtering. Tydeligere lederskap fra departementet kan også bidra til å redusere interessekonflikter mellom ulike offentlige etater i tilfeller hvor ønske om mer digitalisering kommer i konflikt med økt sikkerhet.

Utvalget er opptatt av å sette Justis- og beredskapsdepartementet i stand til å ta større lederskap. Slik utvalget ser det, har NSM en sentral rolle som Justis- og beredskapsdepartementets fagmiljø innenfor IKT-sikkerhet på sivil side. De understøtter også Forsvarsdepartementet i deres ansvar for IKT-sikkerhetsområdet i forsvarssektoren. Utvalget anbefaler at Justis- og beredskapsdepartementet og Forsvarsdepartementet gjennomgår modellen for styring av NSM. I dette arbeidet må økonomiske og administrative konsekvenser vurderes. I tillegg kan det komme utgifter i forbindelse med å gjennomføre en slik vurdering av gjeldende styringsmodell for NSM, for eksempel gjennom kjøp av konsulenttjenester eller lignende.

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 i departementet. Oslo Economics påpeker i sin rapport at 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.

Vedlegg 1

Relevant IKT-sikkerhetsregelverk

Det følger av mandatet at utvalget skal kartlegge relevant sektorspesifikt og tverrsektorielt regelverk. Utvalget har tatt utgangspunkt i at et regelverk stiller krav om IKT-sikkerhet hvis det inneholder bestemmelser om beskyttelse av IKT-systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene. Med begrepet «tverrsektorielt regelverk» forstås regelverk som stiller krav til offentlige og/eller private virksomheter i to eller flere samfunnssektorer. Begrepet «regelverk» avgrenses til å omfatte lov og forskrift. For statsforvaltningen omfattes også instrukser.

I fremstillingen av eksisterende relevant regelverk presenteres først tverrsektorielt regelverk. Deretter gjennomgås IKT-sikkerhetsregelverket i relevante sektorer. Utvalget har lagt vekt på det regelverket som primært gjelder IKT-sikkerhet. Det betyr at sektorer og virksomheter kan ha mer oppmerksomhet rettet mot IKT-sikkerhet enn det fremstillingen gir uttrykk for, men da for eksempel som en del av internkontrollen eller som regelverk om forebyggende sikkerhet. Utvalget har vurdert om regelverket ivaretar alle elementene som inngår i forsvarlig nasjonal IKT-sikkerhet, som er presentert i punkt 2.2.2.

1 Tverrsektorielt regelverk

1.1 Sikkerhetsloven[1]

Det følger av mandatet at utredningen skal være avgrenset mot bestemmelser, organisering og myndighet som følger av sikkerhetsloven og forslaget til ny sikkerhetslov (Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet). Utvalget mener likevel at den nye sikkerhetsloven vil legge viktige føringer for IKT-sikkerheten i Norge, og at det derfor er naturlig og relevant å presentere den her.

Gjeldende lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) blir avløst av ny lov 1. januar 2019. Utvalget har derfor valgt å fokusere på den nye loven.

I oktober 2016 overleverte Traavik-utvalget sin utredning med forslag til ny sikkerhetslov til regjeringen.[2] Utvalget peker på at samfunnet står overfor nye trusler og sårbarheter, at gjeldende sikkerhetslov ikke har vært praktisert etter intensjonen, og at det er behov for en styrket samhandling i det forebyggende sikkerhetsarbeidet.

Et sentralt tema for Traavik-utvalget, som også ligger til grunn for utformingen av lovforslaget, er avveiningen mellom behovet for en helhetlig og sektorovergripende tilnærming til forebyggende sikkerhet på den ene siden og ivaretakelse av den enkelte samfunnssektors særegenheter og ekspertise på den andre. Traavik-utvalget konkluderer med at den beste løsningen for balansert ivaretakelse av begge aspekter er ett felles regelverk for alle samfunnssektorer. Det tverrsektorielle aspektet ivaretas av Forsvarsdepartementet og Justis- og beredskapsdepartementet, med NSM som utøvende organ. Det sektorspesifikke aspektet ivaretas ved at det enkelte sektordepartementet gis mer myndighet, samtidig som det ansvarliggjøres i større grad enn etter eksisterende sikkerhetslov. For å tydeliggjøre behovet for samhandling mellom nasjonale og sektorvise myndigheter foreslår Traavik-utvalget egne bestemmelser om hvordan denne samhandling skal foregå.

Andre viktige endringer er at flere informasjonssystemer skal beskyttes mot et bredere spekter av risikoer enn i dag, objektbegrepet suppleres med infrastruktur, krav til sikkerhetsgraderte anskaffelser og sikkerhetsklarering samt rettsregler om eierskapskontroll.

Traavik-utvalgets rapport ble fulgt opp av regjeringen i Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet. Proposisjonen bygger i all hovedsak på anbefalingene fra Traavik-utvalget. Forslaget ble lagt frem for Stortinget i juni 2017, og et enstemmig Storting vedtok loven

[1] Sikkerhetsloven (lov 1. juni 2018 nr. 24 om nasjonal sikkerhet).

[2] NOU 2016: 19 *Samhandling for sikkerhet – beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.*

27. februar 2018. Loven og tilhørende forskrifter trer i kraft etter planen 1. januar 2019.

Formål og virkeområde

Formålet med lov om nasjonal sikkerhet er å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Formålet skal oppnås ved å forebygge, avdekke og motvirke tilsiktede hendelser som direkte eller indirekte kan skade de nevnte nasjonale verdiene.

Loven legger til grunn at et sett med *grunnleggende nasjonale funksjoner* må være identifisert for at de nasjonale sikkerhetsinteressene kan ivaretas. Eksempler på områder hvor det er slike funksjoner, er strømforsyning, vannforsyning, helsetjenester og transport. Totalforsvarskonseptet kan fungere som et veiledende utgangspunkt for hvilke funksjoner som skal omfattes. DSB har utarbeidet en oversikt over samfunnets kritiske funksjoner. I oversikten inngår flere av de grunnleggende nasjonale funksjonene.[3] Hvilke konkrete funksjoner som anses som grunnleggende nasjonale funksjoner, må vurderes konkret avhengig av både hvilke verdier som legges til grunn for vurderingen, og hvilke kriterier som legges til grunn for kritikalitet. Konkret hvilke funksjoner som skal omfattes, følger ikke direkte av lovens bestemmelser, men vil følge av departementenes identifisering i egen sektor, jf. § 2-1.

Pliktsubjektene etter loven er statlige, fylkeskommunale og kommunale organer, leverandører av varer og tjenester innen sikkerhetsgraderte anskaffelser og private virksomheter som av andre spesifiserte årsaker er underlagt loven etter vedtak av et departement. Det siste gjelder private virksomheter som råder over informasjon, informasjonssystemer, objekter eller infrastruktur, eller driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner. Med begrepet *avgjørende betydning* har lovgiveren ment å omfatte aktører som har en sentral rolle i opprettholdelsen av den aktuelle funksjonen. Vurderingen skal baseres på hvilken betydning bortfall eller svekkelse av virksomheten har for den funksjonen som virksomheten understøtter.

Sikkerhetskrav

Verdiene som skal sikres, er informasjon, informasjonssystemer, objekter og infrastruktur som er avgjørende for grunnleggende nasjonale funksjoner. De grunnleggende og generelle sikkerhetskravene loven stiller, er at virksomhetene må (i) ha et styringssystem for sikkerhet som er integrert i virksomhetsstyringen, (ii) regelmessig gjennomføre risikovurderinger, (iii) gjennomføre sikkerhetstiltak for å oppnå et forsvarlig sikkerhetsnivå, (iv) dokumentere tiltakene og (v) varsle om sikkerhetstruende virksomhet. Verdiene skal beskyttes ved å iverksette menneskelige, digitale og fysiske sikkerhetstiltak, og tiltakene skal være egnet som barriere eller for deteksjon, verifikasjon eller reaksjon. Samlet skal tiltakene gi et forsvarlig sikkerhetsnivå i virksomheten.

Videre stilles det enkelte spesifikke krav om sikringen av de ulike verdiene. Når det gjelder skjermingsverdige informasjonssystemer, skal de i henhold til lovens kapittel 6 sikres slik at de fungerer som de skal, at uvedkommende ikke får tilgang til informasjonen som behandles i systemene, at informasjonen som behandles i systemene, ikke endres eller går tapt, og at informasjonen som behandles i systemene, er tilgjengelig. I tillegg stilles det krav om godkjenning av informasjonssystemer og at virksomheten kontinuerlig skal overvåke egne informasjonssystemer (sikkerhetslogging). Det er også tatt inn bestemmelser som gir hjemmel for, men ikke krav om, å gjennomføre inntrengingstesting og kommunikasjons- og innholdskontroll av informasjonssystemene.

De nevnte bestemmelsene gjelder for alle skjermingsverdige informasjonssystemer som omfattes av loven. Avhengig av hva det enkelte informasjonssystemet blir brukt til, vil flere av de øvrige av sikkerhetslovens bestemmelser også få anvendelse. For skjermingsverdige informasjonssystemer som behandler sikkerhetsgradert informasjon, får også bestemmelsene om personellsikkerhet i kapittel 8 og sikkerhetsgraderte anskaffelser i kapittel 9 anvendelse. For skjermingsverdige informasjonssystemer som er utpekt eller inngår i et skjermingsverdig objekt eller en infrastruktur, får også bestemmelsene om objekt og infrastruktursikkerhet i kapittel 7 anvendelse, i tillegg til kapittel 8 og 9.

Reglene om sikkerhetsgraderte anskaffelser gjelder der leverandøren av en vare eller tjeneste kan få tilgang til eller skal tilvirke sikkerhetsgradert informasjon, og der anskaffelsen krever tilgang til et skjermingsverdig objekt eller en infrastruktur. Det følger av § 9-2 at før en slik anskaffelse iverksettes, skal virksomheten inngå en sikkerhetsavtale med leverandøren. Avtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar.

[3] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner.*

I § 9-4 er det tatt inn en varslingsplikt ved anskaffelser til et skjermingsverdig informasjonssystem, et objekt eller en infrastruktur. Virksomheten skal vurdere om anskaffelsen kan innebære en ikke ubetydelig risiko for at den aktuelle verdien kan rammes av eller bli brukt til sikkerhetstruende virksomhet. Kongen i statsråd kan i hvert enkelt tilfelle fatte vedtak om at anskaffelsen ikke skal gjennomføres, eller at det skal settes vilkår for denne.

Tilsynelatende gjelder det ikke bestemmelser om fysisk sikkerhet eller personell- eller leverandørsikkerhet for skjermingsverdige informasjonssystemer som ikke behandler sikkerhetsgradert informasjon, og heller ikke er utpekt som eller inngår i et skjermingsverdig objekt eller en infrastruktur.

Det slås imidlertid fast i særmerknadene til § 6-2 at «[v]ed utarbeidelse av tilstrekkelige sikkerhetstiltak bør det ses hen til internasjonale standarder for beskyttelse av informasjonssystemer». Traavik-utvalget uttalte blant annet at «[e]r et systems funksjonalitet viktig, og det er enkelt å skaffe seg fysisk tilgang til systemet, er det naturlig nok ikke tilstrekkelig å iverksette logiske sikkerhetstiltak. Da er det også behov for fysisk beskyttelse, og personer som skal ha tilgang, må være autorisert». De nærmere kravene om fysisk sikkerhet og personell- og leverandørsikkerhet vil følge av forskriftene til sikkerhetsloven.

Myndigheter

Sikkerhetsmyndighetens ansvar følger av § 2-2. Sikkerhetsmyndigheten har det overordnede ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven, og at sikkerhetstilstanden i alle sektorer kontrolleres. Sikkerhetsmyndigheten har et overordnet ansvar for at det føres tilsyn med hvordan virksomhetene etterlever loven, og skal utarbeide grunnleggende kriterier for tilsyn. Videre skal sikkerhetsmyndigheten innhente og vurdere informasjon som har betydning for forebyggende sikkerhetsarbeid, gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav om tiltak, bidra til å utvikle sikkerhetstiltak og holde oversikt over hvilke virksomheter som er utpekt etter vedtak.

Sikkerhetsmyndigheten skal også legge til rette for informasjonsdeling, slik at virksomhetene får tilgang til opplysninger som er av betydning for det forebyggende sikkerhetsarbeidet, blant annet trusselinformasjon. Sikkerhetsmyndigheten skal i samråd med sektormyndigheter og andre relevante myndigheter sikre at det etableres nødvendige fora for informasjons- og erfaringsutveksling.

Gjennomføring av tilsyn reguleres i sikkerhetsloven kapittel 3. I utgangspunktet kan sektordepartementet bestemme at myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, skal føre tilsyn også med etterlevelsen av sikkerhetsloven i sektoren. I praksis betyr dette at sektormyndigheter kan føre tilsyn såfremt disse har kompetanse til det. Dersom det ikke er utpekt tilsynsmyndighet i sektoren, skal sikkerhetsmyndigheten føre tilsyn med virksomheter som omfattes av loven. Nærmere bestemmelser om hvilke krav som skal stilles til tilsynsmyndighetene, vil følge av forskriftene. Tilsynsmyndighetene har etter § 3-6 mulighet til å gi pålegg om gjennomføring av tiltak som er nødvendige for å ivareta lovens formål.

Sikkerhetsmyndigheten skal i tillegg føre tilsyn med departementene og de utpekte tilsynsmyndighetene, jf. § 3-1 tredje ledd. Et slikt tilsyn skal blant annet undersøke om sektormyndighetenes tilsyn etter sikkerhetsloven føres i tråd med sikkerhetslovens krav og de grunnleggende kriteriene for tilsyn som er fastsatt av sikkerhetsmyndigheten.

I § 3-2 er det en egen bestemmelse om samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar. Første ledd bestemmer at det skal inngås en samarbeidsavtale, og at gjennomføring av tilsyn skal samordnes med andre tilsynsmyndigheter så langt det er mulig. Etter andre ledd skal sikkerhetsmyndigheten utarbeide og utvikle grunnleggende kriterier for tilsyn og legge til rette for felles opplæring av tilsynspersonell. Når det er nødvendig, kan sikkerhetsmyndigheten medvirke til forberedelse og gjennomføring av tilsyn som i utgangspunktet skal utføres av et sektortilsyn.

Oppsummering

Sikkerhetsloven stiller langt på vei krav om forsvarlig IKT-sikkerhet. Loven stiller kun krav om å sikre seg mot tilsiktede handlinger. Det er kun skjermingsverdige informasjonssystemer som skal beskyttes etter loven. Lovens bestemmelser om personellsikkerhet og sikkerhetsgraderte anskaffelser gjelder ikke for alle informasjonssystemer.

1.2 Personopplysningsloven[4]

Justis- og beredskapsdepartementet fremla i statsråd 23. mars 2018 forslag til ny lov om behandling av personopplysninger (personopplysningsloven).[5] Forordningen fikk anvendelse i EU-statene 25. mai 2018 og trådte i kraft i Norge 20. juli 2018.[6]

Den nye personopplysningsloven avløser gjeldende personopplysningslov og består av to hovedelementer. For det første gjøres EUs personvernforordning til norsk lov gjennom en inkorporasjonsbestemmelse. Forordningen er tatt inn som vedlegg til loven og vil på mange områder danne utgangspunktet for lovreguleringen. For det andre vil en rekke bestemmelser i den norske lovteksten supplere reglene i forordningen.

Formål og virkeområde

Loven og personvernforordningen gjelder ved helt eller delvis automatisert behandling av personopplysninger og ved ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register. Loven og personvernforordningen gjelder ikke når annet er bestemt i eller med hjemmel i lov.[7]

Pliktsubjektene i loven er den behandlingsansvarlige og databehandleren. Den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Databehandleren er den som behandler personopplysninger på vegne av den behandlingsansvarlige.

Hvem som er de viktigste aktørene i regelverket, endres ikke. Det er fortsatt den registrerte som skal vernes, og det stilles krav til den behandlingsansvarlige og databehandleren. En av endringene er at forordningen stiller flere direkte krav og gir større ansvar til databehandleren enn tidligere.

Sikkerhetskrav

Den forrige personopplysningsloven § 13 stilte krav om informasjonssikkerhet til både den behandlingsansvarlige og databehandleren. Det het i første ledd at

> [d]en behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

Den nye personopplysningsloven har ingen egne bestemmelser om informasjonssikkerhet, men det er krav om sikkerhet i både artikkel 24, 25 og 32.

Artikkel 24 om den behandlingsansvarliges ansvar fastsetter en plikt til å gjennomføre «egnede tekniske og organisatoriske tiltak», jf. artikkel 24 nr. 1. Tiltakene skal både «sikre» og «påvise» at behandlingen utføres i samsvar med forordningens krav. Det skal tas hensyn til «behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Etter artikkel 24 nr. 2 skal tiltakene omfatte «iverksetting av egnede retningslinjer for vern av personopplysninger», dersom dette står i et rimelig forhold til behandlingsaktivitetene. Overholdelse av godkjente atferdsnormer eller sertifiseringsmekanismer kan brukes som en faktor for å påvise at forpliktelsene overholdes, jf. artikkel 24 nr. 3.[8]

Plikten etter artikkel 24 må sees i sammenheng med blant annet reglene om innebygd personvern og personvern som standardinnstilling, jf. artikkel 25. Personopplysningsloven og forskriften har i dag ingen bestemmelser som tilsvarer forordningens bestemmelser om innebygget personvern eller personvern som standardinnstilling. Plikten til å sørge for innebygd personvern følger av artikkel 25 nr. 1, som bestemmer at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak «både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen». Kravet om tiltak allerede fra tidspunktet for fastsettelse av midlene som skal benyttes, innebærer at det ved utvikling av løsninger for behandling av

---

4 Personopplysningsloven (lov 15. juni 2018 nr. 38 om behandling av personopplysninger).

5 Prop. 56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordningen (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.*

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

7 Jf. § 2.

8 Prop. 56 LS (2017–2018) *Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordningen (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen,* s. 110.

personopplysninger må bygges inn personverntiltak fra begynnelsen av.[9]

Personvern som standardinnstilling innebærer at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det «som standard» bare behandles personopplysninger som er nødvendige for hvert spesifikke formål. Forpliktelsen gjelder mengden personopplysninger, omfanget av behandlingen, lagringstiden og tilgjengeligheten av personopplysningene. Det er særlig nevnt i artikkel 25 nr. 2 at tiltakene skal sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall personer uten den registrertes medvirkning. Etter artikkel 25 nr. 3 kan en godkjent sertifiseringsmekanisme i henhold til artikkel 42 brukes som en faktor for å påvise at kravene til innebygget personvern og personvern som standardinnstilling er oppfylt.[10]

Artikkel 32 fastslår at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», jf. artikkel 32 nr. 1. Eksempler på slike tiltak fremgår av bokstav a til d. En angivelse av sentrale elementer i risikovurderingen følger av artikkel 32 nr. 2. Overholdelse av godkjente atferdsnormer etter artikkel 40 eller en godkjent sertifiseringsmekanisme etter artikkel 42 kan brukes som en faktor for å påvise at kravene til informasjonssikkerhet er oppfylt, jf. artikkel 32 nr. 3. Etter artikkel 32 nr. 4 skal den behandlingsansvarlige og databehandleren sikre at enhver som handler på vegne av den behandlingsansvarlige eller databehandleren, bare behandler opplysninger etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes rett pålegger en plikt til behandling.[11]

I forbindelse med høringen om den nye personopplysningsloven uttalte departementet om sikkerhetsbestemmelsene at:[12]

> [e]tter departementets vurdering vil imidlertid anvendelse av reglene i artikkel 32 trolig lang på vei gi samme resultat som gjeldende regler slik de er formulert i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.

Departementet gikk derfor inn for at forordningen artikkel 32 skulle gis anvendelse som en videreføring av personopplysningsloven § 13.

Datatilsynet har utarbeidet en veileder om internkontroll og informasjonssikkerhet.[13] Blant annet gis det veiledning om hvordan styringssystem for informasjonssikkerhet kan iverksettes. Når det gjelder sikring av IKT-systemer, viser veilederen til NSMs grunnprinsipper for IKT-sikkerhet.

Oppsummering

Personopplysningsloven stiller krav om forsvarlig IKT-sikkerhet for de IKT-systemene som loven omfatter. Det er krav om både risikovurdering og beskyttelse. Det er spesifikke krav til tekniske og organisatoriske løsninger, krav om innebygd personopplysningsvern og krav til utforming av informasjonssystemer og -arkitektur. Det stilles også sikkerhetskrav til databehandleren som behandler personopplysninger på vegne av den behandlingsansvarlige.

Det er kun virksomheter og systemer som behandler personopplysninger, som er omfattet av regelverket.

1.3 Lov om elektroniske tillitstjenester[14]

Lov om tillitstjenester ble tatt inn i EØS-avtalen 9. februar 2018. Loven ble vedtatt av Stortinget i juni og trådte i kraft 15. juni 2018. Loven avløste da samtidig lov om elektronisk signatur (esignaturloven). Det nye regelverket skal bidra til økt elektronisk samhandling mellom næringsdrivende, innbyggere og offentlige myndigheter på tvers av landegrensene i EØS.

Bakgrunnen for loven er EU-forordningen om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre markedet (eIDAS-forordningen). eIDAS-forordningen trådte i kraft i EU 1. juli 2016. Formålet med eIDAS-forordningen er å sikre et velfungerende marked og oppnå et passende sikkerhetsnivå for elektronisk identifikasjon og tillitstjenester.

eIDAS-forordningen består av to deler. Første del regulerer elektronisk identifisering (eID), som Difi er ansvarlig for. Andre del regulerer tillitstjenester, som Nkom er tilsynsmyndighet for.

---

9 Ibid.

10 Ibid.

11 Ibid. s. 112.

12 Justis- og beredskapsdepartementet (2017) *Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett – høringsnotat.* Punkt 13.5.3.

13 Datatilsynet (2018) *Internkontroll og informasjonssikkerhet, veileder.*

14 Lov om elektroniske tillitstjenester (lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked).

Formål og virkeområde

Artikkel 2 definerer virkeområdet. Forordningen gjelder for elektroniske identifikasjonsordninger som har blitt meldt inn av en medlemsstat. Videre gjelder den for tilbydere av tillitstjenester som er etablert i EU. Begrepet «tillitstjenester» er i artikkel 3 nr. 16 definert som en elektronisk tjeneste som normalt utføres mot betaling, herunder fremstilling, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektronisk registrerte leveringstjenester og sertifikater knyttet til disse tjenestene, eller fremstilling, kontroll og validering av sertifikater for nettstedsautentisering, eller lagring av elektroniske signaturer, segl eller sertifikater knyttet til disse tjenestene.[15]

Forordningen gjelder ikke for tillitstjenester som utelukkende er brukt innenfor lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer.[16]

Sikkerhetskrav

Forordningen legger til rette for å oppnå elektronisk samhandling mellom innbyggere i EU ved å regulere tillitstjenester. Tillitstjenestene er avgrenset til å omfatte de tjenestene som er tilgjengelige og omsettes på det åpne markedet. Forordningen styrker dagens eksisterende krav om elektronisk signatur og innfører krav til flere typer elektroniske tillitstjenester. De fleste kravene i forordningen gjelder for kvalifiserte tillitstjenester, og disse er i artikkel 3 nr. 17 definert som tillitstjenester som oppfyller forordningens krav.[17]

Lov om tillitstjenester regulerer flere nye typer tjenester, inkludert sertifikater for elektroniske segl (virksomhetssertifikater) og nettstedsertifikater (SSL/TLS-sertifikater). Tillitstjenester benyttes blant annet ved bruk av nettbank og ved innlogging på offentlige tjenester.

Alle tilbydere av tillitstjenester må iverksette tekniske og organisatoriske tiltak for å håndtere sikkerhetsrisikoen ved de tjenestene de tilbyr. Tilbyderne skal også melde fra til Nkom om sikkerhetshendelser som i betydelig omfang påvirker tillitstjenesten. Melding skal sendes Nkom innen 24 timer etter at tilbyderen har blitt oppmerksom på hendelsen.

Oppsummering

Lov om elektroniske tillitstjenester stiller krav om forsvarlig IKT-sikkerhet for de IKT-systemene som omfattes av loven (betalingssystemer og identifikasjonssystemer).

1.4 Forvaltningsloven[18]

Formål og virkeområde

Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) gjelder for alle forvaltningsorganer. Loven hjemler blant annet forskrift om elektronisk kommunikasjon med og i forvaltningen (eforvaltningsforskriften).[19]

Sikkerhetskrav

Loven regulerer ikke IKT-sikkerhet direkte, det følger imidlertid taushetsplikt for «enhver som utfører tjeneste eller arbeid for et forvaltningsorgan» for opplysninger om noens personlige forhold og forretningsrelaterte opplysninger som det vil være av konkurransemessig betydning å hemmeligholde jf. § 13 første ledd. Bokstav c i § 13 c fastslår at «[d]okumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal forvaltningsorganet oppbevare på betryggende måte». Det er forskriftshjemmel til å gi nærmere krav til oppbevaring av dokumenter og annet materiale som omhandler taushetspliktbestemmelser.

Videre er det forskriftshjemmel i § 15 a om elektronisk kommunikasjon mellom forvaltningen og publikum og elektronisk saksbehandling og kommunikasjon i forvaltningen. Begge bestemmelsene understøttes av krav i beskyttelsesinstruksen og eforvaltningsforskriften.

Eforvaltningsforskriften gir konkrete føringer ved bruk av elektronisk kommunikasjon i et forvaltningsorgan, blant annet i § 5. Det vises her til at risiko for uberettiget innsyn i opplysningene ved bruk av elektronisk kommunikasjon må «være forebygget på tilfredsstillende måte», jf. § 5, første ledd.

---

15 Prop. 71 LS (2017–2018) *Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen*, s. 10 og 11.

16 Ibid., s. 10.

17 Ibid., s. 27.

18 Forvaltningsloven (lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker).

19 Eforvaltningsforskriften er hjemlet i både forvaltningsloven, arkivloven og lov om elektroniske tilleggstjenester.

Eforvaltningsforskriften har ingen definisjon av informasjonssikkerhet, men hjemmelen for forskriften sier blant annet at det kan gis nærmere bestemmelser om signering, autentisering, sikring av integritet og konfidensialitet (forvaltningsloven § 15 a punkt b).

For de aller fleste forvaltningsorganer oppfylles eforvaltningsforskriftens sikkerhetskrav gjennom det samme styringssystemet som de følger etter den tidligere personopplysningsforskriften. Med eforvaltningsforskriften vil tilsvarende krav også gjelde for forvaltningsorganer som ikke behandler personopplysninger.

På forvaltningslovens område suppleres informasjonssikkerhetskravene i personopplysningsloven av kravene i eforvaltningsforskriften § 15. Forskriftens krav om informasjonssikkerhet er mer detaljerte enn personopplysningsloven, men legger til rette for samordning av krav og tiltak. Forskriften nevner personopplysningslovens krav spesielt.

Eforvaltningsforskriften har lagt opp til visse muligheter for å harmonisere sikkerhetsnivået på tvers av forvaltningsorganer, dels ved det veiledningsansvaret Difi er tildelt i medhold av § 15, og dels ved det koordinerende organet som utpekes i medhold av § 36. Det er også gitt en forskrift om IT-standarder i forvaltningen med hjemmel i forvaltningsloven § 15 a, og Difi foreslår årlig endringer av denne som forelegges Kommunal- og moderniseringsdepartementet for beslutning.

Oppsummering

Forvaltningsloven og eforvaltningsforskriften stiller krav om IKT-sikkerhet, men har noen mangler. For det første er det usikkert om forskriften gjelder for alle relevante IKT-systemer i offentlig forvaltning. For det andre stilles det relativt vage sikkerhetskrav. For det tredje har eforvaltningsforskriften ikke bestemmelser om tilsyn.

1.5 Sivilbeskyttelsesloven[20]

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven) har som formål å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når riket er i krig, når krig truer, når rikets selvstendighet eller sikkerhet er i fare, og ved uønskede hendelser i fredstid, jf. § 1.

Etter § 14 plikter kommunen å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer, og hvordan de i så fall kan påvirke kommunen. Resultatet av dette arbeidet skal vurderes og sammenstilles i en helhetlig risiko- og sårbarhetsanalyse. Med utgangspunkt i risiko- og sårbarhetsanalysen etter § 14 skal kommunen utarbeide en beredskapsplan. Beredskapsplanen skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelser. Som et minimum skal beredskapsplanen inneholde en plan for kommunens kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media, jf. § 15.

I DSBs veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen er cyberangrep og hacking anført som to eksempler på tilsiktede uønskede hendelser som kommunen skal vurdere.[21]

Oppsummering

I den grad sivilbeskyttelsesloven stiller krav om IKT-sikkerhet er kravene vagt utformet.

1.6 Aksjeloven og allmennaksjeloven[22]

Formål og virkeområde

Lov om aksjeselskaper (aksjeloven) og lov om allmennaksjeselskaper (allmennaksjeloven) gjelder for selskaper som har valgt aksjeselskap eller allmennaksjeselskap som selskapsform, og gir til sammen en samlet regulering av de to selskapsformene.

Sikkerhetskrav

§ 1-6 i begge lovene stiller krav til utarbeidelse og oppbevaring av dokumentasjon som kreves utarbeidet etter aksjeloven. Bestemmelsen ble tilføyd ved lov 16 juni 2017 nr. 71 (med ikrafttredelse 1. juli 2017). Bestemmelsene ble fremmet som en

[20] Sivilbeskyttelsesloven (lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret).

[21] Direktoratet for samfunnssikkerhet og beredskap (2014) *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen.* s. 62

[22] Aksjeloven (lov 13. juni 1997 nr. 44 om aksjeselskaper). Allmennaksjeloven (lov 13. juni 1997 nr. 45 om allmennaksjeselskaper).

del av forslaget til modernisering og forenkling av aksjelovgivningen.[23]

Bestemmelsen gjelder kun for «dokumentasjon som kreves utarbeidet etter aksjeloven». Eksempler på dette er aksjeeierboken, stiftelsesdokumenter, generalforsamlingsprotokoller og styreprotokoller. Bestemmelsen gjelder altså ikke sikring av all informasjon, tjenester eller systemer hos selskaper underlagt de to lovene.

Bestemmelsen stiller først og fremst krav om at dokumentasjonen skal være sikret mot urettmessig endring, ødeleggelse og tap. Kravet skal også ivareta behovet for notoritet, aktørenes mulighet til signering på hensiktsmessig måte og videreformidling av dokumentasjon. Bestemmelsen sidestiller fysisk og elektronisk kommunikasjon og utarbeidelse hvor aksjeloven har krav om skriftlighet.

I forarbeidene til bestemmelsen ble det vurdert at det var behov for å sikre at dokumentasjon er beskyttet mot endring, men at det ikke er behov for eksplisitte krav til dette i aksjelovene.[24]

Departementet viste til bokføringsloven § 13 tredje ledd første punktum, som krever at dokumentasjon skal oppbevares «ordnet» og være «betryggende sikret mot ødeleggelse, tap og endring». På grunn av den verdien selskapsdokumentasjon kan ha, mente departementet at det kan være hensiktsmessig å pålegge selskapene en eksplisitt plikt til å sikre dokumenter mot ødeleggelse, tap og endring. Departementet skriver videre at:[25]

> [e]n generell plikt til å ha IT-systemer som sikrer mot endring av dokumenter, eller som sporer hvem som har endret et dokument og når det ble gjort, vil påføre selskapene en økonomisk og administrativ byrde. De som velger aksjeselskaps- og allmennaksjeselskapsformen, oppnår begrenset ansvar. De må derfor i en viss utstrekning godta at selskapet, blant annet av hensyn til kreditorer, pålegges flere byrder enn de som velger selskapsformer med ubegrenset deltakeransvar. Departementet antar at strenge krav til IT-systemene vil begrense selskapenes muligheter med hensyn til valg av medium for dokumentasjon. En mulig konsekvens er at selskaper istedenfor elektroniske løsninger velger papirbasert lagring eller ikke følger loven. Det vil kunne hindre automatisert kommunikasjon og rapportering til offentlige myndigheter og andre aktører. Departementet foreslår derfor at det i utgangspunktet skal være opp til det enkelte selskap å vurdere hva som vil være tilfredsstillende informasjonssikkerhet. Løsningen selskapet velger, må imidlertid være slik at dokumentasjonen kan oppbevares på en betryggende måte. Løsningen må gi en forholdsmessig sikkerhet mot endring, ødeleggelse og tap. I tillegg må det foretas sikkerhetskopiering. Skulle senere erfaringer tilsi at det er behov for nærmere regulering av hva som er en betryggende oppbevaringsmåte, vil det være hensiktsmessig å regulere dette i forskrift. Det foreslås derfor en hjemmel til å gi nærmere bestemmelser i forskrift.

Det er ikke gitt noen nærmere krav i forskrift til hva som er betryggende oppbevaringsmåte.

Oppsummering

Aksjeloven og allmennaksjeloven inneholder ikke krav om forsvarlig IKT-sikkerhet. Det er enkelte bestemmelser om sikring av informasjon, men det stilles ikke krav om sikring av IKT-systemer som understøtter virksomhetenes produksjon av varer og tjenester.

1.7 Arkivloven[26]

Formål og virkeområde

Lov om arkiv (arkivloven) med tilhørende forskrifter gjelder for alle offentlige organer med unntak for Stortinget, Riksrevisjonen, Sivilombudsmannen og andre organer for Stortinget.[27] Alle organene plikter å ha arkiv, og arkivene skal være ordnet og innrettet slik at dokumentene er trygge informasjonskilder for samtid og ettertiden.

Sikkerhetskrav

Loven inneholder en vid forskriftshjemmel i § 12: «Kongen gjev utfyllande føresegner om journalsystem, arkivnøklar, arkivinstruksar, dokument-

[23] Prop. 112 L (2016–2017) *Endringer i aksjelovgivningen mv. (modernisering og forenkling)*. Lovforslaget tar utgangspunkt i utredningen NOU 2016: 22 *Aksjelovgivning for økt verdiskaping* som aksjelovutvalget overleverte til Nærings- og fiskeridepartementet 21. oktober 2016.

[24] Prop. 112 L (2016–2017) *Endringer i aksjelovgivningen mv. (modernisering og forenkling)*. s. 23.

[25] Ibid. s. 23–24.

[26] Arkivloven (lov 4. desember 1992 nr. 126 om arkiv).

[27] Riksarkivaren kan i tillegg registrere visse privatarkiv som særskilt verneverdige. En slik registrering medfører at private blir underlagt visse retningslinjer som følger av loven.

kvalitet, arkivutstyr, arkivlokale, arkivavgrensingar, kassasjon, bortsetjingsarkiv, avlevering, refusjonsreglar m.m., og om rett til å klaga over Riksarkivarens avgjerder.»[28]

Forskrifter om *dokumentkvalitet, arkivutstyr* og *arkivlokale* vil kunne omfatte krav om IKT-sikkerhet.

Frem til 1. januar 2018 inneholdt arkivforskriften kapittel 4 detaljerte krav om fysisk sikkerhet for arkivrommet. Det var klare krav til organisering av arkivet, arkivsystemet, lagringsmedium, backup, rutiner for mottak av informasjon, utlevering, kassasjon og så videre. Kravene var primært knyttet til tilgjengelighet, men integritet omfattes også av bestemmelsene.

Kulturdepartementet har revidert og vedtatt en ny versjon av arkivforskriften og riksarkivarens forskrift.[29] Den nye arkivforskriften erstatter detaljerte krav med overordnede og funksjonelle krav. Disse endringene legger til rette for tilpasning til ulike organisatoriske og teknologiske løsninger. Det er nå krav til lagringsmedium og format (§ 6) og krav til arkivlokale (§ 7), men krav til system for elektronisk journal og arkiv skal fastsettes av Riksarkivaren (§ 11). Mer detaljerte tekniske og arkivfaglige bestemmelser er flyttet til forskrift om tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver, som fastsettes av Riksarkivaren.

I riksarkivarens forskrift § 3-1 (3) står det at system for journalføringspliktige saksdokumenter, jf. arkivforskriften § 9, skal følge krav som Riksarkivaren med hjemmel i arkivforskriften § 11 har fastsatt i Norsk arkivstandard (Noark).

Noark setter krav til systemenes informasjonsinnhold (hvilke opplysninger som skal registreres og gjenfinnes), datastruktur (utforming av data og deres relasjon), funksjonalitet (hvilke funksjoner systemene skal støtte) og brukergrensesnitt (hvordan systemet kommuniserer med brukerne). Det er Riksarkivaren som har tilsynsmyndighet med lov og forskrift.

Oppsummering

Arkivloven stiller noen krav om IKT-sikkerhet. De kravene som stilles er vagt utformet.

1.8 Bokføringsloven[30]

Formål og virkeområde

Lov om bokføring (bokføringsloven) med forskrifter gjelder for alle som har regnskapsplikt etter regnskapsloven. Formålet med regelverket er å sørge for at regnskapsrapportering er tilfredsstillende sikret og dokumentert.

Sikkerhetskrav

Regelverket regulerer krav om sikring av regnskapsmateriale mot endringer og sletting. Det stilles ingen krav om konfidensialitet. Kravene er formulert i lovens § 13 hvor det fremgår at «[o]ppbevaringspliktig regnskapsmateriale skal oppbevares ordnet og være betryggende sikret mot ødeleggelse, tap og endring». I bokføringsforskriften kapittel 7 stilles det krav til oppbevaringsmedium og sikkerhetskopi.[31]

Etter bokføringsforskriften § 7-5 kan bokføringspliktige «oppbevare elektronisk regnskapsmateriale i et annet EØS-land dersom avtale eller overenskomst sikrer norske skatte- og avgiftsmyndigheter tilfredsstillende adgang til regnskapsinformasjonen for kontrollformål i oppbevaringstiden, og slik oppbevaring ikke vil være til hinder for effektiv norsk politietterforskning». I tillegg må de informere Skattedirektoratet om hvilket regnskapsmateriale som oppbevares i utlandet, hvor regnskapsmaterialet oppbevares, og hvordan kontrollmyndighetene til enhver tid kan få adgang til regnskapsmaterialet.

Loven og forskriftene inneholder ingen øvrige krav til IKT-systemer eller tjenester.

Skatteetaten er utøvende forvaltningsmyndighet etter bokføringsloven.

---

[28] Vedtatte forskrifter under § 12:
Riksantikvarens forskrift. Forskrift 19. desember 2017 nr. 2286 om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver.
Forskrift om offentlege arkiv. Forskrift 15. desember 2017 nr. 2105.
Helsearkivforskriften. Forskrift 18. mars 2016 nr. 268 om Norsk helsearkiv og Helsearkivregisteret.
Kjernejournalforskriften. Forskrift 31. mai 2013 nr. 563 om nasjonal kjernejournal.
Forskrift om trossamfunn. Forskrift 19. april 2005 nr. 345 om registrerte og uregistrerte trossamfunn.
Eforvaltningsforskriften. Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen.
Forskrift om personellsikkerhet 29. juni 2001 nr. 722.
Forskrift om tilskot til livssynssamfunn 1. desember 1988 nr. 996.

[29] Vedtatt i statsråd 15.12.2017. Ikrafttredelse fra 1.1.2018. Høringsnotatet gjennomgår både arkivmessige utfordringer og fordeler ved bruk av skytjenester, men omtaler ikke IKT-sikkerhet eksplisitt.

[30] Bokføringsloven (lov 19. november 2004 nr. 73 om bokføring).

[31] Bokføringsforskriften. Forskrift 1. desember 2004 nr. 1558 om bokføring.

Oppsummering

Bokføringsloven stiller noen krav om IKT-sikkerhet. De kravene som stilles er vagt utformet.

1.9 Straffeloven[32]

Straffeloven inneholder ingen bestemmelser som regulerer forsvarlig IKT-sikkerhet. Derimot inneholder straffeloven flere bestemmelser om datakriminalitet.

De mest sentrale bestemmelsene i straffeloven om datakriminalitet er § 201 (Uberettiget befatning med tilgangsdata, dataprogram mv.), § 204 (Innbrudd i datasystem) og § 206 (Fare for driftshindring).

Hacking er straffbart etter § 201, som omfatter forsettlig handling som uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen a) passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem, eller b) dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem.

Innbrudd i datasystem er straffbart etter § 204. Det er ikke et vilkår for straff at gjerningspersonen har gjort seg kjent med dataene eller informasjonen i datasystemet, det er tilstrekkelig at personen har skaffet seg tilgang til dem. Det er ikke et vilkår at innbruddet skjer ved å bryte en beskyttelse, jf. «eller på annen uberettiget måte».[33]

Datamaskinens tilgjengelighet er vernet gjennom § 206, som gjelder fare for driftshindringer. Handlinger som gjør datasystemer utilgjengelige, vil normalt rammes av den alminnelige bestemmelsen om skadeverk, jf. § 351, eller forsøk på slikt skadeverk.[34]

Oppsummering

Bestemmelsene om datakriminalitet i straffeloven har hovedsakelig innretning mot at en handling er skjedd. Det er ingen bestemmelser om straffeansvar for handlinger som leder opp til datakriminalitet.

[32] Straffeloven (lov 20. mai 2005 nr. 28 om straff).

[33] Ot.prp. nr. 22 (2008–2009) *Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning),* s. 403.

[34] Ibid. s. 405.

2 Sektorregelverk

Utvalget har kartlagt eksisterende krav om IKT-sikkerhet i sektorregelverk. Regelverkene er valgt ut basert på sektorer som vil være underlagt NIS-direktivet, og sektorer som inngår i DSBs oversikt over samfunnets kritiske funksjoner.[35]

Utvalget har vurdert i hvilken grad sektorregelverk har krav om forsvarlig IKT-sikkerhet. Utvalget legger til grunn at det kan være formuleringer eller krav som brukes til å sikre IKT-systemer, tjenester eller leveranser i regelverk utover det som er nevnt, men mener denne presentasjonen omfatter de viktigste.

Næringsberedskapsloven og forurensingsloven har ikke særskilte krav om IKT-sikkerhet.[36] Lovene omtales ikke nærmere nedenfor.

2.1 Elektroniske kommunikasjonsnett og -tjenester

Om sektoren

Denne sektoren omfatter elektronisk kommunikasjon gjennom kommersielle nett og Nødnett.[37]

Regulering av IKT-sikkerhet i sektoren

I ekomsektoren er krav om IKT-sikkerhet hovedsakelig formulert som sikkerhets- og beredskapsplikter som er pålagt tilbydere av elektroniske kommunikasjonsnett og -tjenester i Norge. De er i nedfelt i ekomloven, ekomforskriften, klassifiseringsforskriften og forskrift om prioritet i mobilnett, i tillegg til enkeltvedtak fra Nkom.[38] I hovedsak er kravene i ekomloven kapittel 2 og spesielt ekomloven §§ 2-7, 2-9 og 2-10 og ekomforskriften kapittel 8.

Lov om elektronisk kommunikasjon (ekomloven) regulerer kommersielle ekomtilbydere i Norge, og er grunnlaget for reguleringen av den nasjonale kommunikasjonsinfrastrukturen. Formålet med loven er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester gjennom effektiv bruk

[35] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner*

[36] Næringsberedskapsloven (lov 16. desember 2011 nr. 65 om næringsberedskap). Forurensingsloven (lov 13. mars 1981 nr. 6 om vern mot forurensninger og om avfall).

[37] Ibid. s. 82.

[38] Ekomforskriften. Forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste. Klassifiseringsforskrifta. Forskrift 10. september 2012 nr. 866 om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett. Forskrift om prioritet i mobilnett. Forskrift 21. oktober 2013 nr. 1241.

av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse og stimulere til næringsutvikling og innovasjon.

Ekomloven § 2-10 sier at tilbyder skal tilby ekomnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig, og opprettholde nødvendig beredskap. Myndigheten kan gjennom vedtak eller forskrift presisere hva som er forsvarlig sikkerhet og nødvendig beredskap. Etter § 2-7 har en tilbyder plikt til å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i egne elektroniske kommunikasjonsnett og -tjenester. Videre kan myndigheten fatte enkeltvedtak, inngå avtale eller gi forskrift om at tilbyderne skal gjennomføre tiltak for å oppfylle nasjonale behov for sikkerhet, beredskap og funksjonalitet. Dette er ment å sikre tiltak som går ut over forsvarlighetsnivået nevnt ovenfor. Merkostnadene knyttet til slike tiltak kompenseres av staten. § 2-9 pålegger tilbydere og installatører taushetsplikt og plikt til å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder, får anledning til selv å skaffe seg kjennskap til slike opplysninger.

Klassifiseringsforskriften skal sikre nettutstyr i anlegg mot uønsket ytre fysisk påvirkning, og retter seg mot tilbydere av elektroniske kommunikasjonsnett som benyttes til offentlig elektronisk kommunikasjonstjeneste (nettilbydere). Nettilbydere skal klassifisere alle anlegg ut fra hvor viktig eget nettutstyr i anleggene er for offentlige elektroniske kommunikasjonstjenester. Sentralt i klassifiseringsforskriften er bestemmelsen som krever at nettilbyderne gjennomfører en helhetlig risiko- og sårbarhetsvurdering knyttet til sine anlegg, og sørger for at anlegg i de ulike klassene er forsvarlig sikret i samsvar med denne vurderingen. Nkom har utarbeidet egen veiledning for klassifiseringsforskriften og skjema for rapportering.

I ekomforskriften § 8-2 har tilbydere plikt til å utarbeide og vedlikeholde beredskapsplaner. Det forutsettes at det ligger dokumenterte risiko- og sårbarhetsvurderinger til grunn for disse beredskapsplanene. Det fremkommer også av § 8-2 at tilbyderne på forespørsel skal delta på beredskapsøvelser arrangert av myndigheten.

Varsling

Etter ekomloven § 2-7 fjerde ledd plikter en tilbyder å varsle myndighetene straks dersom det foreligger særlig risiko for brudd på sikkerheten eller sikkerhetsbrudd som har krenket personvernet til en abonnent eller bruker.

Etter ekomforskriften § 8-5 skal en tilbyder «varsle Nasjonal kommunikasjonsmyndighet om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester».

Tilsyn

Nkom er tilsynsmyndighet og fører tilsyn med blant annet IKT-sikkerhet. Tilsynsmyndigheten kan kreve opplysninger som er nødvendige for gjennomføringen av loven eller vedtak gitt i medhold av loven. Den som er gjenstand for tilsyn, har medvirkningsplikt. Myndigheten har påleggskompetanse.

Sanksjoner

For å sikre at krav fastsatt i eller i medhold av ekomloven oppfylles, kan Nkom fastsette tvangsmulkt, jf. ekomloven § 10-7. Ved forsettlig eller uaktsom overtredelse av blant annet §§ 2-4 til 2-10, kan Nasjonal kommunikasjonsmyndighet pålegge overtredelsesgebyr.

Oppsummering

Sektoren for elektronisk kommunikasjonsnett og –tjenester er underlagt krav om «forsvarlig sikkerhet». Dette omfatter også forsvarlig IKT-sikkerhet, men kravet til forsvarlig IKT-sikkerhet er i liten grad detaljert i regelverket. Mye av detaljstyringen gjøres gjennom veiledning, tilsyn og enkeltvedtak fattet av Nkom.

2.2 Finansielle tjenester

Om sektoren

Finansiell stabilitet er et hovedmål for myndighetenes styring av finanssektoren. Dette innebærer at det finansielle systemet må være robust overfor forstyrrelser, slik at det er i stand til å formidle finansiering, utføre betalinger og omfordele risiko på en tilfredsstillende måte. Det finansielle systemet består av finansmarkeder, finansinstitusjoner og finansiell infrastruktur.[39]

Finanstilsynet er ansvarlig leder og sekretariat for Beredskapsutvalget for finansiell infrastruktur (BFI). Hvert år redegjør Finanstilsynet i en egen rapport for sitt syn på risikoen og sårbarheten innen finanssektoren knyttet til finansforetakenes bruk av IKT.

[39] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner*, s. 82.

Regulering av IKT-sikkerhet i sektoren

Krav om IKT-sikkerhet i finansnæringen er hovedsakelig regulert gjennom forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften), som gjelder for norske banker og finansforetak.[40] Forskriften er hjemlet i betalingssystemloven, børsloven og finanstilsynsloven.[41] Forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet og skal sikre at IKT-virksomheten leverer de tjenestene som er avtalt, også der hele eller deler av IKT-virksomheten er utkontraktert til andre aktører. Den stiller blant annet krav om planlegging og organisering av sikkerhetsarbeidet, risikoanalyse og avviks- og endringshåndtering.

For å vurdere om finansforetakene etterlever kravene i IKT-forskriften, benytter Finanstilsynet såkalt egenevaluering. Spørsmålene er basert på Cobit, ITIL, ISO og andre kilder, tilpasset av Finanstilsynet for det norske finansmarkedet. Finanstilsynet har utarbeidet en veileder for etterlevelse av IKT-forskriften § 5 om sikkerhet og risiko- og sårbarhetsanalyser. I tillegg har de utarbeidet veiledninger som er tilpasset spesielle foretak, mindre sparebanker og eiendomsmeglingsforetak.

For kredittinstitusjoner er det gitt nærmere krav om risikostyring og internkontroll i CRR/CRD IV-forskriften §§ 27–31.[42] Det følger blant annet av § 27 at det skal etableres retningslinjer for operasjonell risiko som skal omfatte beredskapsplaner for å sikre at driften kan videreføres og tap begrenses ved alvorlige driftsforstyrrelser.

Børsloven har bestemmelser om taushetsplikt (§ 14). I dette ligger det indirekte et krav om at regulerte markeder skal ha et kontrollsystem som sikrer at innsyn i taushetsbelagt informasjon er avgrenset i størst mulig grad, og at tilgang til slik informasjon blir kontrollert.

Verdipapirhandelloven[43] har bestemmelser om innsideinformasjon, taushetsplikt og tilbørlig informasjonshåndtering. I dette ligger det indirekte et krav om at foretakene skal ha et kontrollsystem som sikrer at innsyn i taushetsbelagt informasjon er avgrenset i størst mulig grad, og at tilgang til slik informasjon blir kontrollert.

Varsling

IKT-forskriften § 9 stiller krav om at foretakene skal rapportere til Finanstilsynet om avvik som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data. Rapporteringen skal normalt omfatte hendelser som foretaket selv kategoriserer som svært alvorlig eller kritisk, men kan også omfatte andre avvik.

Tilsyn

Finanstilsynet fører tilsyn med de aktuelle virksomhetene. Dette inkluderer tilsyn med IKT-sikkerheten i virksomhetene. Virksomhetene har medvirkningsplikt, og tilsynet har påleggskompetanse.

Sanksjoner

Finanstilsynet har etter finanstilsynsloven påleggsmyndighet. Blant annet kan tilsynet gi pålegg om at foretaket skal innrette internkontrollen sin etter de bestemmelsene tilsynet fastsetter, jf. § 4, og om å stanse virksomhet, jf. § 4 a.

I medhold av finanstilsynsloven § 10 kan departementet bestemme at det skal betales løpende mulkt ved forsettlig eller uaktsom overtredelse av bestemmelser gitt i eller i medhold av loven.

Finansforetaksloven gir i § 22-2 departementet hjemmel til å gi pålegg og tvangsmulkt ved overtredelse av bestemmelser gitt i eller i medhold av loven.[44] Tilsvarende hjemmel finnes i betalingssystemloven § 6-3.

Verdipapirhandelloven § 16-3 og børsloven § 47 gir Finanstilsynet hjemmel til å gi pålegg om retting og stansing.

Oppsummering

IKT-forskriften som gjelder for finanssektoren stiller krav om forsvarlig IKT-sikkerhet. Den sikrer alle systemer som er av betydning for foretakets virksomhet. Forskriftens krav om sikkerhet og

[40] Forretningsbanker, sparebanker, finansieringsforetak, forsikringsselskaper, private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond, børser og autoriserte markedsplasser, verdipapirforetak, forvaltningsselskaper for verdipapirfond, oppgjørssentraler, verdipapirregistre, inkassoforetak, eiendomsmeglerforetak, betalingsforetak, e-pengeforetak og systemer for betalingstjenester.

[41] Betalingssystemloven (lov 17. desember 1999 nr. 95 om betalingssystemer m.v.). Børsloven (lov 29. juni 2007 nr. 74 om regulerte markeder). Finanstilsynsloven (lov 7. desember 1956 om tilsynet med finansforetak mv.).

[42] CRR/CRD IV-forskriften. Forskrift 22. august 2014 nr. 1097 om kapitalkrav og nasjonal tilpasning av CRR/CRD IV.

[43] Verdipapirhandelloven (lov 29. juni 2007 nr. 75 om verdipapirhandel).

[44] Finansforetaksloven (lov 10. april 2015 nr. 17 om finansforetak og finanskonsern).

dokumentasjon må ivaretas ved eksterne tilkoblinger eller brukere.

2.3 Helse og omsorg

Om sektoren

Denne sektoren omfatter helse- og omsorgstjenester.

Regulering av IKT-sikkerhet i sektoren

Den viktigste kilden til IKT-sikkerhet i sektoren er Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen). Normen er ikke en egen lov eller forskrift, men en samling av krav om personvern og informasjonssikkerhet som helsesektoren har utarbeidet, og som er basert på regulering.[45] Normen er derfor per definisjon *soft law*, men fordi den gir uttrykk for gjeldende regulering, er den omhandlet her og ikke i punkt 19.3.

Formålet med Normen er å etablere mekanismer hvor virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. Ifølge Datatilsynet er Normen et egnet verktøy i arbeidet for å etterleve personopplysningslovens og helseregisterlovens bestemmelser om informasjonssikkerhet.[46] [47] Helseregisterloven, personopplysningsloven og øvrig regelverk stiller enkelte krav om behandling av helse- og personopplysninger utover det som er tema for Normen.

Innenfor helsesektoren er det gjennomgående at alle krav som stilles om IKT-sikkerhet, har med behandlingen av personopplysninger å gjøre. Kravene er også nesten likelydende. Både helsetilsynsloven, helseberedskapsloven, helseregisterloven, pasientjournalloven og 19 forskrifter stiller alle nesten likelydende krav om sikring av informasjon. Kravene bygger i stor grad på det som er spesifisert i personvernforordningen artikkel 32.[48]

Det er også andre funksjoner i regelverket enn sikring av informasjon. Helsetilsynsloven hjemler for eksempel forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.[49] Formålet med forskriften er å bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og til at øvrige krav i helse- og omsorgslovgivningen etterleves. I forskriften presiseres det at den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (styringssystem). Videre presiseres plikten til å dokumentere, planlegge, gjennomføre, evaluere og korrigere.

Forskrift om IKT-standarder i helse- og omsorgstjenesten bidrar til at virksomheter i helse- og omsorgstjenesten som yter helsehjelp, bruker IKT-standarder for å fremme sikker og effektiv elektronisk samhandling.[50] Forskriften gjelder private og offentlige virksomheter innen helse- og omsorgstjenesten som bruker behandlingsrettede helseregistre, jf. pasientjournalloven § 2 bokstav d. Direktoratet for e-helse gir ut en katalog med oversikt over obligatoriske og anbefalte standarder.

I NAV-loven § 10 fremkommer det at Arbeids- og velferdsdirektoratet skal påse at det utarbeides planer for beredskap i etaten. Planene skal inneholde krav om opprettholdelse av driftssikkerhet for behandling av krav om ytelser og for utbetaling, til lagring av materiell og utstyr, og til øvelser og opplæring av personell. Direktoratet skal videre påse at avtaler med leverandører av varer og tjenester inneholder krav om leveringsdyktighet og informasjonssikkerhet ved kriser i fred- og krigstid, og det skal sikre arbeidskraftbehovet til samfunnsviktige virksomheter ved krise i fred eller krig samt opprettholde systemer for kartlegging av samfunnsviktige virksomheter og deres behov.

I forskrift om rekvirering og utlevering av legemidler fra apotek kan departementet med hjemmel i § 9-3 stille særskilte krav om oppbevaring av EDB-baserte reseptopplysninger.[51] Det gjelder også resepter og rekvisisjoner som er overført elektronisk.

Pasientjournalloven gjelder all behandling av helseopplysninger som er nødvendig for å yte,

---

45 Norsk Helsenett. *Hva er Normen?* Hentet fra: https://www.nhn.no/hva-er-normen/

46 Direktoratet for e-helse. *Datatilsynets vurdering av Normen.* Hentet fra: https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/datatilsynets-vurdering-av-normen

47 Helseregisterloven (lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger).

48 Helsetilsynsloven (lov 30. mars 1984 nr. 15 om statlig tilsyn med helse- og omsorgstjenesten m.m.). Helseberedskapsloven (lov 23. juni 2000 nr. 56 om helsemessig og sosial beredskap). Pasientjournalloven (lov 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp).

49 Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten. Forskrift 28. oktober 2016 nr. 1250.

50 Forskrift om IKT-standarder i helse- og omsorgstjenesten. Forskrift 1. juli 2015 nr. 853.

51 Forskrift om legemidler fra apotek. Forskrift 27. april 1998 nr. 455 om rekvirering og utlevering av legemidler fra apotek.

administrere eller kvalitetssikre helsehjelp til enkeltpersoner. Lovens formål er at behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at relevante og nødvendige opplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell, samtidig som vernet mot at opplysninger gis til uvedkommende, ivaretas, og sikrer pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.

Helseregisterloven gjelder for behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten. Formålet med loven er å legge til rette for innsamling og annen behandling av helseopplysninger for å fremme helse, forebygge sykdom og skade og gi bedre helse- og omsorgstjenester. Loven skal sikre at behandlingen foretas på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste.

Formålet med helseberedskapsloven er å «verne befolkningens liv og helse og bidra til at nødvendig helsehjelp, helse- og omsorgstjenester og sosiale tjenester kan tilbys befolkningen under krig og ved kriser og katastrofer i fredstid. For å ivareta lovens formål, skal virksomheter loven omfatter kunne fortsette og om nødvendig legge om og utvide driften under krig og ved kriser og katastrofer i fredstid, på basis av den daglige tjeneste, oppdaterte planverk og regelmessige øvelser, slik det er bestemt i eller i medhold av loven».

Varsling

Etter Normen punkt 6.3 skal Datatilsynet varsles dersom det har blitt foretatt en uautorisert utlevering av helse- og personopplysninger.

Det følger av helseberedskapsloven § 2-3 at virksomheter loven omfatter, plikter å varsle om forhold innen helse- og omsorgstjenesten eller sosialtjenesten som kan gi grunnlag for tiltak etter denne lov. Varsel gis til departementet eller den myndighet departementet bestemmer.

I helse- og omsorgssektoren er det for øvrig en rekke bestemmelser med krav om å varsle om uønskede hendelser. Disse hendelsene er imidlertid primært relatert til personskade og/eller bivirkninger ved pasientbehandlingen.

Tilsyn

Det finnes i dag ikke et eget sektortilsyn for IKT-sikkerhet på helseområdet. Statens helsetilsyn er øverste tilsynsmyndighet og har det overordnede faglige tilsynet med helse- og omsorgstjenestene og folkehelsearbeid, jf. helsetilsynsloven § 1. Statens helsetilsyn har myndighet til å pålegge retting av avvik, jf. § 5. Fylkesmannen er faglig underlagt Statens helsetilsyn og fører tilsyn. Helsedirektoratet har en koordinatorrolle for sektorens innsats ved kriser. Det gjelder også hendelser som inkluderer svikt i IKT-systemer.

Datatilsynets oppgaver tar i hovedsak utgangspunkt i personopplysningsloven med hovedfokus på personvern, men de har i tillegg tilsynsansvar for pasientjournalloven. Tilsyn med helseregistrene vil i hovedsak utføres av Datatilsynet.

Sanksjoner

Helsetilsynsloven § 5 gir Statens helsetilsyn adgang til å gi pålegg om å «rette på forholdene».

Pasientjournalloven §§ 27, 28 og 29 gir Datatilsynet hjemmel til henholdsvis å gi pålegg, fastsette tvangsmulkt og gi overtredelsesgebyr ved overtredelser av bestemmelser gitt i eller i medhold av loven. Tilsvarende hjemler følger av helseregisterloven §§ 27, 28 og 29.

Oppsummering

Reguleringen i helse- og omsorgssektoren stiller i hovedsak krav om forsvarlig sikring av informasjon. Det inkluderer krav om sikring av IKT-systemer som behandler pasientinformasjon, men det er få krav om sikring av IKT-systemer som ikke har den type informasjon.

2.4 Kraftforsyning

Om sektoren

Kraftforsyning omfatter de systemer og leveranser som er nødvendige for å ivareta samfunnets behov for elektrisk energi til oppvarming, husholdning, produksjon, transport med mer, og fjernvarme der slike anlegg er utbygd.[52]

Regulering av IKT-sikkerhet i sektoren

For elektrisitetssektoren gjelder energiloven.[53] Loven hjemler beredskapsforskriften. Energiloven stiller både krav om informasjonssikkerhet

[52] Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner,* s. 86.

[53] Energiloven (lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.).

(§ 9-3) og krav om sikring av system og anlegg i beredskapsforskriften.

Beredskapsforskriften gjelder forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring og fordeling av elektrisk energi eller fjernvarme.

Det følger av beredskapsforskriften § 1-3 at den gjelder for virksomheter som helt eller delvis eier eller driver anlegg eller system som er, eller kan bli, av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.

Beredskapsforskriften stiller krav om internkontroll, varsling og rapportering, risikovurderinger, tilgangskontroll og tilgang til systemene fra leverandører. I tillegg er kravene i forskriften differensiert, slik at de viktigste selskapene er underlagt de strengeste sikkerhetskravene.

NVE sendte forslag til revidert beredskapsforskrift på høring før jul 2017.[54] Forslaget bygger på anbefaling fra Lysne-utvalget og NVEs egen gjennomgang av eksisterende regelverk for å styrke arbeidet med å håndtere de risikoer som følger med digitaliseringen.[55] Forskriftsendringene vil tre i kraft fra 1. januar 2019.[56]

Forslaget innebærer at det stilles krav om grunnsikring for alle digitale informasjonssystemer hos alle virksomheter som er underlagt forskriften. Kravene gjelder alle nettselskaper, omsettere, produsenter, fjernvarmevirksomheter og andre aktører som kontrollerer produksjon, omforming, overføring, omsetning og fordeling av energi på til sammen minst 100 GWh per år, og som vil kunne ha en vesentlig betydning for energiforsyningen.

Den digitale grunnsikringen innebærer at virksomheter plikter å sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Grunnsikring for digitale informasjonssystemer skal være i henhold til anerkjente standarder og normer, deriblant å identifisere og dokumentere, sikre og oppdage, håndtere og gjenopprette. I tillegg til at det er krav om ROS-analyse og tjenesteutsetting.

Varslingskrav

Det er varslings- og rapporteringsplikt for virksomhetene til beredskapsmyndigheten for alle ekstraordinære situasjoner. Varslet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson. Det er foreslått å splitte denne bestemmelsen i to, en for varsling når noe ekstraordinært skjer, og en for rapportering etter at hendelsen er over, jf. forslag til §§ 2-5 og 2-6.

I forslaget § 6-9 er det lagt opp til at «[v]irksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til det sektorvise responsmiljøet».

Hendelseshåndtering behandles gjennom KraftCERT og kraftforsyningens beredskapsorganisasjon (KBO). KBO ledes av beredskapsmyndigheten (NVE).

Tilsyn

Det er i energiloven § 10-1 hjemmel til å føre kontroll med at bestemmelser gitt i eller i medhold av energiloven blir overholdt. NVE fører tilsyn med virksomhetenes etterlevelse av IKT-sikkerhetskrav i beredskapsforskriften.

Sanksjoner

Energiloven §§ 10-1, 10-3 og 10-7 hjemler henholdsvis pålegg, tvangsmulkt og overtredelsesgebyr. Det samme gjør beredskapsforskriften §§ 8-4 og 8-5.

Oppsummering

Regelverket til kraftsektoren stiller krav om forsvarlig IKT-sikkerhet. Det er mange selskaper og systemer som kan være utenfor virkeområdet til grunnsikringen i og med at det er først og fremst bare KBO-enheter som det stilles krav til. Dette gjelder særskilt omsettere av elektrisk energi.

2.5 Justissektoren

Om sektoren

Justissektoren omfatter i grove trekk domstolene, politi og påtalemyndighet og kriminalomsorgen. I tillegg inngår oppgaver hvor ansvaret er tillagt Tolletaten og helseforetak.

Regulering av IKT-sikkerhet i sektoren

Innenfor justissektoren er det først og fremst krav om IKT-sikkerhet som gjelder personopplys-

---

54 Norges vassdrags- og energidirektorat (2017) *Forslag til endringer i beredskapsforskriften*

55 Norges vassdrags- og energidirektorat (2017) *Regulering av IKT-sikkerhet.*

56 Norges vassdrags- og energidirektorat (2018) *Oppsummeringsdokument: endringer i beredskapsforskriften – krav til IKT-sikkerhet m.m.*

ninger, som er regulert gjennom eksisterende lovgivning. Eksempler på dette er politiregisterloven § 15, SIS-loven § 3 og SIS-forskriften kapittel 7, som stiller krav som samsvarer kravene i personopplysningsloven.[57] Det er også eksempler på forskriftshjemler for ivaretakelse av informasjonssikkerhet, slik som straffegjennomføringsloven § 4 e.[58]

Flere av bestemmelsene inneholder formuleringer som kunne vært brukt til å stille sikkerhetskrav til systemer og tjenester, men forarbeidene er klare på at formålet med bestemmelsene er sikring av personopplysninger.

Utvalgets gjennomgang har kartlagt to forskrifter som omtaler mer enn sikring av informasjon:

1. Politiregisterforskriften § 73-3 første ledd stiller krav til at politiet skal foreta nedtegning av alle behandlinger som følger av tilgangen til VIS, slik at det er mulig å kontrollere om søkene er tillatt, om behandlingen er lovlig og for å utføre internkontroll og sikre datakvalitet og datasikkerhet, og om systemet fungerer korrekt.[59]
2. I ELSAM-forskriften § 12 er det (i tillegg til krav til tilfredsstillende informasjonssikkerhet) krav til at elektronisk kommunikasjon mellom domstolen og en registrert bruker skal sikres med tilfredsstillende innloggingssystem og betryggende metode for å autentisere kommunikasjonspartene.[60]

Oppsummering

Regelverket innenfor justissektoren stiller delvis krav om forsvarlig IKT-sikkerhet. Det er enkelte bestemmelser om sikring av informasjon, men det stilles ikke krav om sikring av IKT-systemer som understøtter virksomhetenes produksjon av varer og tjenester.

2.6 Olje- og gass

Om sektoren

Produksjon av olje og gass inngår ikke i DSBs rapport om kritiske samfunnsfunksjoner. Det er ikke klarlagt om denne sektoren vil bli omfattet av et regelverk som gjennomfører NIS-direktivet i norsk rett. Lysne-utvalget inkluderte Olje- og gassektoren i sin gjennomgang av kritiske samfunnsfunksjoner.

Regulering av IKT-sikkerhet i sektoren

Olje- og gassindustrien har en funksjonsbasert regulering innenfor helse, miljø og sikkerhet. Petroleumsloven stiller krav til sikkerhet (kapittel 9), og § 10-1 setter krav om forsvarlig petroleumsvirksomhet.[61] Blant annet skal petroleumsvirksomheten ivareta hensynet til sikkerhet for de økonomiske verdiene som innretninger og fartøyer representerer. I dette ligger også et krav om sikring av driftstilgjenglighet. Det følger av særmerknaden til bestemmelsen at sikkerhetsbegrepet skal tolkes vidt.

Kravene er funksjonelle og angir sjelden et spesifikt nivå for oppfyllelse. Det angis gjennom henvisninger til standarder i de enkelte veiledningene til forskriftsbestemmelsene. Selve systemet for dette følger av rammeforskriften § 24.[62] Sikkerhetsreglene er omfattende, og det følgende er et utdrag av de mest relevante reglene.

Etter styringsforskriften § 7 skal den ansvarlige fastsette og videreutvikle mål og strategier for å forbedre helse, miljø og sikkerhet.[63] Operatøren skal sikre at det er samsvar mellom kortsiktige og langsiktige mål på ulike områder, på ulike nivå og mellom ulike deltakere i virksomheten. Målene skal uttrykkes slik at det er mulig å ta stilling til graden av måloppnåelse.

Det følger av styringsforskriften § 17 at det skal utføres risikoanalyser som gir et nyansert og mest mulig helhetlig bilde av risikoen forbundet med virksomheten. Risikoanalysene skal blant annet identifisere og analysere risikoreduserende tiltak, jf. rammeforskriften § 11 og styringsforskriften §§ 4 og 5.

---

57 Politiregisterloven (lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten). SIS-loven (lov 16. juli 1999 nr. 66 om Schengen informasjonssystem (SIS)). SIS-forskriften. Forskrift 21. desember 2000 nr. 1365 til lov om Schengen informasjonssystem.

58 Straffegjennomføringsloven (lov 18. mai 2001 nr. 21 om gjennomføring av straff mv.).

59 Visa Information System. Politiregisterforskriften. Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten.

60 ELSAM-forskriften. Forskrift 28. oktober 2016 nr. 1528 om elektronisk kommunikasjon med domstolene.

61 Petroleumsloven. Lov 19. juni 2015 nr. 65 om petroleumsvirksomhet.

62 Rammeforskriften. Forskrift 12. februar 2010 nr. 158 om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg.

63 Styringsforskriften. Forskrift 29. april 2010 nr. 611 om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg.

Styringsforskriften § 4 bestemmer at ved reduksjon av risiko som nevnt i rammeforskriften § 11, skal den ansvarlige velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.

Forskrift om Petroleumsregisteret § 5-1 stiller krav om at opplysninger i Petroleumsregisteret blir samlet inn, registrert, oppbevart og benyttet på en forsvarlig måte. Det skal tas sikkerhetskopier av Petroleumsregisteret.

Regelverket legger altså til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak. Dette gjøres gjennom risiko- og beredskapsanalyser i de enkelte selskapene. Bransjens egenutviklede standarder legges til grunn for arbeidet. Næringen har selv, gjennom Norsk olje og gass, utarbeidet spesifikke retningslinjer for informasjonssikkerhet i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer. Retningslinjene er basert på ISO 270001/2-standarden.

Hendelseshåndtering

Det følger av styringsforskriften § 17 at det skal gjennomføres beredskapsanalyser. Det følger videre av aktivitetsforskriften § 76 at det skal utarbeides beredskapsplaner som til enhver tid beskriver beredskapen og inneholder aksjonsplaner for de definerte fare- og ulykkessituasjonene.[64] Aktuelle bekjempelsesmetoder skal være beskrevet i beredskapsplanen. Aktivitetsforskriften § 77 setter krav til den faktiske håndteringen av fare- og ulykkessituasjoner.

Varsling

Etter styringsforskriften § 29 skal operatøren sikre varsling til Petroleumstilsynet ved fare- og ulykkessituasjoner som har ført til, eller under ubetydelig endrede omstendigheter kunne ha ført til død, alvorlig og akutt skade, akutt livstruende sykdom, alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer, slik at innretningens eller landanleggets integritet er i fare eller ved akutt forurensning. Veiledningen til bestemmelsen presiserer at dette også gjelder «situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse)».

Petroleumstilsynet har utarbeidet et standardskjema for varsling av hendelser, hvor det blant annet skal fylles inn tidspunkt for hendelsen, hvem som var involvert, hendelsesforløpet og skadeomfanget.

Tilsyn

Det er hjemmel i petroleumsloven § 10-3 til å føre tilsyn med at bestemmelsene gitt i eller i medhold av petroleumsloven blir overholdt av alle som driver petroleumsvirksomhet som omfattes av loven.

Petroleumstilsynet fører tilsyn med næringens arbeid med IKT-sikkerhet. I mai/juni 2017 ble det gjennomførte en tilsynskampanje med alle operatører med felt og anlegg i drift og redere med alle flyttbare innretninger (primært borerigger) som er registrert i et nasjonalt skipsregistersom (SUT). Tilsynet rettet seg mot virksomhetenes arbeid med beskyttelse av datasystemer på anlegg og innretninger som ivaretar styring av prosessene, overvåker mulige gassutslipp eller branntilløp og foretar sikker nedstengning av innretninger og anlegg.

Sanksjoner

Det er hjemmel i § 10-3 til å gi pålegg og § 10-16 hjemler flere tvangsmidler, herunder tvangsmulkt. Overtredelsesgebyr er ikke regulert, men i § 10-13 gis Kongen myndighet til å kalle tilbake tillatelser som er gitt i medhold av loven.

Oppsummering

Sikkerhetskravene er generelt utformet og det er uklart om de inkluderer IKT-sikkerhet.

2.7 Satellittbaserte tjenester

Om sektoren

Satellittbaserte tjenester har et bredt spekter av bruksmuligheter, som har til felles at de leveres ved hjelp av satellitter. En satellitt er et legeme som går i bane rundt jorden. Satellitter bærer nyttelaster til ulike formål og er plassert i baner som er tilpasset formålet. Satellitter kan ha nyttelaster for jordobservasjon, navigasjon, kommunikasjon eller vitenskapelige undersøkelser, eller en kombinasjon av disse.

Regulering av IKT-sikkerhet i sektoren

Sektoren er hovedsakelig underlagt krav om IKT-sikkerhet i ekomloven og sikkerhetsloven.

[64] Aktivitetsforskriften. Forskrift 29. april 2010 nr. 613 om utføring av aktiviteter i petroleumsvirksomheten.

Utover dette stiller § 6 i forskrift om etablering, drift og bruk av jordstasjon for satellitt krav om drift og sikring av jordstasjoner. Det er der eksplisitte krav om at en jordstasjon skal sikres slik at uvedkommende ikke får adgang til stasjonen eller kjennskap til innholdet i data som sendes til eller mottas fra en satellitt.

Oppsummering

Det er uklart om det stilles tilstrekkelige krav om IKT-sikkerhet til virksomhetene i sektoren.

2.8 Transport

Gjennomgangen under er inndelt i luftfartssystemet, jernbanesystemet, det maritime transportsystemet og veitransportsystemet.

2.8.1 Luftfartssystemet

Regulering av IKT-sikkerhet i sektoren

Luftfartsloven regulerer både sivil og militær luftfart.[65] Blant annet reguleres landingsplasser og flysikringstjenesten. Ulike deler av sektoren er regulert ulikt. Flysikringstjenesten kan sies å ha kommet lengst når det gjelder IKT-sikkerhet. Det følger av forskrift om flysikringstjenester at tjenesteleverandøren plikter å ha et sikkerhetsstyringssystem. Indirekte stilles det krav om sikring av relevante IKT-systemer.[66]

Det pågår regelverksarbeid i regi av Det europeiske luftfartssikkerhetsbyrået (EASA), som ønsker et helhetlig fokus på IKT-sikkerhet i luftfarten. Regelverket vil omfatte både lufthavner, flyselskap og flysikringstjenesten. Regelverket antas å kunne tre i kraft i løpet av 2020. FNs luftfartsorganisasjon, ICAO, har vedtatt en folkerettslig bindende standard som krever at luftfartsaktører gjennomfører risikovurderinger, identifiserer de kritiske systemene sine og innfører tiltak for å sikre disse. Standarden trådte i kraft i november 2018.

Varsling

Det fremgår ikke eksplisitte krav om varsling av sikkerhetshendelser i det gjeldende regelverket. Det legges likevel til grunn at luftfarten har et omfattende rapporteringssystem hvor alle hendelser som har betydning for flysikkerheten, i utgangspunktet skal rapporteres. Hendelser innen IKT-sikkerhet skal også rapporteres i den grad de har betydning for flysikkerheten.

Tilsyn

Luftfartstilsynet fører tilsyn med IKT-sikkerheten, i hovedsak flysikringstjenesten.

Sanksjoner

Luftfartsloven §§ 13 a-4 og 13 a-5 gir hjemmel for henholdsvis å fastsette tvangsmulkt og å gi pålegg om overtredelsesgebyr i forbindelse med overtredelser av loven eller bestemmelser fastsatt med hjemmel i loven, herunder forskrift om felles krav for yting av flysikringstjenester.

Oppsummering

Samlet sett stilles det i sektoren per i dag bare delvis krav om IKT-sikkerhet. Med det pågående internasjonale regelverksarbeidet ser det ut til at virksomheter i luftfartssektoren på sikt blir underlagt hensiktsmessige krav om IKT-sikkerhet.

2.8.2 Jernbanesystemet

Regulering av IKT-sikkerhet i sektoren

Jernbaneloven gir departementet hjemmel til å fastsette forskrift om sikring mot tilsiktede uønskede handlinger, herunder bestemmelser om kriseledelse, om taushetsplikt og om hvilke virksomheter som skal omfattes av forskriften.[67] Hjemmelen inkluderer også IKT-sikkerhet.[68]

Samferdselsdepartementet har delegert til Statens jernbanetilsyn å fastsette forskrifter etter loven. Sikringsforskriften pålegger jernbanevirksomheter å arbeide systematisk og proaktivt for å unngå tilsiktede uønskede handlinger og begrense konsekvensene av dem.[69]

Sikringsforskriften stiller krav til styringssystemer, herunder ansvar for oppgaver som utføres av leverandører, krav til dokumentasjon, taushetsplikt, prosedyrer, ansvarsforhold, beredskap, kompetansekrav, opplæring og så videre. Virk-

---

65 Luftfartsloven (lov 11. juni 1993 nr. 101 om luftfart).

66 Jf. forskrift 22. desember 2014 nr. 1902 om felles krav for yting av flysikringstjenester.

67 Jernbaneloven (lov 11. juni 1991 nr. 100 om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. § 6 a).

68 Prop. 107 L (2014–2015) *Om endringer i jernbaneloven (sikring mot tilsiktede uønskede handlinger),* jf. Innst. 311 L (2014–2015) *Innstilling fra transport- og kommunikasjonskomiteen om endringer i jernbaneloven (sikring mot tilsiktede uønskede handlinger)*.

69 Sikringsforskriften. Forskrift 1. juli 2015 nr. 848 om sikring på jernbane.

somhetene skal utarbeide risikovurderinger, og det stilles krav om hvordan disse skal følges opp og oppdateres. Videre stilles det krav om systematisk gjennomføring av revisjoner, oppfølging av uønskede hendelser, beredskapsøvelser og oppfølging av avvik.

Varsling

Sikringsforskriften stiller krav til at jernbanevirksomheter skal ha styringssystem som dekker sikring, inkludert IKT-sikkerhet. Krav om systemer omfatter også etterlevelse og praktisering av bestemmelsene i systemet. Det stilles krav om at virksomhetene skal sikre at nødvendige tiltak blir satt i verk raskest mulig, og beredskapen skal blant annet omfatte beredskapsplanverk med tydelig rollefordeling, varslingslister og innsatsplaner.

Tilsyn

Statens jernbanetilsyn fører tilsyn med at bestemmelsene i sikringsforskriften overholdes, jf. jernbaneloven § 11.

Sanksjoner

Jernbaneloven § 13 hjemler tvangsmulkt ved manglende oppfylling av pålegg. § 14 gir hjemmel til å fastsette forskrift om gebyr for kontrolltiltak som gjennomføres for å sikre at loven eller vedtak i medhold av loven blir fulgt.

Oppsummering

Dagens regulering stiller langt på vei krav om forsvarlig IKT-sikkerhet. Kravene er imidlertid vagt utformet og avhenger av virksomhetens eget initiativ til å sørge for et forsvarlig sikkerhetsnivå.

2.8.3 Det maritime transportsystemet

Regulering av IKT-sikkerhet i sektoren

Havne- og farvannsloven skal legge til rette for god fremkommelighet, trygg ferdsel og forsvarlig bruk og forvaltning av farvannet i samsvar med allmenne hensyn og hensynet til fiskeriene og andre næringer.[70] Loven skal også legge til rette for effektiv og sikker havnevirksomhet som ledd i sjøtransport og kombinerte transporter samt for effektiv og konkurransedyktig sjøtransport av personer og gods innenfor nasjonale og internasjonale transportnettverk. Loven hjemler to særlig relevante forskrifter.

Det følger av havneanleggssikringsforskriften § 10 andre ledd og havnesikringsforskriften § 9 andre ledd at det skal utarbeides en sikringsplan for hvert enkelt anlegg på bakgrunn av en sårbarhetsvurdering.[71] [72] Krav til sårbarhetsvurderingen og sikringsplanen følger av henholdsvis vedlegg 1 og 2. Det er eier av havneanlegget som er ansvarlig for at oppgavene og forpliktelsene følges opp.

Skipssikkerhetsloven skal trygge liv og helse, miljø og materielle verdier ved å legge til rette for god skipssikkerhet og sikkerhetsstyring, herunder hindre forurensing fra skip, sikre et fullt forsvarlig arbeidsmiljø og trygge arbeidsforhold om bord på skipet samt et godt og tidsmessig tilsyn.[73] Loven stiller krav om å etablere, gjennomføre og videreutvikle et dokumenterbart og verifiserbart sikkerhetsstyringssystem i rederiets organisasjon og på det enkelte skipet, for å kartlegge og kontrollere risiko samt sikre etterlevelse av krav fastsatt i eller i medhold av lov eller i sikkerhetsstyringssystemet selv.

ISM-koden (International Safety Management Code) er den internasjonale normen for sikkerhetsstyringssystemer på skip, og er tatt inn i norsk rett gjennom forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger. ISM-koden regulerer blant annet krav til sertifisering, revisjon og avvikshåndtering. Regelverket har ikke eksplisitte krav om IKT-sikkerhet, men kravene er generelt utformet og passer også for vurdering og håndtering av slik risiko.

International Maritime Organization (IMO) har vedtatt resolusjon MSC.428(98) som angir at rederiene senest innen første årlige revisjon etter 1. januar 2021 skal innarbeide vurdering og håndtering av risiko knyttet til sikkerhet i nettverk og digitale løsninger som en del av sikkerhetsstyringssystemet. Bakgrunnen for resolusjonen er at disse risikoene faller inn under operasjonelle trus-

[70] Havne- og farvannsloven (lov 19. juni 2015 nr. 65 om havner og farvann).

[71] Havneanleggssikringsforskriften. Forskrift 29. mai 2013 nr. 538 om sikring av havneanlegg gjelder for havneanlegg som betjener passasjerskip og lasteskip med bruttotonnasje 500 eller mer og enkelte flyttbare boreinnretninger som er i internasjonal fart.

[72] Havnesikringsforskriften. Forskrift 29. mai 2013 nr. 539 om sikring av havneanlegg. Forskriften skal styrke sikringen i de områder av havnen som ikke er omfattet av havneanleggssikringsforskriften, og underbygge de sikringstiltakene som er iverksatt i medhold av denne.

[73] Skipssikkerhetsloven (lov 16. februar 2007 nr. 9 om skipssikkerhet).

ler som allerede dekkes av ISM, og som sikrer at dette blir gjort.

Innen ferjetransporten er virksomheter som er underlagt krav etter forskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger omfattet av Sjøfartsdirektoratets tilsynsmyndighet (ISM sertifisering).

Når det gjelder kvalitetskrav, er det per i dag ikke særskilte krav til IKT-vurderinger, men det er fastsatt retningslinjer for oppfølging av *cyber security* som skal være tatt hensyn til i rederienes sikkerhetsstyringssystemer, senest innen første årlige revisjon etter 1. januar 2021.

Varsling

Forskrift om sikring av havner § 6 bestemmer at sikringshendelser skal varsles til Kystverket. Med sikringshendelse menes «[e]n mistenkelig handling eller omstendighet som utgjør en trussel mot et skip, et havneanlegg eller en havn».

Det følger av ISM-koden punkt 9.1 at sikkerhetsstyringssystemet skal omfatte fremgangsmåter som sikrer avvik, ulykker og farlige situasjoner rapporteres til selskapet, undersøkes og analyseres med det formål å forbedre sikkerheten og hindringen av forurensning.

Tilsyn

Kystverket fører tilsyn med havner og havneanlegg, herunder deres oppfyllelse av sikringsregelverkene. I den utstrekning enhetens IKT-systemer er beskyttet under dette regelverket, vil dette omfattes av tilsynet. Kystverket har ifølge forskrift om sikring av havneanlegg § 20 andre ledd myndighet til å gi de pålegg og gjøre de vedtak som er nødvendig for gjennomføring av bestemmelsene i forskriften. Tilsvarende myndighet følger av forskrift om sikring av havner § 18.

Det følger av skipssikkerhetsloven § 41 første ledd at kongen fastsetter hvem som skal ha tilsynsmyndighet etter loven. Det skal blant annet føres tilsyn med sikkerhetsstyringssystemet, og det er plikt til å medvirke til tilsynet. Tilsyn er for øvrig inngående regulert i blant annet forskrift 22. desember 2014 nr. 1893.

Sanksjoner

Havne- og farvannsloven § 54 gir departementet hjemmel til å «gi forskrifter om gebyr for kontrolltiltak og tilsyn som gjennomføres for å sikre at loven eller vedtak i medhold av loven blir fulgt». Etter § 58 kan «myndigheten» utferdige forelegg mot den som innen fastsatt frist unnlater å etterkomme pålegg eller forbud som er gitt med hjemmel i loven. Havne- og farvannsloven § 60, forskrift om sikring av havneanlegg § 22 og forskrift om sikring av havner § 20 hjemler tvangsmulkt.

Skipssikkerhetsloven kapittel 8 til 10 regulerer sanksjoner og straff. § 50 hjemler tvangsmulkt, § 55 hjemler overtredelsesgebyr, og § 56 hjemler overtredelsesgebyr mot rederiet. Blant annet er overtredelse av § 6 om rederiets alminnelige plikter mulig grunnlag for ileggelse av overtredelsesgebyr.

Nærmere bestemmelser om overtredelsesgebyr følger av forskrift 2. juli 2007 nr. 852 om fastsettelse og gjennomføring av overtredelsesgebyr etter lov 16. februar 2007 nr. 9 om skipssikkerhet (skipssikkerhetsloven) § 55 og § 56.

Oppsummering

Per i dag stilles det bare delvis krav om forsvarlig IKT-sikkerhet. Med det pågående internasjonale regelverksarbeidet ser det ut til at virksomheter i denne sektoren på sikt vil bli underlagt hensiktsmessige krav om IKT-sikkerhet.

2.8.4 Veitransportsystemet

Regulering av IKT-sikkerhet i sektoren

Det foreligger per i dag ingen lov- eller forskriftsregulering som stiller krav om IKT-sikkerhet på området trafikkstyring. I stedet gjelder interne retningslinjer som definerer rutiner for bruk, drift og utvikling av automasjonsnettet og SCADA-systemet samt tilhørende nettverk. Vegdirektoratet sørger sammen med regionene i Statens vegvesen for en samordning, der krav og rutiner videreutvikles i takt med endringer i omgivelsene og inngår i etatens kvalitetssystem.

Når det gjelder autonome kjøretøy så er det mulig gjennom forskrift om utprøving av selvkjørende motorvogn å kreve dokumentert hvordan systemet, teknologien og hvordan informasjonssikkerhet er ivaretatt.[74]

I Nasjonal transportplan, en stortingsmelding som kan likestilles med *soft law*, fremheves det at transportvirksomhetene har et selvstendig ansvar for å sikre egne IKT-systemer, herunder informasjonen som ligger i disse systemene. IKT-sikkerhet skal inngå som en integrert del av transportvirksomhetenes arbeid med sikring av kritisk infrastruktur. Viktige IKT-systemer og sensi-

[74] Forskrift 19. desember 2017 nr. 2240 om utprøving av selvkjørende motorvogn.

tiv informasjon skal identifiseres og sikres mot både tilsiktede og utilsiktede uønskede hendelser. Forebyggende tiltak er viktige og skal videreføres i planperioden. Virksomhetene skal videre gjennomføre og delta i relevante IKT-øvelser og vurdere behovet for inntrengingstester for å prøve motstandskraften i egne IKT-systemer.[75]

Hendelseshåndtering

I Nasjonal transportplan står det at virksomhetene skal overvåke egen IKT-infrastruktur for å kunne oppdage og håndtere dataangrep. I tillegg til å ha egne IKT-sikkerhetsmiljøer er relevante virksomheter i transportsektoren tilknyttet NSM NorCERT og det nasjonale varslingssystemet for digital infrastruktur (VDI) som sikrer kontinuerlig overvåking av datatrafikken og beskytter mot angrep.[76]

Oppsummering

Det er i liten grad krav om forsvarlig IKT-sikkerhet i regelverket som regulerer veitransportssektoren.

2.9 Drikkevann

Om sektoren

Drikkevannssektoren omfatter produksjon og forsyning av drikkevann.

Regulering av IKT-sikkerhet i sektoren

Drikkevannsforskriften er den primære forskriften som regulerer produksjon og forsyning av drikkevann.[77] Formålet med forskriften er å beskytte menneskers helse ved å stille krav om sikker levering av tilstrekkelige mengder helsemessig trygt drikkevann som er klart og uten fremtredende lukt, smak og farge. Forskriften gjennomfører rådsdirektiv 98/83/EF (drikkevannsdirektivet) i norsk rett. Det er vannverkseieren som er ansvarlig for at kravene til vannforsyningssystemer etterleves, herunder at forsyningen av drikkevann oppfyller kravene til tilfredsstillende mengde og tilfredsstillende kvalitet.

Sikkerhetstiltakene har tradisjonelt primært vært knyttet til andre årsaker enn svikt i digital kommunikasjon, men også slike årsaker har det vært fokusert på i den senere tid. Mattilsynets veiledning av april 2017 til vannforsyningssystemene om utarbeiding av beredskapsplaner nevner derfor IKT som et område som må tas med i farekartleggingen.

Drikkevannsforskriften ble revidert i 2016 og stiller nå krav om forebyggende sikring ved at vannverkseieren skal sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig fysisk sikret, og at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk (§ 10). I veilederen til bestemmelsen trekkes det frem eksempler på hva som bør vurderes for å kunne avgjøre om styringssystemene er tilstrekkelig sikret mot dataangrep.

Hendelseshåndtering

Drikkevannsforskriften stiller krav til vannverkene om å kunne levere drikkevann til enhver tid, og at de skal ha forebyggende sikring og beredskap til å håndtere hendelser. Om årsaken er knyttet til svikt i nett- eller informasjonssystem eller andre forhold, så skal mulige hendelser kartlegges og kunne håndteres.

Varsling

Mattilsynet og abonnentene skal varsles ved avvik i vannkvaliteten. Andre avvik er ikke varslingspliktige til Mattilsynet. Varsling knyttet til svikt i elektroniske komponenter eller signaloverføringer er følgelig ikke varslingspliktig etter drikkevannsforskriften med mindre de medfører avvik i vannkvaliteten.

Tilsyn

Det er Mattilsynet som er tilsynsmyndighet. Mattilsynet fører i henhold til drikkevannsforskriften § 28 tilsyn med alle vannforsyningssystemer. Med samme hjemmel kan Mattilsynet fatte nødvendige vedtak for å sikre etterlevelse av forskriftens krav.

Sanksjoner

Mattilsynet gis i matloven § 23 myndighet til å fatte nødvendige vedtak for gjennomføring av bestemmelser gitt eller i medhold av loven.[78] Tilsynet kan etter § 26 fastsette tvangsmulkt.

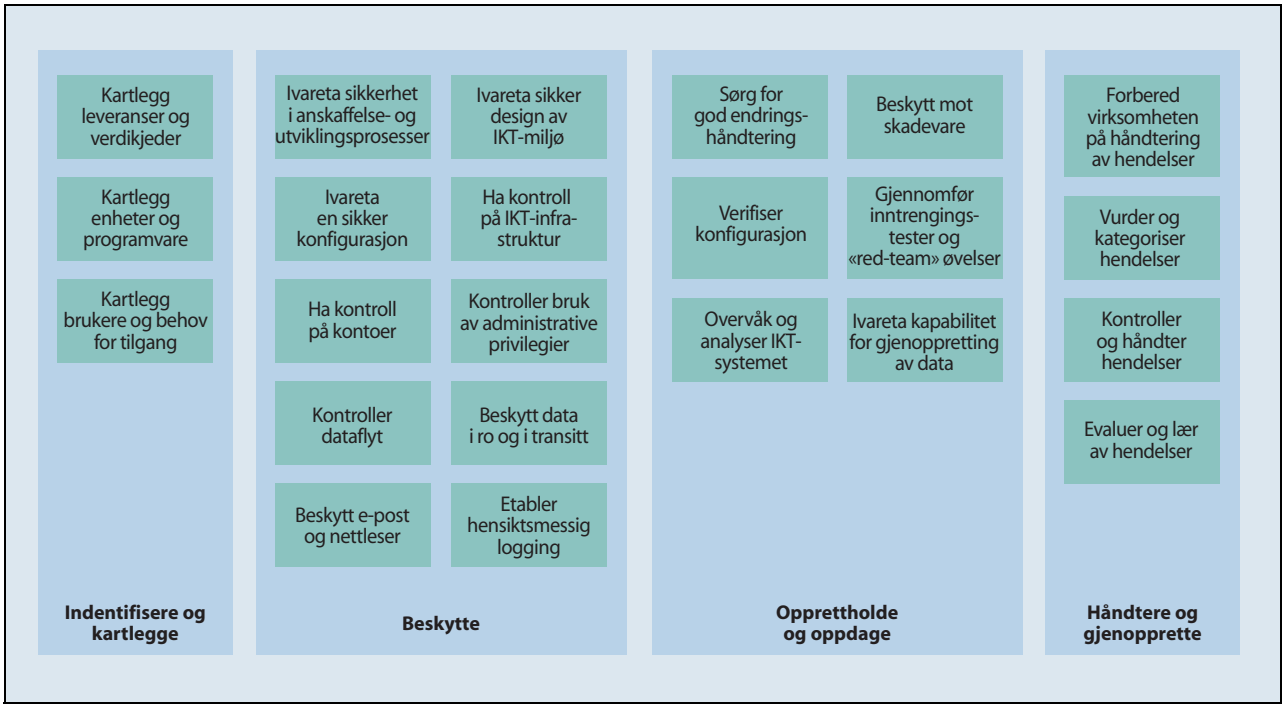
---

[75] Meld. St. 33 (2016–2017) *Nasjonal transportplan 2018–2019,* kap. 12.3.2.

[76] Ibid.

[77] Drikkevannsforskriften. Forskrift 22. desember 2016 nr. 1868 om vannforsyning og drikkevann, fastsatt med hjemmel i blant annet lov 19. desember 2003 nr. 124 om matproduksjon og mattrygghet mv. (matloven).

[78] Matloven (lov 19. desember 2003 nr. 124 om matproduksjon og mattrygghet mv.).



Figur 1.1 NSMs oversikt over grunnprinsippene

Oppsummering

Regelverket stiller krav om forsvarlig IKT-sikkerhet.

3 Soft law

Mange virksomheter følger veiledere og standarder som ikke er regulert gjennom lov og forskrift når det gjelder krav om IKT-sikkerhet. For mange virksomheter er det egne bransjestandarder som følges. I tillegg er det standarder som er av mer generell karakter. De to mest relevante veiledningene på området er NSMs grunnprinsipper for IKT-sikkerhet og ISO 27000. I tillegg er Statens standardavtaler (SSA) relevante standard kontraktmaler for anskaffelser for kjøp av IT og konsulenttjenester.

3.1 NSMs Grunnprinsipper for IKT-sikkerhet

NSM har gjennom sine grunnprinsipper for IKT-sikkerhet definert et sett med anbefalinger for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. Grunnprinsippene bygger på anerkjente standarder og rammeverk både i Norge og EU, deriblant ISO 27000-serien.

Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system. De beskriver også hvorfor det bør gjøres.

Hovedpunktene i prinsippene er:

1. Identifisere og kartlegge – gjør risikovurdering
2. Beskytte – sikre dine verdier
3. Opprettholde og oppdage – vær bevisst
4. Håndtere og gjenopprette – lær av dine utfordringer

Hvert grunnprinsipp har underliggende teknologiske og organisatoriske sikringstiltak som beskriver hva som bør gjøres. Figur 1.1 viser NSMs oversikt over hva som inngår i de fire hovedkategoriene.

På bakgrunn av grunnprinsippene og erfaringer med å utvikle tekniske sikkerhetstiltak for beskyttelse av sikkerhetsgraderte IKT-systemer har NSM anbefalt ti tiltak mot dataangrep. De er inndelt i to deler. Del 1 omfatter fire enkle tiltak. Del to omfatter seks tiltak, som forutsetter at virksomheten har en IT-avdeling som styrer sikkerheten til virksomhetens klienter.

Tiltakene tar utgangspunkt i Windows 7 og målgruppen er store og middels store virksomheter, primært i offentlig forvaltning. Dersom virksomheten har moderne maskin- og programvare, innebærer ikke tiltakene at man skal kjøpe inn spesielle sikkerhetsprodukter. Primært handler disse tiltakene om å utnytte viktige sikkerhetsfunksjoner i Windows bedre. Disse tiltakene hindrer blant annet ukjent (og dermed potensielt skadelig) programvare å starte opp uansett hva sluttbrukeren måtte gjøre, for eksempel i forbindelse

med lesing av e-post, bruk av minnepinner eller surfing på internett.

De ti tiltakene gir ikke hundre prosent sikkerhet mot alle typer angrep, for eksempel tapping av brukerkommunikasjon over internett, tjenestenektangrep, angrep fra avanserte statlige aktører og angrep der angriperen har fysisk tilgang til utstyret. Tiltakene forhindrer heller ikke at lettlurte brukere oppgir sensitive opplysninger på nett. Tiltakene til NSM er som følger:

Del 1

1. Oppgrader program- og maskinvare.
2. Installer sikkerhetsoppdateringer så fort som mulig.
3. Ikke tildel administratorrettigheter til sluttbrukere.
4. Blokker kjøring av ikke-autoriserte programmer

Del 2

5. Aktiver kodebeskyttelse mot ukjente sårbarheter.
6. Herde applikasjoner.
7. Bruk klientbrannmur.
8. Bruk sikker oppstart og diskkryptering.
9. Bruk antivirus/antiskadevare.
10. Ikke installer mer funksjonalitet enn nødvendig.

3.2 ISO Standarder

ISO er en verdensomfattende sammenslutning av nasjonale standardiseringsorganer. Organisasjonen utarbeider og publiserer internasjonale standarder. En standard kan for eksempel være en måleenhet eller et styringssystem.[79]

Standardisering utføres av faggrupper som får innspill fra eksperter og interessenter. Det finnes rundt 3000 tekniske grupper, og cirka 50 000 eksperter bidrar årlig til organisasjonen. Vedtak av standarder skjer ved avstemning blant medlemsorganisasjonene.[80]

Standardene i ISO/IEC 27000-serien har til hensikt å sikre virksomheters informasjon og å ha et system for dette. Serien inneholder råd for god praksis, sertifiseringsstandarder og retningslinjer for hjelp ved innføring.[81]

I Norge har Difi tilgjengeliggjort standarder i ISO/IEC 27000-serien for statsforvaltningen og inngått en rammeavtale med Standard Online, Standard Norges salgsselskap, om tilgang til standarder for 203 statlige enheter. Blant de mest sentrale standardene i serien er:[82]

- *NS-EN ISO/IEC 27000*
  Holder rede på sammenhengene mellom standardene og begreper som benyttes i serien.
- *NS-EN ISO/IEC 27001*
  Stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Denne standarden er grunnlag for sertifisering, og resten av serien er en utdypning av og veiledning i denne standarden.
- *NS-EN ISO/IEC 27002*
  Gir god praksis med tanke på hva en bør gjøre, hva en bør vurdere og hva en bør ha på plass når det gjelder informasjonssikkerhet.
- *NS-ISO/IEC 27003*
  Skisserer mulige strategier for å iverksette en prosess for å innføre et ledelsessystem for informasjonssikring.
- *NS-ISO/IEC 27004*
  Hjelper til med hvordan man måler tilstanden før, under og etter innføringen av sikringstiltak.
- *NS-ISO/IEC 27005*
  Omhandler risikostyring av informasjonssikkerhet.

3.3 Standardkontrakter

Statens standardavtaler (SSA) er kontraktsmaler for kjøp av IT og konsulenttjenester, med unntak for kjøp av rådgivningstjenester innen bygg og anlegg. SSAene er utarbeidet av Difi med innspill fra både kunde- og leverandørsiden og er gratis å bruke.

SSAene har en del generelle krav om sikkerhet og personvern. I tillegg til de generelle avtaletekstene skal det fylles ut bilag med kravspesifikasjoner (kunden) og løsningsbeskrivelser (leverandøren). Det er i bilagene at avtalen tilpasses den konkrete anskaffelsen. Det må gjøres konkrete vurderinger av krav om sikkerhet i hver anskaffelse, og de relevante kravene må beskrives i kravspesifikasjoner/bilag til avtalen.

En del av avtalen har krav til informasjonssikkerhet. De er utformet på denne måten:

---

79 Trygve Holtebekk, *ISO*, Store Norske leksikon.

80 Ibid.

81 Standard Norge, hentet fra: https://www.standard.no/fagomrader/ikt/it-sikkerhet/

82 Ibid.

> Leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten.
>
> Dette innebærer at Leverandøren skal iverksette forholdsmessige tiltak for å sikre konfidensialitet av Kundens data samt tiltak for å sikre at data ikke kommer på avveie. Videre skal Leverandøren iverksette forholdsmessige tiltak mot utilsiktet endring og sletting av data samt mot angrep av virus og annen skadevoldende programvare.

Flere av avtalene har også krav til beskyttelse og behandling av personopplysninger som skal samsvare med de kravene som følger av personopplysningsloven.

Per oktober 2018 hadde Difi tilgjengelig følgende avtaler:

Avtale om løpende tjenestekjøp (SSA-L): Avtalen egner seg til kjøp av standardiserte skytjenester («as a service»-leveranser). Tjenesten kan også omfatte installasjon, konfigurering, tilpasning og/eller integrasjoner dersom dette spesifiseres i bilag 1. Tjenesten omfatter drift og vedlikehold.[83] Avtalen har krav til at leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten, jf. punkt 6.1 i avtalen.

Bistandsavtalene (SSA-B og SSA-B enkel): Avtalen er egnet til konsulentkjøp når man har behov for kompetanse, men ikke vet hvordan sluttresultatet skal bli. Konsulenten har ikke resultatansvar (resultatet/behovet er ikke klart definert). SSA-B skal ikke brukes for konsulentkjøp med tilknytning til bygg og anlegg.[84] Avtalen inneholder ingen formulerte krav om IKT-sikkerhet.

Driftsavtalen (SSA-D): Driftsavtalen regulerer et vidt spekter av driftssituasjoner med vekt på standardiserte driftstjenester. Etableringen av driftstjenesten kan deles opp i delleveranser.[85] Avtalen stiller krav om at leverandøren skal holde kunden orientert om endringer som kan ha betydning for kundens bruk av driftstjenesten eller for sikkerheten i løsningen før endringene iverksettes. Det er også krav om endringslogg, jf. punkt 2.2.3 i avtalen. Sikkerhetsoppdateringer skal alltid foretas uten unødig opphold, jf. punkt 2.2.9.

Det er også krav om at leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten, jf. punkt 9.2.

Kjøpsavtalen (SSA-K): Avtalen er egnet til kjøp av IT-utstyr og/eller programvare. Avtalen er også egnet for kjøp av tilpasning av programvare dersom man på forhånd kan spesifisere nøyaktig hvordan IT-utstyret og/eller programvaren skal tilpasses. Leverandøren leverer utstyret og/eller programvaren ferdig tilpasset.[86] Avtalen inneholder ingen formulerte krav om IKT-sikkerhet.

Oppdragsavtalen (SSA-O): Avtalen er egnet til oppdrag der sluttresultatet er klart beskrevet av kunden. Konsulenten får et selvstendig ansvar for en ferdig leveranse/oppdrag, og kunden skal ikke ha behov for å følge opp konsulenten under arbeidet.[87] Avtalen stiller krav om at konsulenten skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av oppdraget, jf. punkt 3.6 i avtalen.

Rammeavtalen (SSA-R): Rammeavtaler egner seg bedre enn ordinære kjøpsavtaler dersom man skal kjøpe tjenester/varer over en gitt periode (ikke som et engangskjøp) og/eller kjøpsomfanget er noe uvisst. Rammeavtalen egner seg bedre enn SSA-B og SSA-O dersom det er behov for konsulenttjenester til mer enn én leveranse eller ett oppdrag.[88] Avtalen inneholder ingen formulerte krav om IKT-sikkerhet.

Smidigavtalen (SSA-S): Avtalen er beregnet på større programvareanskaffelser hvor det skal benyttes smidig utviklingsmetodikk.[89] Avtalen stiller krav om at leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten, jf. punkt 9.2.

Det er kundens ansvar å konkretisere relevante funksjonelle og sikkerhetsmessige krav for leveransen i bilag 1, jf. punkt 9.1 i avtalen.

Utviklings- og tilpasningsavtalen (SSA-T): Avtalen er egnet for kjøp av programvare som skal utvikles eller tilpasses for kunden dersom kunden ikke på forhånd kan spesifisere nøyaktig hvordan

---

[83] Direktoratet for forvaltning og IKT (2018) *Avtale om løpende tjenestekjøp (SSA-L)*.

[84] Direktoratet for forvaltning og IKT (2015) *Bistandsavtalene (SSA-B og SSA-B enkel)*.

[85] Direktoratet for forvaltning og IKT (2018) *Driftsavtalen (SSA_D)*.

[86] Direktoratet for forvaltning og IKT (2018) *Kjøpsavtalen (SSA-K)*.

[87] Direktoratet for forvaltning og IKT (2018) *Oppdragsavtalen (SSA-O)*.

[88] Direktoratet for forvaltning og IKT (2015) *Rammeavtalen (SSA-R)*.

[89] Direktoratet for forvaltning og IKT (2018) *Smidigavtalen (SSA-S)*.

programvaren skal utvikles/tilpasses. Avtalen er egnet der leverandørens spesifiseringsarbeid (utarbeidelse av detaljspesifikasjon) ønskes gjennomført i nært samarbeid med kunden.[90] Avtalen stiller krav om at leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten, jf. punkt 9.2.

Det er kundens ansvar å konkretisere relevante funksjonelle og sikkerhetsmessige krav for leveransen i bilag 1, jf. punkt 9.1 i avtalen.

Vedlikeholdsavtalen (SSA-V): Avtalen regulerer levering av vedlikehold og service for programvare og/eller utstyr. Avtalen gir også mulighet for kompletteringskjøp, lisensutvidelser eller ytterligere utvikling i begrenset omfang innenfor et angitt målbilde for den aktuelle løsningen.[91] Hvis ikke annet fremgår av bilag 1 og 2, skal vedlikeholdstjenesten som et minimum omfatte feilretting og ytelser som er nødvendige for å opprettholde programvarens samvirke med annen programvare som er omfattet av vedlikeholdstjenesten (se bilag 3). Avtalen stiller krav om at leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav om informasjonssikkerhet i forbindelse med gjennomføring av tjenesten, jf. punkt 9.2.

Det er kundens ansvar å konkretisere relevante funksjonelle og sikkerhetsmessige krav for leveransen i bilag 1, jf. punkt 9.1 i avtalen.

[90] Direktoratet for forvaltning og IKT (2018) *Utviklings- og tilpasningsavtalen (SSA-T)*.

[91] Direktoratet for forvaltning og IKT (2018) *Vedlikeholdsavtalen (SSA-V)*.

Vedlegg 2

Relevant EU-regelverk

1 EUs NIS-direktiv

NIS-direktivet ble vedtatt i EU 6. juli 2016.[1] Det har som formål å styrke IKT-sikkerheten i EU ved å pålegge medlemsstatene å sørge for at samfunnsviktige virksomheter gjennomfører tiltak. Hver medlemsstat plikter å etablere en nasjonal strategi for IKT-sikkerhet, en nasjonal kompetent sikkerhetsmyndighet, et nasjonalt kontaktpunkt og en nasjonal enhet som skal håndtere digitale sikkerhetshendelser. Det stilles også krav om deltakelse i to internasjonale samarbeidsfora, det vil si en samarbeidsgruppe for strategisk styring (NIS samarbeidsgruppe) og et nettverk for nasjonale responsmiljøer (CSIRT nettverk). Videre plikter medlemsstatene å sørge for at tilbydere av samfunnsviktige tjenester og enkelte digitale tjenester vurderer sikkerhetsrisikoen knyttet til bruk av nettverk og informasjonssystemer, og at de varsler om alvorlige sikkerhetshendelser.

Direktivet trådte i kraft 8. august 2016, og medlemstatene måtte implementere de fleste av direktivets krav innen 9. mai 2018. Norge er foreløpig ikke forpliktet til å gjennomføre NIS-direktivet fordi prosessen med å innlemme direktivet i EØS-avtalen ikke er ferdig. Den norske regjeringen besluttet i desember 2016 å anse direktivet som EØS-relevant og akseptabelt. Island har inntatt samme posisjon. Liechtenstein har foreløpig ikke tatt endelig stilling. Det følger av utvalgets mandat at de skal legge til grunn at NIS-direktivet skal gjennomføres i norsk rett. For utvalget er direktivets bestemmelser om sikkerhets- og varslingskrav for virksomheter og hvilke krav som stilles til nasjonale myndigheter, mest relevant, og gjennomgangen nedenfor konsentrerer seg derfor om dette.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

1.1 Sikkerhets- og varslingskrav for virksomheter

Direktivets krav retter seg mot virksomheter som leverer tjenester som er viktige for å opprettholde et velfungerende samfunn og næringsliv. Virksomhetene er delt i to hovedkategorier, tilbydere av samfunnsviktige tjenester (*operators of essential service*, se artikkel 4(4)) og tilbydere av digitale tjenester (*digital service providers*, se artikkel 4(6)). Alle tjenestene er listet opp i direktivets vedlegg II og III.

1.1.1 Tilbydere av samfunnsviktige tjenester

1.1.1.1 Virkeområde

En virksomhet anses som tilbyder av en samfunnsviktig tjeneste dersom tre kumulative kriterier er oppfylt (artikkel 5(2)):

(i) Virksomheten tilbyr en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter (artikkel 5(2)(a)). Det er tilstrekkelig å fastslå at virksomheten leverer en slik tjeneste som er opplistet i direktivet vedlegg II. Det er kun den delen av virksomheten som leverer den aktuelle tjenesten, som omfattes. For eksempel vil trafikkstyringen på en stor flyplass omfattes, mens butikkområdet ikke omfattes. Vedlegget utgjør utgangspunktet for direktivets virkeområde og omfatter følgende samfunnssektorer (ikke uttømmende):
- energi (elektrisitet, olje og gass)
- transport (luft, jernbane, sjø og vei)
- helse (helsetjenester)
- bank
- finansmarkedsinfrastruktur
- drikkevannsforsyning og -distribusjon
- digital infrastruktur:
  - IXP – internet exchange point
  - DNS – domain name server service provider
  - TLD – top level domain name registries

Se direktivet vedlegg II for nærmere spesifisering av hvilke tjenester som omfattes.

(ii) Tjenesteleveransen er avhengig av nettverk og informasjonssystemer (artikkel 5(2)(b)). Direktivet gir ikke nærmere veiledning om hva som ligger i dette.

(iii) Det tredje kriteriet er at en hendelse i virksomhetens nettverk og informasjonssystemer ville hatt vesentlig forstyrrende virkning på tjenesteleveransen (artikkel 5(2)(c)). Ved vurderingen av om en sikkerhetshendelse kan få vesentlig forstyrrende effekt på tjenesteleveransen, skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Artikkel 6 inneholder en ikke uttømmende liste med tverrsektorielle momenter som skal vurderes:
- antall brukere som baserer seg på tjenesten
- andre vedlegg II-sektorers avhengighet av tjenesten
- omfanget og varigheten av mulige virkning av hendelser på økonomiske og samfunnsmessige aktiviteter og samfunnssikkerhet
- virksomhetens markedsandel
- geografisk område som kan rammes av hendelsen
- viktigheten av virksomhetens bidrag til leveranse av tjenesten, med tanke på alternative tjenestetilbydere

Det endelige virkeområdet for direktivet skal fastlegges gjennom en utpekingsprosess i regi av hver enkelt medlemsstat. Det er opp til medlemsstatene hvordan denne prosessen gjennomføres, så lenge direktivets krav om å opprette en liste over alle operatører av essensielle tjenester oppfylles. Listen skal oppdateres jevnlig og minst hvert andre år.

1.1.1.2 Sikkerhets- og varslingskrav

Sikkerhetskravene følger av artikkel 14(1) og (2). Virksomheten skal iverksette tekniske og organisatoriske tiltak som er hensiktsmessige og står i et rimelig forhold til risikoen som knytter seg til virksomhetens nettverks- og informasjonssystemer. For å sikre opprettholdelse av tjenesteleveransen skal virksomheten iverksette tiltak som er egnet til å forebygge og redusere virkningen av hendelser som truer sikkerheten i virksomhetens IKT-systemer. Ved vurderingen av hvilke tiltak som skal iverksettes, skal virksomheten ta hensyn til den tekniske utviklingen.

Litt forenklet sagt stiller direktivet krav om at virksomheten skal gjennomføre en vurdering av risikoen som knytter seg til IKT-systemene virksomheten bruker for å levere samfunnsviktige tjenester. Virksomheten skal så iverksette tiltak som er egnet til å redusere denne risikoen.

I fortalen er det sagt lite om hva som ligger i dette, og den kan ikke sies å gi særlig veiledning utover det som allerede følger av direktivbestemmelsene. Det fremgår av fortalepunkt 44 blant annet at landene gjennom innføring av passende lovgivningstiltak og frivillige bransjenormer skal fremme en risikostyringskultur som inkluderer risikovurdering og gjennomføring av proporsjonale sikkerhetstiltak. I fortalepunkt 46 står det at risikostyringstiltak omfatter tiltak for å identifisere risikoer for hendelser, med sikte på å forebygge, avdekke og håndtere hendelser og begrense skaden.

Det skal varsles om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen (artikkel 14(3)). Ved vurderingen av om innvirkningen har vært betydelig, skal det legges vekt på antall brukere av tjenesten som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen. Varselet skal dessuten inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser.

Direktivet stiller krav om at nasjonale myndigheter skal føre tilsyn med virksomhetenes etterlevelse av kravene, jf. artikkel 15(1).

1.1.2 Tilbydere av digitale tjenester

1.1.2.1 Virkeområde

Den andre kategorien virksomheter omfatter tilbydere av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester, i det videre omtalt som tilbydere av digitale tjenester eller DSP (*digital service providers*).

Det følger av direktivet artikkel 4(5) at med digital tjeneste menes tjenester som nevnes i NIS-direktivet vedlegg III. Videre henvises det til definisjonen av tjenester i europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske regler og standarder og informasjonssamfunnstjenester (kodifisering) artikkel 1(1)(b):

> «service» means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services

I vedlegg I til direktivet er det tatt inn en veiledende liste over tjenester som ikke omfattes av definisjonen.

Bestemmelsene i dette direktivet er gjennomført i lov 17. desember 2004 nr. 101 om europeisk meldeplikt for tekniske regler m.m. (EØS-høringsloven). I § 3 nr. 5 menes med *informasjonssamfunnstjeneste* «enhver tjeneste som vanligvis ytes mot vederlag, og som formidles elektronisk over avstand og etter individuell anmodning fra en tjenestemottaker».[2] Også her henvises det til en liste over tjenester som ikke omfattes av definisjonen.

De tre digitale tjenestene som omfattes av NIS-direktivet, defineres i artikkel 4(17), 4(18) og 4(19). En skytjeneste (*cloud computing service*) er en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser. En nettbasert markedsplass (*online marketplace*) er en digital tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen. En nettbasert søkemotor (*online search engine*) er en digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

Ifølge artikkel 16(11) omfattes ikke mikrovirksomheter og små virksomheter, jf. Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003 om definisjonen av mikroforetak og små og mellomstore bedrifter.[3] Det vil si at virksomheter som har færre enn 10 ansatte, og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 2 millioner euro, ikke omfattes av direktivet.

Det skal ikke foretas en identifisering av tilbydere av digitale tjenester, i motsetning til ordningen for tilbydere av samfunnsviktige tjenester.

For denne kategorien skal det være lik regulering i hele EU. Det er derfor ikke noe nasjonalt handlingsrom hva gjelder sikkerhetskravene eller definisjonen av de digitale tjenestene som er omfattet. Dette har blant annet sammenheng med at aktiviteten er grenseoverskridende av natur. Av samme grunn har kommisjonen i medhold av artikkel 16(10) utarbeidet et gjennomføringsregelverk som konkretiserer direktivets krav om sikkerhet og varsling.[4]

1.1.2.2 Sikkerhets- og varslingskrav

Sikkerhetskravene følger av artikkel 16, hvor det står at tilbydere av digitale tjenester skal ha en risikobasert tilnærming til sikkerhetsarbeidet. De skal iverksette sikkerhetstiltak som står i et rimelig forhold til risikoen virksomheten står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med særlig henblikk på opprettholdelse av tjenesteleveransen.

Det går tydelig frem av premissene til direktivet at det skal stilles lavere sikkerhetskrav til disse tjenestene, da de anses noe mindre viktige enn de samfunnsviktige tjenestene. Det følger av artikkel 17 at myndighetene kun skal kontrollere disse virksomhetene dersom de får klare indikasjoner på at direktivets krav ikke er fulgt. Det forutsettes dessuten i fortalepunkt 57 at sikkerhetsnivået for denne kategorien virksomheter skal harmoniseres i EU.[5]

1.2 Myndigheter

Medlemsstatene skal utpeke eller etablere et nasjonalt kontaktpunkt, en eller flere kompetente myndigheter og et eller flere hendelseshåndteringsmiljøer (artikkel 8 og 9).

Det nasjonale kontaktpunktet skal sikre samarbeid mellom medlemslandene, med relevante myndigheter i andre land, med NIS-samarbeidsgruppen og med CSIRT-nettverket. Rollen som nasjonalt kontaktpunkt kan tildeles en allerede eksisterende myndighet.

Den kompetente myndigheten skal kunne føre tilsyn med virksomhetenes etterlevelse av direktivet. Rollen som kompetent myndighet kan tildeles en eller flere eksisterende nasjonale myndigheter. Både det nasjonale kontaktpunktet og den kompetente myndigheten skal samarbeide med politiet og Datatilsynet.

Hendelseshåndteringsmiljøet, eventuelt hendelseshåndteringsmiljøene, skal oppfylle kravene som følger av vedlegg I til direktivet, dekke minst virkeområdet til direktivet og være ansvarlig for risiko- og hendelseshåndtering i henhold til en konkret plan. Et hendelseshåndteringsmiljø kan

---

2 I direktivet defineres begrepet *tjeneste* med blant annet begrepet *information society service*, mens loven definerer begrepet *informasjonssamfunnstjeneste*. Dette innebærer ikke en realitetsforskjell.

3 Høring om en mulig revisjon av rekommandasjonen ble startet av EU-kommisjonen 6. februar 2018.

4 EU (2018) *Commission implementing regulation (EU) 2018/151*.

5 Ibid.

utpekes eller etableres som en del av en kompetent myndighet.

Slik som direktivets krav er utformet, står medlemslandene fritt til å organisere seg slik de vil, så lenge de tre funksjonene er på plass. For Norges del er det altså ikke nødvendig å endre på gjeldende organisering innenfor IKT-sikkerhet for å oppfylle direktivets krav. Imidlertid må det vurderes om NSM oppfyller direktivets krav om kompetent myndighet, om gjeldende hendelseshåndteringsmiljøer oppfyller direktivets krav, og om myndighetene har tilstrekkelige hjemler til å føre tilsyn med etterlevelse av direktivets krav til virksomhetene.

2 Cybersecurity Act[6]

Forslaget til en ny forordning om ENISA og IKT-sikkerhetssertifisering (heretter Cybersecurity Act) består av tre deler: først en generell del, deretter en del om ENISA og til slutt en del om sertifisering av IKT-produkter og -tjenester.[7]

Del I inneholder formål, virkeområde og definisjoner. Formålet med forordningen er å sikre et velfungerende indre marked med et høyt nivå av cybersikkerhet, motstandsdyktighet og tillit i EU. Dette skal man oppnå ved å fastsette mål og oppgaver for EUs Cybersikkerhetsbyrå (ENISA) samt å etablere et felleseuropeisk rammeverk for sikkerhetssertifisering av IKT-produkter og tjenester (jf. artikkel 1). Forordningen inngår som et element i EUs digitaliseringsstrategi, som har som formål å stimulere til økonomisk vekst og øke EUs konkurransekraft. Forslaget gir ENISA en sterkere og mer sentral rolle ved at byrået skal understøtte medlemslandenes gjennomføring av NIS-direktivet, og ved å motvirke trusler på en mer aktiv måte.

2.1 ENISA

Del II innebærer at ENISA skal få et permanent og styrket mandat. ENISAs navn foreslås også endret til EUs Cybersikkerhetsbyrå (EU Cybersecurity Agency). På anmodning fra medlemslandene skal byrået kunne bistå operativt i grenseoverskridende cyberhendelser. Byrået skal utvikle og administrere et EU-rammeverk for sikkerhetssertifisering av IKT-produkter og -tjenester. Forordningen setter i denne sammenheng også et krav om at medlemslandene skal etablere tilsynsmyndigheter for sikkerhetssertifisering.

Målene for ENISAs arbeid følger av artikkel 4:

- Byrået skal være et ekspertisesenter og bistå i EU-kommisjonens arbeid med cybersikkerhet
- Byrået skal bistå unionen og medlemslandene med å utvikle og implementere strategier for cybersikkerhet
- Byrået skal støtte kapasitetsbygging og beredskap ved å bistå unionen, medlemslandene og offentlige og private interessenter, for å øke egenbeskyttelsen av nettverks- og informasjonssystemer og utvikle ferdigheter og kompetanse innenfor cybersikkerhet
- Byrået skal fremme samarbeid og koordinering mellom medlemsland, unionen og relevante interessenter, herunder privat sektor, om saker knyttet til cybersikkerhet
- Byrået skal øke cybersikkerhetskapabiliteter på EU-nivå for å komplettere medlemslandenes tiltak for å forebygge og håndtere cybertrusler, særlig i grenseoverskridende cyberhendelser
- Byrået skal fremme bruken av sertifisering, blant annet ved å bidra til etablering og vedlikehold av et felleseuropeisk rammeverk for sikkerhetssertifisering, for å øke transparens og verifisering av IKT-produkter og -tjenester med det formål å styrke tilliten til det digitale indre marked
- Byrået skal bidra til økt kunnskap og kompetanse om cybersikkerhet for både privatpersoner og virksomheter

2.2 Sertifisering av IKT-produkter og -tjenester

Forordningen del III foreslår et nytt regelverk for sikkerhetssertifisering av IKT-produkter og -tjenester, jf. art 43 og 44. Noe av bakgrunnen for dette er at trusselbildet og økningen av IKT-kriminalitet har tvunget frem ulike nasjonale sertifiseringsregelverk. Konsekvensen er blant annet fragmenterte og lite hensiktsmessige ordninger som ikke samspiller effektivt inn mot EUs indre marked (interoperabilitetsutfordringer).

Målet med et felleseuropeisk regelverk er å fremme IKT-sikkerhet som et konkurransefortrinn og bidra til forbrukernes tillit til IKT-produktene, samtidig som IKT-sikkerhetsnivået blir hevet. Et felles regelverk vil også kunne redusere sertifiseringskostnader. Initiativet supplerer og

---

6 Basert på Regjeringen (2018) *Cybersecurity Act. Foreløpig posisjonsnotat.*

7 Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification («Cybersecurity Act») KOM (2017) 477.

støtter også gjennomførelsen av NIS-direktivet ved å gi de virksomheter som er omfattet av direktivet, et verktøy for å påvise etterlevelse av direktivet for hele EU. Forslaget innfører ikke direkte operasjonelle sertifiseringsordninger, men etablerer et rammeverk av regler for innførelse av spesifikke europeiske sertifiseringsordninger for IKT-produkter og -tjenester, som blir utarbeidet av ENISA og vedtatt ved «gjennomførelsesrettsakter» (beskrevet lenger nede).

En cybersikkerhetssertifiseringsordning vil i henhold til forslaget attestere at IKT-produktene og -tjenestene som er sertifisert oppfyller fastsatte sikkerhetskrav. For eksempel beskyttelsesevne mot kompromittering, tilgjengelighet, autentisering, integritet og konfidensialitet av de dataene som oppbevares eller behandles i produktet eller tjenesten. De europeiske sertifiseringsordningene vil ikke selv utvikle tekniske standarder, men benytte eksisterende standarder om tekniske krav og evalueringsprosedyrer som produktene skal overholde. Sertifiseringsordningene skal utformes slik at de, basert på relevans for den aktuelle produkt- eller tjenestegruppen, tar hensyn til flere sikkerhetsmål (jf. artikkel 45), herunder

- beskytte data mot utilsiktet eller uautorisert behandling eller ødeleggelse
- sikre at kun autoriserte personer, programmer eller maskiner har adgang til dataene, blant annet gjennom tilstrekkelig logging av type data og hvilke handlinger som er utført
- sikre tilgjengelighet og tilgang til data (restore) ved tilfeller av fysiske eller tekniske hendelser
- sikre at IKT-produkter og -tjenester innehar ajourført programvare fri for kjente sårbarheter og er gitt mekanismer for sikker oppdatering

Videre innebærer forslaget at ordningene skal fastsette flere spesifikke elementer knyttet til omfang og innhold i cybersikkerhetssertifiseringen. Det omfatter blant annet valg av aktuelle IKT-produkter og -tjenester, spesifisering av cybersikkerhetskrav (f.eks. med henvisning til relevante standarder eller tekniske spesifikasjoner), evalueringskriterier og -metoder og det tillitsnivået de er ment å garantere, herunder grunnleggende, betydelig eller høyt, jf. artikkel 46 og 47. Det foreslås ulike sertifiseringsordninger for ulike kategorier av produkter og tjenester: kritiske applikasjoner og høyrisikoapplikasjoner (fra biler til kraftstasjoner), mye brukte digitale tjenester, nettverk og systemer (fra rutere til e-post, brannmur og antivirus) og masseproduserte tilkoblede produkter som utgjør tingenes internett (f.eks. lyspærer og nettkameraer), e-post eller brannmurer. Det skal være frivillig å benytte seg av sertifiseringsregelverket.

Nasjonale sikkerhetssertifiseringsordninger for IKT-produkter og -tjenester som omfattes av en europeisk sertifiseringsordning, vil i henhold til forordningens artikkel 49(1) opphøre fra det tidspunkt som følger av gjennomføringsrettsakten hvor ordningen vedtas, jf. artikkel 44(4). Formålet er å sikre harmonisering og unngå fragmentering av det indre marked. Medlemslandene skal heller ikke vedta nye nasjonale sertifiseringsordninger for IKT-produkter og -tjenester som allerede er omfattet av en europeisk ordning. Allerede utstedte attester i henhold til en nasjonal sertifiseringsordning vil være gyldig frem til utløpsdato, jf. artikkel 49(3).

Forslaget innebærer at det må utpekes en myndighet i hvert land som kan føre tilsyn med sertifiseringen, herunder at etterlevelsesorganene overholder regelverket, at de attester som organene har utstedt, er i overenstemmelse med kravene som følger av forordningen, og at de er i henhold til den europeiske cybersikkerhetssertifiseringsordningen. Den nasjonale myndigheten skal kunne behandle klager i forbindelse med attester utstedt av etterlevelsesorganene.

Forslaget legger opp til at det etableres en europeisk cybersikkerhetssertifiseringsgruppe, jf. artikkel 53, bestående av alle medlemslands nasjonale sertifiseringstilsynsmyndigheter. Gruppen skal både gi råd til kommisjonen i cybersikkerhetssertifiseringspolitikk og samarbeide med ENISA om å utarbeide forslag til europeiske cybersikkerhetssertifiseringsordninger. Gruppen kan også foreslå for kommisjonen konkrete ordninger som ENISA bør få i oppdrag å utarbeide. Kommisjonen innehar formannskapet og sekretariatsfunksjonen for gruppen med bistand fra ENISA, jf. artikkel 50. Medlemslandene skal ifølge forslaget fastsette rettsregler for sanksjoner for brudd på forordningens bestemmelser og de europeiske sertifiseringsordninger. Sanksjonene skal være effektive, stå i rimelig forhold til bruddet og ha avskrekkende effekt, jf. artikkel 54. Effekten av ENISAs nye rolle og virkningen av sertifiseringsordningen skal evalueres hvert femte år.

Vedlegg 3

Regulering og organisering i andre land

1 Erfaringer fra andre land

Utfordringene på IKT-sikkerhetsområdet er ikke særegne for Norge, og internasjonalt er det ulike løsninger for organisering og regulering innenfor IKT-sikkerhet. Utvalget har valgt å rette oppmerksomheten mot land som er sammenlignbare med Norge, og land som utvalget mener har kommet langt når det gjelder å regulere og organisere IKT-sikkerhet.

1.1 Ulik forvaltningstradisjon – ulik organisering

Det er vanskelig å sammenligne organiseringen i land uten samtidig ha kunnskap om hvordan sentralforvaltningen er bygget opp. Ulike land har ulik forvaltningstradisjon og er ulikt organisert på departementsnivået. Hvilket departement som har hovedansvar for IKT-sikkerhet, varierer mellom landene. I Sverige og Nederland har justisdepartementet ansvaret, i Danmark har forsvarsdepartementet ansvaret, mens i Finland er det Kommunikationsministeriet som har ansvar for nasjonal IKT-sikkerhet. Disse departementene kan ha oppgaver som går utover tilsvarende departements oppgaver i Norge. I noen land, som Danmark og Finland, er ansvaret for ekomsikkerhet og nasjonal IKT-sikkerhet lagt til samme departement. Det vanligste i landene vi har sett nærmere på, er at ekomsikkerhet og nasjonal IKT-sikkerhet er lagt til ulike departementer, som i Norge. Storbritannia skiller seg noe ut fra de øvrige landene. Ansvaret for politikkutforming og koordinering innenfor IKT-sikkerhet er lagt til Cabinet Office, som er direkte underlagt statsministeren.

I den svenske modellen er direktorater og andre underlagte myndighetsorganer mer uavhengig av det overordnede departementet enn i Norge, og det er kun en samlet regjering som kan instruere underlagte etater. Som i Sverige utøver den finske regjeringen i hovedsak sin myndighet som et samlet kollegium, mens myndighetsutøvelsen i Norge vanligvis tar utgangspunkt i hver enkelt ministers konstitusjonelle ansvar. I Finland er departementene relativt små og fungerer primært som politiske sekretariater, og mye av forvaltningsmyndigheten er lagt til underliggende etater.

Den største forskjellen på organiseringen i Norge og Sverige er at samordningsansvaret for IKT-sikkerhet, og den nasjonale CERT-funksjonen, er lagt til myndigheten som har ansvar for samfunnssikkerheten, Myndigheten för samhällsskydd och beredskap (MSB). I Norge er MSBs ansvar delt mellom DSB og NSM, og delvis Difi for offentlig sektor. I Sverige er således arbeidet med IKT-sikkerhet i større grad enn i Norge integrert med det øvrige samfunnssikkerhetsarbeidet.

I Danmark er arbeidet med samfunnssikkerhet, herunder IKT-sikkerhet, lagt inn under Forsvarsministeriet. Ministeriene i Danmark er autonome, og enheter som Beredskapsstyrelsen og Center for Cybersikkerhed (CFCS) er ikke underlagte etater, men en del av selve ministeriet. Den danske styringsmodellen krever stor grad av samordning mellom sektorer på IKT-sikkerhetsområdet, men har den fordelen at arbeidet med sikkerhet og beredskap på nasjonalt nivå er samlet i ett ministerium.

Av landene utvalget har sett nærmere på, skiller Estland seg mest ut fra de øvrige. Det kan skyldes at det er forholdsvis kort tid siden Estland gjenoppsto som selvstendig stat etter Sovjetunionens sammenbrudd, og dermed har kunnet organisere seg uten å måtte ta hensyn til historikk og etablerte strukturer. De har valgt å legge et bredt ansvar for IKT-sikkerhet i en egen etat, og et departement, Ministry of Economic Affairs and Communication, har totalansvaret innenfor IKT-sikkerhet. Unntaket er i forbindelse med internasjonale problemstillinger, hvor Ministry of Foreign Affairs har et ansvar.

1.2 Konsolidering av miljøer

På tross av landenes ulike forvaltningstradisjoner og organisering av sentrale myndigheter kan det se ut som trenden er at ulike miljøer innenfor IKT-sikkerhet konsolideres i større enheter med bredere virkefelt. Dette kan omfatte alt fra den nasjonale CERT-funksjonen til råd og veiledning til næringslivet og befolkningen.

Danmark etablerte Center for Cybersikkerhed (CFCS) i 2012, Nederland åpnet sitt National Cyber Security Centrum (NCSC) i 2012, og Storbritannias National Cyber Security Center (NCSC) ble operativt i 2016.

I Sverige og Finland er samordningsansvaret for IKT-sikkerhet lagt til etablerte etater med tilgrensende ansvar. I Sverige er ansvaret lagt til MSB, mens det i Finland er lagt til ekommyndigheten FICORA. I Finland kalles riktignok den delen av FICORA som har dette IKT-sikkerhetsansvaret, for National Cyber Security Center Finland (NCSC), men det fremheves ikke i samme grad som i andre land at dette er et senter.

1.3 Offentlig–privat samarbeid

Konsolideringen av IKT-sikkerhetsmiljøene har flere årsaker, men en viktig begrunnelse har vært ønsket om å styrke det forebyggende arbeidet gjennom enhetlig og tilgjengelig råd og veiledning og å styrke offentlig–privat samarbeid. Storbritannia, for eksempel, legger stor vekt på at NCSC skal preges av åpenhet og transparens, og at de er helt avhengige av godt offentlig–privat samarbeid for å nå målet om et sikkert Storbritannia. Ettersom landet har forholdsvis svak regulering av IKT-sikkerhetsområdet, er det helt avhengig av at virksomhetene har et bevisst forhold til IKT-sikkerhet og har egeninteresse i å ha forsvarlig IKT-sikkerhet. NCSC har derfor utviklet løsninger for informasjonsdeling og offentlig–privat samarbeid. Et premiss for å få til dette er, ifølge NCSC, at de ikke er en regulatorisk myndighet og dermed ikke har sanksjonsmyndighet overfor aktørene de samhandler med.

I Nederland vektlegges det også at ingen etat eller myndighet alene kan møte IKT-sikkerhetsutfordringene, og nederlandske NCSC fremhever, som britene, tillit som en kritisk suksessfaktor for vellykket offentlig–privat samarbeid. Tillit bygges gjennom gode samarbeidsordninger, som for eksempel senterets bruk av liaisoner fra næringslivet og samarbeid med sektorvise informasjons- og analysesentre hvor private virksomheter og utvalgte offentlige etater deltar.

I Finland fremgår det ikke at offentlig–privat samarbeid er en stor del av det finske NCSCs portefølje. Det kan skyldes at det i Finland allerede er sterk tradisjon for slikt samarbeid, og at det derfor ikke er nødvendig å uttrykke dette eksplisitt. Samarbeidet mellom myndighetene og private virksomheter skjer blant annet gjennom organisasjoner som Finnish Information Security Cluster (FISC), som ble stiftet i 2012 av de viktigste IKT-sikkerhetsselskapene i Finland.

Landene over er eksempler på ulike tilnærminger til offentlig–privat samarbeid. Felles for alle land utvalget har sett nærmere på, er at myndighetene ikke alene ser seg i stand til å løse IKT-sikkerhetsutfordringene. Et godt offentlig–privat samarbeid vurderes derfor gjennomgående som avgjørende for å lykkes.

1.4 Ulik tilnærming til regulering

Hvis man ser på reguleringen av IKT-sikkerhet i andre land, kan det konstateres at også denne har ulike tilnærminger. Enkelte land har krav nedfelt i tverrsektorielle reguleringer, mens andre land har IKT-sikkerhetskrav primært i sektorspesifikk regulering.

Land som Estland, Tyskland og Frankrike har en tilnærming med høy grad av sentralisering og tverrsektoriell regulering. I disse landene er det samtidig etablert sterke sentrale fagmyndigheter innen IKT-sikkerhet, med kompetanse til å stille utfyllende krav. På den andre siden har man Storbritannia, hvor omfanget av reguleringer er lite, og hvor de i større grad baserer seg på at virksomhetene selv må ta ansvar for egen IKT-sikkerhet. Andre land, som Danmark, har valgt en mellomløsning hvor enkelte forhold er regulert tverrsektorielt, mens andre er regulert gjennom sektorlovgivningen.

De samme trekkene ser man i landenes tilnærming til implementering av NIS-direktivet (se vedlegg 2). En del land velger å implementere direktivet gjennom egen lov, mens andre implementerer direktivet gjennom lovgivning i de enkelte sektorene.

De klareste fellestrekkene mellom de ulike landene finner vi knyttet til de kravene som stilles til beskyttelse av personopplysninger. På dette området har de fleste europeiske land tverrsektorielle krav om IKT-sikkerhet nedfelt i en egen personopplysningslov. Disse lovene ble inntil nylig bygget på Europaparlaments og rådsdirektiv 95/46/EF av 24. oktober 1995, og stiller i det alt vesentligste sammenfallende krav om beskyttelse av personopplysninger. På tilsvarende måte stiller

GDPR tverrsektorielle krav om hvordan personopplysninger skal sikres i landene i EU/EØS-området.

2 Gjennomgang av land

2.1 Sverige

Departementsnivå

På politisk nivå har Justitiedepartementet omtrent samme ansvar for IKT-sikkerhet som Justis- og beredskapsdepartementet har i Norge. I internasjonale problemstillinger arbeider Justitiedepartementet tett med Utrikesdepartementet.

Näringsdepartementet har ansvar for samordning av IKT-politikken, herunder digital agenda, regulering av elektronisk kommunikasjon, nettsikkerhet, og Internet Governance. Departementet har også etatsstyringsansvar for Post- och telestyrelsen, og har følgelig et ansvar som i Norge er delt mellom Kommunal- og moderniseringsdepartementet og Samferdselsdepartementet.

Sentrale fagmyndigheter

Myndigheten för samhällsskydd och beredskap (MSB) er den sentrale fagmyndigheten for IKT-sikkerhet på sivil side i Sverige. MSB tilsvarer i stor grad DSB i Norge, men har et betydelig større ansvar på IKT-sikkerhetsområdet enn DSB. Det er mer sammenlignbart med NSMs ansvar som fagmyndighet innenfor IKT-sikkerhet.

På IKT-sikkerhetsområdet skal MSB støtte og samordne det arbeidet som utføres i sivil sektor. MSB skal også foreta en fortløpende analyse av trusselutviklingen på området. I dette inngår det å gi råd og veiledning om forebyggende arbeid til statlige myndigheter, kommuner og landsting samt foretak og organisasjoner. Myndigheten skal rapportere til regjeringen om status på IKT-sikkerhetsområdet og kan i denne sammenheng også komme med forslag til tiltak.

MSB har også ansvar for å forebygge og håndtere IKT-hendelser, herunder drifte CERT-SE.

Post- och telestyrelsen (PTS) fører tilsyn med elektronisk kommunikasjon i Sverige. Begrepet elektronisk kommunikasjon innbefatter her telekommunikasjoner, IT og radio. PTS tilsvarer Nkom i Norge og har omtrent samme rolle innenfor IKT-sikkerhet som Nkom. Datainspektionen tilsvarer Datatilsynet i Norge og har tilnærmet samme mandat.

Sentrale samordningsarenaer

I tillegg til de sentrale fagmyndighetene er tre sentrale samordningsarenaer viktige i den svenske organiseringen. Samverkansgruppen för informationssäkerhet (SAMFI) består av et antall myndigheter som alle har et særskilt ansvar for samfunnets informasjonssikkerhet. Myndighetene i SAMFI støtter hverandre gjennom informasjonsutveksling og samarbeid, og drøfter spørsmål innen følgende hovedområder:

- Strategi, handlingsplan og forskrifter
- Tekniske spørsmål og standardiseringsspørsmål
- Nasjonal og internasjonal utvikling innen informasjonssikkerhet
- Informasjonsvirksomhet
- Øvelser og trening
- Ledelse og forebygging av IKT-hendelser

Informationssäkerhetsrådet er et privat–offentlig råd med bred representasjon fra offentlige og private virksomheter, og det er ledet av MSB.

Rådet bistår MSB med

- informasjon om utviklingstrender innen informasjonssikkerhet herunder beskyttelse av informasjon og sikring av informasjonssystemer
- synpunkter på innretning, prioritering og gjennomføring av MSBs arbeid på området
- kvalitetssikring av MSBs arbeid

Rådet skal bidra til spredning av informasjon om MSBs arbeid med informasjonssikkerhet i samfunnet.

Nationella telesamverkansgruppen (NTSG) består av de største markedsaktørene innen elektronisk kommunikasjon. Her samarbeider disse, på frivillig basis, med PTS om å styrke den nasjonale elektroniske infrastrukturen.

Regulering

For statlige organer har MSB fastsatt *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet* av 1. mars 2016. Regelverket stiller krav til at statlige virksomheter med utgangspunkt i et styringssystem for sikkerhet skal gjennomføre et systematisk og risikobasert informasjonssikkerhetsarbeid. De skal ta hensyn til ISO 27001 og 27002 i arbeidet. Virksomhetene skal definere ansvar, roller og myndighet i arbeidet med informasjonssikkerhet, utarbeide en informasjonssikkerhetspolicy, og dokumentere

sikkerhetsarbeidet. Virksomheten skal verdivurdere informasjonen sin med utgangspunkt i behovet for konfidensialitet, integritet og tilgjengelighet og iverksette risikobaserte tiltak for å beskytte informasjonen. Forskriften stiller også krav til at virksomhetene skal ha rutiner for å håndtere hendelser som kan påvirke sikkerheten.

Gjennom *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter* av 1. mars 2016 pålegges statlige myndigheter en rapporteringsplikt til MSB. Hendelser som alvorlig kan påvirke informasjonssikkerheten, skal rapporteres. Der hvor statlige virksomheter benytter private underleverandører, skal disse i outsourcingsavtalen pålegges en tilsvarende rapporteringsplikt.

For å iverksette NIS-direktivet i svensk rett har Riksdagen i juni 2018 vedtatt *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster.* Regjeringen har fastsatt en forordning koblet til den nye loven. Lov og forordning trådte i kraft 1. august 2018.

Fra 25. mai 2018 er GDPR implementert i svensk rett og regulerer sikring av personopplysninger.

2.2 Danmark

Departementsnivå

På politisk nivå er Forsvarsministeriet ansvarlig for samordningen på IKT-sikkerhetsområdet. Det nasjonale senteret for cybersikkerhet, Center for Cybersikkerhed, er underlagt Forsvarsministeriet.

Ervervs- og Vækstministeriet arbeider for å fremme IT-sikkerhet og ansvarlig datahåndtering i små og mellomstore virksomheter. De ivaretar sekretariatet for Virksomhetsrådet for IT-sikkerhet, og lanserte blant annet *sikkehedstjekket.dk* sammen med Rådet for Digital Sikkerhed i 2016. *Sikkerhetstjekket.dk* skal gjennom målrettet informasjon og veiledning styrke IT-sikkerheten i virksomhetene. Ministeriet har også gitt ut *Privacykompasset* (2015), som veileder virksomhetene i håndtering av personvern innenfor eksisterende lovgivning og den nye personvernforordningen. De er ansvarlige for tilsynet av de spesifikke databeskyttelsesreglene i e-Databeskyttelsesdirektivet for telesektoren, som blant annet omfatter kommunikasjonshemmeligheter, trafikk- og lokasjonsdata og databrudd og er implementert i dansk rett.

Utenrigsministeriet ivaretar internasjonale spørsmål relatert til IKT-sikkerhet.

Sentrale fagmyndigheter

I 2012 ble Center for Cybersikkerhed (CFCS) opprettet som en sammenslåing av MilCERT og GovCERT. CFCS er en del av Forsvarets etterretningstjeneste, som ligger under Forsvarsministeriet. Senteret er den nasjonale IKT-sikkerhetsmyndighet for danske myndigheter og virksomheter og fungerer som nasjonalt kompetansesenter på cybersikkerhetsområdet. CFCS har også ansvaret for informasjonssikkerhet og beredskap i telesektoren. Det betyr blant annet at de fører tilsyn på området og skal bidra til at det er et høyt sikkerhetsnivå i IKT-infrastrukturen. Videre skal senteret oppdage, analysere og bidra til å avverge avanserte IKT-angrep mot myndigheter og virksomheter som eier/drifter samfunnsviktige funksjoner (for eksempel finanssektoren, statsforvaltningen, telenettet, vannforsyning). Senteret utarbeider halvårlige trusselvurderinger. CFCS ivaretar den danske nasjonale CERT-funksjonen. CFCS har ansvarsområder som i Norge ivaretas av NSM, Nkom og delvis DSB.

Datatilsynet tilsvarer det norske Datatilsynet. Det er en uavhengig myndighet, administrativt underlagt Justitsministeriet.

Digitaliseringsstyrelsen har ansvaret for å fremme digitaliseringen av offentlig sektor i Danmark, herunder å styrke rammene for statsforvaltningens IKT-sikkerhet gjennom innføring av sikkerhetsstandarden ISO 27001. Styrelsen publiserer informasjons- og veiledningsmateriell primært rettet mot statsforvaltningen og innbyggerne for å øke bevisstheten om IKT-sikkerhet, og de fører tilsyn med Statens IT på vegne av alle statens kunder.

Beredskapsstyrelsen har mange oppgaver tilsvarende DSB i Norge og utgir en årlig nasjonal risikovurdering som forutsettes å inngå som et grunnlag for myndighetenes og virksomhetenes risikovurderinger.

Sentrale samordningsarenaer

Det er flere sentrale samordningsarenaer i Danmark. Den tværministerielle kontaktgruppe vedrørende cybersikkerhed er underlagt CFCS. Gruppen skal sikre at departementenes toppledelse har oppdatert kunnskap om hvilke cybertrusler statlige myndigheter står overfor, og hvordan de – i tett dialog med CFCS – kan styrke beskyttelsen mot avanserte IKT-angrep. Gruppen møtes fast to til tre ganger i året, eventuelt ved behov.

Det Strategiske Samarbejdsforum for Cybersikkerhed er også underlagt CFCS, og er en sam-

arbeidsarena der samfunnsviktige virksomheter i privat sektor (foreløpig bare IT- og telesektoren, finanssektoren, transportsektoren, forsvarsindustrien og energi- og forsyningssektoren) samt bransjeorganisasjoner inviteres til dialog/informasjonsutveksling med tanke på beskyttelse av samfunnsviktig infrastruktur og funksjoner. Formålet med arenaen er at CFCS skal understøtte virksomhetenes egeninnsats på området på bakgrunn av den informasjonen som blir delt i forumet. Gruppen møtes fast to til tre ganger i året, eventuelt ved behov.

Rådet for Digital Sikkerhed er en uavhengig privat forening som består av et bredt spekter av aktører (virksomhetsmedlemmer) i offentlig og privat sektor og i akademia, og som fokuserer på IKT-sikkerhet og personvern. Formålet med rådet er i felleskap å skape bedre IKT-sikkerhet i Danmark.

Regulering

Lov om Center for Cybersikkerhed av 25. juni 2014 etablerer lovgrunnlaget for CFCS. Loven pålegger CFCS å understøtte et høyt informasjonssikkerhetsnivå i IKT-infrastruktur som samfunnsviktige funksjoner er avhengige av. CFCS skal drive en nettsikkerhetstjeneste, som er sammenlignbar med det norske VDI-systemet. Gjennom tjenesten overvåkes de tilknyttede virksomheters nettverkskommunikasjon. Loven definerer de rettslige rammene for denne tjenesten. Tilknytning til nettsikkerhetstjenesten er som i Norge basert på frivillighet. De øverste statsorganene, statlige, regionale og kommunale myndigheter og andre virksomheter som forvalter samfunnsviktige funksjoner, kan etter anmodning bli tilsluttet nettsikkerhetstjenesten. Etter loven har CFCS hjemmel til å behandle innhold- og trafikkdata fra nettverkene til de tilsluttede virksomhetene innenfor formålet å understøtte et høyt informasjonssikkerhetsnivå i samfunnet. CFCS er unntatt fra den danske personopplysningsloven. Senterets behandling av personopplysninger er derfor uttømmende regulert i senterets eget rettsgrunnlag.

Lov om net- og informationssikkerhed av 15. desember 2015 etablerer en hjemmel for at CFCS kan fastsette regler i form av minimumskrav om informasjonssikkerhet hos tilbydere av ekomtjenester. Formålet med disse reglene er å bidra til å sikre en robust ekominfrastruktur. Loven gir også hjemmel for at det fastsettes nærmere bestemmelser om rapporteringsplikt til CFCS. Dette omfatter en plikt til å rapportere om hvordan ekomnettene er innrettet og blir driftet, om større planlagte anskaffelser til nettene og om sikkerhetsbrudd som kan ha vesentlige driftsmessige konsekvenser. I disse tilfellene kan tilbyderne også pålegges å underrette allmenheten. CFCS kan også gi regler som er nødvendig for å sikre ekomtjenester i beredskapssituasjoner og andre ekstraordinære situasjoner. CFCS fører tilsyn med etterlevelsen av bestemmelsene gitt i og i medhold av *lov om net- og informationssikkerhed*.

Danmark implementerte NIS-direktivet gjennom reguleringer i den enkelte sektor. Gjennom dette vil man oppnå at det fastsettes målrettede sikkerhetskrav tilpasset den enkelte sektor. I tilknytning til implementering av NIS-direktivet ble en ny *lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester* vedtatt 8. mai 2018. Dette lovforslaget implementerer de deler av direktivet som stiller sikkerhetskrav til samtrafikkpunkter (*internet exchange points*). Loven gir CFSC hjemmel til å stille nærmere sikkerhetskrav og føre tilsyn. Loven tilrettelegger videre for at CFCS kan ivareta de tverrgående myndighetsoppgaver som følger av direktivet, herunder funksjonen som nasjonalt kontaktpunkt og nasjonalt responsmiljø (CSIRT).[1]

Lov nr. 522 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) av 23. mai 2018 regulerer behandlingen av personopplysninger i Danmark og implementerer GDPR i dansk rett.

2.3 Finland

Departementsnivå

Det finske finansdepartementet har ansvaret for digitaliseringen av offentlig sektor i Finland, herunder IKT-sikkerhet i offentlig sektor. Kommunikationsministeriet har ansvaret for nasjonal IKT-sikkerhet og elektronisk kommunikasjon. Utrikesministeriet har ansvaret for å ivareta Finlands interesser i internasjonale IKT-sikkerhetsspørsmål.

Sentrale fagmyndigheter

I Finland er Kommunikationsverket (FICORA), tilsvarende Nkom i Norge, den sentrale fagmyndigheten på IKT-sikkerhetsområdet. FICORA er

[1] Forsvarsministeriet (2017) *Høring over udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.* – 27.10.2017.

underlagt Kommunikationsministeriet, og på IKT-sikkerhetsområdet har de oppgaver som i Norge ligger under NSM. The National Cyber Security Centre Finland (NCSC-FI) er en del av FICORA. Senteret er tillagt den nasjonale CERT-funksjonen, som tidligere het CERT-FI.

Nationella säkerhetsmyndigheten (NSA) er underlagt Utrikesministeriet og har ansvar for å følge opp internasjonale avtaler og for gradert kommunikasjon med utlandet og mellom sentrale myndigheter.

Regulering

I Finland er det ikke gitt sektorovergripende reguleringer av IKT-sikkerhet. IKT-sikkerhet reguleres derimot i en rekke sektorspesifikke særlover. Sentral i denne sammenheng er *Information Society Code (917/2014)*. Denne loven regulerer ekomtjenester og stiller også krav til at tilbydere av ekomtjenester skal ivareta IKT-sikkerhet. Større sikkerhetsbrudd eller forhold som kan utgjøre en trussel mot informasjonssikkerheten, skal rapporteres til FICORA. Loven stiller overordnede sikkerhetskrav og gir FICORA hjemmel til å stille utdypende krav i forskrifter.

NIS-direktivet er implementert i finsk rett gjennom endringer i en rekke ulike sektorlover. I desember 2017 fremmet den finske regjeringen et forslag til parlamentet om implementering av NIS-direktivet. Forslaget vil medføre endringer i *Information Society Code, Aviation Act, Railway Act, Vessel Traffic Service Act, Act on Security Measures on certain Ships and in Ports serving them and on monitoring the Security Measures, Act on Transport Services, Electricity Market Act, Natural Gas Market Act, Act on the Control of the Electricity and Natural Gas Market, Water Services Act* og *Act on the Financial Supervisory Authority.*[2] Forslaget ble vedtatt og gitt ikrafttredelse den 9. mai 2018.[3]

Government Decree on information security in central government (681/2010) stiller krav til hvordan statlige myndigheter skal beskytte sensitiv informasjon, herunder sikkerhetsgradert informasjon, personopplysninger og annen informasjon som kan skade offentlige interesser som kommer uvedkommende i hende. Instruksen har en helhetlig tilnærming til sikkerhet, hvor krav om IKT-sikkerhet inngår som ett av flere elementer.

Personal Data Act (523/1999) stiller krav om sikring av personopplysninger. Ny lovgivning som skal implementere GDPR i finsk rett, er under utarbeidelse, men synes ennå ikke endelig vedtatt.

2.4 Storbritannia

Departementsnivå

I Storbritannia har Cabinet Office en koordinerende rolle innenfor IKT-sikkerhet, men hvert departement har ansvar for IKT-sikkerhet i egen sektor. Cabinet Office er direkte underlagt statsministeren, men gir støtte til hele regjeringen på flere politikkområder. Department of Digital, Culture, Media and Sport er ansvarlig departement for ekom og internett, og de gjennomfører også *The Cyber security breaches study* med jevne mellomrom. Home Office er ansvarlig departement for politiet og dermed også for IKT-kriminalitetsbekjempelse, og Foreign and Commonwealth Office er ansvarlig for Storbritannias internasjonale IKT-sikkerhetsstrategi og IKT-sikkerhetsarbeid.

Sentrale fagmyndigheter

Cyber and Government Security Directorate (CGSD) er en del av Cabinet Office og bistår og gir råd i forbindelse med prioriteringer og strategisk retning for IKT-sikkerhetsarbeidet. CGSD koordinerer National Cyber Security Program (NCSP) og er ansvarlig for den nasjonale IKT-sikkerhetsstrategien.

Government Communications Headquarters (GCHQ), som er underlagt Foreign and Commonwealth Office har ansvar for å identifisere trusler og sårbarheter på IKT-sikkerhetsområdet og støtter forsvaret i deres operasjoner. National Cyber Security Centre (NCSC) er en del av GCHQ og skal bidra til å beskytte vitale interesser i landet mot uønskede hendelser. Senteret gir råd og veiledning og håndterer hendelser, og ivaretar den nasjonale CERT-funksjonen i Storbritannia. Det ble etablert i 2016 og er en sammenslåing av elementer både innenfor og utenfor GCHQ, herunder National Technical Authority for Information Assurance (CESG), the Centre for Cyber Assessment (CCA), CERT-UK, Gov-CERT og cyberdelen av Centre for Protection of National Infrastructure (CPNI). Sistnevnte har fortsatt en viss rådgivningsrolle og samarbeider tett med NCSC. Bakgrunnen for

---

2 Finnish Government (2017) *Government proposal: Improvements to information secutiry of essential services to society.* Pressemelding 22.12.2017.

3 Finnish Government (2018) *Legislative amendments increasing information secutiry of services essential to society into force.* Pressemelding 11.5.2018.

etableringen av senteret var et ønske om bedre koordinering og entydig råd og veiledning fra myndighetene, og bedre utnyttelse av myndighetenes kompetanse ved å samle den under samme tak.

Selv om NCSC er en del av etterretnings- og sikkerhetsorganisasjonen GCHQ, er samhandling med næringsliv og andre offentlige etater en sentral del av NCSCs virksomhet. De har til enhver tid om lag 100 *secondees,* personer ansatt i næringslivet eller andre offentlige virksomheter, som jobber i senteret to til tre dager i uken. Dette gir virksomhetene kompetanseheving, og det gir NCSC essensiell sektorkunnskap i tillegg til arbeidskraft. Samhandlingen med næringslivet er i all hovedsak basert på tillit, og senteret ønsker ikke å være en regulatorisk myndighet for å svekke denne tilliten.

Ofcom er den britiske ekommyndigheten og følger i noen grad opp IKT-sikkerhet i ekomsektoren. Det er i første rekke en markedsregulator og ivaretar forbrukerinteresser. Etaten er underlagt Department of Digital, Culture, Media and Sport.

Information Commissioner's Office (ICO) forvalter de britiske personvernreglene, inkludert GDPR, og forvalter tjenestetilbyderdelen (RDSP) av NIS-direktivet.

Sentrale samordningsarenaer

National Security Council består av de mest relevante departementenes ministre og ledes av statsministeren. Rådet skal til enhver tid være oppdatert på mulige trusler mot Storbritannia, herunder IKT-sikkerhet, og koordinere nødvendige tiltak.

Regulering

Storbritannia har i liten utstrekning lovregulerte krav om IKT-sikkerhet.

Storbritannia har i forskrift av 19. april 2018 implementert NIS-direktivet i britisk rett.[4] Forskriften er gitt med hjemmel i *European Communities Act fra 1972*. Det er myndighetenes intensjon at forskriften og kravene som følger av NIS-direktivet, skal fortsette å gjelde også etter deres uttreden fra EU. Ansvaret for å implementere forskriftens krav om IKT-sikkerhet følger i utgangspunktet sektorprinsippet, med flere ulike departementer som kompetente myndigheter. NCSC etableres som internasjonalt kontaktpunkt knyttet til implementeringen av direktivet, samt som CSIRT i henhold til direktivet.

Storbritannia gjennomførte i 2016 et *Cyber Security Regulation and Incentives Review*, hvor det i tilknytning til behovet for en bredere regulering av IKT-sikkerhet trekkes følgende konklusjon:[5]

> The Review has considered whether there is a need for regulation beyond data protection. Following detailed consideration of evidence from stakeholders and available literature, it concluded that additional cyber security regulation on organisations across the wider economy is not currently justified. It should ultimately be for organisations to manage their own risk in respect of their own sensitive data and online presence, and it should be in their commercial interests to invest in their protection. Government is clear that all businesses have a responsibility to consider their own cyber security and act in their business interests to protect themselves from cyberattack.

Data Protection Act 2018 No 625 av 23. mai 2018 gir bestemmelser som sikring av personopplysninger og implementerer GDPR i britisk rett.

2.5 Nederland

Departementsnivå

Ministry of Security and Justice har samordningsansvaret for IKT-sikkerhet i Nederland, og for utformingen av IKT-sikkerhetspolitikken. Ministry of Economic Affairs and Climate Policy har ansvar for utformingen av IKT-politikken og for å regulere ekomsektoren. Nederlands internasjonale arbeid med IKT-sikkerhet forvaltes av Ministry of Foreign Affairs.

Sentrale fagmyndigheter

National Coordinator for Counterterrorism and Security (NCTV) tilsvarer delvis NSM og DSB og er en etat i Ministry of Security and Justice. De har hovedansvar for

- å analysere og redusere identifiserte trusler
- å overvåke og beskytte personer, eiendom, tjenester, arrangementer og viktige sektorer
- cybersikkerhet
- å beskytte eiendom, enkeltpersoner, sektorer og nettverk
- krisehåndtering og krisekommunikasjon

[4] The Network and Information Systems Regulations 2018 No 506 av 19. april 2018. UK regulation.

[5] HM Government (2016) *Cyber Security Regulations and Incentives Review – December 2016.*

Det nederlandske Data Protection Agency er som Datatilsynet i Norge en uavhengig etat som skal sørge for etterlevelse av personvernlovgivningen. Authority for Consumers and Markets er Nederlands regulatoriske myndighet for ekomsektoren, tilsvarende Nkom i Norge.

National Cyber Security Centre (NCSC) har ansvar for å koordinere nasjonal trussel- og hendelseshåndtering, øke bevisstheten i samfunnet om IKT-sikkerhet, gi råd og veiledning, dele informasjon om trusler og hendelser, bistå ved hendelseshåndtering (herunder med teknisk analyse) og styrke den operasjonelle samordningen. NCSC er Nederlands nasjonale CERT, og det er underordnet NCTV i Ministry of Security and Justice. Senteret har utstrakt offentlig–privat samarbeid, særlig gjennom liaisoner, partnerskap og informasjonsdelingsarenaer. De har også ansvar for å følge opp ICT Response Board (IRB), som er et offentlig–privat samarbeid knyttet til oppfølging og beskyttelse av samfunnskritisk IKT-infrastruktur.

Sentrale samordningsarenaer

Cyber Security Council ble etablert i 2011 og ledes av Ministry of Security and Justice. Rådets mandat er å koordinere og føre tilsyn med implementeringen av tiltakene i National Cyber Security Strategy 2 gjennom å

- drøfte og komme med råd om myndighetenes, private aktørers og akademias («*knowledge institutions*») arbeid med IKT-sikkerhet
- komme med innspill til prioriteringer knyttet til ressursbruk for å imøtekomme IKT-sikkerhetstrusler mv.
- vurdere nasjonale FoU-behov
- dele informasjon

Rådet har 15 medlemmer fra sentrale myndigheter, private aktører og akademia, og det har et eget sekretariat, som gir råd på forespørsel. Rådet kan også – på eget initiativ – ta opp aktuelle saker og problemstillinger.

Regulering

I 2017 ble *Dutch Data Processing and Cybersecurity Notification Obligation Act* vedtatt. Loven kodifiserer oppgavene til NCSC og etablerer hjemmelsgrunnlag for at senteret kan behandle de personopplysninger som er nødvendig for å utføre sine oppgaver. Loven introduserer også en rapporteringsplikt til NCSC for nærmere definerte sikkerhetsbrudd. Rapporteringsplikten retter seg mot det som kalles *vital operator.* Hvilke virksomheter som er omfattet av dette begrepet, vil bli klargjort i understøttende regelverk. I forarbeidene uttales det imidlertid at virksomheter innen elektrisitet, gass, vannforsyning, ekom, finans, transport og offentlig sektor som et minimum vil være omfattet.[6] Rapporteringsplikten knytter seg til sikkerhetsbrudd som har påvirket, eller kan påvirke, tilgjengeligheten eller påliteligheten til de produktene eller tjenestene virksomheten leverer. *Dutch Data Processing and Cybersecurity Notification Obligation Act* implementerer ikke kravene i NIS-direktivet fullt ut. Direktivet vil derfor bli implementert gjennom en egen lovgivningsprosess. Et lovforslag om implementeringen av NIS-direktivet ble vedtatt av, parlamentet i februar 2018.

The GDPR Implementation Act av 22. mai 2018 stiller krav om sikring av personopplysninger og implementerer GDPR i nederlandsk rett, gjeldende fra 25. mai 2018.

2.6 Estland

Departementsnivå

I Estland er Ministry of Economic Affairs and Communication ansvarlig departement for landets IKT-politikk, herunder IKT-sikkerhetspolitikken. Departementet har blant annet ansvar for å gjennomføre Estlands Cyber Security Strategy. Ministry of Foreign Affairs er ansvarlig departement for internasjonale avtaler og internasjonalt samarbeid på IKT-sikkerhetsområdet.

Sentrale fagmyndigheter

Estonia Information Systems Authority (EISA) organiserer, koordinerer og administrerer utvikling av statens informasjonssystemer, organiserer aktiviteter knyttet til IKT-sikkerhet og håndterer sikkerhetshendelser i estiske nettverk. Etaten er underlagt Ministry of Economic Affairs and Communication. Den nasjonale CERT-funksjonen, CERT-EE, er underlagt EISA.

Estonian Defence League er en organisasjon bestående av frivillige mannskaper, som er underlagt Ministry of Defence. Formålet med organisasjonen er å sikre Estlands suverenitet, og de bidrar på en rekke sivile beredskapsområder, også på IKT-sikkerhetsområdet. De har en egen cybergruppering, som samarbeider tett med

[6] Explanatory Memorandum Dutch Data Processing and Cybersecurity Notification Obligation Act – UNOFFICIAL TRANSLATION.

estiske myndigheter, og tilbyr opplæring og råd og veiledning innenfor IKT-sikkerhet.

Estonian Technical Regulatory Authority er ekommyndigheten i Estland, men de har i liten grad ansvar for IKT-sikkerhet i ekom. Etatens rolle er som markedsregulator og frekvensforvalter.

Sentrale samordningsarenaer

I 2009 ble Cyber Security Council etablert som en del av National Security Committee. Rådet skal sørge for god samordning mellom ulike etater og kontrollere gjennomføringen av Cyber Security Strategy. Rådet ledes av generalsekretæren (tilsvarende departementsråd i Norge) i Ministry of Economic Affairs.

Regulering

The System of security measures for information systems regulation av 20. desember 2007 stiller sikkerhetskrav til IKT-systemer som benyttes av offentlig forvaltning (*the state and local government*). Forskriften er hjemlet i den estiske offentlighetsloven (*Public Information Act* av 15. november 2000). Forskriften krever at det skal gjøres risikovurderinger av IKT-systemene. Vurderingen skal ta i betraktning det aktuelle systemets behov for henholdsvis tilgjengelighet, integritet og konfidensialitet. Basert på vurderingen skal systemene tilordnes en sikkerhetsklasse og sikres med tiltak tilpasset den aktuelle klassen. Forskriften krever videre at offentlige virksomheter skal etablere et styringssystem for sikkerhet og gjennomføre uavhengige sikkerhetsrevisjoner. Rapportene fra sikkerhetsrevisjonene skal sendes til Ministry of Economic Affairs and Communication via EISA.

The Security measures for information systems of vital services and related information assets av 14. mars 2013 stiller krav om sikring av IKT-systemer som benyttes for vitale tjenester. Forskriften er gitt med hjemmel i *Emergency Act* av 8. februar 2017. Formålet med forskriften er å sikre funksjonaliteten til disse systemene og evnen til å gjenopprette dem ved forstyrrelser. Vitale tjenester er i *Emergency Act* definert til å omfatte elektrisitet og gassforsyning, drivstofforsyning, ekomtjenester, digital ID og digital signatur, helsetjenester, banktjenester, vannforsyning og avløp samt veitransport. Forskriften stiller krav til at tjenesteyteren skal foreta en risikovurdering av IKT-systemene som understøtter disse tjenestene. Systemer som tjenestene er avhengige av, skal sikres med tiltak valgt etter en risikovurdering. Tjenesteyteren skal etablere et styringssystem for sikkerhet. Dette skal være basert på ISO 27001:2006 og kravene i *The System of security measures for information systems regulation*. Større sikkerhetshendelser i systemene skal rapporteres til EISA. EISA kan skal informere andre berørte aktører. EISA kan også gi pålegg om sikkerhetstiltak til tjenesteyteren.

Personal Data Protection Act av 15. februar 2007 stiller krav om sikring av personopplysninger. Ny lovgivning som skal implementere GDPR i estisk rett, er under utarbeidelse, og et lovutkast foreligger høsten 2018, men er per november 2018 ennå ikke vedtatt.

2.7 Tyskland

Departementsnivå

Bundesministerium des Innern, für Bau und Heimat har ansvaret for nasjonal IKT-sikkerhet i Tyskland. Den internasjonale delen av dette ansvaret ligger under Auswärtiges Amt.

Sentrale fagmyndigheter

Bundesamt für Sicherheit in der Informationstechnik (BSI) er den nasjonale fagmyndigheten på IKT-sikkerhet i Tyskland. Tysklands nasjonale CERT-funksjon, CERT-Bund, drives i regi av BSI. Sammen med IT-Lagezentrum, IT-Krisenreaktionszentrum og Cyber-Abwehrzentrum utgjør de den nasjonale håndteringskapasiteten i Tyskland, alt innenfor rammene av BSI. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) er Tysklands svar på DSB. Det arrangerer blant annet øvelser og har et ansvar innenfor krisehåndtering. Innenfor IKT-sikkerhet jobber det tett sammen med BSI og Cyber-Abwehrzentrum. Bundesnetzagentur er den tyske regulatoriske myndigheten for ekom og er primært markedsregulator og frekvensforvalter.

Sentrale samordningsarenaer

Cyber-Abwehrzentrum i BSI har et koordineringsansvar mellom etater. Senteret samarbeider direkte med Bundes–amt für Verfassungs–schutz Constitution (BfV), som tilsvarer det norske PST. Senteret samarbeider også direkte med BBK. Sicherheitskabinett er et uformelt forum ledet av kansleren. Forumet diskuterer og beslutter innenfor alle sikkerhetsområder.

Regulering

BSIs oppgaver følger av og er forankret i en egen lov: *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* av 14. august 2009. Loven fastsetter at BSI skal utøve rollen som overordnet føderal IKT-sikkerhetsmyndighet. Blant oppgavene er å forebygge og avverge trusler mot føderale IKT-systemer, utvikle IKT-sikkerhetstiltak og produkter til bruk for føderale myndigheter, forestå testing, evaluering og godkjenning av IKT-sikkerhetsmekanismer, utvikle og drifte kryptosystemer for beskyttelse av føderal informasjon, gi råd, veiledning og bistand innen IKT-sikkerhet samt avdekke og koordinere håndteringen av uønskede hendelser mot kritisk IKT-infrastruktur.

Loven gir BSI kompetanse til å fastsette minimumsstandarder for hvordan føderal IKT-infrastruktur skal sikres, og utarbeide tekniske veiledninger innen IKT-sikkerhet. Øvrige føderale myndigheter har rapporteringsplikt til BSI hvis de oppdager sårbarheter eller blir utsatt for angrep eller forsøk på angrep. Loven gir BSI hjemmel til å foreta sikkerhetsmessig overvåkning av føderale IKT-systemer, og gir bestemmelser om hvordan innsamlet informasjon skal behandles.

Ved *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* av 24. juli 2015 ble det gjennomført endringer i BSI-loven og flere andre lover som gir bestemmelser om IKT-sikkerhet. Bakgrunnen for disse endringene var at det tidligere ikke var noen enhetlig tilnærming til sikkerhet i kritisk IKT-infrastruktur. Målsetningen med endringsloven var å styrke sikkerheten hos eiere av kritisk IKT-infrastruktur.[7] Kritisk infrastruktur betyr her infrastruktur hvor tap eller forstyrrelser i funksjonaliteten vil kunne få alvorlige konsekvenser for den offentlige sikkerheten innen sektorene energi, IT, ekom, transport, trafikk, helse, vann- og matforsyning, finans og forsikring. 2015-loven stiller krav til at eiere av kritisk IKT-infrastruktur skal implementere nødvendige organisatoriske og tekniske tiltak for å sikre disse systemenes tilgjengelighet, integritet, autentisitet og konfidensialitet. Eiere av kritisk IKT-infrastruktur eller deres bransjeorganisasjoner kan foreslå industrispesifikke sikkerhetsstandarder for å imøtekomme kravene. BSI gis myndighet til å vurdere om foreslåtte standarder er tilstrekkelige. BSI kan selv, eller ved bruk av en kvalifisert tredjepart, føre tilsyn med om tilstrekkelige tiltak er implementert. Gjennom loven pålegges videre eiere av kritisk IKT-infrastruktur å rapportere nærmere definerte IKT-sikkerhetshendelser til BSI. Ved uønskede hendelser i infrastrukturen kan BSI etter anmodning bistå i hendelseshåndteringen og i denne sammenheng iverksette de tiltak som er nødvendig for å gjenopprette sikkerheten og funksjonaliteten i systemet. Etter samtykke fra den berørte virksomheten kan BSI benytte en kvalifisert tredjepart hvis dette er nødvendig for å kunne gjenopprette sikkerheten i systemet raskt nok.

Gjennom en endringslov av 23. juni 2017 ble det tatt inn nye bestemmelser i BSI-loven som stiller sikkerhetskrav også til digitale tjenesteleverandører. Dette var for å implementere de deler av NIS-direktivet som ikke allerede var dekket.

Bundesdatenschutzgesetz (Federal Data Protection Act) av 30. juni 2017 stiller krav om sikring av personopplysninger og implementerer GDPR i tysk rett.

2.8 Frankrike

Departementsnivå

I Frankrike har statsministeren det øverste ansvar for IKT-sikkerhetspolitikken. Ansvaret forvaltes gjennom Secrétariat général de la défense et de la sécurité nationale Security (SGDSN), som er en interdepartemental enhet plassert direkte under statsministeren. Særlig forsvarsdepartementet jobber tett med SGDSN for å utvikle Frankrikes cyberkapabiliteter.

Sentrale fagmyndigheter

ANSSI er det nasjonale fagmiljøet for IKT-sikkerhet i Frankrike, og det er en etat direkte underlagt statsministeren på dette området. Formelt sett rapporterer ANSSI som etat til SGDSN. ANSSI har et bredt ansvar for IKT-sikkerhet i Frankrike og jobber med bevisstgjøring av befolkningen så vel som sikring av kritiske systemer for staten. Den nasjonale CERT-funksjonen, CERT-FR, er underlagt ANSSI.

ARCEP er den regulatoriske ekommyndigheten i Frankrike. Det er en kvasiautonom uavhengig etat. Med kvasiautonom menes at etaten er uavhengig, samtidig som regjeringen oppnevner etatens styre. ARCEP har ingen definert rolle innenfor nasjonal IKT-sikkerhet i Frankrike, men er i første rekke markedsregulatorisk myndighet og frekvensforvalter.

CNIL i Frankrike tilsvarer Datatilsynet i Norge og jobber med å følge opp den franske personvernlovgivningen.

---

[7] Federal Office for Information Secutiry (2015) *The State of IT Security in Germany 2015*, s. 42–43.

Sentrale samordningsarenaer

Utvalget har ikke lykkes med å identifisere etablerte samordningsarenaer i Frankrike. Det fremgår imidlertid av offisielle nettsider og den nasjonale IKT-sikkerhetsstrategien at samarbeid mellom myndighetsaktører og offentlig–privat samarbeid er helt nødvendig på IKT-sikkerhetsområdet. For eksempel ble det ved innføringen av Critical Infrastructures Information Protection-reguleringen (CIIP) i 2013 nedsatt arbeidsgrupper av private og offentlige virksomheter for å skape en bred felles forståelse av regulering, begrepsapparatet og lovens betydning for de ulike sektorene.

Regulering

Frankrikes rettslige rammeverk for IKT-sikkerhet består av flere lover og forordninger (*décrets*). I 2013 ble det innført et relativt omfattende regelverk som stiller krav til beskyttelse av kritisk informasjonsinfrastruktur (CIIP), og det har siden blitt videreutviklet.

Act No. 2013-1168 of 18 December 2013 on Military Planning for the years 2014 to 2019 inneholder bestemmelser som gir statlige myndigheter ansvar for å ivareta sikkerheten i samfunnskritisk infrastruktur / infrastruktur som understøtter kritiske samfunnsfunksjoner. Med hjemmel i denne loven kan staten fastsette sikkerhetskrav til systemene, kreve at deteksjonssystemer blir implementert i infrastrukturen, kontrollere sikkerheten i systemene gjennom revisjoner samt pålegge operatørene å iverksette beredskapstiltak ved større kriser.

Decree No. 2015-351 of 27 March 2015 fastsetter nærmere bestemmelser om hvordan disse kravene skal implementeres. Virksomheter med kritiske samfunnsfunksjoner skal identifisere den kritiske IKT-infrastrukturen sin og rapportere oversikter over denne til ANSSI. Forordningen gir ANSSI kompetanse til å fastsette nærmere krav til hvordan disse systemene skal sikres. Samfunnskritiske IKT-systemer skal være tilknyttet et deteksjonssystem. Dette kan enten være det statlige systemet som drives av ANSSI, eller et deteksjonssystem levert av en kvalifisert tjenesteleverandør. Hendelser som kan påvirke sikkerheten eller driften av systemene, skal rapporteres til ANSSI. Det skal gjennomføres kontroll/revisjoner av sikkerheten i systemene. Dette gjennomføres av ANSSI eller en kvalifisert tjenesteleverandører.

Decree No. 2015-350 of 27 March 2015 regulerer ulike sikkerhetsmessige sertifiseringsordninger. Forordningen etablerer for det første et regime for evaluering og sertifisering av sikkerhet i IKT-produkter, hvor ANSSI er sertifiseringsmyndighet. Forordningen etablerer videre et system for å kvalifisere leverandører av ulike IKT-sikkerhetstjenester. Leverandørens kvalifikasjoner vurderes i denne prosessen opp mot standarder fastsatt av ANSSI, og kvalifisering gis for en periode på tre år. ANSSI fører kontroll med at leverandørene i perioden innfrir forutsetningene som stilles for kvalifiseringen.

NIS-direktivet er implementert i fransk rett gjennom *Act No. 2018-133 of 26 February 2018 on various provisions for adaptation to European Union law in the field of security* og *Decree No. 2018-384 of 23 May 2018 on the security of the networks and information systems of essential service operators and digital service providers*. Implementeringen av direktivet bygger på de strukturene som allerede er etablert gjennom eksisterende regelverk om beskyttelse av kritisk informasjonsinfrastruktur.

Act of 14. May 2018 concerning the protection of personal data stiller krav om sikring av personopplysninger og implementerer GDPR i fransk rett.

Vedlegg 4

Datagrunnlag

Hvem utvalget har hatt møter med

23. april 2018:	Nasjonal sikkerhetsmyndighet, Direktoratet for forvaltning og IKT, Datatilsynet
24. april 2018:	KS, Broadnet, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal kommunikasjonsmyndighet
29. mai 2018:	Justis- og beredskapsdepartementet, Samferdselsdepartementet, Forsvarsdepartementet, Olje- og energidepartementet, Kommunal- og moderniseringsdepartementet, Nærings- og fiskeridepartementet, Statsministerens kontor

Hvem utvalget har fått innlegg fra

20. november 2017:	Sekretariatet v/Christian Frederik Mathiessen om NIS-direktivet og arbeidet med ny sikkerhetslov med forskrifter
20. november 2017:	Lovavdelingen i Justis- og beredskapsdepartementet v/Øyvind Molven om ny personvernforordning (GDPR)
18. desember 2017:	FFI v/Ingar Bentstuen om teknologitrender og sikkerhetsutfordringer
18. desember 2017:	Utvalgsleder Olav Lysne om funn fra NOU 2015: 13
15. januar 2018:	Felles cyberkoordineringssenter, Nasjonal sikkerhetsmyndighet, Kripos, Etterretningstjenesten, Politiets sikkerhetstjeneste om trussel- og sårbarhetsbildet
5. mars 2018:	Sekretariatet v/Anders Bjønnes om myndighetenes arbeid med IKT-sikkerhet i et historisk perspektiv

Hvem utvalget har hatt workshop med

7. mars 2018	Norsk Informasjonssikkerhetsforum (ISF) (Hans Christian Holte, Lillian Røstad, sekretariatet)

Hvem utvalget har holdt innlegg for

2. februar 2018:	Abelias og Watchcoms Sikkerhetsforum (Hans Christian Holte)
27. februar 2018:	Fylkesmennenes årlige sikkerhetskonferanse (Lillian Røstad)
9. mars 2018:	Forsvarets høyskole/Sjefskurs (Hans Christian Holte)
25. april 2018:	Skate (Hans Christian Holte)
3. mai 2018:	Jon Bings minneseminar 2018. Rettslige rammer for IKT-sikkerhet: Nye reformer i lys av «gamle» tanker (Hans Christian Holte)
29. mai 2018:	Norges Bank og Finanstilsynets årlige seminar om betalingssystemer og IKT i finanssektoren (Hans Christian Holte)

Hvem sekretariatet har hatt samtaler med

11. oktober 2017:	Sekretariatet for NOU 2017: 11 *Bedre bistand, Bedre beredskap*
6. desember 2017:	Direktoratet for samfunnssikkerhet og beredskap
7. desember 2017:	Direktoratet for forvaltning og IKT
8. desember 2017:	Nasjonal sikkerhetsmyndighet
13. desember 2017:	Datatilsynet
19. desember 2017:	Nasjonal kommunikasjonsmyndighet
16. januar 2018:	Førsteamanuensis Jostein Askim, Institutt for statsvitenskap, Universitetet i Oslo
18. januar 2018:	Astri Hildrum, Direktoratet for forvaltning og IKT
14.-15. februar 2018:	Møte i London med britiske myndigheter (National Cyber Security Centre, Department of Media Culture and Sports, Cabinet Office) og representanter for britisk næringsliv (Tech UK, NCC Group og QinetiQ)
22. mars 2018:	Møte i Stockholm med svenske myndigheter (Justitiedepartementet, Försvarsdepartementet og Näringsdepartementet)
5. april 2018:	Tommy Tranvik, Avdeling for forvaltningsinformatikk, Universitet i Oslo
25. april 2018:	Møte i København med Center for Cybersikkerhed, Forsvarets Efterretningstjeneste og Forsvarsministeriet
27. april 2018:	Teknologirådet v/ direktør Tore Tennøe, Hilde Lovett, Åke Refsdal Moe og Joakim Valevatn
4. mai 2018:	Sekretariatet til forvaltningslovsutvalget

Hvem utvalgsleder og sekretariatsleder har hatt møte med

1.desember 2017:	Referansegruppen
23. mars 2018:	Referansegruppen

Utvalgets referansegruppe har bestått av medlemmer fra

Justis- og beredskapsdepartementet, Forsvarsdepartementet, Kommunal- og moderniseringsdepartementet, Samferdselsdepartementet, Nærings- og fiskeridepartementet og Statsministerens kontor.

Hvilke virksomheter som har gitt skriftlige innspill

Abelia
Akademikerne
Alternativ Data
Andøya Space Center
Apple
Arbeids- og velferdsdirektoratet
Barne- og likestillingsdepartementet
BDO
Broadnet
Brønnøysundregistrene
Cisco
Cyberforsvaret
Datatilsynet
Direktoratet for e-helse
Direktoratet for forvaltning og IKT
Direktoratet for samfunnssikkerhet og beredskap
Distriktsenergi
Energi Norge
Finans Norge
Finanstilsynet
Folkehelseinstituttet
Forbrukerrådet
Forsvarets forskningsinstitutt
Fylkesmannen i Aust- og Vest-Agder
Fylkesmannen i Oppland

Fylkesmannen i Rogaland
Fylkesmannen i Telemark
Fylkesmannen i Vestfold
Fylkesmannen i Østfold
Færder kommune
Gassco
Harstad kommune
Helse Nord
Helse- og omsorgsdepartementet
Helse Sør-Øst
HelseCERT
Helsedirektoratet
Hydro
IKT-Norge
Jernbanedirektoratet
Justervesenet
Justis- og beredskapsdepartementet
Klima- og miljødepartementet
Kommunal informasjonssikkerhet (Kins)
Kommunal- og moderniseringsdepartementet
Konkurransetilsynet
KraftCERT
Kripos
KS
Kulturdepartementet
Kunnskapsdepartementet
Kystverket
Landbruks- og matdepartementet
LO
Luftfartstilsynet
Mattilsynet
Meteorologisk institutt
Microsoft Norge
Miljødirektoratet
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet
Nets
Norges rederiforbund
Norges vassdrag- og energidirektorat
NorSIS
Norsk Forening for Elektro og Automatisering
Norsk Helsenett
Norsk olje og gass
Norsk Romsenter
NSB
Nærings- og fiskeridepartementet
Næringslivets sikkerhetsorganisasjon
Næringslivets sikkerhetsråd
Olje- og energidepartementet
Oljedirektoratet
Oslo Kommune
Pensjonstrygden for sjømenn
Petroleumstilsynet
Politidirektoratet
Posten
Politiets sikkerhetstjeneste
Samferdselsdepartementet
Sjøfartsdirektoratet
Skatteetaten
Statens jernbanetilsyn
Statens vegvesen
Statnett
Statsministerens kontor
Telenor
Telia
Uninett
Unio
Utdanningsdirektoratet
Valgdirektoratet
Vegtilsynet

Ekstern bistand

- Oslo Economics har på oppdrag fra utvalget utarbeidet en samfunnsøkonomisk analyse av utvalgets foreslåtte anbefalinger (følger som digitalt vedlegg).
- Teknologirådet har på oppdrag fra utvalget gitt bistand til tekst i kapittel 4 «Teknologitrender og sikkerhetsutfordringer».
- Direktoratet for forvaltning og IKT har bidratt med innspill til tekst om offentlige anskaffelser.
- NTB Arkitekst har på oppdrag fra utvalget språkvasket utredningen.
- Konsis har på oppdrag fra utvalget utarbeidet illustrasjonene i utredningen.

Vedlegg 5

Forkortelser

4G	Fjerde generasjons mobiltjenester i mobilnett
5G	Femte generasjons mobiltjenester i mobilnett
ANEC	The European Association for the Co-ordination of Consumer Representation in Standardisation (Europeisk organisasjon som forsvarer forbrukerinteresser i standardiseringsarbeidet)
BEUC	The European Consumer Organisation (Den europiske paraplyorganisasjonen for forbrukerorganisasjoner)
CE-merking	Communauté Européenne, deklarasjon på at et produkt oppfyller visse krav
CERT	Computer Emergency Response Team
Difi	Direktoratet for forvaltning og IKT
DNK	Direktoratet for nødkommunikasjon
DSB	Direktoratet for samfunnssikkerhet og beredskap
e-ID	elektronisk identifikasjon
Ekomnett	Elektronisk kommunikasjonsnett
ENISA	European Network and Information Security Agency
EOS-tjenestene	Etterretningstjenesten, Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Forsvarets sikkerhetsavdeling.
EU	Den europeiske union
EØS	Det europeiske økonomiske samarbeidsområdet
FN	De forente nasjoner
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HMS	Helse, miljø og sikkerhet
HR-tjenester	Human resource tjenester
IKT	Informasjons- og kommunikasjonsteknologi
IoT	Internett of Things
ISF	Norsk informasjonssikkerhetsforum
ISO	International Organization for Standardization
KI	Kunstig intelligens
KINS	Kommunal Informasjonssikkerhet
NATO	North Atlantic Treaty Organization
NIS-direktiv	EUs direktiv om sikkerhet i nettverk og informasjonssystemer
Nkom	Nasjonal kommunikasjonssmyndighet
NorCERT	Norwegian Computer Emergency Response Team
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
PST	Politiets sikkerhetstjeneste

SERTIT	Sertifiseringsmyndigheten for IT-sikkerhet i produkter og systemer
SON	Sikret offentlig nett
SSA	Statens standardavtaler
SSB	Statistisk sentralbyrå
VDI	Varslingssystem for digital infrastruktur

Vedlegg 6

Litteraturliste

Oversikt over litteratur det er henvist til i utredningens del I-V

Agenda Kaupang (2014) *Evaluering av Difi.*

Andreoni, J., Erard, B., & Feinstein, J. (1998) *Tax Compliance.* Journal of Economic Literature, 36(2), 818–860.

Arbeidstilsynet m.fl (2014) *Tilsynsmyndighetenes retningslinje for samordnet tilsyn og felles tilsynsprofil*

Baldwin, R., Cave, M. og Lodge, M. (2012). *Understanding Regulation,* Oxford: Oxford University Press.

Bentstuen, Ole Ingar; Farsund, Bodil Hvesser; Øverlien, Lasse; Køien, Geir (2017) *Sikkerhetsutfordringer i fremtidens EKOM-tjenester.* FFI-rapport 17/17047

BEUC/ANEC (2018) *Cybersecurity for connected products.* Position Paper, 2018

Consumers International (2016) *Connection and protection in the digital age. The Internet of Things and challenges for consumer protection*.

Direktoratet for byggkvalitet (2016) *Hva er sentral godkjenning.* Hentet fra: https://dibk.no/sentral-godkjenning/hva-er-sentral-godkjenning/

Direktoratet for ehelse (2018) *Kurs.* Hentet fra: https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/kurs

Direktoratet for forvaltning og IKT (2015) *Statens styring av kommunene.* 2015:19.

Direktoratet for forvaltning og IKT (2016) *Nytt veg- og jernbanedirektorat*. 2016:3

Direktoratet for forvaltning og IKT (2017) *Evaluering av tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid – tredje tilsynsrunde.* 2017:4

Direktoratet for forvaltning og IKT (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen kunnskapsgrunnlag.*2018: 4

Direktoratet for forvaltning og IKT (2018) *Innkjøpsordning/markedsplass for skytjenester* 2018: 6.

Direktoratet for samfunnssikkerhet og beredskap (2014) *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*

Direktoratet for samfunnssikkerhet og beredskap (2016) *Kommuneundersøkelsen 2016* – Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/kommuneundersokelsen_2016pdf.pdf

Direktoratet for samfunnssikkerhet og beredskap (2016) *Retningslinjer for varsling og rapportering på samordningskanal.*

Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner.*

Direktoratet for samfunnssikkerhet og beredskap (2018) *Internt notat om Elektro og ekom konvergerer* av 10.04.2018

Direktoratet for økonomistyring (2018) *Veileder i samfunnsøkonomiske analyser*

Direktoratet for økonomistyring og Direktoratet for forvaltning og IKT (2017) *Departementers styring av samarbeidsoppgaver som gis til underliggende virksomheter.*

Dokument 1 (2018–2019) *Riksrevisjonens årlige revisjon og kontroll – budsjettåret 2017*, Hentet fra: https://www.riksrevisjonen.no/rapporter/Sider/ArligRevisjonOgKontroll2017.aspx

Dokument 3:6 (2015–2016) *Riksrevisjonens undersøkelse av digitalisering av kommunale tjenester.*

DSB (2017) *Tverrsektoriell evaluering av øvelse IKT16*

ENISA (2017) *Baseline Security Recommendation for Internet of Things in the context of critical information infrastructure*, November 20, 2017.

Etterretningstjenesten (2018) *Fokus 2018*,

European Commission (2017) *COM (2017) 476 final/2, Making the most of NIS – towards the effective implementation of Directive*.

European Commission *Rapid Alert System for Dangerous non-food Products.* Hentet fra: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/page rapex/index_en.htm

European Data Protection Supervisor, *Big Data & Digital Clearinghouse.* Hentet fra: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en

Feld, L.P. and Frey, B.S. (2007) *Tax Compliance as the Result of a Psychological Tax Contract: The Role of Incentives and Responsive Regulation*. Law and Policy, 29, 102–120.

Forbrukerrådet (2011) *Klage på brukervilkår knyttet til Sony PlayStation 3, 26.01.2011*

Forbrukerrådet (2016) *Cayla og i_que bryter flere norske lover.* Hentet fra: https://www.forbrukerradet.no/siste-nytt/cayla-og-i-que-bryter-flere-norske-lover/.

Fornyings-, administrasjon- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet med handlingsplan*.

Forsvarsdepartementet og Justis- og beredskapsdepartementet (2018) *Støtte og samarbeid*.

Frost, & Sullivan. (2017) *Global Information Security Workforce Study.*

Furuseth, Helge Rager (2013) *Etterlevelse av regelverk for informasjonssikkerhet,* Masteroppgave ved Avdeling for forvaltningsinformatikk, UiO, Våren 2013

Future of Humanity Institute et al. (2018) *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Februar 2018. Hentet fra: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

Gartner (2017) *Gartner Says 8.4 Billion Connected «things» Will be in use in 2017.* Hentet fra: https://www.gartner.com/newsroom/id/3598917

Gordon et al. (2015) *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon–Loeb Model,* Journal of Information Security, 2015, 6, 24–30.

Gordon, Lawrence; Martin Loeb (November 2002) *The Economics of Information Security Investment. ACM Transactions on Information and System Security. 5 (4): 438–457.*

Haugland, Anders (2012) «Bruk av funksjonsbasert regelverk og rettslige standarder», i Lindøe, P.H., Kringen, J., Braut G.S. (2012) *Risiko og tilsyn.*

Holte, Hans Christian (2017) *Harde og myke virkemidler*, Ukeavisen Ledelse 10. februar 2017

Hood, C.C. og Margetts, H.Z. (2007) *The Tools of Government in the Digital Age.* New York. Palgrace Macmillian.

Innst. 14 S (2016–2017) *Innstilling fra familie- og kulturkomiteen om bevilgninger på statsbudsjettet for 2017*,

Instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering fastsatt i kgl.res. 19. juni 2015.

ISO/IEC 29147:2014 *Information technology – Security techniques – Vulnerability disclosure*.

Justis- og beredskapsdepartementet (2000) *Lovteknikk og lovforberedelse*

Justis- og beredskapsdepartementet (2017) *Instruks for departementenes arbeid med samfunnssikkerhet* 1. september 2017.

Justis- og beredskapsdepartementet brev av 14.12.2017, vedlagt rammeverket – versjon per 07.12.17.

Justis- og beredskapsdepartementet *(2018) Utkast til høringsnotat om NIS-lov*

Kommunal Informasjonssikkerhet *Om oss.* Hentet fra: https://kins.no/om-oss/

Kommunal- og moderniseringsdepartementet (2015) *Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015–2017*.

Kommunal- og moderniseringsdepartementet (2015). *Hva er statsforvaltningen?* Hentet fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/forvaltningsutvikling/hva-er statsforvaltningen/id2397949/

Kommunal- og moderniseringsdepartementet (2018) *Virksomhets- og økonomiinstruks for Fylkesmannen* av 13.09.2018.

Kongelig resolusjon 10. mars 2017: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*.

Kongelig resolusjon 10. mars 2017: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*.

Kongelig resolusjon 22. mars 2013: *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*.

KS (2017) *Digitaliseringsstrategi for kommuner og fylkeskommuner 2017–2020.*

Lied, H. (2016, 31. oktober) En snill orm prøver å fikse internett. *NRK*. Hentet fra: https://nrkbeta.no/2016/10/31/en-snill-orm-prover-a-fikse-internett/

Loopia (2018) *1 av 3 kommuner i Norge har for dårlig nettside-sikkerhet.* Hentet fra: https://www.loopia.no/presse/#/blog_posts/1-av-3-kommuner-i-norge-har-for-daarlig-nettside sikkerhet-71254

Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*

Meld. St. 27 (2015–2016) *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.*

Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*

Meld. St. 39 (2012–2013) *Mangfold av vinnere.*

Myndigheten för samhällsskydd och beredskap (2018) *Redovisning av vissa vidtagna åtgärder*

för att förbereda genomförandet av NIS-direktivet

Nasjonal kommunikasjonsmyndighet (2017) *EkomROS 2017*.

Nasjonal sikkerhetsmyndighet (2015) *Sikkerhetsfaglig råd.*

Nasjonal sikkerhetsmyndighet (2016) *Helhetlig IKT-risikobilde 2016.*

Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for IKT-sikkerhet*. Hentet fra https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf

Nasjonal sikkerhetsmyndighet (2018) *Anbefaling om landvurdering ved tjenesteutsetting.*

Nasjonal sikkerhetsmyndighet (2018) *Konseptnotat, Nasjonalt cybersikkerhetssenter – en del av NSM*. 24. august 2018.

Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018*

Nasjonal sikkerhetsmyndighet (2018) *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området «Beslutt leveransemodell» i NSMs grunnprinsipper for IKT-sikkerhet.*

Nasjonal sikkerhetsmyndighet (2018) *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*

Nationaal Cyber Security Centrum (2018) Coordinated Vulnerability Disclosure: the Guideline. Hentet fra: https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html.

National Cyber Security Center (2018) *GDPR Security Outcomes*

National Cyber Security Center (2018) *NIS Guidance Collection*. Hentet fra: https://www.ncsc.gov.uk/content/files/NIS%20Guidance%20Collection%201.0.pdf

NATO Commitment to enhance resilience, erklæring fra NATO-toppmøtet 8.-9. juli 2016.

NIFU (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud.*

Norges Bank (2018) *Finansiell infrastruktur*

Norges vassdrags- og energidirektorat (2017) *Forslag til endringer i beredskapsforskriften* 2017/6

Norges vassdrags- og energidirektorat (2017) *Regulering av IKT-sikkerhet* 2017/26

Norges vassdrags- og energidirektorat (2018) *Oppsummeringsdokument: endringer i beredskapsforskriften – krav til IKT-sikkerhet m.m.* 2018/92

NorSIS (2015) *Kommune CSIRT 2015*.

NOU 1992: 32 *Bedre struktur i lovverket*. Lovstrukturutvalgets delutredning II

NOU 2015: 10 *Lov om regnskapsplikt*

NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*

NOU 2016: 19 *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.*

NOU 2016: 3 *Ved et vendepunkt: Fra ressursøkonomi til kunnskapsøkonomi – Produktivitetskommisjonens andre rapport*

Næringslivets sikkerhetsråd (2018) *Mørketallsundersøkelsen 2018*

OpenAI (2017) *Attacking Machine Learning with Adversarial Examples* Hentet fra: https://blog.openai.com/adversarial-example-research/

Politiets sikkerhetstjeneste (2018) *Trusselvurdering 2018.*

Ponemon (2017) *Third Party Data Risk Study Your Organization Can't Afford to Ignore.* Hentet fra: https://www.opus.com/about/press_releases/opus-ponemon-announce-results-of-2017-third-party-data risk-study/

Prop. 1 S (2017–2018) *Justis- og beredskapsdepartementet.*

Prop. 151 S (2015–2016) *Kampkraft og bærekraft*.

Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*.

Prop. 160 L (2016–2017) *Endringer i regnskapsloven mv. (forenklinger)*.

Prop. 62 L (2015–2016) *Endringer i forvaltningsloven mv. (administrative sanksjoner mv.)*

Regjeringen (2018) *Cybersecurity Act – foreløpig posisjonsnotat* 05.02.2018

Rykkja. L. (2017) Håndtering av ekstremvær, flom og skred. I Askim m.fl. (2017) *En smartere stat.* Universitetsforlaget.

Schneier, Bruce (2018) *Click Here to Kill Everybody*. New York: W.W. Norton and Company

Sjåfjell, Beate, *CSR-rapporteringsplikt for store selskaper. Lov om endringer i regnskapsloven og enkelte andre lover* (NIP-2013-2-29)

St.meld. nr. 17 (2002–2003) *Om statlige tilsyn*

St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap*.

Teknologirådet (2018) *Kunstig intelligens – muligheter, utfordringer og en plan for Norge.*

Telenor (2018) *Hva er 5G?* Hentet fra: https://www.telenor.no/om/teknologi-norge/dette-er-5g.jsp

Telenor (2018) *Sterkere sammen, Digital sikkerhet 2018.*

Tranvik, Tommy (2012) *Kommunal regeletterlevelse. Illusjoner og realiteter på personvernområdet.* Tidsskrift for samfunnsforskning, nr. 2, s. 131–156.

UK Department for Digital, Culture, Media & Sport *(2018) Secure by Design: Improving the cyber security of consumer Internet of Things – Report*,7 March 2018.

UK Department for Digital, Culture, Media and Sport (2016) *Cyber Security Regulation and Incentives Review.*

University of Surrey (2017) *5G Whitepaper: 5G Security Overview.*

Utenriksdepartementet (2017) *Internasjonal cyberstrategi for Norge.*

Norges offentlige utredninger 2017

Arbeids- og sosialdepartementet:
NOU 2017: 3 Folketrygdens ytelser til etterlatte
NOU 2017: 10 Grunnlaget for inntektsoppgjørene 2017

Barne- og likestillingsdepartementet:
NOU 2017: 6 Offentlig støtte til barnefamiliene
NOU 2017: 8 Særdomstoler på nye områder?
NOU 2017: 12 Svikt og svik

Finansdepartementet:
NOU 2017: 1 Markeder for finansielle instrumenter
NOU 2017: 4 Delingsøkonomien
NOU 2017: 13 Ny sentralbanklov. Organisering av Norges Bank og Statens pensjonsfond utland
NOU 2017: 14 Nye regler om markedsmisbruk – sanksjoner og straff
NOU 2017: 15 Revisorloven

Helse- og omsorgsdepartementet:
NOU 2017: 16 På liv og død

Justis- og beredskapsdepartementet:
NOU 2017: 2 Integrasjon og tillit
NOU 2017: 5 En påtalemyndighet for fremtiden
NOU 2017: 8 Særdomstoler på nye områder?
NOU 2017: 9 Politi og bevæpning
NOU 2017: 11 Bedre bistand. Bedre beredskap

Kulturdepartementet:
NOU 2017: 7 Det norske mediemangfoldet
NOU 2017: 17 På ein søndag?

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Omslagsillustrasjon: Shutterstock

Trykk: 07 Media AS – 12/2018