DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Meld. St. 38

(2016–2017)

Melding til Stortinget

IKT-sikkerhet

Et felles ansvar

Innhold

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Meld. St. 38

(2016–2017)

Melding til Stortinget

IKT-sikkerhet

Et felles ansvar

Tilråding fra Justis- og beredskapsdepartementet 9. juni 2017, godkjent i statsråd samme dag.
(Regjeringen Solberg)

Figur 1.1

Illustrasjon: M. Sylstad, NSM.
Kilde: Bilde hentet fra Colourbox.

Del I
Innledning

1 Sammendrag

Dette er den første stortingsmeldingen om IKT-sikkerhet. Det er flere grunner til at IKT-sikkerhet vies mye oppmerksomhet. Den digitale utviklingen er en avgjørende del av vår verdiskapning og vekst. Digitaliseringen har bidratt til et tryggere og mer sikkert samfunn. Folk kan lettere komme i kontakt med hverandre og få rask tilgang til informasjon. Digitaliseringen har også medført at samfunnets risikobilde har endret seg. Ingen sektorer, og få nasjoner, kan i dag kontrollere sin digitale sårbarhet alene. Digitalt sårbarhetsutvalg (Lysneutvalget)[1] viser til at Norge ligger langt fremme når det gjelder digitalisering, noe som gjør at vi som samfunn tidlig møter sårbarhetsutfordringene.

Trusselvurderinger viser at fremmede stater er villige til å bruke ulike virkemidler for å få tilgang til sensitiv og skjermingsverdig informasjon og påvirke politiske, økonomiske og forvaltningsmessige beslutninger. Det er store økonomiske tap knyttet til IKT-kriminalitet. I tillegg skjer det en rekke ganger at IKT-systemer svikter på grunn av menneskelige feil, programvarefeil, utstyrsfeil, naturhendelser eller en kombinasjon av disse.

For å sikre effektivisering gjennom økt digitalisering av det norske samfunnet må IKT-løsninger og digitale tjenester være tilstrekkelig sikre og pålitelige. Virksomheter og privatpersoner må ha tillit til at systemer og nettverk både fungerer slik de skal, og ivaretar personvernet til den enkelte. God IKT-sikkerhet og evne til å håndtere uønskede digitale hendelser er en forutsetning for å oppnå denne tilliten.

Utfordringene i det digitale rommet er grenseoverskridende – på tvers av land, sektorer og virksomheter, og utviklingen går svært fort. Hybride trusler visker ut det tradisjonelle skillet mellom fred og krig og utfordrer tradisjonell ansvarsplassering mellom sivil og militær sektor. Regjeringen ønsker derfor å styrke samarbeidet mellom private og offentlige virksomheter, mellom sivile og militære virksomheter og på tvers av landegrenser. På nasjonalt nivå vil Justis- og beredskapsdepartementet, Forsvarsdepartementet og Utenriksdepartementet ytterligere styrke sitt samarbeid på området.

Lysneutvalget kommer med en rekke anbefalinger for å redusere digitale sårbarheter i samfunnet. Denne meldingen gir en oversikt over status på oppfølgingen av utvalgets anbefalinger. Statusoversikten viser at det er behov for å jobbe parallelt med et bredt spekter av områder innenfor IKT-sikkerhet. Vårt samfunn vil aldri kunne være helt beskyttet mot utfall av eller angrep mot digital infrastruktur og digitale systemer, men vi må evne å iverksette de riktige sikkerhetstiltakene for å redusere risikoen og for å kunne gjenopprette normal funksjon så fort som mulig. Justis- og beredskapsdepartementet vil benytte oversikten til å følge opp departementene i det videre arbeidet med nasjonal IKT-sikkerhet.

Statusoversikten er et sentralt kunnskapsgrunnlag for regjeringens videre arbeid. Regjeringen vil legge vekt på et helhetlig og systematisk arbeid med forebyggende IKT-sikkerhet. Et sentralt tiltak vil være å nedsette et utvalg som skal utrede rettslig regulering på IKT-sikkerhetsområdet. Utvalget skal blant annet utrede behovet for og eventuelt foreslå en nasjonal IKT-sikkerhetslov, med virkeområde utenfor sikkerhetsloven. Utvalget skal også se på organisatoriske spørsmål. Utover dette vil regjeringen etablere og videreutvikle strategiske møteplasser for spørsmål knyttet til nasjonal IKT-sikkerhet og internasjonalt samarbeid, møteplasser som også støtter opp under offentlig–privat samarbeid.

Regjeringen er opptatt av å styrke vår nasjonale evne til å avdekke og håndtere digitale angrep. Videre ønsker regjeringen å legge til rette for god informasjonsdeling og håndtering gjennom etablering og videreutvikling av nasjonalt rammeverk for digital hendelseshåndtering. Justis- og beredskapsdepartementet har tatt initiativ til et arbeid for å bedre samarbeidet og informasjonsflyten knyttet til digital hendelseshåndtering i Norge. Videre er koordineringen mellom Etterretningstjenesten, Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og politiet for øvrig styrket.

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

Regjeringen vil legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse gjennom en nasjonal kompetansestrategi for IKT-sikkerhet. IKT-sikkerhet gjelder alle. Ved at de unge tidlig lærer trygg bruk og forstår nødvendigheten av IKT-sikkerhet, legges grunnlaget for at oppvoksende generasjoner har med seg IKT-sikkerhetskompetanse inn i det videre utdanningsløpet og arbeidslivet.

Vårt samfunn består av en rekke kritiske samfunnsfunksjoner som må opprettholdes til enhver tid av hensyn til samfunnets og befolkningens grunnleggende behov. Disse samfunnsfunksjonene forutsetter at man har en IKT-infrastruktur som virker nær sagt overalt og hele tiden. Regjeringen er opptatt av at vi som samfunn har en trygg og pålitelig IKT-infrastruktur. En av hovedanbefalingene fra Lysneutvalget var å redusere avhengigheten av Telenors kjernenett. Regjeringen gjennomfører regulatoriske og økonomiske tiltak for å gjøre de elektroniske ekomnettene mer robuste i takt med utviklingen i trusselbildet og den tekniske utviklingen, og har i Meld. St. 33 (2016–2017) *Nasjonal transportplan 2018–2029* prioritert midler til etablering av en pilot for alternativt kjernenett.

2 Bakgrunn, rammer og meldingens innhold

Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* ble lagt frem for Stortinget i desember 2016. I meldingen er IKT-sikkerhet trukket frem som ett av regjeringens sentrale områder innenfor samfunnssikkerhet. Meldingen legger særlig vekt på et helhetlig og systematisk arbeid med forebyggende IKT-sikkerhet og vår nasjonale evne til å avdekke og håndtere digitale angrep. Videre vektlegges samfunnets behov for god IKT-sikkerhetskompetanse på alle nivåer og en trygg og pålitelig IKT-infrastruktur. I Meld. St. 27 (2015–2016) *Digital agenda for Norge* er IKT-sikkerhet og personvern en av hovedprioriteringene i regjeringens IKT-politikk.

I den senere tid er det utarbeidet flere analyser om digitale sårbarheter. Disse bidrar til folkeopplysning og bevisstgjøring, men også til å gi myndigheter og virksomhetsledere et beslutningsgrunnlag for å utforme politikk og tiltak for å redusere sårbarheter.

Et sentralt kunnskapsgrunnlag er NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* (Lysneutvalget). Utvalget vurderte digitale sårbarheter på flere nivåer – både på et overordnet samfunnsnivå og i tekniske infrastrukturer og systemer. Lysneutvalget gir en rekke anbefalinger for å redusere digitale sårbarheter i samfunnet og i kritiske samfunnsfunksjoner. Utredningen ble overlevert justis- og beredskapsministeren 30. november 2015.

Del III i denne meldingen gir en oversikt over status på myndighetenes vurdering og oppfølging av Lysneutvalgets anbefalinger og en oversikt over prioriteringer i det videre oppfølgingsarbeidet. Justis- og beredskapsdepartementet vil benytte statusoversikten til å følge opp departementene i sivil sektor i det videre arbeidet med nasjonal IKT-sikkerhet.

Statusoversikten i del III viser at det behov for en bred tilnærming til arbeidet med IKT-sikkerhet fremover. Flere sektorer arbeider med samme type utfordringer, for eksempel når det gjelder å utvikle kompetanse innenfor IKT-sikkerhet eller å håndtere en alvorlig digital hendelse. På grunnlag av vurderingene i del III, sammen med eksisterende kunnskapsgrunnlag, utviklingstrekk og utfordringsbilde på området, vil regjeringen vektlegge utvalgte tverrsektorielle områder. Regjeringen mener at disse områdene er av særlig betydning for nasjonal IKT-sikkerhet:

- Forebyggende IKT-sikkerhet – virksomheters egenevne
- Avdekke og håndtere digitale angrep
- IKT-sikkerhetskompetanse
- Kritisk IKT-infrastruktur

Regjeringens vektlagte områder og tiltak for å bedre IKT-sikkerheten beskrives i del II. For å lykkes innenfor disse områdene er regjeringen opptatt av å styrke offentlig–privat, internasjonalt og sivilt–militært samarbeid, som omtales nærmere i kapittel 5.

I tillegg til tiltak som fremgår av denne meldingen, følger regjeringen opp NOU 2016: 19 *Samhandling for sikkerhet*. Sammenlignet med gjeldende sikkerhetslov, vil forslagene i denne utredningen på flere måter kunne løfte den nasjonale IKT-sikkerheten. Flere virksomheter utenfor offentlig sektor blir underlagt loven. Virksomheter som er underlagt loven, plikter å sørge for et forsvarlig sikkerhetsnivå for alle informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner. For nærmere omtale, se punkt 6.1.

3 Utviklingstrekk og betydningen av IKT-sikkerhet

Det er høye forventninger til at digitale tjenester tilbys og er tilgjengelige hele tiden, samtidig som tjenestene skal være robuste og motstå trusler og farer. Svikt eller sikkerhetsbrudd kan inntreffe i en kombinasjon av flere forhold. Det kan være tilsiktede handlinger og forsøk på misbruk så vel som menneskelig svikt, feil i utstyr eller uklar organisering. Sentralt for å håndtere krevende og sammensatte hendelser er kompetanse. Etterspørselen etter IKT-sikkerhetskompetanse har økt.

Mange utfordringer knyttet til IKT-sikkerhet utvikler seg raskere enn offentlige og private virksomheter klarer å respondere. I årene som kommer, vil vi møte stadig større og mer komplekse sikkerhetsutfordringer. IKT-infrastruktur og -systemer blir mer globale, omfattende og integrerte. Flere enheter kobles til internett. Skyløsninger brer om seg både i det private og i jobbsammenheng. Behovet for å redusere kostnader og tilgang til kompetanse, gjør at flere IKT-funksjoner settes ut til tredjepart, særlig i lavkostland. Utviklingen skaper avhengigheter og sårbarheter som går på tvers av sektorer, ansvarsområder og landegrenser.

Trusselvurderinger forteller at fremmede stater er villige til å bruke en rekke virkemidler for å få tilgang til sensitiv og skjermingsverdig informasjon og for å påvirke politiske, økonomiske og forvaltningsmessige prosesser og beslutninger. De samme virkemidlene benyttes også av nasjonale og internasjonale kriminelle aktører. Det digitale rommet, i kombinasjon med informasjonstilfanget, skaper også muligheter for påvirkningsoperasjoner i et omfang og med en effekt som vi kanskje aldri før har sett.

IKT-sikkerhet innebærer å være bevisst hele spekteret av digitale sårbarheter. IKT-sikkerhet omfatter både tekniske og administrative sikringstiltak og innebærer beskyttelse av både IKT-systemer og informasjonen i disse. IKT-sikkerhet handler derfor om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Begrepet IKT-sikkerhet brukes i denne meldingen synonymt med begrepet cybersikkerhet.

Integritet, konfidensialitet og tilgjengelighet er viktige sikkerhetsmål når det gjelder å ivareta IKT-sikkerhet:[1]

- Konfidensialitet innebærer at informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til den.
- Integritet innebærer at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter.
- Tilgjengelighet innebærer at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

Den enkelte virksomhet vil vekte de ulike målene ulikt ut fra hvilket formål virksomheten har eller skal understøtte, og hvilke krav og risikobilde den må forholde seg til. Et virkemiddel for å nå sikkerhetsmålene er sporbarhet, for å ha oversikt over hvem som har vært inne i systemer, og hvem som har håndtert eller endret informasjon. Sporbarhet blir stadig viktigere gitt utviklingstrekkene knyttet til påvirkningsoperasjoner og andre uønskede digitale hendelser.

God IKT-sikkerhet er nødvendig for at hverdagen skal fungere godt. Tjenester som bank, handel og helse er flyttet over på digitale plattformer. De fleste bedrifter er avhengig av digitale tjenester i sin produksjon av varer og tjenester.

---

[1] *Nasjonal strategi for informasjonssikkerhet*, 2012.

4 IKT-sikkerhet og personvern

Personvern er en viktig del av retten til respekt for privatlivet – en fundamental menneskerettighet beskyttet i både Grunnloven, Den europeiske menneskerettighetskonvensjonen og FNs konvensjon om sivile og politiske rettigheter. NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet* (Personvernkommisjonen) definerte personvern slik:

> *Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.*

Lysneutvalget fremhevet at i en digital sammenheng har beskyttelse av personopplysninger en særlig viktig rolle i personvernet. Personvernkommisjonen definerer begrepet slik:

> *Personopplysningsvern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold.*

Det er myndighetenes ansvar å ivareta menneskerettighetene og å sørge for sikkerhet og trygghet for befolkningen. Ivaretakelse av personvernet og opprettholdelse av et sikkert samfunn er derfor prioriterte oppgaver for regjeringen.

God IKT-sikkerhet er en forutsetning for ivaretakelsen av personvernet. I både nasjonalt og internasjonalt regelverk om beskyttelse av personopplysninger, finnes det derfor bestemmelser om IKT-sikkerhet. Datatilsynet skriver i sin høringsuttalelse til Lysneutvalgets utredning blant annet at hensynene til personvern og IKT-sikkerhet ofte følger hverandre, og at de vanskelig kan se for seg et godt personvern uten gode sikkerhetsmekanismer i dagens digitale hverdag. Personvern og IKT-sikkerhet henger altså fundamentalt sammen. Når det gjelder gjennomføringen av konkrete sikkerhetstiltak, for eksempel logging i IKT-systemer, kan det likevel oppstå behov for avveining mellom de to hensynene.

Ivaretakelsen av personvernet er en forutsetning for en vellykket digitalisering i samfunnet. Effektiv bruk av IKT styrker næringslivets konkurranseevne og øker samfunnets totale produktivitet.[1] Regjeringen ønsker å utnytte disse fordelene ved å legge til rette for videre digitalisering av samfunnet. Da må vi være bevisst digitaliseringens utfordringer. Blant de større utfordringene er nettopp ivaretakelsen av personvernet, som gjennom digitaliseringen blir satt på stadig nye prøver. Godt personvern er nøkkelen til at brukerne skal ha tillit til digitale løsninger.

Samtidig som vektleggingen av personvern øker, ser vi ulike former for frivillig avståelse av slikt vern. Privatpersoner gir for eksempel fra seg personopplysninger i bytte mot gratis tjenester. Gratis e-post, søkemotorer, spill og sosiale medier er basert på denne modellen. De fleste mobiltelefoner sender opplysninger om brukerens bevegelser, bosted, jobbadresse og personlige gjøremål. Bruken og behandlingen av disse dataene er derfor viktig både i et personvern- og i et IKT-sikkerhetsperspektiv. Det hviler et ansvar på de som samler og behandler personopplysninger, for å sikre at disse dataene ikke blir misbrukt eller kommer på avveie.

---

[1] Meld. St. 27 (2015–2016) *Digital agenda for Norge.*

Figur 5.1

Illustrasjon: M. Sylstad, NSM.
Kilde: Bilde hentet fra Visible Earth/NASA.

Del II
Sentrale områder i arbeidet med IKT-sikkerhet

5 Et felles ansvar

Alle virksomheter har ansvar for å ivareta egen IKT-sikkerhet. Hver enkelt statsråd har et overordnet ansvar for å ivareta IKT-sikkerheten i egen sektor. 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. Berørte fagdepartement, myndigheter og næringslivet skal involveres i dette arbeidet. Krav skal i nødvendig grad være hjemlet i lov og forskrift. Ansvar for IKT-sikkerhet er nærmere beskrevet i punkt 6.4 i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* og i kongelig resolusjon av 10. mars 2017[1].

I Meld. St. 10 (2016–2017) ble det påpekt at både enkeltmennesker og virksomheter har et ansvar for hvordan egne handlinger kan påvirke andres sikkerhet. Dette gjelder også innenfor IKT-sikkerhet.

Samfunnets avhengighet av IKT gjør det nødvendig med et godt samarbeid mellom private selskaper og offentlige virksomheter, på tvers av landegrenser og mellom sivile og militære virksomheter. På nasjonalt nivå vil særlig Forsvarsdepartementet, Utenriksdepartementet og Justis- og beredskapsdepartementet styrke sitt samarbeid på området.

Det fremgår av Meld. St. 10 (2016–2017) at regjeringen skal utarbeide en ny nasjonal strategi for IKT-sikkerhet. I tillegg skal det utarbeides en handlingsplan med konkrete tiltak. Arbeidet ledes av Justis- og beredskapsdepartementet og Forsvarsdepartementet. Denne stortingsmeldingen vil utgjøre en viktig plattform for den kommende strategien. Den nye strategien vil ha en bredere tilnærming til utfordringene enn tidligere nasjonale strategier på området. Styrket samarbeid mellom Justis- og beredskapsdepartementet, Forsvarsdepartementet og Utenriksdepartementet samt behovet for styrking av sivilt–militært, offentlig–privat og internasjonalt samarbeid vil vektlegges.

Regjeringen vil videreutvikle Nettverk for informasjonssikkerhet[2] for å sikre at strategiske spørsmål knyttet til IKT-sikkerhet i Norge og internasjonalt blir diskutert og koordinert. Det vil være et sentralt verktøy for Justis- og beredskapsdepartementets samordningsansvar for IKT-sikkerhet i sivil sektor, for Forsvarsdepartementet i sivil–militære spørsmål knyttet til nasjonal IKT-sikkerhet og for Utenriksdepartementet i deres koordinerende rolle i utenrikspolitiske spørsmål knyttet til det digitale rommet.

Sentrale tiltak:

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

5.1 Offentlig–privat samarbeid

Verken myndighetene, næringslivet eller den enkelte borger kan møte utfordringene i det digitale rommet alene. Offentlig og privat sektor har ulike kapasiteter, kunnskaper og kompetanse som kan utfylle hverandre, til tross for ulike virksomhetsmål. Det pågår allerede mye offentlig–privat samarbeid for å forebygge, avdekke og håndtere digitale hendelser. Et styrket samarbeid mellom

[1] *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innenfor samfunnssikkerhet og IKT-sikkerhet.*

[2] Nettverk for informasjonssikkerhet er en møteplass for departementene for å drøfte sentrale tema innenfor informasjonssikkerhet. Det er samtidig et verktøy for Justis- og beredskapsdepartementets samordningsansvar for IKT-sikkerhet i sivil sektor.

myndigheter og privat sektor vil kunne bidra til bedre situasjonsforståelse, bedre beslutninger og bedre tilgang til flere ressurser som kan utfylle hverandre.

Regjeringen vil opprette et eget forum for offentlig–privat samarbeid for å støtte opp under det nasjonale arbeidet med IKT-sikkerhet. Deltakere i forumet vil være relevante representanter fra myndigheter, næringsliv, akademia og interesseorganisasjoner. Det skal primært være eiere eller forvaltere av kritisk infrastruktur eller kritiske samfunnsfunksjoner, eller sentrale aktører innenfor IKT-sikkerhet. Forumet skal kunne foreslå tiltak og gi råd til myndighetene.

I arbeidet med en ny nasjonal strategi for IKT-sikkerhet ønsker regjeringen en bred involvering av både offentlige og private aktører. Forumet for offentlig–privat samarbeid vil delta i arbeidet med den kommende nasjonale IKT-strategien.

5.2 Internasjonalt samarbeid

Internasjonalt samarbeid er avgjørende for utviklingen av globale retningslinjer og for å redusere og bekjempe trusler i det digitale rommet. Norge har egeninteresse av gode og forutsigbare rammevilkår i det digitale rommet. Vi har samtidig en grunnleggende og langsiktig interesse av et sikkert, robust, åpent og fritt digitalt rom. Det er derfor viktig for Norge å være med på å utforme de internasjonale rammevilkårene og spillereglene som former dette rommet. Det inkluderer utviklingen av normer for statlig opptreden, internasjonalt samarbeid for å bekjempe IKT-kriminalitet og internasjonalt samarbeid om styrket IKT-sikkerhet.

Utvikling av internett og digitale tjenester og produkter foregår imidlertid i all hovedsak gjennom private selskap og forsknings- og utviklingsmiljøer. I tillegg er selve ryggraden i internett, den globale digitale infrastrukturen, i all hovedsak i privat eie. Dette bidrar til konkurranse, innovasjon og utvikling. Samtidig betyr det at sentrale beslutninger om det digitale rommet i stor grad blir fattet av kommersielle og ikke-statlige aktører utenfor de tradisjonelle mellomstatlige arenaene vi kjenner. Denne utviklingen tilsier et økt behov for både offentlig–privat og internasjonalt samarbeid.

Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken* viser til en kraftig økning i IKT-kriminalitet når flere utviklingsland tilkobles internett. I mange land er ikke forebyggende IKT-sikkerhet prioritert eller god nok. Norge kan spille en viktig rolle ved å bistå med kapasitetsbygging i utviklingsland, slik at flere land i større grad evner å håndtere digitale utfordringer og digitale trusler. I stortingsmeldingen foreslås også flere andre tiltak for det utenrikspolitiske arbeidet, blant annet at det skal utarbeides en internasjonal cyberstrategi for Norge. Strategien skal tydeliggjøre regjeringens overordnede mål innenfor hele spekteret av internasjonal politikk for det digitale rommet, der IKT-sikkerhet er ett av flere elementer.

Utviklingen og implementeringen av EUs strategi for et digitalt indre marked vil ha stor betydning også for Norge gjennom EØS-tilknytningen. Strategiens tre pilarer er 1) å bedre forbrukernes og bedriftenes muligheter for e-handel, 2) å forbedre rammevilkårene for digitale nettverk og tjenester og 3) å digitalisere industrien og legge bedre til rette for informasjonsdeling på tvers av sektorer og landegrenser.

IKT-sikkerhet inngår i pilar 2, der to av tiltakene er å arbeide for å styrke IKT-sikkerhetsbransjen og integrere sikkerhet i en tidlig fase av ny teknologiutvikling. Det tredje og mest omfattende tiltaket er å vedta og gjennomføre EU-direktivet om nettverks- og informasjonssystemsikkerhet (NIS-direktivet). Direktivet setter krav til medlemslandenes arbeid med IKT-sikkerhet, til virksomheter som leverer tjenester som er essensielle for det indre markeds samfunnsmessige og økonomiske aktiviteter, og til tilbydere av enkelte digitale tjenester. Norge er invitert inn i flere samarbeidsfora om det videre arbeidet med gjennomføring av direktivet. Justis- og beredskapsdepartementet representerer Norge i arbeidet. Se nærmere om NIS-direktivet under punkt 22.5.

EUs byrå for nettverks- og informasjonssikkerhet (ENISA) utvikler generelle anbefalinger innenfor IKT-sikkerhet, bidrar til utvikling av regelverk og retningslinjer og samarbeider med operative enheter i Europa. Norge deltar i ENISA uten stemmerett. Gjennomføringen av NIS-direktivet vil styrke byrået ved at det får tildelt rollen som faglig knutepunkt for det nettverket av nasjonale fagmyndigheter som direktivet etablerer. Norsk deltakelse i ENISA blir derfor enda viktigere enn det er i dag.

Som en del av midtveisgjennomgangen av strategien for det digitale indre markedet la EU-kommisjonen i mai 2017 frem sin plan for å revidere strategien for cybersikkerhet fra 2013. Samtidig skal ENISA evalueres. Evalueringen skal berede grunnen for en mulig revisjon av byrået.

Internasjonalt samarbeid om IKT-sikkerhet foregår også i andre internasjonale fora og i mel-

lomstatlige organisasjoner som NATO, OECD og FN, men også i samarbeid med næringslivet, akademia og samfunnet for øvrig. Se omtale av NATO under punkt 5.3. Regjeringen vil delta og bidra aktivt for å løse globale utfordringer relatert til IKT-sikkerhet.

5.3 Sivilt–militært samarbeid

En endret sikkerhetspolitisk situasjon, kombinert med hybride[3] trusler, aktualiserer sivilt–militært samarbeid i det digitale rommet mer enn noen gang. Forsvarssektoren og sivil sektor benytter i økende grad felles IKT-infrastruktur, og tjenester kjøpes av kommersielle aktører. Det innebærer at også digitale sårbarheter er felles. Et godt samarbeid mellom sivile og militære myndigheter er avgjørende.

Det moderniserte totalforsvarskonseptet omfatter gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn. Konseptet omhandler forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret fra fred via sikkerhetspolitisk krise til væpnet konflikt. Det er ikke lenger en forutsetning at beredskapslovgivningen trer i kraft, for at støtten kan sies å være innenfor rammen av totalforsvarskonseptet.[4]

Regjeringen besluttet i november 2016 at Justis- og beredskapsdepartementet skal etablere et program for videreutvikling av totalforsvaret og øke motstandsdyktigheten i samfunnskritiske funksjoner. Bakgrunnen for å igangsette dette arbeidet er NATOs forventninger til medlemslandene om å styrke robustheten i samfunnskritiske funksjoner, vedtatt i NATO i februar 2016.[5]

NATO setter i større grad enn tidligere sivilt beredskapsarbeid og sivilt–militært samarbeid på dagsordenen. Årsaken er at sivil beredskap, krisehåndtering og robuste kritiske samfunnsfunksjoner er en forutsetning for det enkelte lands, og dermed alliansens, samlede beredskap og forsvar. Robust og tilgjengelig IKT-infrastruktur er nødvendig for å opprettholde alle kritiske samfunnsfunksjoner og en innsatsfaktor i NATOs grunnleggende forventninger til medlemslandene.

I 2016 signerte Norge en revidert samarbeidsavtale med NATO om beskyttelse mot digitale trusler. Avtalen sikrer informasjonsdeling mellom partene, noe som øker både Norges og NATOs evne til å verne IKT-systemer mot digitale angrep.

NATOs stats- og regjeringssjefer sluttet seg til en felles cybererklæring under NATO-toppmøtet sommeren 2016. For NATO og medlemslandene er det viktig å arbeide for økt IKT-sikkerhet på tvers av sektorer i samfunnet og mellom land. Norge må følge opp de forpliktelsene som ligger i cybererklæringen.

---

[3] Hybride trusler og virkemidler forstås som aktørers bruk av økonomiske, politiske og militære midler til å utnytte sårbarheter for å oppnå noe, for eksempel å skape uro i et samfunn. Aktørene kan være statlige eller ikke-statlige. DSB skal i 2017 utvikle et scenario basert på hybride trusler i sin årlige rapport "Krisescenarioer".

[4] *Støtte og samarbeid – En beskrivelse av totalforsvaret i dag* (Regjeringen 2015).

[5] For mer informasjon, se http://www.nato.int/cps/en/natohq/topics_49158.htm?selectedLocale=en.

6 Forebyggende IKT-sikkerhet – virksomheters egenevne

Regjeringen er opptatt av å legge til rette for at virksomheter kan øke egenevnen til å forebygge uønskede digitale hendelser. Svaret på utfordringene innebærer ikke bare økte ressurser eller styrking av kapasitet. Hensiktsmessige regelverk og hensiktsmessig organisering står også sentralt for å sikre våre verdier.

Virksomheter er avhengige av komplekse digitale verdikjeder, og andres sårbarhet blir til egen sårbarhet. Det er nødvendig at virksomheter har tilstrekkelig oversikt over egen sårbarhet. En god oversikt setter virksomheten i stand til å vurdere hensiktsmessige tiltak.

Sentrale tiltak:

- nedsette et utvalg som skal utrede rettslig regulering på IKT-sikkerhetsområdet og organisering av tverrsektorielt ansvar
- legge bedre til rette for at virksomheter kan vurdere og prioritere tiltak innenfor IKT-sikkerhet gjennom systematisering og utvikling av anbefalinger og krav
- utvikle og vedlikeholde et godt og tilgjengelig kunnskapsgrunnlag som gjør enkeltindivider, virksomheter og myndigheter i stand til å treffe riktige tiltak for å opprettholde tilstrekkelig sikkerhet i sine IKT-systemer

6.1 Rettslig regulering på IKT-sikkerhetsområdet

I Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* vises det til at norske virksomheter må forholde seg til ulike regelverk om IKT-sikkerhet. Noen regelverk er sektorspesifikke, mens andre er tverrsektorielle. Regelverkene har til dels ulike formål og hensyn og benytter ofte ulike begrep og metoder. Den raske digitaliseringen av samfunnet har ført til at reguleringer og lovgivning ikke alltid er tilpasset dagens behov.

Digitaliseringen har de siste årene bidratt til langt flere tverrsektorielle utfordringer. Flere av disse utfordringene knytter seg til sikkerhetsmessige forhold. Det kan være ulik forståelse av trussel- og risikobildet i sektorene og manglende oversikt over hvordan sikkerheten i egen sektor også kan få konsekvenser for andre sektorer. Dette kan føre til fragmentert regulering og manglende helhetstenkning i utformingen av krav til IKT-sikkerhet, noe som også gjør det utfordrende for virksomhetene å holde oversikt over og etterleve de ulike kravene.

EUs NIS-direktiv pålegger medlemsstatene å sørge for et minimumsnivå for den nasjonale IKT-sikkerheten. Direktivet skal sørge for at hvert medlemsland har en enhetlig og tverrsektoriell tilnærming til IKT-sikkerhet. Det er åpning for ulike løsninger i ulike land for de fleste sektorer.

Gjeldende personopplysningslov har tverrsektorielle regler om IKT-sikkerhet. Også EUs nye

Boks 6.1 Sikkerhetsutvalgets vurderinger

Gjennom en sektorvis identifisering av viktige samfunnsfunksjoner, virksomheter og infrastrukturer skal en nasjonal og tverrsektoriell sikkerhetsmyndighet kunne få en helhetlig oversikt over vår nasjonale sikkerhetstilstand. Utvalget foreslår også at det stilles krav til at virksomhetene beskytter sine særlig viktige informasjonssystemer. Dette vil omfatte alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer. Lovforslaget gir blant annet virksomheter som omfattes av loven, plikt til å gjennomføre sikkerhetslogging, og hjemmel for gjennomføring av inntrengingstesting. Samlet skal loven bidra til å bedre den nasjonale IKT-sikkerheten og dermed redusere våre samlede digitale sårbarheter. Videre vil systematikken bedre sikkerhetsmyndighetens mulighet til å få en helhetlig og nasjonal oversikt over sårbarheter, inkludert de digitale, og andre utfordringer. Dette skal igjen danne grunnlaget for å jobbe målrettet for å redusere sårbarhetene våre.

personverndirektiv stiller krav til IKT-sikkerheten.

I NOU 2016: 19 *Samhandling for sikkerhet* foreslår utvalget en forbedret systematikk for regulering av forebyggende nasjonal sikkerhet (se boks 6.1). Utvalget foreslår et utvidet virkeområde i forhold til dagens sikkerhetslov.

Det er behov for å vurdere om dagens rettslige regulering av nasjonal IKT-sikkerhet er hensiktsmessig innrettet. Regjeringen vil nedsette et utvalg som skal kartlegge relevant sektorspesifikt og tverrsektorielt regelverk innenfor IKT-sikkerhet. Det skal vurderes om eksisterende regelverk er konsistent, og ivaretar de nye digitale samfunnsutfordringene. Det skal vurderes om det er behov for harmonisering av eksisterende lovverk. Videre skal utvalget utrede behovet for og eventuelt foreslå en nasjonal IKT-sikkerhetslov. Utredningen skal være avgrenset mot bestemmelser, organisering og myndighet som følger av sikkerhetsloven og forslag til ny sikkerhetslov.

6.2 Organisering av tverrsektorielt ansvar

Regjeringen vil i forbindelse med utredningen om rettslig regulering på IKT-sikkerhetsområdet (se punkt 6.1) også utrede organisatoriske forhold, som for eksempel tverrsektoriell koordinering, rådgivning, tilsyn, varsling av hendelser og utarbeiding av sikkerhetskrav.

Digitaliseringen har 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.

Utnyttelsen av fellesskapets ressurser må optimaliseres for å oppnå god IKT-sikkerhet. Utvalget skal vurdere om ansvar, roller og oppgaver er hensiktsmessig fordelt og organisert mellom etater med tverrsektorielt ansvar på IKT-sikkerhetsområdet. Utvalget skal også se på muligheter for koordinering, samarbeid og synergieffekter mellom offentlig og privat sektor slik at nasjonal IKT-sikkerhet ivaretas og styrkes.

6.3 Systematisering og utvikling av anbefalinger og krav

Myndighetene kommer med en rekke anbefalinger og krav på IKT-sikkerhetsområdet. Det pågår mye systematisk og godt arbeid med å implementere disse (se boks 6.2 om oppfølging av nasjonale krav og anbefalinger innenfor IKT-sikkerhet i Klima- og miljødepartementet). Det kan imidlertid være krevende for virksomheter å forholde seg til omfanget av anbefalinger og krav. Regjeringen vil derfor gjennom den kommende handlingsplanen til nasjonal strategi for IKT-sikkerhet legge til rette for at virksomheter på en enklere måte kan vurdere og prioritere tiltak innenfor IKT-sikkerhet ut fra virksomhetenes størrelse og modenhetsnivå.[1]

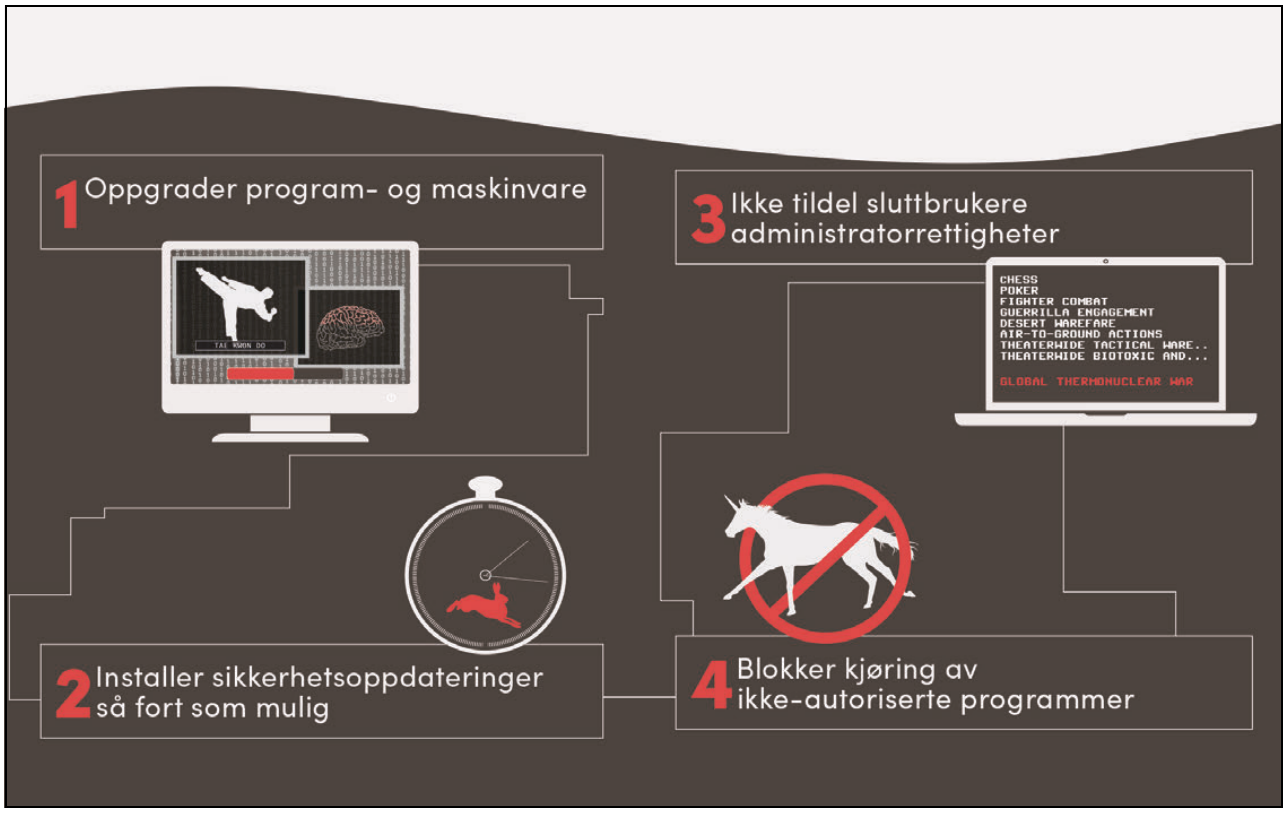
Kommunal- og moderniseringsdepartementet vurderer, i samarbeid med Justis- og beredskapsdepartementet, hvordan IKT-sikkerhetsarbeidet i statsforvaltningen bør videreutvikles. Sentrale anbefalinger fra *Handlingsplan for informasjonssikkerhet i statsforvaltningen (2015–2017)* vil bli innarbeidet i den kommende handlingsplanen til nasjonal strategi for IKT-sikkerhet.

Nasjonal sikkerhetsmyndighet (NSM) har i 2017 startet arbeidet med å etablere et rammeverk for tiltak innenfor IKT-sikkerhet, basert på anerkjente standarder og definerte grunnprinsipper. Rammeverket vil bli videreutviklet for å reflektere endringer i teknologi og risiko. Formålet er å etablere et sett med de viktigste tiltakene for sikring av samfunnsviktige IKT-løsninger. Dette arbeidet vil være et viktig grunnlag for regjeringens kommende handlingsplan, og det vil sammen med rammeverk for digital hendelseshåndtering (se punkt 7.2) gi en helhet i arbeidet med IKT-sikkerhet i Norge.

Boks 6.2 Et eksempel på oppfølging av nasjonale krav og anbefalinger innenfor IKT-sikkerhet

Klima- og miljødepartementet har besluttet å legge en langsiktig plan for å redusere IKT-sårbarhet i sektoren. I miljøforvaltningens IKT-strategi for 2016–2020 ble det lagt vekt på å øke IKT-sikkerheten i sektoren. Under strategiens målsetninger er det satt opp konkrete tiltak for å oppfylle målene. Det omfatter blant annet å etablere et felles miljø for IKT-drift i miljøforvaltningen. NSM har tatt til orde for færre IKT-miljøer i offentlig sektor, blant annet i Sikkerhetsfaglig råd 2015.

[1] For nærmere omtale av ny nasjonal strategi for IKT-sikkerhet, se Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*.



Figur 6.1 Tiltak mot digitale angrep.

Illustrasjon: M. Sylstad, NSM.

NSM vil i 2017 også etablere en arena for erfaringsoverføring, slik at offentlige og private virksomheter i større grad skal få koordinerte, tilrettelagte og hensiktsmessige råd og veiledning på IKT-sikkerhetsområdet. Regjeringen vil fortsette å støtte Norsk senter for informasjonssikring (NorSIS) (se boks 6.3) i sitt arbeid. NorSIS er en viktig bidragsyter som gir råd og veiledning til små og mellomstore virksomheter og skaper økt bevissthet i befolkningen om IKT-sikkerhetsutfordringer.

6.4 Tjenesteutsetting

Mange virksomheter velger å anskaffe IKT-tjenester fra en eller flere eksterne leverandører i stedet for å produsere dem selv. Leveransene kan gjennomføres internt i virksomheten eller eksternt av nasjonale eller internasjonale leverandører. Det kan også være kombinasjoner av disse.

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Det kan også gi lavere og mer forutsigbare kostnader og bidra til bedre prioritering av virksomhetens kjerneområder. Dette fordrer at virksomheten besitter kompetanse til å følge opp leverandører de setter ut tjenester til. Samtidig må virksomheten være bevisst hvilke verdier som eksponeres ved tjenesteutsetting, og iverksette nødvendige tiltak. Behovet for konfidensialitet, integritet og tilgjengelighet bør særlig vektlegges i vurderingene, og hvilke lover, krav og regler som gjelder for sektoren nasjonalt og internasjonalt.

Det eksisterer i dag få skyleverandører med anlegg i Norge. Tjenesteutsetting ved bruk av skytjenester innebærer derfor at lagring og prosessering primært utføres på skyleverandørens anlegg utenfor Norge og dermed utenfor nasjonal kontroll. En nærmere omtale av tjenesteutsetting og skytjenester finnes i punkt 22.10. Se boks 6.4 for IKT-tjenesteutsetting i helsetjenesten.

Regjeringen er opptatt av at virksomhetene er bevisste ved bruk av tjenesteutsetting og følger råd og anbefalinger. Det er utarbeidet flere veiledere for å rettlede virksomheter som vurderer tjenesteutsetting, blant annet av Datatilsynet, Direktoratet for forvaltning og IKT (Difi), Direktoratet for e-helse, NorSIS og Uninett. NSM skal også utarbeide en temarapport om tjenesteutsetting i løpet av 2017.

Boks 6.3 NorSIS

NorSIS er en uavhengig organisasjon som arbeider for økt kunnskap om og forståelse for IKT-sikkerhet. NorSIS mottar økonomisk støtte fra Justis- og beredskapsdepartementet og er en del av myndighetenes nasjonale satsing på IKT-sikkerhet.

En viktig oppgave for NorSIS er å gi råd og veiledning til befolkningen, bedrifter og offentlige virksomheter. Det største enkeltstående tiltaket er «nasjonal sikkerhetsmåned», som arrangeres i oktober hvert år. Sikkerhetsmåneden er en nasjonal dugnad for å skape oppmerksomhet om informasjonssikkerhet som er relevant for både virksomheter og privatpersoner. I 2016 fikk 420 000 ansatte tilgang til e-læring under sikkerhetsmåneden. Dette er en økning på nesten 60 000 fra 2015. I tillegg ble det holdt en rekke sikkerhetsrelaterte foredrag rundt omkring i Norge.

NorSIS har utarbeidet flere veiledere som retter seg mot private virksomheter. NorSIS samarbeider blant annet med NSM og Nkom om nettvett.no. Dette er en tjeneste hvor man finner informasjon, råd og veiledning om sikrere bruk av internett. Informasjonen er rettet både mot forbrukere og mot små og mellomstore virksomheter. Formålet med tjenesten er å bidra til en mer enhetlig og koordinert informasjonsflyt om sikkerhet og sikkerhetskultur knyttet til IKT. NorSIS drifter og har redaktøransvaret for tjenesten, mens NSM og Nkom bidrar til videreutvikling og finansiering.

6.5 Inntrengingstester

Kartlegging og forsøk på inntrenging skjer kontinuerlig mot enheter koblet på internett. Inntrengingstesting er et effektivt tiltak for å avdekke sårbarheter og teste motstandskraften i IKT-systemer. Dette gjøres gjennom målrettet søk, analyse og forsøksvis utnyttelse av sårbarheter, feil og mangler. Sårbarheter i infrastruktur tilknyttet internett kan også utføres ved bruk av kartleggingsverktøy, som for eksempel Allvis NOR (se boks 6.5).

Justis- og beredskapsdepartementet anbefaler bruk av inntrengingstester. En rekke virksomheter har fulgt anbefalingen, og i de aller fleste tilfeller har dette avdekket alvorlige sårbarheter og bidratt til at disse er blitt håndtert.

Virksomheter som er underlagt sikkerhetsloven, kan be NSM om slik bistand. NSM har gjennomført slike tester blant annet i Justis- og beredskapsdepartementet, Forsvarsdepartementet og Utenriksdepartementet. Andre virksomheter kan benytte private selskaper til å utføre testingen. Ulike sektorer kan også bygge opp egen kompetanse til å gjennomføre tester, slik som for eksempel Norsk Helsenett SF har gjort. Systematisk gjennomføring og oppfølging av slike tester vil kunne redusere sårbarheten i systemene til virksomheter og gjøre dem mer motstandsdyktige mot digitale angrep.

Regjeringen oppfordrer samfunnskritiske virksomheter til å benytte inntrengingstester for å avdekke sårbarheter og teste motstandskraften i egne IKT-systemer.

6.6 Kunnskapsgrunnlag

I den senere tid er det produsert flere analyser om digital sårbarhet. Disse tjener flere formål. De bidrar til folkeopplysning og bevisstgjøring, men er først og fremst et beslutningsgrunnlag for myndigheter og virksomhetsledere med tanke på å utforme politikk og tiltak for å redusere sårbarheter.

I 2015 utarbeidet NSM rapporten *Helhetlig IKT-risikobilde* for første gang. Rapporten utgis

Boks 6.4 IKT-tjenesteutsetting i helsetjenesten

Helsetjenesten er avhengig av private leverandører for å utvikle og innføre løsninger og gjennomføre service, vedlikehold og drift.

I forbindelse med at Helse Sør-Øst RHF var i ferd med å sette ut drift av IKT-infrastruktur til en internasjonal leverandør, ble det avdekket sviktende rutiner og risikovurderinger. Tjenesteutsetting til eksterne driftsoperatører fordrer kontrollregimer og risiko- og sårbarhetsanalyser som sikrer at krav til behandling av personopplysninger ivaretas.

Helse- og omsorgsministeren vil derfor sette i gang et arbeid for å se på håndtering av informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren.

Boks 6.5 Allvis NOR

Både nasjonalstater, organisasjoner og privatpersoner kartlegger sårbarheter fra internett. I Norge ble dette fenomenet for alvor gjort kjent for allmennheten gjennom Dagbladets «Null CTRL»-artikkelserie i 2013/2014.

NSM har i ettertid av denne artikkelserien etablert en lignende kartleggingstjeneste, Allvis NOR. Allvis NOR leter gjennom tilknyttede virksomheters internetteksponerte IKT-grensesnitt for å avdekke sårbare eller feil konfigurerte tjenester og utstyr, slik at virksomheten selv kan redusere sine sårbarheter. Tjenesten er samtykkebasert. Allvis NOR ble videreutviklet til å kunne avdekke den spesifikke sårbarheten som ble utnyttet av løsepengeviruset omtalt som «WannaCry» i mai 2017. NSM opplevde økt etterspørsel etter tjenesten under denne hendelsen.

Allvis NOR gir myndighetene innsikt i det offentlige Norges sikkerhetstilstand på internett og sikrer at utviklingen kan følges over tid. Allvis NOR vil være et nyttig supplement til ordinær inntrengingstesting og vil kunne bidra til å bedre grunnsikringen i samfunnet.

årlig. Hensikten med de årlige rapportene er å skape et felles situasjonsbilde som gjør virksomheter og myndigheter i stand til å treffe riktige tiltak. I tillegg skal den være et verktøy for virksomheter i deres arbeid med å utarbeide risikovurderinger. NSM har fått i oppdrag å videreutvikle rapporten i samarbeid med andre relevante virksomheter.

Eksempler på andre analyser er NorSIS' årlige rapport om trusler og trender. Rapporten viser sikkerhetsutfordringer som både enkeltpersoner og samfunnet for øvrig må forholde seg til. I tillegg utarbeides det årlige analyser av blant annet Politiets sikkerhetstjeneste, Etterretningstjenesten, Kripos, Direktoratet for samfunnssikkerhet og beredskap (DSB), Finanstilsynet og Nasjonal kommunikasjonsmyndighet (Nkom). Ulike sektorers og virksomheters risikoanalyser, evalueringer etter øvelser og hendelser, forskning på området og vurderinger fra privat næringsliv bidrar til den totale oversikten. Analysene har noe ulik tilnærming og ulike målgrupper, men ofte er det et gjennomgående tema at utfordringene på IKT-sikkerhetsområdet er tverrsektorielle.

Regjeringen vil utvikle, vedlikeholde og støtte opp om et godt og tilgjengelig kunnskapsgrunnlag som gjør enkeltindivider, virksomheter og myndigheter i stand til å treffe riktige tiltak.

6.7 Kultur, ledelse og holdninger

I Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* fremhever regjeringen betydningen av kultur, ledelse og holdninger for samfunnssikkerheten i Norge. Hvordan vi forholder oss til risiko, og hvor godt vi er forberedt på en alvorlig hendelse, påvirkes av våre holdninger og den kulturen vi er en del av. Ikke minst gjelder dette for IKT-sikkerhet. Sikkerhet var lettere å vurdere da det som skulle sikres, var noe fysisk, håndfast og stabilt. Låsbare skap og fysiske hindre lar seg lett forstå. I den digitale verden kan man bli mer fremmedgjort når det gjelder sikkerhet. Vi har ikke lenger den samme oversikten over sårbarhetsbildet. Et digitalt angrep vil ofte ikke være synlig for den som blir rammet. Behovet for å øke bevisstheten om sårbarhet og sikkerhetstrusler, samt øke kompetansen til den enkelte, blir stadig mer relevant.

God styring av sikkerheten i virksomhetene legger grunnlaget for tilfredsstillende sikring av verdier. Ledelsesforankring av sikkerhetsarbeidet samt forpliktelse gjennom avsetting av ressurser til sikring av informasjon og informasjonssystemer er viktig. All sikring starter med en verdivurdering – hvilke innsatsfaktorer og verdier er viktige for vår virksomhet, samarbeidspartnere, samfunnet som helhet etc. Strukturerte verdi- og risikovurderinger gir oversikt over verdier og i hvilken grad disse er utsatt for risiko. Vurderingene er både et styringsverktøy – hva må gjøres for å oppnå et tilfredsstillende sikkerhetsnivå – og de bidrar til risikoerkjennelse i virksomhetene.

Regjeringen vil arbeide for at sikkerhetskulturen i virksomheter og samfunnet generelt forbedres, blant annet ved kompetansehevende tiltak og bedre risikoerkjennelse.

6.8 Personvern og forebyggende IKT-sikkerhet

Når sikkerhetstiltak skal utarbeides, må tiltakets mulige konsekvenser for personvernet vurderes. I den grad tiltaket får konsekvenser for personvernet, stilles det i nasjonale og internasjonale regelverk nærmere krav til gjennomføring av tiltakene. I NOU 2016: 19 *Samhandling for sikkerhet* ble for-

holdet mellom forebyggende sikkerhet og personvern beskrevet. Utvalget listet opp fem punkter med prinsipper og retningslinjer som ble lagt til grunn for arbeidet med å utrede en ny lov om forebyggende nasjonal sikkerhet. Listen kan tjene som utgangspunkt også for arbeidet med IKT-sikkerhet:

- presisjon i formuleringen av hjemmel for sikkerhetstiltaket (lovkravet)
- vurdere hvilken effekt man får ved sikkerhetstiltaket, sett opp mot allerede eksisterende tiltak (formålsmessighet)
- vurdere forholdsmessigheten mellom den sikkerhetsmessige effekten og hvor mye tiltakene griper inn i personvern og rettssikkerhet (forholdsmessighet)
- vurdere alternative og mindre inngripende tilnærminger som kan gi samme effekt (subsidiaritetsprinsippet)
- etablere tilstrekkelige personvern- eller rettssikkerhetsgarantier der det gjøres inngrep i den enkeltes rettssfære (prosessuelle mekanismer)

Som nevnt under punkt 6.5 anses inntrengingstesting som et godt IKT-sikkerhetstiltak. Mange IKT-systemer behandler personopplysninger. Dette er et eksempel på et sikkerhetstiltak der de nevnte prinsippene må anvendes før iverksettelse, og der sikkerhetshensyn må avveies mot personvernhensyn.

7 Avdekke og håndtere digitale angrep

Regjeringen er opptatt av å styrke vår nasjonale evne til å avdekke og håndtere digitale angrep. Digitale angrep kan være krevende å oppdage og kan i ytterste konsekvens utgjøre en trussel mot nasjonale interesser og krenkelse av norsk suverenitet. Aktørene kan være andre stater, organiserte ikke-statlige grupperinger og private rettssubjekter. Målet til angriperne kan være å begå vinningskriminalitet, drive utpressing eller ødelegge eller endre informasjon eller funksjonalitet. Det kan også være å skaffe seg informasjon om stats- og forretningshemmeligheter, forskningsresultater eller teknologiske nyvinninger fra kommersielle bedrifter. Problemstillingene er ofte globale, og risikoen for straff og konsekvenser er lav.

Sett fra et stats- og samfunnssikkerhetsperspektiv er den største trusselen de aktørene som har ressurser til å gjennomføre handlinger som vi ikke oppdager, som oppdages for sent, som kan forårsake skader på kritisk infrastruktur, eller som kan påvirke demokratiske prosesser. I denne kategorien finner vi ofte statlige aktører, særlig andre lands sikkerhets- og etterretningstjenester.

En utfordring kan være at det oppstår usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for å bekjempe alvorlige digitale angrep. Regjeringen er derfor opptatt av å legge til rette for samarbeid og deling av informasjon.

Sentrale tiltak:

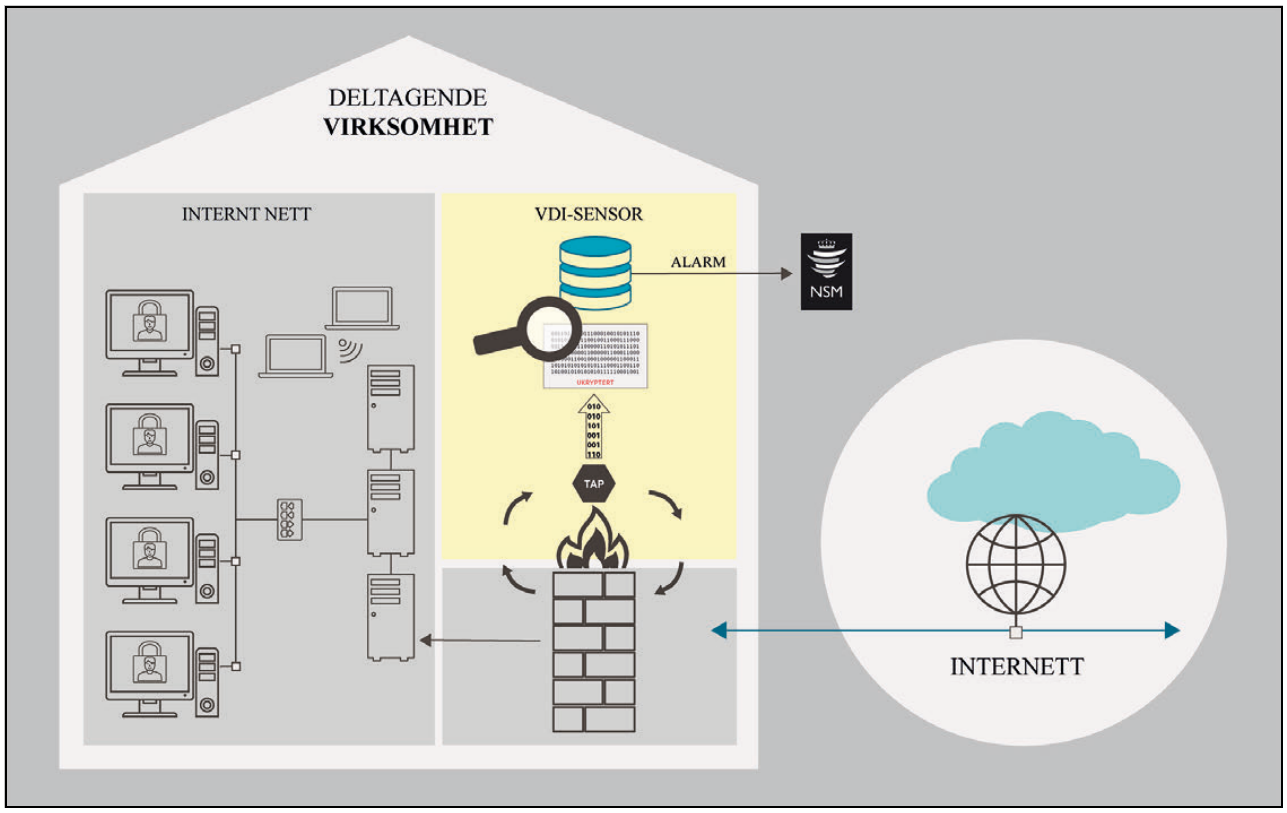
- videreutvikle det nasjonale varslingssystemet for digital infrastruktur (VDI) for å øke evnen til å avdekke digitale angrep
- etablere og videreutvikle et nasjonalt rammeverk for digital hendelseshåndtering som fører til mer effektiv håndtering og bedre samvirke mellom aktører
- etablere et informasjonsdelingsarbeid for å bedre samarbeidet mellom offentlige og private virksomheter ved digitale hendelser og etablere en teknisk plattform for deling av informasjon
- utrede og konkretisere hvordan en form for digitalt grenseforsvar kan etableres og lovreguleres
- gjøre politiet bedre i stand til å bekjempe kriminalitet i det digitale landskapet
- øke den nasjonale evnen til å motstå alvorlige digitale angrep gjennom videreutvikling av samarbeidet mellom Etterretningstjenesten, NSM, PST og politiet for øvrig
- forbedre NSMs evne til å analysere alvorlige digitale angrep mot samfunnskritisk infrastruktur og informasjon

7.1 Varslingssystemet for digital infrastruktur

Evnen til å avdekke og håndtere digitale angrep avhenger av et samspill mellom myndigheter, sektormiljøer og offentlige og private virksomheter. NSM drifter den nasjonale responsfunksjonen for alvorlige digitale angrep mot kritisk infrastruktur og er ansvarlig for å organisere og drifte det nasjonale varslingssystemet for digital infrastruktur (VDI). VDI er et nettverk av sensorer som er plassert hos både offentlige og private virksomheter som eier kritisk infrastruktur. Informasjon fra sensorene bidrar til en nasjonal evne til tidlig deteksjon og verifikasjon av koordinerte og målrettede angrep. Regjeringen ønsker å oppgradere sensorteknologien i VDI.[1]

Regjeringen fremmet i Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven* et forslag om å lovfeste virksomheten som i dag utøves av NSM gjennom NorCERT og VDI. Ved behandlingen av Innst. 352 L (2015–2016) vedtok Stortinget at NSM skulle ha ansvaret for en nasjonal responsfunksjon og et varslingssystem for digital infrastruktur. Regjeringen vurderte også i denne sammenheng om det burde etableres en hjemmel for å kunne pålegge enkelte virksomheter med kritisk infrastruktur å tilknytte seg VDI. På bakgrunn av høringsinstansenes tilbakemeldinger kom regjeringen til at et slikt pålegg måtte utredes nærmere og ses i sam-

[1] Prop. 151 S (2015–2016) *Langtidsplan for forsvarssektoren*.



Figur 7.1 Varslingssystem for digital infrastruktur (VDI).

Illustrasjon: M. Sylstad, NSM.

menheng med en vurdering av den fremtidige finansieringsmodellen for NorCERT og VDI.

7.2 Rammeverk for digital hendelseshåndtering

Regjeringen er opptatt av at samvirket mellom aktører for å håndtere alvorlige digitale angrep styrkes. Regjeringen har besluttet at det skal etableres et nasjonalt rammeverk for å håndtere digitale hendelser. En første versjon av rammeverket ferdigstilles i 2017 (se boks 7.1). Rammeverket beskriver den nasjonale strukturen for hvordan Norge organiserer seg for å håndtere digitale hendelser. Det vil bidra til at relevante aktører effektivt kan utøve sitt ansvar i en koordinert nasjonal respons ved et digitalt angrep. Rammeverket skal også beskrive rutiner for varsling og informasjonsdeling, og etablere et enhetlig begrepsapparat. Rett informasjon til rett tid er avgjørende for at virksomheter skal kunne forebygge, avdekke og håndtere digitale hendelser, og for at de har et riktig situasjonsbilde. Deling av informasjon mellom virksomheter, responsmiljøer, departementene og NSM er avgjørende for dette.

For å sikre at alle relevante aktører mottar korrekt varslingsinformasjon og settes i stand til å gjøre nødvendige tiltak, har myndighetene besluttet at det skal etableres sektorvise responsmiljøer. Responsmiljøene skal ha oversikt i egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM. Sektorvise responsmiljøer er en sentral forutsetning i rammeverket for nasjonal hendelseshåndtering. Sektorvise responsmiljøer er omhandlet flere steder i del III.

Et utkast til rammeverk ble benyttet under den nasjonale øvelsen IKT16 i november 2016. Erfaringer fra øvelsen blir nå benyttet i arbeidet med å ferdigstille rammeverket (se oversikten over foreløpige funn i boks 7.2).

Dersom det oppstår svikt i kritiske samfunnsfunksjoner på grunn av digitale angrep, vil det medføre behov for krisehåndtering på samfunnsnivå av en rekke aktører, som beredskapsetater, kommuner eller frivillige organisasjoner, tilsvarende som for andre hendelser som rammer kritiske samfunnsfunksjoner.

Boks 7.1 Nasjonalt rammeverket for digital hendelseshåndtering

Rammeverket skal bidra til å

- tydeliggjøre ansvar og roller for myndighetsaktører og andre sentrale aktører innenfor digital hendelseshåndtering
- kommunisere hva offentlige og private virksomheter selv må være forberedt på å håndtere, og hva slags støtte og koordinering som kan forventes fra det nasjonale responsmiljøet (NSM)
- tydeliggjøre og styrke rammene for samarbeidet mellom virksomheter, responsmiljøet i sektoren, NSM, Etterretningstjenesten, PST og politiet for øvrig
- videreutvikle evnen til å dele relevant informasjon og rapportere om digitale angrep
- tydeliggjøre kontaktpunkter mot andre land og organisasjoner

7.3 Informasjonsdeling

Informasjonsdeling er avgjørende for å avdekke og håndtere digitale angrep. Dette har et forbedringspotensial og var et sentralt tema i Lysneutvalgets utredning. Utvalget mente det var et uutnyttet handlingsrom for deling av informasjon. NSM har derfor fått i oppdrag å igangsette et arbeid for å bedre samarbeidet og informasjonsflyten knyttet til digital hendelseshåndtering i Norge. Målet for arbeidet er å sikre at det kan gjøres vurderinger av digitale hendelser på tvers av sektorer, og å sikre toveis informasjonsutveksling og koordinering mellom NSM og ulike responsmiljøer. Regjeringen er særlig opptatt av å få til et godt offentlig–privat samarbeid på området, og relevante aktører fra offentlig og privat sektor skal derfor involveres i arbeidet. Arbeidet skal også se på hvordan informasjon og samvirke kan forbedres utover de virksomheter som i dag fanges opp av nasjonalt rammeverk for digital hendelseshåndtering.

NSM har også iverksatt flere tiltak knyttet til informasjonsdeling. NSM samler responsmiljøer sektorvis hver måned for gjennomgang av digitale hendelser, samt diskusjon av utviklingsbehov og policyavklaringer for samarbeidet. Det gjennomføres også ukentlig videokonferanse med responsmiljøene i de ulike sektorene. Det er et mål å samle alle disse responsmiljøene om et felles rapporteringsformat.

Boks 7.2 Foreløpige funn fra Øvelse IKT16

Formålet med øvelse IKT16 var å sette Norge i bedre stand til å håndtere et større digitalt angrep som rammer på tvers av sektorer. Læring var prioritert i planlegging, gjennomføring og oppfølging av øvelsen. DSB ledet arbeidet med øvelsen.

Noen foreløpige funn fra øvelsen:

- Nasjonalt rammeverket for digital hendelseshåndtering danner grunnlag for en god måte å håndtere en samlet koordinert respons på digitale angrep på.
- Det er behov for forventningsavklaringer mellom virksomheter knyttet til informasjonsdeling og situasjonsbilde.
- NSMs ugraderte nasjonale situasjonsbilde var en viktig kilde til informasjon.
- Det er ulik organisering og ulikt modenhetsnivå i responsmiljøene i de ulike sektorene. Det er viktig å favne ulike miljøer i en koordinert nasjonal respons i videreutviklingen av rammeverket.
- Det er behov for ansvars- og rolleavklaring mellom virksomhetenes IKT-miljøer og beredskapsmiljøer. Begge typer miljø må involveres i krisehåndteringen og det er avgjørende at de samarbeider godt.

Endelig evalueringsrapport vil foreligge i løpet av 2017.

NSM har utarbeidet et ugradert nasjonalt situasjonsbilde, tilgjengelig via en portal med påloggingsmulighet for responsmiljøene i de ulike sektorene og nasjonale beslutningstakere. Formålet er at informasjon skal kunne deles raskt og sikkert. Portalen ble testet under øvelse IKT16, og erfaringene viste at portalen ble en viktig kilde til informasjon. Våren 2017 ble portalen operativ på ugradert plattform, og NSM vurderer mulighetene for å utvikle en tilsvarende portal på graderte kommunikasjonsplattformer. I løpet av 2017 vil NSM også utvikle løsninger for automatisert deling av varsler og teknisk informasjon med responsmiljøene i de ulike sektorene. NSM utveksler ukentlige rapporter med de nordiske landenes CERT-funksjoner.

7.4 Digitalt grenseforsvar

Utfordringene med å avdekke digitale angrep berører også spørsmålet om et digitalt grenseforsvar i Norge. Forsvarsdepartementet nedsatte i 2016 et utvalg (Lysne II) for å utrede de prinsipielle sidene ved en eventuell tilgang for Etterretningstjenesten til digital kommunikasjon inn og ut av Norge. Utredningen peker på utviklingstrendene i samfunnet som aktualiserer behovet for nye etterretningsmetoder med innsyn i datastrømmer som krysser den norske landegrensen. Nesten all trafikk har flyttet seg fra radio og satellitt til digitale signaler i kabler. Etterretningstjenesten har i dag ingen systemer for å kontrollere digital kommunikasjon over landegrensen, og den har liten eller ingen egen tilgang til informasjonen som flyter i kommunikasjonskablene.

Utvalget leverte sin rapport 26. august 2016 og anbefalte innføring av et digitalt grenseforsvar med klar innramming og meget strenge kontrollmekanismer for å ivareta personvernet. En rekke aktører har engasjert seg i den offentlige debatten, og motstridende synspunkter er blitt fremmet i en omfattende høringsrunde.

Regjeringen mener at det er behov for å styrke Norges evne til å beskytte seg mot ytre trusler i og ved bruk av det digitale rommet, og at det er behov for å etablere en form for digitalt grenseforsvar. Regjeringen vil derfor utrede og konkretisere hvordan et digitalt grenseforsvar kan etableres og lovreguleres. I en slik utredning vil det være avgjørende å finne en balanse mellom den sikkerhets- og etterretningsmessige effekten et digitalt grenseforsvar kan få, og de personvernrelaterte spørsmålene som en slik tilgang reiser. Regjeringen tar sikte på at et høringsnotat med lovforslag kan sendes på høring i 2018.

7.5 IKT-kriminalitet

IKT-kriminalitet øker i omfang. IKT-kriminalitet deles ofte inn i kriminalitet rettet mot selve IKT-systemene, og kriminelle handlinger begått ved hjelp av IKT.

Flere rapporter og utredninger viser behov for å styrke politiets kompetanse og kapasitet på området. I politiets egen omverdensanalyse fra 2015 pekes det på at tempoet i teknologiutviklingen er så høyt at politiet hele tiden utfordres. Utviklingen stiller nye krav til politiets oppgaveløsning, i form av både mer spisset kompetanse og ny teknologi.

Justis- og beredskapsdepartementet utarbeidet i 2015 en strategi for å bekjempe IKT-kriminalitet. Dette er departementets første strategidokumentet på feltet, og det retter seg blant annet mot å styrke kompetanse og kapasitet, bygge kunnskap, styrke forskningen og kartlegge teknologiske behov og løsninger.

Ett av tiltakene i strategien er å etablere et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet. Lysneutvalget støttet forslaget om et nasjonalt senter med en særskilt bistandsfunksjon for å støtte politidistriktene både polititaktisk og påtalefaglig. Politidirektoratet (POD) har utarbeidet et konkret forslag til hvordan det kan etableres et slikt senter i politiet for å forebygge og bekjempe IKT-kriminalitet, herunder hvilke oppgaver som skal legges til senteret, organisatorisk forankring og ressursbehov. Forslaget innebærer at politiet må avsette betydelige ressurser. For noen funksjoner må behovet dekkes ved ekstern rekruttering av kompetanse som politiet ikke har i dag. Forslaget må derfor behandles i det ordinære budsjettarbeidet, og vurderes opp mot andre viktige tiltak.

Regjeringen er opptatt av at digital kompetanse må bygges i alle politidistrikt slik at politiet har tilstrekkelige forutsetninger for å bekjempe IKT-kriminalitet. I det digitale rommet har politi og påtalemyndighet mindre muligheter for å pågripe, tiltale og iretteføre. Det medfører at politiets innsats i enda større grad enn ellers må rettes mot forebyggende arbeid, etterretning, avdekking, stansing og gjenoppretting av lovlig situasjon ved tilstedeværelse i det digitale rommet.

Verktøyene for å håndtere digitale spor må være oppdaterte i tråd med den teknologiske utviklingen, og politiets etterforskningsmetoder må holde tritt med de kriminelles bruk av moderne teknologi. For at politiet skal ha nødvendig kompetanse, må politiutdanningen styrkes. Det gjelder både grunnutdanningen og etter- og videreutdanningen. Ansatte uten politiutdanning, herunder spesialister med høy teknologisk spisskompetanse bør få politifaglig tilleggsutdanning. Som del av Justis- og beredskapsdepartementets strategi av 2015 for å bekjempe IKT-kriminalitet har POD utarbeidet en egen strategi for digital kompetanseheving.

Regjeringen har også gitt politiet viktige verktøy i kampen mot alvorlig kriminalitet gjennom lovendringer. Stortinget vedtok i juni 2016, på grunnlag av Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*, å gi politiet utvidet adgang til å benytte skjulte tvangsmidler ved etterforskning, avverging og forebyg-

ging av alvorlige lovbrudd. Utvidelsene gjelder blant annet metoder som kommunikasjonskontroll, hemmelig ransaking, romavlytting, teknisk sporing og kameraovervåking. Lovendringene trådte i kraft 17. juni 2016. I tillegg åpnes det for bruk av et nytt skjult tvangsmiddel i form av dataavlesing. Disse reglene trådte i kraft 9. september 2016. Den 5. april 2017 la regjeringen dessuten frem et forslag til Stortinget om lovendringer som vil sikre politiet tilgang til mobiltelefoner, nettbrett og andre datasystemer som åpnes ved fingeravtrykk og annen biometrisk autentisering.

Bakgrunnen for disse lovendringene og forslagene er et endret kriminalitets- og trusselbilde og den teknologiske utviklingen. Terrorfaren har økt betraktelig, alvorlig og organisert kriminalitet brer om seg, og kryptert kommunikasjon blir stadig mer vanlig. Det må legges til rette for at politiet har de nødvendige virkemidlene til å kunne beskytte borgerne og samfunnet effektivt i tråd med kravene i politiloven § 2, samtidig som det må tas tilstrekkelig hensyn til borgernes vern mot inngrep.

Et regjeringsoppnevnt utvalg overleverte 18. mai 2017 sin utredning om organisering og oppgaveløsning i politiets særorganer.[2] Utvalget har vurdert fremtidige modeller, og har i vurderingen lagt stor vekt på politiets evne til styrket bekjempelse av IKT-kriminalitet. Utredningen blir sendt på bred høring.

7.6 Koordinering mellom NSM, Etterretningstjenesten, PST og politiet for øvrig

Regjeringen understreker betydningen av et tett og godt samarbeid mellom NSM, Etterretningstjenesten, PST og politiet for øvrig. Det er nødvendig med hurtig informasjonsutveksling og effektive mekanismer for å etablere et felles situasjonsbilde ved digitale angrep. Det vil kunne bidra til at nødvendige mottiltak blir identifisert og iverksatt raskest mulig.

NSM, Etterretningstjenesten og PST har tidligere samarbeidet innenfor rammene av Cyberkoordineringsgruppen. Gruppen hadde regelmessige møter og fremskaffet informasjon og beslutningsgrunnlag til den operative og strategiske ledelsen om trusler og sårbarheter i det digitale rommet. Kripos og Cyberforsvaret deltok i en utvidet del av dette samarbeidet, og Cyberkoordineringsgruppen kunne utvides med representanter fra andre relevante aktører ved behov.

Som beskrevet i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* fikk NSM, Etterretningstjenesten og PST høsten 2016 i oppdrag å etablere et Felles cyberkoordineringssenter, som en videreutvikling av Cyberkoordineringsgruppen.

Felles cyberkoordineringssenter ble opprettet 31. mars 2017 som et permanent, samlokalisert fagmiljø med representanter fra NSM, Etterretningstjenesten og PST. Senteret skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep og understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rommet. Senteret er ikke et selvstendig organ med egen beslutningsmyndighet, og etableringen innebærer ingen endringer i rettsgrunnlag, fullmakter, roller eller oppgaver. Informasjonsdelingen som foregikk mellom Cyberkoordineringsgruppen og Forsvaret, videreføres mellom Felles cyberkoordineringssenter og Forsvaret.

NSM, Etterretningstjenesten og PST har tidligere fått oppdrag om ytterligere å forbedre samarbeidet og øke informasjonsutvekslingen mellom tjenestene og Kripos med hensyn til håndtering av digitale angrep og kriminalitet i det digitale rommet. Tjenestene og Kripos har foreslått overfor Justis- og beredskapsdepartementet og Forsvarsdepartementet at også Kripos bør inngå som en permanent deltaker i Felles cyberkoordineringssenter. Forslaget er til vurdering hos departementene.

7.7 Åpenhet om digitale angrep

Regjeringen er opptatt av at det skal være åpenhet om digitale angrep. På oppdrag fra Justis- og beredskapsdepartementet har NSM tidligere utarbeidet anbefalinger for hvordan åpenhet om digitale angrep bør vurderes. Retningslinjene ble utformet i samarbeid med Difi, POD, NorSIS og Næringslivets Sikkerhetsråd.

Åpenhet danner grunnlag for læring og bidrar til å sette virksomhetene bedre i stand til å forebygge, avdekke og håndtere hendelser. Det gir også virksomheter og myndigheter bedre forutsetninger for å forstå utfordringene i det digitale rommet. Samtidig må offentliggjøring og deling av informasjon praktiseres på en slik måte at taushetspliktbestemmelser ivaretas, og fordelene må vurderes opp mot mulige negative konsekvenser. Regjeringen oppfordrer både offentlige og private

[2] NOU 2017: 11 *Bedre bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer.*

virksomheter til å følge anbefalingene om åpenhet.

7.8 Analysekapasitet

Alvorlige digitale angrep er blitt mer avanserte og vanskeligere å oppdage. Det er tid- og kompetansekrevende å gjennomføre analyser av slike angrep. Til tross for økt egenevne i virksomhetene til å håndtere hendelser, har høyere kompleksitet i den enkelte hendelse ført til en betydelig etterspørsel etter NSMs analysekompetanse. Samtidig har NSM begrenset analysekapasitet til å møte denne etterspørselen. Regjeringen vil derfor styrke den nasjonale kapasiteten ved å forbedre NSMs evne til å avdekke og analysere alvorlige digitale angrep mot samfunnskritisk infrastruktur og informasjon, jf. Prop. 151 S (2015–2016) *Kampkraft og bærekraft*.

8 IKT-sikkerhetskompetanse

Regjeringen ønsker å legge til rette for å styrke IKT-sikkerhetskompetansen i Norge og arbeide for at kompetansebehovene for IKT-sikkerhet i samfunnet og næringslivet blir ivaretatt.

IKT-sikkerhetskompetanse er en knapp ressurs nasjonalt og internasjonalt. Behovet for mer og bedre utdannet IKT-sikkerhetspersonell er understreket både i Lysneutvalgets utredning, i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* og i Meld. St. 27 (2015–2016) *Digital agenda for Norge*. Regjeringen har de siste årene lagt til rette for bedre utdanningskapasitet og økt forskning på IKT-sikkerhet.

Sentrale tiltak:

- etablere en nasjonal kompetansestrategi for IKT-sikkerhet, der blant annet behovet for studieplasser og forskningssatsning vurderes
- gjennom den påbegynte fagfornyelsen i grunnopplæringen, vurdere hvorvidt IKT-sikkerhet er tilstrekkelig inkludert i den grunnleggende digitale kompetansen elevene skal tilegne seg
- styrke IKT-sikkerhetskompetansen i tilsyn
- legge vekt på systematisk oppfølging og læring etter både øvelser og hendelser, også ved digitale hendelser

8.1 Nasjonal kompetansestrategi for IKT-sikkerhet

Det fremgår av Meld. St. 10 (2016–2017) at regjeringen vil utarbeide en nasjonal kompetansestrategi innenfor IKT-sikkerhet. Målet med strategien er å legge til rette for langsiktig oppbygging av kompetanse. Strategien vil omhandle tiltak for å styrke den nasjonale kapasiteten innenfor forskning og utdanning. Den vil også omhandle bevisstgjøringstiltak rettet mot befolkningen og virksomheter.

IKT-sikkerhetskompetanse har inngått i flere ulike strategier, stortingsmeldinger og andre dokumenter tidligere, men dette er første gang det utvikles en strategi som omhandler kompetanseutfordringen under ett.

For å gi et godt grunnlagsmateriale til den kommende kompetansestrategien for IKT-sikkerhet er Norsk institutt for studier av innovasjon, forskning og utdanning (NIFU) gitt i oppdrag å kartlegge fremtidens behov for IKT-sikkerhetskompetanse i arbeidslivet (se boks 8.1). Rapporten som utarbeides, skal bidra til å identifisere gapet mellom tilgjengelig kompetanse og etterspørselen etter den.

Justis- og beredskapsdepartementet vil i samarbeid med blant annet Kunnskapsdepartementet ha ansvar for å utvikle strategien. For å sikre god forankring vil regjeringen legge til grunn at relevante aktører skal involveres i arbeidet. Arbeidet med kompetansestrategien vil også bli sett i sammenheng med behovet for å øke IKT-kompetansen generelt og avansert IKT-kompetanse spesielt.[1]

Boks 8.1 NIFUs kompetansekartlegging

NIFU har kartlagt antall studenter ved IKT-sikkerhetsutdanningene og IKT-utdanninger med kurs i IKT-sikkerhet i Norge i perioden 2012–2016, og hvor mange som er uteksaminert i samme periode. Kartleggingen viser en økning i antall studenter fra 166 i 2012 til 358 i 2016 ved studieprogram i IKT-sikkerhet, og en økning fra 1582 i 2012 til 2695 studenter i 2016 på studieprogram med kurs i IKT-sikkerhet.

NIFUs prosjekt er fortsatt i en tidlig fase, men en foreløpig beregning viser at til tross for en forventet stabil økning av personer med avansert IKT-sikkerhetskompetanse, øker gapet mellom tilbud og etterspørsel.

[1] Meld. St. 27 (2015–2016) *Digital agenda for Norge*.

8.2 Grunnskole og videregående opplæring

Digital kompetanse har blitt en viktig del av grunnskolen og videregående opplæring. I utviklingen av elevenes digitale kompetanse er det viktig at det i tillegg til mulighetene som finnes i teknologien, også er fokus på trygg bruk. Elevene må forstå behovet for oppdatering av programvare, jevnlige sikkerhetskopier og farene ved ukritisk bruk av nedlastet programvare og nettbaserte tjenester.

Regjeringen følger opp dette gjennom Meld. St. 28 (2015–2016) *Fag – Fordypning – Forståelse – En fornyelse av Kunnskapsløftet*. I oppfølgingen vil det vurderes hvorvidt IKT-sikkerhet er tilstrekkelig inkludert i den grunnleggende digitale kompetansen elevene skal tilegne seg. Relevante fagplaner for videregående opplæring vil også vurderes i oppfølgingen av meldingen.

8.3 Høyere utdanning

For å minske gapet mellom tilbud og etterspørsel på IKT-sikkerhetsområdet er det avgjørende at det utdannes nok mennesker med relevant kompetanse.

Regjeringen har de siste årene fulgt opp både Meld. St. 27 (2015–2016) og Lysneutvalget gjennom å øremerke flere studieplasser til IKT og IKT-sikkerhet. I revidert nasjonalbudsjett for 2015 ble 45 studieplasser øremerket IKT og 200 studieplasser andre teknologi- og realfag. I budsjettet for 2016 ble det fordelt 100 studieplasser til IKT. I revidert nasjonalbudsjett for 2016 ble 65 studieplasser øremerket IKT-sikkerhet og 135 studieplasser øremerket helse- og IKT-utdanning. For 2017 ble 500 studieplasser for ett kull øremerket til IKT, og ved fordeling av studieplassene ble institusjonene blant annet bedt om å ta hensyn til behov for IKT-sikkerhet.

Stadig flere utdanningsinstitusjoner legger inn emner om IKT-sikkerhet som en del av IKT-utdanninger. Det er også viktig at IKT-sikkerhets- og

Figur 8.1 Utdanning.

Illustrasjon: M. Sylstad, NSM.
Kilde: Bilde hentet fra Colourbox.

personvernsrelaterte problemstillinger er en del av andre utdanninger, for eksempel jus, økonomi og ledelse.

De siste årene har det vært en betydelig økning i søkningen til IKT-utdanninger. Dette bidrar til økt konkurranse om studieplassene, noe som kan gi økt kvalitet og raskere gjennomstrømming. På sikt vil de øremerkede studieplassene medføre en betydelig økning av antallet kandidater med IKT- og IKT-sikkerhetskompetanse.

Regjeringen vil utarbeide en nasjonal kompetansestrategi for IKT-sikkerhet. Strategien skal blant annet vurdere behovet for studieplasser.

8.4 Forskning

Norge er avhengig av å bygge fremragende og varige forskningsmiljøer innenfor IKT-sikkerhet. Det er flere gode forskningsmiljøer på IKT-sikkerhet i Norge, for eksempel Forsvarets forskningsinstitutt, NTNU Center for Cyber and Information Security (CCIS) på Gjøvik, Simula Research Laboratory og universitetene i Oslo og Bergen.

Forskningsrådets program IKTPLUSS og EUs program Horizon 2020 finansierer det meste av IKT-sikkerhetsforskningen i Norge i dag. Regjeringen oppfordrer næringslivet og offentlig sektor til i større grad å involvere seg i forskning, både som bestillere og som partnere. Ordninger som nærings-ph.d. og offentlig ph.d. er etablerte, men har potensial for å bli brukt mer.

I Justis- og beredskapsdepartementets FoU-strategi for samfunnssikkerhet (2015–2019) er trygg digitalisering av samfunnet et prioritert forskningstema innenfor justissektoren. I strategien beskrives også partnerskap med forskningsinstitusjoner som et viktig virkemiddel. Gjennom utvidet kontakt mellom forskning, utdanning, myndigheter og sluttbrukere øker muligheten for gjensidig dialog som kan gi mer treffsikre og anvendbare prosjekter.

Gjennom IKTPLUSS bevilget regjeringen i 2015 150 mill. kroner til IKT-sikkerhetsprosjekter. Dette er prosjekter som nå er i full gang. Regjeringen har også økt antall rekrutteringsstillinger (postdoktor- og stipendiatstillinger) til realfag og teknologi. I statsbudsjettet for 2017 er 16 nye rekrutteringsstillinger ved universiteter, høgskoler og instituttsektoren øremerket til IKT-sikkerhet. Regjeringen foreslår i Revidert nasjonalbudsjett 2017 å bevilge midler til ytterligere 4 nye rekrutteringsstillinger til NTNU. Rekrutteringsstillingene skal gå til CCIS på Gjøvik. Nye rekrutteringsstillinger vil bidra til å styrke forskning og kunnskap om IKT-sikkerhet.

Justis- og beredskapsdepartementet finansierer også forskning på samfunnssikkerhetsfeltet generelt. Den største satsingen foregår i regi av forskningsprogrammet SAMRISK ved Norges forskningsråd. Programmet har som mål å bidra til bedre motstandskraft, forebygging, beredskap, redningsarbeid, krisehåndtering og læring. SAMRISK er et sektorovergripende og tverrfaglig program. Programmets aktiviteter sees også i sammenheng med NordForsks satsing på samfunnssikkerhet og EUs sikkerhetsforskning.

Regjeringen vil utarbeide en nasjonal kompetansestrategi for IKT-sikkerhet. Strategien skal blant annet vurdere behovet for forskning på området.

8.5 Etter- og videreutdanning

Det er viktig at det gis tilbud om etter- og videreutdanning til personer som har behov for IKT-sikkerhetskompetanse på arbeidsplassen. Etter- og videreutdanning kan organiseres fleksibelt og på den måten nå mange, for eksempel gjennom IKT-støttede, desentraliserte og samlingsbaserte utdanninger. Det er viktig at det er god kontakt mellom tilbydere og oppdragsgivere ved utvikling av slike kurs, slik at tilbudene blir i samsvar med arbeidsmarkedets behov.

Regjeringen mener både studiepoenggivende etter- og videreutdanning, sertifiseringskurs og andre målrettede IKT-sikkerhetskurs er nødvendig. Skal vi på kort sikt ha mulighet til å heve IKT-sikkerhetskompetansen i samfunnet, må det være et bredt tilbud tilpasset ulike brukere. Det fordrer at utdanningsinstitusjoner og kurstilbydere har tilstrekkelig kapasitet og tilbud, og at arbeidsgivere setter av ressurser til at ansatte kan ta etter- og videreutdanning.

Regjeringen oppfordrer arbeidsgivere i både offentlig og privat sektor til å prioritere etter- og videreutdanning av medarbeidere for bygge tilstrekkelig IKT-sikkerhetskompetanse i virksomhetene.

8.6 Kompetansen i tilsyn

Tilsyn er et virkemiddel for myndighetene for å etterse at regler og krav etterleves av virksomhetene. Den tekniske utviklingen og kontinuerlige endringer i måten IKT-systemer brukes, leveres og driftes på, krever økt IKT-sikkerhetskompe-

tanse hos tilsynsmyndigheter. Blant annet peker Lysneutvalget på dette i sin utredning. Det er i dag et potensial for økt samarbeid mellom tilsynene om IKT-sikkerhet for å bedre kompetansen.

For å forbedre IKT-sikkerheten og kvaliteten på IKT-sikkerhetstilsyn som gjennomføres i de ulike sektorene, vil Justis- og beredskapsdepartementet og Forsvarsdepartementet utrede og etablere en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter. Hensikten er å bidra til informasjonsutveksling og kompetanseoverføring og på denne måten øke kvaliteten på sektorenes tilsyn med IKT-sikkerhet. NSM vil lede arenaen. Se også punkt 22.7.

Det er et mål at tilsynene selv skal ha økt kompetanse til å utføre tilsyn på IKT-sikkerhetsområdet. NSM skal, sammen med sektortilsynene, vurdere å etablere en sentral kapasitet med IKT-sikkerhetskompetanse som skal benyttes som en ressurs for tilsynsmyndighetene. Denne sentrale kapasiteten kan bestå av personer fra tilsynene. Det kan også vurderes om det finnes kommersielle tilbud som kan avhjelpe en eventuell kompetansemangel.

8.7 Øvelser

Øvelser er et nyttig virkemiddel for å bli bedre til å forebygge, avdekke og håndtere uønskede digitale hendelser. Alle aktører og virksomheter som har ansvar for kritiske samfunnsfunksjoner, og som er avhengige av fungerende IKT-infrastruktur og -tjenester, har et eget ansvar for å gjennomføre øvelser. Mange større nasjonale tverrsektorielle øvelser i regi av DSB har hatt digitale sårbarheter som en del av øvelsene. Digitale sårbarheter var hovedtema i den nasjonale øvelsen IKT16 og i Nkoms nasjonale cyberøvelse for ekom- og kraftsektoren (NCEK 2015).

Flere av anbefalingene fra Lysneutvalget trekker frem øvelser som et virkemiddel for å redusere den digitale sårbarheten. I del III i denne meldingen beskrives øvelser som viktige tiltak for flere sektorer når status på anbefalingene fra Lysneutvalget blir gjennomgått.

Læring etter øvelser er krevende. Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* legger vekt på systematisk oppfølging og læring etter både øvelser og hendelser. Regjeringen ønsker størst mulig læringsutbytte fra øvelser og hendelser. Regjeringen vil derfor innføre nye krav til oppfølging av funn fra hendelser og øvelser i den statlige forvaltningen i sivil sektor.

Alle hendelser og øvelser skal i utgangspunktet evalueres. Funn og læringspunkter skal følges opp gjennom en ledelsesforankret tiltaksplan. Oppfølging av øvelser og hendelser skal ikke anses som avsluttet før alle punktene i tiltaksplanen er fulgt opp tilfredsstillende eller utkvittert gjennom en ledelsesforankret vurdering. Resultater av oppfølgingen av øvelser og hendelser over en viss størrelse eller alvorlighetsgrad skal rapporteres til overordnet instans.

Justis- og beredskapsdepartementet vil sammen med øvrige relevante departementer legge økt vekt på å benytte også internasjonale øvelser til å trene forebygging og håndtering av digitale hendelser, særlig øvelser i NATO-regi (se boks 8.2 om NATO og øvelser).

Boks 8.2 NATO og øvelser

NATOs krisehåndteringsøvelse Crisis Management Exercise øver opp alliansens strategisk-politisk nivå, i hovedstedene og i NATOs organisasjon. Scenarioene for øvingsrekken varierer fra år til år mellom krisehåndteringsoperasjoner i fredstid og kollektivt forsvar. Beskyttelse mot digitale trusler er ofte blant elementene som øves. Deltakere i øvelsene, foruten NATO-institusjonene og medlemslandene, kan eksempelvis være NATOs partnerland og observatører fra humanitære organisasjoner og EU. Øvingsrekken har vært gjennomført siden 1992.

NATOs årlige cyberøvelse på operativt nivå, Cyber Coalition, har som målgruppe de miljøene i NATO og medlemslandene som skal håndtere cyberhendelser, på operativt og delvis teknisk nivå. Cyber Coalition 2016 var alliansens så langt største øvelse på området, med deltakelse fra 27 NATO-land og partnerland foruten deltakelse fra EU, industriaktører og akademia. Øvingsrekken har vært gjennomført siden 2008.

9 Kritisk IKT-infrastruktur

Vårt samfunn består av en rekke kritiske samfunnsfunksjoner, som energiforsyning, finansielle tjenester og satellittbaserte tjenester. Dette er funksjoner som må opprettholdes til enhver tid av hensyn til samfunnets og befolkningens grunnleggende behov. En rekke av disse samfunnsfunksjonene forutsetter at man har en IKT-infrastruktur som virker nær sagt overalt og hele tiden.

IKT-infrastrukturer består av både informasjons- og kommunikasjonsinfrastrukturer (internettjenester, elektroniske kommunikasjonsnett etc.) og informasjons- og kommunikasjonssystemer som er en del av den kritiske samfunnsfunksjonen.[1] Det kan eksempelvis være sentrale styrings- og kontrollsystemer, administrative systemer og logistikksystemer.

Beskyttelse av kritisk IKT-infrastruktur er et av hovedsatsingsområdene til EUs byrå ENISA. Alle medlemsland i EU oppfordres til å prioritere dette i sine nasjonale IKT-sikkerhetsstrategier. NATO setter også i større grad enn tidligere sivilt beredskapsarbeid og sivilt–militært samarbeid på dagsordenen. Sivil beredskap, krisehåndtering og robuste samfunnskritiske funksjoner er en forutsetning for det enkelte lands og dermed alliansens samlede beredskap og forsvar.

Regjeringen er opptatt av at kritisk IKT-infrastruktur må være robust og pålitelig, slik at uønskede hendelser i størst mulig grad unngås, samtidig som man raskt må kunne gjenopprette normalsituasjonen ved en uønsket hendelse. Vi må også være i stand til å sikre at uvedkommende ikke får tilgang til informasjonen som formidles gjennom slik infrastruktur. Beskyttelse av kritisk IKT-infrastruktur er sentralt i det arbeidet regjeringen gjør innenfor IKT-sikkerhet. En del av dette arbeidet er å delta på internasjonale arenaer (se boks 9.1 om Meridian).

Lysneutvalget trekker frem den nasjonale infrastrukturen for elektronisk kommunikasjon (ekom) som en sentral komponent som inngår i nær sagt alle digitale verdikjeder.[2] I tråd med anbefalingene fra Lysneutvalget og Samferdselsdepartementets oppfølging av ekomplanen[3] ble Nkom gitt i oppdrag å vurdere sårbarhetsreduserende tiltak knyttet til samfunnets og samfunnskritiske funksjoners avhengighet av Telenors kjerneinfrastruktur, og hvordan ulike transportnett og utlandsforbindelser kan kombineres for å øke den samlede nasjonale kapasiteten og sikkerheten i ekomnettene. I rapporten *Robuste og sikre nasjonale transportnett – Målbilder og sårbarhetsreduserende tiltak* fra april 2017 følger Nkom opp oppdraget og redegjør for dagens situasjon, forventet utvikling i markedet og hva som må til av eventuelle regulatoriske og budsjettmessige tiltak for å heve sikkerheten i de norske ekomnettene. Rapporten er et viktig kunnskapsgrunnlag for regjeringens videre arbeid på området.

I tillegg må virksomheter med ansvar for kritiske samfunnsfunksjoner som er sterkt avhengige av elektronisk kommunikasjon selv vurdere tiltak som kan redusere risikoen for utfall i kommunikasjonen.

Sentrale tiltak:

- prioritert midler til etablering av en pilot for alternativt kjernenett, jf. Meld. St. 33 (2016–2017) Nasjonal transportplan 2018–2029
- arbeide videre med konkretisering av mulige statlige tiltak som kan bidra til å legge til rette for flere fiberkabler til utlandet
- arbeide for et sterkt kommunikasjonsvern i Norge

[1] The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.

[2] Se også scenario om «Cyberangrep mot ekom-infrastruktur», Nasjonalt risikobilde (DSB, 2014). Scenarioet viser kritiske samfunnsfunksjoners avhengighet av ekominfrastrukturen.

[3] Meld. St. 27 (2015–2016) *Digital agenda for Norge.*

Boks 9.1 Meridian

Meridian er en årlig internasjonal møtearena for myndighetsrepresentanter som arbeider med nasjonal regelverksutvikling knyttet til beskyttelse av kritisk IKT-infrastruktur. Formålet med arenaen er å utveksle erfaringer for hvordan man håndterer nasjonale og globale utfordringer.

Meridian har bidratt til utformingen av «Good Practice Guide on CIIP for governmental policy-makers». Guiden gir en god oversikt over fremgangsmåten for å beskytte kritisk IKT-infrastruktur. Den er ment å være spesielt nyttig for land som skal i gang med en slik prosess for å identifisere og beskytte kritisk IKT-infrastruktur, men er også nyttig for land som har kommet lenger på feltet.

Norge skal være vertskap for den 13. konferansen i rekken, som vil bli holdt i Oslo i oktober 2017.

9.1 Alternative kjernenett og robusthet i de regionale transportnettene

Utbygging av norske ekomnett er i hovedsak finansiert og drevet av kommersielle utbyggere som selv velger utbyggingsstrategi og utformer egne tjenester og forretningsmodeller. Regjeringen og tilbyderne av elektronisk kommunikasjon gjennomfører for tiden omfattende tiltak for å styrke sikkerheten og robustheten i de norske ekomnettene. I Norge er det i dag bare Telenor som leverer et nasjonalt kjernenett utelukkende basert på egen infrastruktur. Andre sentrale tilbydere av transmisjon er avhengige av Telenor eller partnere for å klare å levere et nett med tilsvarende kapasitet, dekning, robusthet og uavhengighet. Selv om Telenors kjernenett bygges og driftes med en meget høy grad av sikkerhet, og over tid har vist stor pålitelighet, representerer avhengigheten til én enkelt aktørs nett en sårbarhet som bør håndteres. Regjeringen vil at Norge skal ha et sterkt og robust ekomnett, og er opptatt av å gjøre noe med denne sårbarheten.

I Meld. St. 33 (2016–2017) *Nasjonal transportplan 2018–2029* har regjeringen prioritert midler til etablering av en pilot for alternativt kjernenett i perioden 2018–2021. Pilotprogrammet skal demonstrere sikkerhetsbehovet og det kommersielle grunnlaget for å investere i kjernenett som konkurrerer med Telenors nett. Målet for pilotprogrammet er å etablere et fungerende marked for alternative kjernenett som samfunnskritiske virksomheter og andre brukere kan benytte.

For å realisere målet med pilotprogrammet, og på sikt legge til rette for et reelt fullverdig alternativ til Telenors transportnett, mener Nkom at det er aktuelt å se nærmere på følgende kategorier av tiltak:[4]

- Altibox, Broadnet og Telenor reserverer mørk fiber/bølgelengde hos hverandre på spesielt utsatte strekk for å styrke egen robusthet
- Statlig støtte til nye fiberkabler i strategisk viktige områder i samarbeid med Telenor, Broadnet, Altibox, Forsvaret (Nord–Sør, Vestlandet, Finnmark)
- Statlig støtte til å tilrettelegge for ekstra redundans og tilbyderdiversitet på transportnettdelen av mobilnettene

Nkoms vurdering er at det er behov for å etablere flere sammenhengende fiberforbindelser på sentrale strekk mellom ulike regioner av landet som er viktige for nasjonal beredskap og sikkerhet. Tiltakene begrenses mot investeringer som tilbyderne selv må gjøre for å kunne levere en forsvarlig ekomtjeneste til sine brukere. Regjeringen vil arbeide sammen med ekomtilbyderne for å knytte sammen spesielt viktige strekk i eksisterende fibernett.

9.2 Utenlandsforbindelser

Nkom leverte i 2016 en rapport[5] om tilgangen til fiberinfrastruktur i Norge og føringer ut av landet. Rapporten viser at det er bra tilgang til alternative fiberføringer i store deler av landet, men ikke overalt. Rapporten viser også at det meste av den internasjonale trafikken rutes via osloområdet og videre ut i verden gjennom Sverige.

Etablerte tilbydere av transmisjon har foreløpig ikke ønsket å endre på dagens trafikkhåndtering mot utlandet. Tilbyderne viser begrenset interesse for og vilje til å ta i bruk nye føringsveier ut av landet. Regjeringen vil arbeide videre med konkretisering av mulige statlige tiltak som kan bidra til å legge til rette for flere fiberkabler til utlandet.

---

4 Nkom, 2017, *Robuste og sikre nasjonale transportnett – Målbilder og sårbarhetsreduserende tiltak*.

5 Nkom, 2016, *Kartlegging og vurdering av infrastruktur som kan nyttiggjøres av datasentre*.

9.3 Nød- og beredskaps-kommunikasjon

Nød- og beredskapsaktører er avhengige av gode og sikre kommunikasjonsløsninger i sitt daglige virke og i kriser. Med Nødnett har disse aktørene en god løsning for sikret talekommunikasjon.

Nød- og beredskapsaktørers behov, også for data, kan fordre nye løsninger. Både teknologiutviklingen og utviklingen i trusselbildet peker i retning av at nød- og beredskapsetater vil ha behov for mobile bredbåndsløsninger med høy grad av sikkerhet og robusthet. Det vil kreve betydelig involvering og ressurser fra statlig side for å realisere en fremtidig løsning for sikre og robuste mobile bredbåndstjenester for nødetatene. Staten må ta ansvar for å legge til rette for tilfredsstillende rammer og tjenester til dette formålet uansett om behovene skal realiseres over de kommersielle ekomnettene, gjennom et eget nett for nød- og beredskapsetater eller gjennom en kombinasjonsløsning.

Regjeringen har gjennom ekomplanen uttrykt et mål om at de offentlige ekomnettene i størst mulig grad skal kunne bære fremtidige tjenester for nød- og beredskapsetater. Regjeringen har videre besluttet at frekvensressurser i 700 MHz-båndet skal tas i bruk til mobile tjenester når de blir tilgjengelige. Nkom har dialog med blant annet DSB og Forsvarsmateriell om relevante problemstillinger og behov, og ulike løsningsmodeller vurderes opp mot samfunnsøkonomisk kost/nytte. IKT-sikkerhetshensyn som integritet, konfidensialitet og tilgjengelighet og særskilt funksjonalitet for denne brukergruppen er viktige vurderingstemaer.

9.4 IKT-sikkerhet i styrings- og kontrollsystemer

Mange av de viktige funksjonene i samfunnet forutsetter døgnkontinuerlig drift av automatiske styrings- og kontrollsystemer. Teknologien som benyttes i disse, er en blanding av vanlig IKT-utstyr og spesialiserte datamaskiner (automatiseringsutstyr). I del III omtales slike samfunnsfunksjoner i kapitlene om energiforsyning, olje og gass, vannforsyning og transport. Dette utstyret har mange av de samme sårbarhetene som vanlig

Figur 9.1 Styringssystemer.

Illustrasjon: M. Sylstad, NSM.
Kilde: Bilde hentet fra Colourbox.

IKT-utstyr, men behovet for døgnkontinuerlig drift og at det benyttes i virksomheter som ikke nødvendigvis har en robust IKT-avdeling, medfører at de er mer sårbare.

Selve styringssystemene trenger sjelden å være koblet til den enkelte virksomhets datanettverk, men slik kobling opprettes ofte fordi det er et ønske om å kunne utføre vedlikehold eller feilsøking, eller for å benytte driftsdata til rapportering og vedlikeholdsstyring. Denne sammenkoblingen medfører at sårbarhetene i styringssystemene er eksponert. Virksomheter må være bevisste på hvordan styrings- og kontrollsystemer sikres og følges opp, og søke å samarbeide for å øke kunnskapen innenfor fagområdet.

9.5 Personvern og kritisk IKT-infrastruktur – kommunikasjonsvern

Kommunikasjonsvern som begrep omfatter rettslig og faktisk beskyttelse av informasjon i transitt, på vei fra ett sted til et annet. Begrepet omfatter også opplysninger om slik informasjon eller kommunikasjon, såkalte metadata. Kommunikasjonsvernet er ofte ansett som en del av det videre begrepet personvern, siden man vanskelig kan tenke seg et effektivt personvern uten at også kommunikasjonen mellom to eller flere parter kan være fortrolig.

Bruk av elektronisk kommunikasjon gir informasjon om en rekke forhold som berører den enkeltes private sfære og personlige integritet, slik som geografisk bevegelsesmønster, kontaktnett osv. Presset om å få tilgang til denne typen data øker også etter hvert som den kommersielle bruken av såkalt stordata øker. Dagens kommunikasjonsvern er bra i Norge, men ny teknologi, nye tjenester og forretningsmodeller utfordrer regelverket.

Ekomtjenester produseres i økende grad i datasentre utenfor norsk territorium. Norsk regulering er derfor ikke alltid tilstrekkelig dersom man ønsker å gjennomføre tiltak for å ivareta personvernet og kommunikasjonsvernet til den enkelte bruker i Norge. Regjeringen vil at Norge skal fortsette å arbeide internasjonalt for å fremme gode løsninger som ivaretar norske brukere.

Figur 10.1

Illustrasjon: M. Sylstad, NSM.
Kilde: Bilde hentet fra Colourbox.

Del III
Oppfølging av Lysneutvalgets anbefalinger

10 Elektronisk kommunikasjon

10.1 Redusere kritikaliteten av Telenors kjerneinfrastruktur

Problembeskrivelse (NOU 2015: 13, punkt 11.7.1)

Telenors kjerneinfrastruktur inngår som en komponent i nær sagt alle digitale verdikjeder. Et utfall i denne kan derfor få alvorlige og samtidige konsekvenser på de aller fleste samfunnsområder, og for kritiske samfunnsfunksjoner. Telenors kjerneinfrastruktur er godt utbygd, den er profesjonelt drevet, og den har historisk sett meget høy stabilitet. Likevel vil infrastrukturen kunne settes ut av spill ved menneskelige feil, rutinesvikt, sabotasje, terror eller utro tjenere. Den totale summen av samfunnsverdier dette nettet bærer, er uakseptabelt høy. Det anbefales at det arbeides mot et målbilde der minst én tilleggsaktør har et landsdekkende kjernenett som er på samme nivå som Telenors med hensyn til dekning, kapasitet, fremføringsdiversitet, redundans og uavhengighet. I Lysneutvalgets utredning anslås kostnadene ved å etablere et alternativt kjernenett til 575 millioner kroner.

Status på tiltak

Utvalgets vurderinger av kritikaliteten av Telenors kjerneinfrastruktur får mye støtte i høringsrunden. I Meld. St. 33 (2016–2017) *Nasjonal transportplan 2018–2029* har regjeringen prioritert midler til etablering av en pilot for alternativt kjernenett i perioden 2018–2021. Pilotprogrammet skal vise sikkerhetsbehovet og det kommersielle grunnlaget for å investere i konkurrerende kjernenett til Telenors nett. Det vises til nærmere omtale av status på tiltaket under punkt 9.1.

10.2 Sikre mangfold blant leverandørene til infrastrukturen

Problembeskrivelse (NOU 2015: 13, punkt 11.7.2)

Det bør tilstrebes å ha en kontrollert heterogenitet i utstyrsleverandørbildet i norsk ekominfrastruktur. Nasjonal kommunikasjonsmyndighet (Nkom) bør i samråd med Konkurransetilsynet ta initiativ til å utrede hvorvidt vi i dag har tilstrekkelige virkemidler for å ivareta dette, eller om det er behov for å etablere virkemidler for å sikre diversitet i utstyr. Denne problemstillingen bør også tas med i utformingen av ny sikkerhetslov (del II).

Status på tiltak

Leverandørbildet i ekombransjen endrer seg over tid. De største produsentene av avansert teleutstyr har tidligere vært fra USA og Europa, men de siste årene har vi sett at stadig mer av det mest avanserte utstyret produseres og leveres av asiatiske selskaper. Ekomtilbyderne velger selv hvilke leverandører de vil benytte, og det er de som må svare for sikkerheten i sine nett og for sine kunder. Dette gjelder uansett om leverandørene kommer fra et land Norge har et sikkerhetspolitisk samarbeid med, eller ikke.

For ekomtilbyderne kan det ha både fordeler og ulemper å knytte seg til én enkelt leverandør av utstyr og tjenester. Ekomtilbyderne kan oppnå lavere driftskostnader og raskere teknologiutvikling, men kan også bli avhengige av leverandøren på både pris og teknologiutvikling. Ikke minst kan de bli sårbare for feil knyttet til én leverandør. Tilbyderne bør derfor se seg tjent med å benytte flere leverandører i sine nett. Ekommyndighetene (Samferdselsdepartementet og Nkom) følger utviklingen i leverandørbildet og gir råd og veiledning, blant annet i Ekomsikkerhetsforum.[1] Sårbarheter som ikke kan håndteres i Ekomsikkerhetsforum, kan løftes til Nkom og Samferdselsdepartementet.

Etter Samferdselsdepartementets vurdering er ikke konkurranseregelverket egnet til å løse de utfordringene som utvalget trekker frem. Formålet med konkurransereguleringen er å ivareta konkurransen i markedet og effektiv ressursbruk. For å unngå å låse seg har ekomtilbydere gjerne mer enn én leverandør av kritiske komponenter.

[1] Et forum der private ekomtilbydere og sikkerhetsmyndigheter deler relevant informasjon.

I NOU 2016: 19 *Samhandling for sikkerhet* behandles problemstillingen i forbindelse med en bredere diskusjon om leverandørsikkerhet, se nærmere utredningen kapittel 11 og 12 om henholdsvis sikkerhetsgraderte anskaffelser og eierskapskontroll. Utvalget anerkjenner problemstillingen og ser den i sammenheng med utfordringer knyttet til utenlandsk eierskap med strategisk viktige selskaper, herunder blant annet forsyningssikkerhet. Det vises i utredningen blant annet til Meld. St. 9 (2015–2016) *Nasjonal forsvarsindustriell strategi*. For virksomheter underlagt sikkerhetsloven gjelder allerede i dag regler som gir mulighet for kontroll med leverandører som får tilgang til skjermingsverdig informasjon eller objekt, jf. sikkerhetsloven kapittel 7. I tillegg foreslår utvalget nye regler som gir myndighetene mulighet for kontroll med eierskapet i strategisk viktige selskaper, jf. lovforslaget kapittel 10.

10.3 Opprette en CSIRT i ekomsektoren i regi av Nkom

Problembeskrivelse (NOU 2015: 13, punkt 11.7.3)

De fleste tilbydere av elektroniske kommunikasjonstjenester i Norge er svært små, og de færreste eier eget nett. Det er nødvendig med en god overgripende håndtering av hendelser i det digitale rommet som favner alle disse små tilbyderne av elektroniske kommunikasjonstjenester. Utvalget anbefaler et «Computer Security Incident Response Team» (CSIRT) med organisatorisk oppheng hos Nkom.

Status på tiltak

Nkom CSIRT ble satt i operativ prøvedrift fra 1. april 2016 ved Nkom i Lillesand. Nkom CSIRT vil være i operativ drift fra 1. juli 2017.[2] Nkom CSIRT ble etablert etter en vurdering av sterke og svake sider ved alternative organisasjonsformer sett i lys av mulige ambisjonsnivåer for ekomsektorens fremtidige responsmiljø. CSIRTs uavhengighet av tilsynsmyndigheten ble vurdert opp mot fordelene med gjensidig nytteverdi av samlokalisering og mulighet for informasjonsutveksling og tilgang til kompetanse. Funksjon og behov for et responsmiljø ble drøftet med de største ekomtilbyderne.

Nkom CSIRT bemannes fra oppstart med fem årsverk og skal bistå ved håndtering av alvorlige hendelser innenfor sektoren samt være bindeledd mellom ekomsektoren og NSM ved sektorovergripende hendelser. Uavhengig av hendelser vil Nkom CSIRT bistå med rådgivning, kompetansebygging og informasjonsdeling og bidra til høyt tillitsnivå og aktørsamarbeid innenfor sektoren. Se nærmere omtale av tiltak for avdekking og håndtering av digitale angrep, herunder informasjonsdeling med NSM, i kapittel 7.

10.4 Aktiv myndighetsutøvelse fra Samferdselsdepartementet og Nasjonal kommunikasjonsmyndighet

Problembeskrivelse (NOU 2015: 13, punkt 11.7.4)

Ekommyndigheten må styrke innsatsen ytterligere ved å veilede tilbyderne om innholdet i rettslige standarder knyttet til sikkerhet og robusthet. En forsvarlig kobling mellom sentrale ekomaktører og de nasjonale sikkerhetstjenestene er helt nødvendig for å ivareta nasjonale sikkerhetsbehov, og det anbefales at dette arbeidet videreutvikles gjennom Ekomsikkerhetsforum.

Det kan være ønskelig med en bredere fremtidig ekomplan som også omfatter ekomperspektivet på tvers av sektorer i Norge, inkludert blant annet Nødnett og fremtidige behov for nødkommunikasjon. Denne bør ta inn over seg hvordan krav til ekomnett og -tjenester gjenspeiler samfunnets økende behov for digitale tjenester. Planen bør inneholde en systematisk oversikt som jevnlig viser hvordan ulike forebyggende tiltak bør prioriteres. Denne oversikten på ekomområdet bør videre benyttes som et bidrag i Justis- og beredskapsdepartementets større oversiktsbilde over IKT-sårbarhet i Norge.

Status på tiltak

Ekomloven setter funksjonelle krav til sikkerhet i ekomnett og -tjenester. Tilbyderne skal tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for sine brukere i fred, krise og krig. Reguleringen krever at tilsynsmyndighetene også må bidra med veiledning og krav, i tillegg til å ha tilsyn med om kravene følges opp. Dette er et vedvarende arbeid som hele tiden må utvikles.

Ekommyndigheten bruker i økende grad ressurser på aktiv veiledning av aktørene i bransjen. Det er viktig at myndigheten kommer tidlig inn i vurderinger tilbyderne gjør om for eksempel tjenestearkitektur, sourcingstrategier med mer. Veiledningsprosessen kan i enkelte tilfeller bli fulgt opp med tilsyn.

[2] Nytt navn fra 1. juli 2017 vil være EkomCERT.

I 2016 fremmet Samferdselsdepartementet en ekomplan for Stortinget som en del av regjeringens samlede IKT-politikk.[3] Samferdselsdepartementet vil vurdere om ekomplanen bør følges opp med en bredere ekomplan og strategi for samfunnets bruk og avhengighet av elektronisk kommunikasjon i tråd med Lysneutvalgets forslag.

Nkom har med innspill fra DSB og Forsvaret allerede gjort vurderinger om å benytte 700 MHz-båndet for mobile datatjenester til nød- og beredskapsaktører. Det ses nå på ulike løsningsmodeller som vurderes opp mot samfunnsøkonomisk kost/nytte. DSB vektlegger at vurderingen må ta hensyn til krav til IKT-sikkerhet som integritet, konfidensialitet og tilgjengelighet og særskilt funksjonalitet for denne brukergruppen.

10.5 Etablere tiltak for å regulere utlevering av trafikkdata til politiet

Problembeskrivelse (NOU 2015: 13, punkt 11.7.5)

Omfanget av politiets uthenting av trafikkdata er rimelig stabilt, mens andelen forespørsler om opphevelse av taushetsplikt for utlevering av signaleringsdata er sterkt økende. Det er mange spørsmål knyttet til forholdet mellom beslutninger om opphevelse av en taushetsplikt med hjemmel i straffeprosessloven § 118 jf. § 230 og menneskerettsloven § 2 jf. den europeiske menneskerettskonvensjonen artikkel 8.

Utvalget mener at formålsutglidning når det gjelder bruk av opplysninger (særlig signaleringsdata), bør utredes. I denne sammenheng bør også dommernes tekniske kompetanse som grunnlag for å ta stilling til innsynsbegjæringer vurderes. Utvalget mener det er behov for å avklare hjemmelsgrunnlaget for regulering av tilgang til signaleringsdata. Utvalget er videre av den oppfatning at bruk av signaleringsdata er blitt så utbredt som etterforskningsverktøy at det bør vurderes å lovregulere dette som et særskilt tvangsmiddel.

Status på tiltak

Spørsmålene om hjemmelsgrunnlaget for signaleringsdata og bruk av signaleringsdata som særskilt tvangsmiddel er vurdert i Prop. 68 L (2015–2016) *Endringer i straffeprosesslover mv. (skjulte tvangsmidler)*. I forbindelse med lovendringene ble hjemmelsgrunnlaget for politiets tilgang til lokasjons- og signaleringsdata i noen grad avklart. Det ble vedtatt et tillegg i § 216 b annet ledd bokstav d om kommunikasjonskontroll som gir politiet hjemmel til å innhente historiske opplysninger fra nett- og tjenestetilbydere om den geografiske plasseringen til et bestemt kommunikasjonsanlegg (lokaliseringsdata), uavhengig av om anlegget er i bruk til kommunikasjon. At politiets tilgang på lokaliseringsdata nå er regulert i straffeprosesslovens kapittel om kommunikasjonskontroll, medfører at politiets bruk av tvangsmiddelet er underlagt domstolskontroll og etterfølgende kontroll av Kontrollutvalget for kommunikasjonskontroll. Lysneutvalget pekte på at det kan være en utfordring for dommere å ha tilstrekkelig teknisk innsikt når de vurderer anmodninger om tilgang til data. Prop. 68 L (2015–2016) behandler ikke denne problemstillingen. Lovendringene innebærer imidlertid at det ikke lenger er samme grunn til å skille mellom de ulike «typer» data.

I tillegg til å benytte reglene om kommunikasjonskontroll kan politiet benytte den utenrettslige ordningen med opphevelse av teletilbydernes taushetsplikt fra Nkom for å få utlevert trafikkdata, herunder signaleringsdata. I 2015 behandlet retten 189 kommunikasjonskontrollsaker, mens Nkom behandlet 1459 saker om fritak for taushetsplikt. Nkom behandler anmodninger om signaleringsdata etter samme regelsett som anmodninger om fritak fra taushetsplikten for trafikkdata, dvs. straffeprosessloven § 118 jf. § 230. Reglene om Nkoms opphevelse av taushetsplikten gjelder også ved beslag eller utleveringspålegg, jf. straffeprosessloven § 203 flg. og § 210. I medhold av § 118 første ledd annet punktum skal Nkom gi samtykke i disse sakene med mindre dette vil utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold. Nkom baserer seg i denne sammenheng på fremstillingen som gis av påtalemyndigheten, eventuelt sammen med annen informasjon som innhentes ved behandlingen av saken. Det kan ikke utelukkes at dagens ordning, hvor opphevelse av taushetsplikten gjøres av Nkom etter straffeprosessloven og ekomloven, kan utfordre kommunikasjonsvernet. Regjeringen vil på denne bakgrunn vurdere om det er behov for ytterligere utredning av kommunikasjonsvernet i norsk rett i forbindelse med implementeringen av EUs nye kommunikasjonsvernforordning, som er til behandling i EU rådet og parlamentet, med planlagt ikrafttredelse våren 2018.

[3] Meld. St. 27 (2015–2016) *Digital agenda for Norge*.

11 Satellittbaserte tjenester

11.1 Tydeliggjøre myndighetsansvar for norsk romvirksomhet

Problembeskrivelse (NOU 2015: 13, punkt 12.5.1)

Satellittbaserte tjenester er en kritisk samfunnsfunksjon. De fleste samfunnsområder er avhengige av digitale satellittbaserte tjenester. Disse tjenestene kan være posisjon, navigasjon, presis tidsangivelse, kommunikasjon, jordobservasjon med mer. Reguleringen av romvirksomheten er hjemlet i ulike lover og forskrifter, og ansvaret for oppfølging av romsektoren er desentralisert. Myndighetsbildet knyttet til området er komplekst, og det anbefales at myndighetsansvaret for romvirksomheten blir tydeliggjort. Hensikten med en slik tydeliggjøring er å øke bevisstheten om sårbarheter, identifisere avhengigheter og stille krav til et sikkerhetsarbeid som evner å se langs hele verdikjeder og dekker helhet og bredde i romvirksomheten.

Lysneutvalget anbefaler at det opprettes en mindre enhet som får i oppgave å vurdere hva som per i dag eksisterer av lover, regler og tilsyn for satellittbaserte tjenester, og deretter utlede hva som må etableres av nytt regelverk, retningslinjer eller tilsynsbehov. Basert på egne vurderinger og en utredning fra Oslo Economics anbefaler utvalget at ansvaret legges til enten Nkom eller DSB. Utvalget mener det kreves en egen vurdering for å kunne beslutte hvilken av disse enhetene som skal ivareta dette ansvaret.

Status på tiltak

Det er stor enighet blant høringsinstansene om at det er nødvendig å tydeliggjøre myndighetsansvaret innenfor romvirksomheten. Majoriteten av høringsuttalelsene støtter imidlertid ikke anbefalingen fra Lysneutvalget om å vurdere å opprette et nytt organ, eller peke ut ett enkelt organ, med særskilt ansvar for å følge opp romvirksomheten på nasjonalt, tverrsektorielt nivå.

Oppfølging av Lysneutvalgets tilrådning om å avklare myndighetsansvaret for norsk romvirksomhet er behandlet i det interdepartementale koordineringsutvalget for romvirksomhet (IKU), ledet av Nærings- og fiskeridepartementet. På bakgrunn av bred enighet i utvalget ble det i 2016 opprettet et underutvalg for sikkerhet under IKU (IKU-S). Formålet med IKU-S er å styrke informasjonsutveksling mellom departementer og etater, slik at tverrsektorielle sårbarheter og sikkerhetstrusler blir synliggjort. Videre har Norsk Romsenter fått i oppdrag av Nærings- og fiskeridepartementet å forestå en kartlegging av dagens plassering av myndighetsansvar samt mulige synergier mellom ulike aktører med slikt ansvar. Departementene i IKU-S har ansvar for å innhente og samordne bidrag fra egen sektor til kartleggingen.

For øvrig har Samferdselsdepartement gitt Norsk Romsenter i oppgave å utarbeide en nasjonal, tverretatlig og tverrsektoriell PNT-strategi (posisjonsbestemmelse, navigasjon og tidsbestemmelse). Strategien skal ta utgangspunkt i dagens situasjon og gi retning for utvikling og anvendelse av bakkebaserte og satellittbaserte navigasjonssystemer i de kommende 10–15 årene. Arbeidet skal ferdigstilles innen juni 2017.

12 Energiforsyning

12.1 Styrke tilsyn og veiledning i IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 13.7.1)

Norges vassdrags- og energidirektorat (NVE) har begrenset kapasitet til å følge opp med tilsyn innenfor IKT-sikkerhet og sårbarhet. Det foreslås å styrke NVE betraktelig på området tilsyn og veiledning.

Et generelt utviklingstrekk er at det legges opp til stadig tettere koblinger mellom driftskontrollsystemer og forretningssystemer. NVE bør kunne spille en viktig rolle i å formidle mønsterpraksis og for øvrig veilede berørte virksomheter i sikker implementering.

Det er i kraftbransjen, som i andre bransjer, en økt trend mot tjenesteutsetting. NVE bør i fellesskap med interesseorganisasjoner og bransjen utarbeide veiledere og krav til tjenesteutsetting i kraftbransjen. Sektoren anbefales å se på internasjonale standarder.

Status på tiltak

IKT-sikkerhet er et prioritert saksområde for NVE. NVE har bygd opp et saksbehandlingsteam som har kompetanse som er essensiell for det viktige arbeidet med tilsyn, veiledning og regelverksutvikling for IKT-sikkerheten i kraftsektoren. Det er viktig å opprettholde dette fagmiljøet og i et langsiktig perspektiv ytterligere styrke direktoratets kompetanse på IKT-sikkerhet. Totalt har NVE økt personellkapasiteten på IKT-sikkerhet med to årsverk. Se også redegjørelsen for etablering av en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter i punkt 22.7.

NVE er engasjert i utviklingsarbeid som grunnlag for å drive veiledning på IKT-sikkerhet. På dette området samarbeider NVE med andre myndigheter, med bransjen og med leverandører.

Det er planlagt tilsyn med driftskontrollsystemer i 2017. Olje- og energidepartementet har i tildelingsbrevet for 2017 bedt NVE om å vurdere sektorens regelverk og tilhørende veiledning med tanke på å styrke IKT-sikkerheten. I 2016 startet NVE et IKT-regelverksprosjekt som har vurdert eksisterende krav til IKT- og driftskontrollsikkerhet. IKT-regelverksprosjektet avsluttes i 2017. Prosjektet har vurdert behov for grunnsikring for alle virksomheter, inkludert sikring ved tjenesteutsetting av IT og strengere sikringskrav til avanserte måle- og styringssystemer (AMS) og driftskontrollsystemer.

IKT-regelverksprosjektet har også vurdert eksisterende regelverk opp mot internasjonale standarder og andre lands regulering. Arbeidet viser at dagens beredskapsforskrift har stor grad av samsvar med ISO 27001/2-standarden for informasjonssikkerhetsledelse, og at Norge gjennom beredskapsforskriften har et godt regelverk for IKT-sikkerhet i energisektoren.

NVE vil følge opp resultatene fra IKT-regelverksprosjektet med forskriftsarbeid og utvikling av veiledere i 2017. NVE etablerte i 2016 et nært samarbeid med NSM, og videre samarbeid inkluderer blant annet utvikling av veiledere til forskrift.

12.2 Stimulere til større og mer ressurssterke fagmiljøer innen IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 13.7.2)

Flere enheter i Kraftforsyningens beredskapsorganisasjon (KBO) er små med få ansatte, og det er en kompetanseutfordring å etablere og opprettholde nødvendige fagmiljøer. NVE bør i samarbeid med interesseorganisasjonene stimulere til større og mer ressurssterke fagmiljøer på IKT-sikkerhet i KBO-enhetene.

Bransjeorganisasjonene har et veletablert system for kurs og opplæring. De bør kunne bidra med å organisere kurs innenfor IKT-sikkerhet, gjerne i samarbeid med andre organisasjoner, eller henvise til NVE, andre myndigheter eller undervisningsinstitusjoner der det er hensiktsmessig. Det bør også utvikles kurs og studieretninger innenfor prosesstyring, systemintegrasjon og IKT.

Kompetansen knyttet til IKT-sikkerhet er varierende blant virksomheter i bransjen. Det anbefales at NVE gjennom sin veiledningsrolle er pådriver for flere øvelser på IKT-sikkerhetsområdet både i sektoren og opp mot andre sektorer det er naturlig å samarbeide med.

Status på tiltak

NVE har dialog med flere fagmiljøer, samarbeidsallianser og interesseorganisasjoner i energisektoren. NVE har gjennom IKT-regelverksprosjektet i 2016/2017 gjennomført flere idédugnader med bransjen og hatt tett kontakt med både kraftprodusenter, nettselskap og IT-leverandører.

NVE har som langsiktig ambisjon at det er etablert et godt samarbeid mellom bransjen og akademia om IKT-sikkerhet og sikkerhet i driftskontrollsystemer, noe Olje- og energidepartementet stiller seg bak. Samarbeidet kan skje gjennom at bransjen bidrar med bransjekunnskap og praktisk innsikt i forskning, undervisning og kursutvikling, og gjennom forskningsprosjekter der bransjen, myndighetene og akademia samarbeider. Tettere samarbeid vil bidra til at det utvikles relevante kurs og etterutdanningstilbud, og at det skapes og formidles ny kunnskap om hvordan virksomhetene i energisektoren beskytter seg mot digitale trusler.

NVE har i 2017 en strategisk satsing på kompetanseheving innenfor IKT-sikkerhet i energisektoren gjennom veiledning, samarbeid med akademia om FoU og utdanning og samarbeid med bransjeforeninger om kurs. NVE har også satt av midler til dette i 2017, inkludert utvikling av en handlingsplan for å heve kompetansen i bransjen. NVE vil også som en del av denne satsingen støtte IKT-sikkerhetsmiljøet ved NTNU CCIS med en bistilling i ca. 20 % som kan bidra med praktisk innsikt og bransjekunnskap ved utformingen av utdanningsopplegg og kurs innenfor IKT-sikkerhet, i første omgang for det akademiske året 2016/2017. Ordningen vil deretter bli evaluert.

NVE tilbyr også fagdager og seminarer for bransjen og driver generelt opplysningsarbeid gjennom foredragsvirksomhet. NVE vil i årene fremover utarbeide og gjennomføre øvelser knyttet til IKT-sikkerhet, noe Olje- og energidepartementet er positive til.

12.3 Bygge et sterkt operativt fagmiljø for IKT-hendelseshåndtering

Problembeskrivelse (NOU 2015: 13, punkt 13.7.3)

Bransjen bør ha et kompetent felles miljø for hendelseshåndtering som både kan koordinere hendelser internt i sektoren og være kontaktpunkt ut mot andre sektorer. Utvalget støtter ideen om å videreutvikle KraftCERT som et sterkt fagmiljø innenfor operativ hendelseshåndtering. NVE må tydeliggjøre krav om tilknytning til et operativt fagmiljø for hendelseshåndtering, enten mot KraftCERT eller mot andre miljøer. Virksomhetene bør ha en tydelig begrunnelse for det alternativet de velger. Det er viktig med avklarte roller mellom responsmiljøene, slik at kraftbransjen opptrer enhetlig overfor andre sektorer.

Status på tiltak

Det har vært viktig for sektoren å øke deteksjons- og håndteringsevnen og sammen med andre sektorer bidra til gode situasjonsbilder for IKT-sikkerhetstilstanden. NVE har vært en pådriver for opprettelsen av KraftCERT. Stadig flere energiselskaper knytter seg til KraftCERT, som i dag har 71 medlemmer. I dag utgjør NVE og KraftCERT til sammen sektorens responsmiljø. KraftCERT er et privat selskap som er etablert av bransjen, og som inngår i KBO etter vedtak fra NVE. Den eksisterende modellen er basert på samarbeid og informasjonsdeling.

NVE vil også arbeide for at KraftCERT fremstår som et faglig sterkt responsmiljø for kraftsektoren med relevante tjenester for bransjen og med et godt samarbeid med NVE. Det er en ambisjon at alle relevante aktører innenfor kraftsektoren benytter KraftCERT, noe Olje- og energidepartementet stiller seg bak, jf. omtale i Energimeldingen (Meld. St. 25 (2015–2016)).

NVE vurderer forslaget om å kreve tilknytning til et responsmiljø. Som en del av dette vurderer NVE om krav bør stilles generelt eller basert på hvor kritiske virksomhetene og systemene er for forsyningssikkerheten.

12.4 Vurdere de sikkerhetsmessige forhold ved å behandle og lagre kraftsensitiv informasjon i utlandet

Problembeskrivelse (NOU 2015: 13, punkt 13.7.4)

Hva som er kraftsensitiv informasjon og skal beskyttes særskilt, går frem av beredskapsforskriften. Samtidig forandrer teknologiutviklingen, økt systemintegrasjon og organisasjonsendringer hos leverandører mulighetsrommet for tjenesteutvikling. Dagens regelverk gir utfordringer for tjenesteutvikling og effektiv drift av kraftforsyningen. Det anbefales at NVE gjør en vurdering av hvilken informasjon som, gitt de endrede teknologiske og organisatoriske rammene, er så kritisk at den ikke bør lagres og behandles utenfor Norges grenser. NVE anbefales å se på hele verdikjeden og identifisere hvilken informasjon i denne som må være under nasjonal kontroll.

Status på tiltak

NVE har gjennom IKT-regelverksprosjektet vært i dialog med andre myndigheter og bransjen for å vurdere verdikjeden til energiforsyningen og dens sårbarheter og identifisere hvilken informasjon i verdikjeden som må være under nasjonal kontroll og lagring. Dette innebærer også å se på om beredskapsforskriften er tilpasset dagens situasjon. I dag regulerer beredskapsforskriften hvilken type informasjon som er å anse som kraftsensitiv, og setter krav til håndtering, beskyttelse og tilgang til kraftsensitiv informasjon. Informasjonen er underlagt taushetsplikt. NVE vil utrede om det er behov for ytterligere restriksjoner på lagring og tilgang til kraftsensitiv informasjon.

Helhetsvurdering av verdikjeder er nærmere omtalt i punkt 22.1 og tjenesteutsetting i punkt 6.4 og 22.10.

12.5 Gjennomføre risiko- og sårbarhetsanalyse for utvidet bruk av AMS

Problembeskrivelse (NOU 2015: 13, punkt 13.7.5)

Innen 1. januar 2019 skal alle strømkunder i Norge ha tatt i bruk smarte målere. De nye målerne inngår i «avanserte måle- og styringssystemer» (AMS), og det innebærer at brukerne får bedre informasjon om strømforbruket sitt, mer nøyaktig avregning og mulighet for automatisk styring av forbruket. Vedtak om innføring av AMS skjedde uten forutgående risiko- og sårbarhetsanalyse. Overgangen til AMS innebærer et stort potensial for økt nettnytte, innovasjon og effektivisering i sektoren. Ukritisk implementering av funksjonalitet som for eksempel knytter AMS tettere sammen med driftskontrollsystemer, vil medføre en sårbarhetsoppbygging med betydelig skadepotensial. Det er viktig med en god og bredt anlagt risiko- og sårbarhetsanalyse i forkant av teknologiskifter, ved bruksendringer og ved system- og organisasjonsendringer. NVE anbefales å gjennomføre nødvendige risiko- og sårbarhetsanalyser for utvidet bruk av AMS inn mot driftskontrollsystemene.

Status på tiltak

Denne problemstillingen følges opp i NVEs IKT-regelverksprosjekt. NVE har gjennomført tre prøvetilsyn på AMS i 2016 og utarbeider en oppdatert veileder til sikkerhet i AMS. NVE har tydeliggjort overfor bransjen at det er viktig å gjennomføre risikoanalyser ved innføringen av AMS, og at nettselskapene er ansvarlige for å sørge for tilstrekkelig sikkerhet i AMS-løsningen. Anbefalingen om at NVE skal gjennomføre risiko- og sårbarhetsanalyse før det vurderes utvidet bruk av AMS, støttes av Olje- og energidepartementet.

NVE vil innhente én eller to årlige rapporter om AMS fra alle nettselskapene i 2017 og 2018 der nettselskapenes vurdering av ulike risikokategorier, blant annet IKT-sikkerhet, inngår. NVE vil følge opp at nettselskapene ivaretar informasjonssikkerheten både under installasjon av AMS og senere i den løpende driften.

12.6 Utarbeide en oppdatert analyse av kraftforsyningens avhengighet av ekom

Problembeskrivelse (NOU 2015: 13, punkt 13.7.6)

Selv om kraftbransjen så langt har klart å håndtere kritiske situasjoner uten kommersiell ekom, kan denne evnen utfordres i fremtiden når enda mer IKT blir lagt til og integrert i kraftinfrastrukturen. NVE og bransjen anbefales å foreta en ny gjennomgang for å etterprøve om dagens krav gir den «uavhengigheten» som regelverket krever.

Status på tiltak

NVE har gjort en gjennomgang av dagens krav. Tematikken tas også opp når NVE gjennomfører revisjoner hos bransjen. Kraftforsyningen har flere barrierer og sikringstiltak for å hindre at sty-

ringsevnen blir borte. Kraftforsyningen har også et eget samband, i tillegg til offentlig kommunikasjonsnett. Drift, gjenoppretting og leverandørstøtte blir imidlertid mer krevende uten tilgang til de ordinære ekomtjenestene. NVE har derfor gitt pålegg til alle KBO-enheter om å styrke egen robusthet ved å ha flere tjenestetilbydere og løsninger for kommunikasjon. NVE følger opp hvordan nettselskapene har løst dette.

Flere KBO-enheter vurderer sin løsning for driftssamband. I den forbindelse vurderes også muligheten for å benytte Nødnett som driftsradio. Alle selskaper, også de som velger Nødnett, må oppfylle forskriftskrav til blant annet nødstrøm i driftssamband. Selskaper som velger å benytte Nødnett, må derfor stille krav til robustheten i Nødnett.

NVE vil i 2017 gjennomføre et FoU-prosjekt på fremtidens sikre løsninger for driftsradio. Dette prosjektet vil gi svar på hvordan kravet til KBO-enhetene om uavhengighet av offentlige kommunikasjonsnett kan ivaretas også i fremtiden.

13 Olje og gass

13.1 Overføre sikkerhetstradisjonen innen HMS til det digitale området

Problembeskrivelse (NOU 2015: 13, punkt 14.7.1)

Olje- og gassektoren har en lang sikkerhetstradisjon, en sterk sikkerhetskultur og høy kompetanse når det gjelder HMS. Denne gode sikkerhetstradisjonen bør videreføres til det digitale området.[1]

Status på tiltak

Petroleumstilsynet (Ptil) har bidratt til overføring av HMS-tradisjonene til det digitale området ved å ansvarliggjøre aktørene i utvikling av gode normer og standarder, og til gjennomføring av egenvurderinger basert på interesse- og arbeidsgiverorganisasjonen Norsk olje og gass' retningslinje NOROG-104.[2] Et viktig arbeid i tiden som kommer, vil være å videreutvikle og tilpasse regelverket innenfor fagområdet. Norsk olje og gass publiserte en ny utgave av retningslinje NOROG-104 5. desember 2016.

DNV GL tok i november 2015 initiativ til å utarbeide standardiserte krav til IKT-sikkerhet for olje- og gassnæringen med utgangspunkt i ISA/IEC-standardene. I dette arbeidet deltar både operatørene, leverandørene, ingeniør- og konsulentselskaper og en representant for Ptil. Arbeidet forventes å være ferdig sommeren 2017 og vil resultere i en anbefalt praksis som vil inngå i DNV GLs portefølje.

13.2 Verdivurdere sektorens anlegg og IKT-systemer og etablere regelverk for digitale sårbarheter

Problembeskrivelse (NOU 2015: 13, punkt 14.7.2)

De sentrale forskriftene for den digitale sårbarheten i sektoren finnes i HMS-forskriftene for petroleumsaktiviteten og i arbeidsmiljøforskriftene. Forskriftene er ikke konkrete når det gjelder digitale trusler, men omfatter implisitt også digital sikkerhet. Utvalget mener det bør foreligge krav fra tilsynsmyndigheten (Ptil) om at det skal være etablert barrierer mot digitale sårbarheter.

I påvente av ny sikkerhetslov og eventuelle pålegg og direktiver fra EU anbefaler utvalget at det settes i gang et arbeid med verdivurdering og klassifisering av anlegg og IKT-systemer.

Status på tiltak

Ptil har utarbeidet og hatt på høring et forslag til presisering av HMS-forskriftenes anvendelse på sikringsområdet, herunder IKT-sikkerhet. Tilsynet avventer oppfølgingen av forslag til ny sikkerhetslov (NOU 2016: 19 *Samhandling for sikkerhet*) før det fastsetter regelverksendringer.

Ptil vil tydeliggjøre og videreutvikle regelverket for å ivareta de utfordringene som næringen står overfor ved endringer i trusselbildet og økt digitalisering. Dette innebærer blant annet å følge opp utviklingen av industristandarder som det kan refereres til i regelverket.

Forankring av IKT-sikkerhetstiltak i virksomhetens ledelse er et av temaene som Ptil tar opp i sine tilsyn. Ptil har i løpet av 2016 gjennomført fem tilsyn med operatører, både med sikring generelt og med IKT-sikring spesielt. IKT-sikringstilsyn er gjennomført som spesifikke tilsyn, som del av større sikringstilsyn eller sammen med andre fagområder. Slike systemtilsyn hos en operatør dekker alle innretninger og anlegg som operatøren er ansvarlig for. Det er dessuten gjennomført møter med entreprenører der IKT-sikring har vært et av temaene.

---

1 Ansvaret for arbeidet med IKT-sikkerhet i olje- og gassektoren ligger hos Arbeids- og sosialdepartementet og følges opp av Petroleumstilsynet.

2 Norsk olje og gass' retningslinje 104: *Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer.*

13.3 Tydeliggjøre rolle og kapasitet hos Petroleumstilsynet

Problembeskrivelse (NOU 2015: 13, punkt 14.7.3)

Petroleumstilsynet (Ptil) har verdikjedekompetanse og kompetanse på teknisk sikkerhet i sektoren, men begrenset kapasitet når det gjelder tilsyn med sektorens IKT-sikkerhet og sårbarhet. Lysneutvalget foreslår at Ptil styrkes betraktelig på dette området.

Status på tiltak

Ptil deltar i faglige fora, både nasjonalt og internasjonalt, for å sikre kompetanse og bygge nettverk. Ptil ser også at særlig kapasiteten, men også kompetansen, innenfor IKT-sikkerhet i tilsynet bør styrkes. Sommeren 2017 vil staben bli styrket ytterligere med kompetanse innenfor tekniske automasjonssystemer og IKT-sikring. Se for øvrig redegjørelsen for etablering av en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter i punkt 22.7.

Ptil vil se på muligheten for å tydeliggjøre utfordringer og utarbeide et risikobilde innenfor IKT-sikkerhet i petroleumsnæringen. Arbeidet omfatter metodeutvikling, informasjonsinnhenting fra næringen og myndigheter, og analysearbeid. Tilsynet vil oppdatere risikobildet årlig for å følge med på effekter av næringens tiltak og identifisere behov for forbedringer.

13.4 Vurdere tilknytning til responsmiljø for IKT-hendelser

Problembeskrivelse (NOU 2015: 13, punkt 14.7.4)

Olje- og gassektoren mangler et felles responsmiljø ved IKT-hendelser. Noen få aktører er tilknyttet NSM, men særlig de mindre selskapene i bransjen faller utenfor et slikt samarbeid. Lysneutvalget anbefaler at virksomhetene i sektoren enten inngår et samarbeid med KraftCERT eller finner andre løsninger for operativt samarbeid.

Bransjen har en egen beredskapsorganisasjon som skal tre i kraft ved større hendelser, jf. sivilt beredskapssystem. Utvalget er ikke kjent med at denne har øvd på å håndtere store IKT-hendelser. Utvalget anbefaler derfor at sektoren gjennomfører øvelser i håndtering av uønskede IKT-hendelser.

Status på tiltak

I høringsuttalelsene til Lysneutvalget sier Norsk Olje og Gass seg enig i at dagens situasjon vedrørende samarbeid og varsling kan forbedres, men understreker at bransjens selskapsstruktur kan gjøre det krevende å finne en enhetlig nasjonal samarbeidsstruktur. KraftCERT ønsker i sin høringsuttalelse petroleumssektoren velkommen til et samarbeid.

Petroleumsnæringen har ikke en felles beredskapsorganisasjon, men varslingssystemet PISAS (Petroleum Industry Security Alert System). Systemet eies av Norsk Olje og Gass og ble brukt av Ptil under kartleggingskampanjen i 2014.[3] Systemet øves månedlig.

Arbeidet innenfor beredskap og hendelseshåndtering skal videreutvikles, herunder operatørens varslingsplikt, inklusiv rapporteringskanal og CERT-løsning. Dette innebærer også å utvikle og gjennomføre nødvendige øvelsesaktiviteter med aktørene i næringen og ansvarlige myndigheter.

Ptil har i møter med næringen tatt opp behovet for et sektorvis responsmiljø i petroleumsnæringen, spesielt overfor operatører med driftsansvar på norsk sokkel som ikke har et internt globalt nettverk. KraftCERT er nå blitt tilgjengelig også for petroleumsvirksomhet.

Petroleumsnæringen ser så langt at deres behov er dekket gjennom det enkelte selskaps samarbeids- eller partneravtaler med NSM eller ved at det utenlandske moderselskapet har avtaler med nasjonalt CERT-miljø. Næringens behov er først og fremst å få etablert sikre kommunikasjonsflater for hurtig varsling av digitale hendelser og gjennomføring av anbefalte tiltak.

Arbeids- og sosialdepartementet mener at det er behov for bedre koordinering av digitale hendelser mellom petroleumsnæringen og myndighetene. For digitale hendelser i petroleumsvirksomheten har Ptil hatt funksjon som informasjonsformidler mellom NSM og petroleumsnæringen og fulgt opp selskapenes tiltak i møter og sikringstilsyn med pliktsubjektene.

Ptil deltok sammen med Arbeids- og sosialdepartementet på øvelse IKT16 (se punkt 7.2 og 8.7). Det ble utarbeidet et eget øvingsdirektiv for Arbeids- og sosialdepartementets sektor med fire sektormål som blant annet omfattet rolleavklaring, planverk, samvirke, aktørkart og kriterier for varsling av alvorlige digitale angrep.

[3] Flere aktører kartlegger aktivt norsk digital infrastruktur. Sommeren 2014 ble det blant annet gjennomført en omfattende kartleggingskampanje mot flere virksomheter innenfor kraft- og petroleumssektorene i Norge.

14 Vannforsyning

14.1 Øke IKT-sikkerhetskompetansen i norske vannverk

Problembeskrivelse (NOU 2015: 13, punkt 15.6.1)

Med mange små enheter er det en utfordring å etablere og opprettholde nødvendige fagmiljøer innenfor IKT-sikkerhet. Utvalget mener at Mattilsynet i samarbeid med Norsk Vann bør stimulere til større og mer ressurssterke fagmiljøer i kommunene. Dette kan gjøres på flere måter, for eksempel ved økt interkommunalt samarbeid eller ved strukturendring.

Utvalget foreslår videre at det tas initiativ for å ta hånd om de nye utfordringene vi står overfor innenfor IKT-sikkerhet. Både myndighetssiden og Norsk Vann bør kunne bidra med å organisere kurs, gjerne i samarbeid med andre organisasjoner som NSM eller undervisningsinstitusjoner der det er hensiktsmessig. Det bør også utvikles kurs og studieretninger innenfor prosesstyring, systemintegrasjon og IKT, noe som kan bidra til at bransjen får den kompetansen som trengs for å drifte systemene i fremtiden.

Status på tiltak

Ny forskrift om vannforsyning og drikkevann (drikkevannsforskriften) som ble gjort gjeldende fra 1. januar 2017, stiller krav om forebyggende sikring ved at alle styringssystemer for vannforsyning skal være tilstrekkelig sikret mot uautorisert tilgang og bruk. Det stilles videre krav om at vannverkseieren skal sørge for at vannforsyningssystemet har, eller gjennom avtale har tilgang til, nødvendig kompetanse. Det er videre krav om at alle som deltar i aktivitet omfattet av forskriften, skal være kjent med betydningen av kravene til forebyggende sikring. Mattilsynet har utarbeidet en veileder til forskriften.[1]

Kravet om forebyggende sikring er nytt i forhold til tidligere drikkevannsforskrift, og kravet om kompetanse er tydeliggjort. Forskriften legger til rette for samarbeid for å styrke kompetansen for eksempel når det gjelder IKT-sikkerhet.

Norsk Vann retter som bransjeorgan mye oppmerksomhet mot IKT-sikkerhet og utgir rapporter og veiledningsmateriell og holder kurs.

Innføring av de nevnte forskriftskravene og Norsk Vanns egne tiltak er viktige skritt på veien for å øke sikkerhetskompetansen i norsk vannforsyning. Bransjen må nå få mulighet til å følge opp kravene. Mattilsynet gjennomførte tilsyn i hele landet med hovedvekt på IKT-sikkerhet i 2016. Helse- og omsorgsdepartementet vil etter en passende tid påse at Mattilsynet følger opp med et nytt nasjonalt tilsynsprosjekt, og evaluere om forskriftskravet har medført endret situasjon. Ytterligere tiltak skal vurderes etter dette.

14.2 Styrke tilsyn og veiledning i IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 15.6.2)

Det er behov for økt oppmerksomhet hos Mattilsynet når det gjelder IKT-sikkerhet. Dette inkluderer utarbeidelse av forskrifter som definerer krav til IKT-sikkerhet, og tilhørende veiledningsmateriell for vannverk. Vannverkene synes å ha behov for utfyllende informasjon utover de generelle kravene som er tillagt vannverkseieren i drikkevannsforskriften. Det bør vurderes et tettere samarbeid mellom de ulike tilsynsmyndighetene for at hvert enkelt tilsyn skal bli bedre i stand til å føre tilsyn med sin sektor knyttet til hendelser som går på tvers av sektorene (vann, strøm, ekom). Relevante myndigheter bør avklare og vedta et nødvendig ambisjonsnivå for IKT-sikkerhet for vannverkene.

Helse- og omsorgsdepartementet har innledet et arbeid med å revidere drikkevannsforskriften med tilhørende veileder. Revisjonen må også inkludere IKT-sikkerhet og IKT utover det generelle kravet om at vannverkseieren er ansvarlig for å levere sikkert drikkevann.

[1] Mattilsynets veileder til forskriften: http://www.mattilsynet.no/mat_og_vann/vann/veiledning_til_drikkevannsforskriften__10_forebyggende_sikring.25134

Status på tiltak

Krav om IKT-sikkerhet i ny drikkevannsforskrift gjeldende fra 1. januar 2017 gjør det enklere for Mattilsynet å følge opp gjennom tilsyn om nødvendig IKT-sikkerhet er på plass. Mattilsynet gjennomførte i 2016 et nasjonalt tilsynsprosjekt rettet mot vannverkenes beredskap med spesielt fokus på vannverkenes beredskap med IKT-systemene. I forkant av tilsynsprosjektet ble det gjennomført opplæring av inspektørene som omfattet tilsyn med IKT-sikkerhet. Dette medførte en styrket kompetanse internt i Mattilsynet.

Ny drikkevannsforskrift gir tydeligere krav om forebyggende sikring og kompetanse ved vannverkene. I Mattilsynets veileder til forskriften utdypes kravene. Mattilsynet plikter i samsvar med forvaltningslovens krav videre å kunne veilede om kravene som stilles i forskriften. Det vil sannsynligvis likevel være slik at Mattilsynet ikke vil inneha tilstrekkelig ekspertkompetanse innenfor IKT-sikkerhet.

Mattilsynet har tatt et første skritt for å øke egen kompetanse for å kunne gi veiledning og føre tilsyn med vannverkenes IKT-sikkerhet. På kort sikt er ytterligere kompetanseheving nødvendig for å styrke Mattilsynets interne kompetanse. Helse- og omsorgsdepartementet forventer at Mattilsynet vedlikeholder slik intern kompetanse, men det er ikke lagt opp til noen bestemt kompetansehevingsplan innenfor dette området. Mattilsynet skal dekke svært mange kompetanseområder, og det bør finne et hensiktsmessig nivå for å kunne utøve tilsyn på en tilstrekkelig måte. Det bør gjøres i tett samhandling med NSM. Se for øvrig redegjørelsen for etablering av en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter i punkt 22.7.

14.3 Bedre systemer for hendelseshåndtering

Problembeskrivelse (NOU 2015: 13, punkt 15.6.3)

Det synes å være et behov for å etablere et felles responsmiljø for hendelseshåndtering. Et eget responsmiljø for vann er kanskje ikke realistisk, tatt i betraktning det store antallet små enheter i vannsektoren, og utvalget skisserer tre alternativer.

Utvalget anbefaler at Helse- og omsorgsdepartementet, i samråd med Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet, utreder muligheten for et responsmiljø for hendelseshåndtering som ivaretar vann og avløp.

Status på tiltak

Et felles responsmiljø for hendelseshåndtering som ivaretar vann og avløp, er ikke utredet, og Helse- og omsorgsdepartementet har ikke konkrete planer om å utrede dette. Nettverk for kompetansestøtte til vannverk ved uønskede hendelser ble etablert fra 1. januar 2017, og administreres av Folkehelseinstituttet. Ordningen innebærer at det opprettes en alarmtelefon, en vaktordning og et nettverk av eksperter innenfor toksikologi, mikrobiologi, epidemiologi og relevant vannfaglig kompetanse. I første omgang vil ikke ekspertise innenfor IKT-sikkerhet inngå. Det er opprettet en referansegruppe for ordningen der DSB er med. Sannsynligvis vil en utvidelse til å omfatte IKT-sikkerhet kunne vurderes innen utgangen av 2017.

14.4 Gjennomføre risiko- og sårbarhetsanalyser før en eventuell innføring av smarte vannmålere

Problembeskrivelse (NOU 2015: 13, punkt 15.6.4)

Innføring av smarte vannmålere, tilsvarende AMS som innføres i energisektoren, knytter vannmålere tettere sammen med driftskontrollsystemer. Dette øker sårbarhetsflaten og kan ha betydelig skadepotensial. Det bør gjennomføres nødvendige ROS-analyser for å forhindre ukritisk implementering av funksjonalitet ved etablering av smarte vannmålere inn mot driftskontrollsystemer.

Status på tiltak

Det foreligger per i dag ikke noe krav om å innføre slike målere. Dersom vannbransjen selv ønsker å ta i bruk smarte vannmålere, har vannverkene/bransjen selv et ansvar for å utrede og forsikre seg om at det ikke svekker IKT-sikkerheten. Det følger av kravet i ny forskrift som trådte i kraft 1. januar 2017. Forslaget om å gjennomføre ROS-analyser er så langt ikke utredet, og Helse- og omsorgsdepartementet har foreløpig ingen planer om å utrede dette.

15 Finansielle tjenester

15.1 Styrke innsatsen på vurdering av fremtidige betalingstjenester

Problembeskrivelse (NOU 2015: 13, punkt 16.7.1)

Utviklingen av nye betalingstjenester går raskt. Ny teknologi og nye løsninger gir både enkeltpersoner og næringslivet mange fordeler. Nye betalingstjenester kan imidlertid medføre sårbarheter når brukervennlighet og «*time to market*» har prioritet. Slike tjenester kan medføre nye digitale sårbarheter, og utfordringene kan ligge utenfor nasjonal kontroll, slik at Norge ikke i like stor grad har mulighet til å påvirke. Finansforetak vil kunne bli involvert i å tilrettelegge løsninger som ikke er tilstrekkelig sikre.

Det er viktig at finansnæringen retter mer oppmerksomhet mot disse problemstillingene, blant annet for å sikre at regelverket også fremover er relevant og tilpasset disse utfordringene. Finansdepartementet bør innta en tydeligere rolle for å følge med på nye aktører som tilbyr bank- og betalingstjenester.

Status på tiltak

Ny teknologi utfordrer innarbeidede forretningsmodeller i finansnæringen. Bruk av ny teknologi og nye forretningsmodeller har mange ønskede virkninger, og lovverket bør ikke være til unødig hinder for utviklingen. Lovverket bør bidra til at utviklingen skjer innenfor hensiktsmessige juridiske rammer, slik at sikkerhets- og beredskapshensyn blir ivaretatt. Utfordringen er å utforme et regelverk som på en god måte balanserer forsiktighetshensyn mot de potensielle gevinstene ved nyskaping og endring. Forholdet mellom innovasjon og regulering i finansmarkedene er nærmere omtalt i avsnitt 3.3.2 i Meld. St. 34 (2016–2017) *Finansmarkedsmeldingen 2016–2017*, der Finansdepartementet blant annet viser til at myndighetene kan bidra til et mer diversifisert og robust tilbud av finansielle tjenester, som igjen reduserer systemisk risiko i finansmarkedene, ved å legge til rette for nye aktører og forretningsmodeller. Finansdepartementet uttalte i meldingen at det bør etableres et lavterskelkontaktpunkt mellom myndighetene og såkalte fintech-virksomheter i Norge. Finanstilsynet gir betydelig veiledning til fintech-virksomheter om regelverksspørsmål i dag, men det kan være behov for å etablere en klarere struktur for veiledning av innovative virksomheter. Finansdepartementet sendte derfor 5. april 2017 brev til Finanstilsynet med spørsmål om hvordan et kontaktpunkt mot fintech-virksomhet kan etableres på en hensiktsmessig måte.

Fremveksten av nye betalingstjenester er en av årsakene til at EUs reviderte betalingstjenestedirektiv, «Payments Services Directive 2» (PSD 2), er vedtatt. Direktivet har blant annet som formål å fremme sikrere tekniske betalingsløsninger og modernisere regelverket i tråd med utviklingen i markedet. Direktivet åpner for nye betalingstjenester og regulerer også samhandling mellom de ulike tjenesteyterne. Det er lagt opp til utfyllende regler som skal ivareta sikkerheten under de nye løsningene. Direktivet er EØS-relevant, og det er ventet at det vil tas inn i EØS-avtalen. Foreløpig er det ikke fastsatt en gjennomføringsfrist for EFTA-landene. Finanstilsynet har utarbeidet et høringsnotat med utkast til lov- og/eller forskriftsbestemmelser som gjennomfører forventede EØS-regler i samsvar med direktivet. Finansdepartementet tar sikte på å sende saken på høring i løpet av 2017.

Finansdepartementet, Finanstilsynet og Norges Bank følger utviklingen på sine respektive ansvarsområder innenfor bank og betalingstjenester. Analyser av risikoutviklingen gjøres jevnlig. Finanstilsynet utarbeider blant annet årlig en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT. I den seneste rapporten, fremlagt 26. april 2017, vurderer Finanstilsynet betalingssystemene generelt som solide og stabile, og viser til at det i 2016 var færre og mindre alvorlige IKT-hendelser enn i tidligere år. Til tross for en økning i tap knyttet til svindel og angrep mot betalingstjenestene ligger tapene fortsatt på et relativt lavt nivå. Mye av årsaken til lave tap er forebyggende tiltak. Norges Bank legger hvert år frem en rapport om finansiell infrastruktur som en del av sitt arbeid for å fremme finansi-

ell stabilitet og et effektivt betalingssystem i Norge.

15.2 Videreføre tverrfaglig samarbeid for god beredskapsevne og håndtering av alvorlige tilsiktede IKT-hendelser

Problembeskrivelse (NOU 2015: 13, punkt 16.7.2)

Det er et godt samarbeid mellom FinansCERT og Beredskapsutvalget for finansiell infrastruktur (BFI). Et forbedringsområde er imidlertid å være mer forberedt på de sjeldne, alvorlige hendelsene, for eksempel hvordan man planlegger beredskapen hvis den elektroniske infrastrukturen blir utilgjengelig over lengre tid.

Utvalget stiller spørsmål ved hvor godt forberedt sektoren vil være til å håndtere de store krisene, og mener BFI, i samarbeid med FinansCERT, må ta initiativ til mer samordnede og komplekse øvelser med tilstrekkelig tyngde og realisme. Videre bør det øves på krisekommunikasjon til kundene.

Status på tiltak

Digitale hendelser følges opp på vanlig måte av tilsynsmyndighetene (Finanstilsynet og Norges Bank) overfor de aktørene det gjelder. Finanstilsynet har tilsyn med finansforetakene og kunderettede betalingstjenester, mens Norges Bank har tilsyn med interbanksystemer. Dette omfatter tilsyn med beredskapsløsningene. IKT-forskriften stiller krav om rapportering av alvorlige og kritiske hendelser til Finanstilsynet. FinansCERT er etablert av finansnæringen og har blitt en sentral aktør i næringens håndtering av sikkerhetshendelser. FinansCERT samarbeider med myndighetene og har fått fast observatørplass i BFI. Næringen har et høyt ambisjonsnivå for både egen og FinansCERTs innsats på dette området. Nordiske finansforetak har nylig blitt enige om å etablere Nordic Financial CERT bygget på dagens norske virksomhet i FinansCERT.

Øvelser er nødvendig for å bli bedre til både å forebygge og å håndtere de alvorlige og sjeldne hendelsene. BFI gjennomfører regelmessig øvelser og legger stor vekt på at øvelsene skal være relevante og realistiske og ta for seg alvorlige scenarioer. Øvelsene kommer i tillegg til øvelser hos de enkelte foretakene og hos myndighetene. Finanstilsynet er sekretariat for BFI og har innsikt i øvelsesaktivitet hos foretak og myndigheter. Tilsynet har derfor gode forutsetninger for å legge opp til øvelser som bidrar til å utfylle annen øvelsesaktivitet. Finanstilsynet følger opp foretakenes øvingsaktivitet og legger vekt på at slike øvelser skal bidra til å styrke den mest operasjonelle delen av hendelseshåndteringen i finanssektoren.

15.3 Analysere sårbarhetskonsekvensene som følge av utkontraktering ut av landet

Problembeskrivelse (NOU 2015: 13, punkt 16.7.3)

Det kan være en utfordring at mange foretak innenfor finanssektoren flytter deler av sin IKT-virksomhet ut av landet. Slik utkontraktering kan være innenfor akseptabel risiko for den enkelte virksomheten, men den samlede samfunnsmessige risikoen kan bli for stor. Det er viktig at virksomhetene har et bevisst forhold til hvilken kompetanse som ikke bør utkontrakteres. Spesielt vil det kunne gjelde beredskapskompetanse, som bør være virksomhetsnær.

Etter utvalgets vurdering må Finansdepartementet gi Finanstilsynet i oppdrag å vurdere hva de langsiktige konsekvensene av offensiv bruk av utkontraktering kan bli. Det bør vurderes om utkontraktering av virksomhet som kan være viktig for samfunnet, bør ha krav om at det til enhver tid skal være en virksom «*cold backup*» lokalt i Norge.

I finanssektoren i Norge er det regler for utkontraktering både i IKT-forskriften og i forskrift om risikostyring og internkontroll, men det bør vurderes om disse bør videreutvikles og detaljeres basert på den foreslåtte kompetansevurderingen. Utvalget mener det er viktig å vise ansvarlighet når det gjelder denne problemstillingen, ettersom utstrakt bruk av utkontraktering på sikt kan bidra til å svekke den nasjonale evnen til utvikling og oppfølging på sentrale kompetanseområder.

Status på tiltak

Finansdepartementet og Finanstilsynet er oppmerksom på at utkontraktering kan endre kvaliteten og stabiliteten i IKT-systemene, og samtidig svekke innsyn i og kontroll med sårbarhetene i de systemene finansforetakene baserer sin virksomhet på. Det ble derfor vedtatt og satt i kraft nye lovregler om dette i 2014. Reglene gjelder hva slags oppgaver finansforetakene kan utkontraktere, og gir Finanstilsynet hjemmel til å kontrollere utkontrakteringen og iverksette tiltak overfor uforsvarlig utkontraktering. Finanstilsynet mottok

i april 2016 en rapport om utkontraktering fra en arbeidsgruppe bestående av representanter fra Norges Bank, Finansdepartementet og Finanstilsynet. Rapporten inneholder vurderinger som kan gi veiledning i praktisering av regelverket. Finanstilsynet tar sikte på å følge opp rapporten i et rundskriv der tilsynet også vil ta hensyn til kommende retningslinjer om utkontraktering og skytjenester fra den europeiske banktilsynsmyndigheten EBA. Problemstillinger knyttet til tjenesteutsetting er også omtalt i punkt 6.4 og 22.10.

15.4 Videreføre og styrke engasjementet for å påvirke internasjonal regulering av IKT-sikkerhetsmekanismer

Problembeskrivelse (NOU 2015: 13, punkt 16.7.4)

I stadig større grad har vi felles regelverk med EU og andre internasjonale aktører. Det er en bekymring at vi kan få lavere sikkerhetskrav i Norge som følge av felles regelverk i EU. Det er viktig at Finansdepartementet tar en gjennomgang av hvilke arenaer Norge har tilgang til, og benytter de mulighetene som finnes for å påvirke utviklingen tidligst mulig. Utvalget er enig med Finanstilsynet i at tilsynsaktivitetene må være à jour med beste praksis, og oppfordrer Finanstilsynet til å videreføre det omfattende samarbeidet som allerede pågår internasjonalt med andre lands og EUs tilsynsorganer.

Status på tiltak

Det er viktig med internasjonalt samarbeid på dette området, og Finansdepartementet vil fortsette å videreutvikle norsk regelverk innenfor EØS-forpliktelsene og andre rammer. EUs regler om IKT-sikkerhet innebærer omfattende krav til blant annet risikostyring, sikkerhetsmessige tiltak og rapportering av uønskede hendelser, og de er i stadig utvikling, jf. for eksempel omtalen av PSD 2 i punkt 15.1 over. Finanstilsynet og Norges Bank deltar i en rekke internasjonale samarbeid og vil bygge videre på dette i ulike fora.

15.5 Styrke beredskapstiltak for utviklingen mot det kontantløse samfunnet

Problembeskrivelse (NOU 2015: 13, punkt 16.7.5)

Ny teknologi og brukervennlige betalingsløsninger bidrar til at stadig færre i Norge bruker kontanter. Full overgang til digitale løsninger (elektroniske penger) kan imidlertid ut fra et beredskapsmessig perspektiv gi økt sårbarhet. Det er mange som vil være avhengige av kontanter i en alvorlig beredskapssituasjon.

Utvalget mener dette er et eksempel på en stor sårbarhet med digitalt utspring som Norge må ha beredskap for. At det eksisterer kontanter, gir i seg selv flere muligheter i en krisesituasjon. Finansdepartementet bør ta initiativ til å se på hvordan dette best kan løses, blant annet gjennom å se til andre lands håndtering av lignende utfordringer.

Status på tiltak

Finanstilsynet og Norges Bank har arbeidet med spørsmål knyttet til beredskap i betalingssystemet over lengre tid og har avgitt forslag til Finansdepartementet om nye regler om bankenes beredskapsansvar for distribusjon av kontanter. Finansdepartementet har sendt forslaget på høring med frist 2. mai 2017. Finanstilsynet og Norges Bank har i tillegg avgitt en orientering til Finansdepartementet om hvordan de – i tråd med sine oppgaver som tilsynsmyndigheter på betalingsområdet – følger opp beredskapen for det elektroniske betalingssystemet.

16 Helse og omsorg

16.1 Sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet

Problembeskrivelse (NOU 2015: 13, punkt 17.7.1)

Flere aktører etterlyser en sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet. Utvalget stiller spørsmål ved hvorfor styringsmuligheten som departementet har til å samkjøre mellom de regionale helseforetakene, ikke benyttes i større utstrekning. Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og oppfylle felles behov og for å unngå divergerende løsninger i regionene.

Utvalget har gjennom sitt arbeid registrert at det er publisert en stor mengde utredninger de siste årene som omhandler IKT i helsesektoren. Flere av disse ser ut til å beskrive dagens utfordringer på en god måte, og det synes å være stor bevissthet i sektoren om hvilke forbedringstiltak som er nødvendige. Utvalget stiller spørsmål ved hvorfor ikke flere av tiltakene er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. Utvalget mener at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det må sikres gjennomføringskraft for disse. Som en del av dette foreslår utvalget at det nye Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT-sikkerhet i helsesektoren.

Utvalget mener det bør vurderes forenklinger i Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.

Status på tiltak

Det er satt i gang flere tiltak for å sikre bedre samordning og styring av IKT-utviklingen i helse- og omsorgssektoren, noe som også styrker IKT-sikkerheten.

Direktoratet for e-helse er etablert fra 1. januar 2016 for å bidra til bedre styring og koordinering på e-helseområdet. IKT-tiltak må sees i sammenheng for å sikre best mulig utnyttelse av både leverandørenes og egne utviklingsressurser. Direktoratet skal i samarbeid med andre relevante aktører bidra til kompetansespredning om informasjonssikkerhet og personvern. Direktoratet for e-helse har myndighets- og premissgiverrollen i det nasjonale arbeidet med IKT-infrastruktur.

Forskrift om IKT-standarder i helse- og omsorgssektoren trådte i kraft 1. september 2015. Forskriften pålegger aktørene i sektoren å bruke elektroniske journalsystemer, å oppdatere adresseregisteret i helsenettet og å bruke standardiserte meldingsformater for utveksling av pasientinformasjon mellom aktørene. Forskriften skal bidra til at elektronisk kommunikasjon skjer effektivt og standardisert. Dette er en begynnelse, og forskriften skal forbedres i takt med utvikling og behov i sektoren.

Justis- og beredskapsdepartementet stiller krav om årlig rapportering om sikkerhetstilstanden i sektorene. Denne rapporteringen er begrenset til sikkerhetsloven. Helse- og omsorgsdepartementet ønsker å vurdere hvilken tilleggsrapportering som er nødvendig og eventuelt skal iverksettes i helse- og omsorgssektoren, og hvem som er best egnet til å ivareta denne oppgaven.

Norsk Helsenett SF har i dag en operativ rolle i arbeidet med informasjonssikkerhet i helse- og omsorgssektoren og drifter blant annet Helse-CERT, som overvåker trafikken på helsenettet, utarbeider sårbarhetsoversikter, gjennomfører inntrengingstesting, bistår med hendelseshåndtering med mer.

Norm for informasjonssikkerhet (Normen) er en bransjenorm, og selv om sekretariatet for tiden ligger i Direktoratet for e-helse, så er det bransjen selv som bestemmer innholdet i normen. Normen baserer seg på gjeldende lover og regelverk, men kan, når det er hensiktsmessig, være strengere enn det lover og regelverk tilsier.

Helse- og omsorgsdepartementet har stilt krav i tildelingsbrev og oppdragsbrev til underliggende virksomheter om å arbeide målrettet med informasjonssikkerhet, jf. sikkerhetsloven, *Nasjonal strategi for informasjonssikkerhet* (2012) med tilhø-

rende handlingsplan og *Handlingsplan for informasjonssikkerhet i statsforvaltningen – 2015–2017* (2015).

16.2 Mer forskning på IKT-sikkerhet innenfor ny helse- og velferdsteknologi

Problembeskrivelse (NOU 2015: 13, punkt 17.7.2)

Etter utvalgets vurdering bør helse- og velferdsteknologi som i stor grad endrer samfunnet, utredes og følges opp av en offentlig debatt før implementering. Utvalget mener det er behov for en mer spisset forskningsinnsats for å se på sikkerhetsaspektene ved teknologien, samtidig som man ivaretar de mulighetene og utfordringene som ny helse- og velferdsteknologi vil gi. Forsøk som pågår med ny helse- og velferdsteknologi, bør videre samordnes nasjonalt for å sikre kompetanseoverføring. Det nye Direktoratet for e-helse bør sikre at disse initiativene samordnes.

Status på tiltak

Det er bevilget 2 mill. kroner i basistilskudd til NTNU CCIS på Gjøvik. Bevilgningen skal støtte opp under arbeidet med informasjonssikkerhet og personvern i helse- og omsorgssektoren. Ytterligere initiativ til spisset forskningsinnsats utover basistilskudd til NTNU CCIS vil bli vurdert senere.

16.3 Etablere løsninger for å imøtekomme utviklingen innenfor helse- og velferdsteknologien

Problembeskrivelse (NOU 2015: 13, punkt 17.7.3)

Ved innføring av helse- og velferdsteknologi bør hovedregelen være at tjenesteeieren av slike løsninger tar et overordnet ansvar for sikkerheten i hele verdikjeden og ikke utelukkende baserer seg på at sikkerheten er ivaretatt av underliggende tjenester som for eksempel ekomtilbydere.

Utvalget støtter Norsk Helsenetts forslag om at helsenettet, i samarbeid med sektoren, bør vurdere om det er sentrale felleskomponenter (innenfor kommunikasjon mot internett) som sektoren behøver for å fremme en trygg innføring av velferdsteknologiske løsninger.

Status på tiltak

Direktoratet for e-helse har igangsatt en utredning av en nasjonal plattform for lagring av data fra velferdsteknologiske løsninger gjennom Nasjonalt velferdsteknologiprogram. Samlet er det bevilget om lag 40 mill. kroner til trygghets- og mestringsoppdraget, som er en del av Nasjonalt velferdsteknologiprogram. Sentralt i oppdraget står utvikling av en referansearkitektur og etablering av infrastruktur på velferdsteknologiområdet. Formålet er å danne rammen for utvikling av velferdsteknologiske tjenester og sikre at data fra slik teknologi kan deles sikkert mellom forskjellige aktører i helse- og omsorgssektoren. Direktoratet for e-helse leder arbeidet i samarbeid med Helsedirektoratet og KS. En slik plattform knytter utstyr og teknologi ute hos brukerne sammen med helse- og omsorgstjenestenes fagsystemer og muliggjør innovasjon og nyutvikling.

16.4 Gjennomføre flere IKT-øvelser der kritiske systemer er ute av funksjon

Problembeskrivelse (NOU 2015: 13, punkt 17.7.4)

Det er behov for beredskap ved bortfall av kritiske IKT-tjenester som skyldes tilsiktede eller utilsiktede hendelser. Mindre grad av manuelle rutiner å falle tilbake på kan i fremtiden gi nye og økte sårbarheter. Utvalget mener det bør gjennomføres flere IKT-øvelser der kritiske systemer er ute av funksjon.

Status på tiltak

Sektoren øver jevnlig på digitale hendelser og IKT-organisasjonene i de regionale helseforetakene er med i beredskapsøvelsene som avholdes. De enkelte sykehusene har planer og rutiner for å håndtere situasjoner hvor kritiske systemer, for eksempel pasientjournalen, er ute av funksjon. Helse- og omsorgsdepartementet deltok i den nasjonale øvelsen IKT16, og en evalueringsrapport er under utarbeidelse.

17 Transport

17.1 Styrke IKT-tilsyn og samarbeid mellom transportgrenene

Problembeskrivelse (NOU 2015: 13, punkt 18.5.1)

Transportbransjen kjennetegnes av økende privatisering og internasjonalisering, noe som medfører en rekke utfordringer, særlig for myndighetenes krisehåndtering. Det anbefales at sektoren går igjennom beredskapsplanene og sjekker disse opp mot digitale sårbarheter og reserveløsninger. Beredskapsplanverket må også ha planer for å håndtere digitale kriser.

Det anbefales at Samferdselsdepartementet styrker tilsynsmyndighetene for transportsektoren innenfor IKT-sikkerhet. Tilsynsmyndighetene må ha kapasitet og kompetanse til å føre tilsyn med og veilede virksomheter på norsk territorium og bidra i internasjonale fora.

Status på tiltak

Lysneutvalgets anbefaling om å styrke IKT-tilsynene i transportsektoren følges i utgangspunktet opp gjennom styringsdialogen mellom Samferdselsdepartementet med underliggende tilsynsmyndigheter og andre virksomheter. Det er imidlertid betydelige forskjeller mellom de fire transportgrenene med hensyn til organisering og fordeling av ansvar og oppgaver mellom ulike typer forvaltningsorganer, herunder hvorvidt det finnes et rendyrket tilsynsorgan i den enkelte sektor, og om IKT-sikkerhet inngår som en naturlig del av tilsynenes oppgaveportefølje. Innen enkelte av transportformene er det dermed krevende uten videre å følge opp anbefalingen om å «styrke IKT-tilsynene» i transportsektoren.

Som grunnlag for videre oppfølging vil Samferdselsdepartementet gjennomføre en nærmere kartlegging innenfor hver enkelt transportform når det gjelder ulike aktørers ansvar og oppgaver, mandater, eksisterende krav og retningslinjer for IKT-sikkerhet med mer. Tilsynsoppgaver knyttet til IKT-sikkerhet vil være en naturlig del av en slik kartlegging, herunder grensesnittet mot tilsyn i andre sektorer. Samferdselsdepartementet vil gjennomføre en slik kartlegging i 2017. Se for øvrig redegjørelsen for etablering av en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter i punkt 22.7.

For å styrke samarbeidet om IKT-sikkerhet i transportsektoren har Avinor AS, Kystverket, Statens vegvesen, Bane NOR SF (tidligere Jernbaneverket) og NSB AS etablert Samarbeidsforum IT-sikkerhet. Gjennom forumet møtes virksomhetene for å utveksle informasjon og erfaringer om IKT-sikkerhet generelt og sikkerhetstruende digitale hendelser spesielt.

17.2 Etablere en felles rapporteringskanal for IKT-hendelser innenfor transportsektoren

Problembeskrivelse (NOU 2015: 13, punkt 18.5.2)

Utvalget mener at det er behov for en felles rapporteringskanal både fra myndighetene til sektoren og fra sektoren til myndighetene når det gjelder IKT-hendelser. Alle relevante aktører i sektoren må kunne varsles. Utvalget mener at Samferdselsdepartementet bør utrede hvordan rapportering av IKT-hendelser bør ivaretas for sektoren.

Status på tiltak

Samferdselsdepartementet har i samråd med relevante underliggende etater vurdert spørsmålet om hvordan rapportering av digitale hendelser bør ivaretas for transportsektoren. Etablering av et felles responsmiljø for hele transportsektoren har blitt vurdert som ett av flere alternativer. På grunn av til dels store ulikheter mellom transportgrenene er det vurdert slik at det i denne sammenhengen ikke er hensiktsmessig å anse transport som én sektor, men snarere fire sektorer eller transportformer: vei, bane, luft og sjø. Følgelig har det ikke blitt ansett som hensiktsmessig med en felles «Transport-CERT», men i stedet har Avinor, Statens vegvesen, Kystverket, Bane NOR og NSB egne responsmiljøer som samarbeider direkte med NSM.

Organiseringen som er beskrevet ovenfor, har blitt videreutviklet og konsolidert i forbindelse med planlegging og gjennomføring av øvelse IKT16 i november 2016. Som del av NSMs arbeid med å etablere et nasjonalt rammeverk for digital hendelseshåndtering har Samferdselsdepartementet og etatene sammen med NSM definert et aktørkart for samferdselssektoren som blant annet beskriver felles varslings- og rapporteringskanaler. Samferdselsdepartementets foreløpige inntrykk etter øvelse IKT16 er at den valgte organiseringen og rapporteringskanalene fungerer hensiktsmessig. Samferdselsdepartementet vil benytte den endelige evalueringen etter øvelsen som grunnlag for eventuelle grep for å videreutvikle transportsektorens håndteringsevne ved digitale hendelser.

17.3 Særskilte tiltak for sjøtransport

Problembeskrivelse (NOU 2015: 13, punkt 18.5.3)

Den maritime sektoren er svært avhengig av digitale systemer for å ivareta sjøsikkerhet og effektivitet. Utvalget observerer at ulike myndigheter har ansvar i en kompleks verdikjede i sjøfarten, samtidig som det mangler en myndighet med et helhetsblikk på digitale sårbarheter i hele verdikjeden. Det anbefales at Kystverket gis et overordnet ansvar for å ha helhetsoversikt over IKT-sikkerheten i maritime verdikjeder og gi råd til departementet om prioriteringer som gjelder digitale sårbarheter.

Det er en uløst problemstilling internasjonalt knyttet til sikret digital utveksling av passasjer- og mannskapsinformasjon og last- og kundedata. Utvalget anbefaler at Samferdselsdepartementet, i samarbeid med andre relevante myndigheter, tar initiativ for å finne en løsning på dette internasjonalt.

Status på tiltak

Både Sjøfartsdirektoratet og Kystverket har sentrale ansvarsoppgaver for å ivareta effektiv og sikker sjøtransport. Sjøfartsdirektoratet er forvaltnings- og tilsynsmyndighet for arbeidet med sikkerhet for liv, helse, miljø og materielle verdier på fartøy med norsk flagg og utenlandske fartøy i norske farvann. I dette mandatet ligger sikring av utstyr og materiell om bord, herunder IKT-sikkerhet. Kystverket er nasjonal etat for kystforvaltning, sjøsikkerhet og beredskap mot akutt forurensning og arbeider aktivt for en effektiv og sikker sjøtransport gjennom å ivareta transportnæringens behov for fremkommelighet og effektive havner.

Som vist i Lysneutvalget (punkt 18.4.1) er ansvaret for å gjennomføre det internasjonale regelverket innenfor maritim sikring delt mellom Samferdselsdepartementet og Nærings- og fiskeridepartementet, ved at Kystverket har ansvar for havner og havneanlegg, mens Sjøfartsdirektoratet har ansvar for skip og personell. Koordinerende myndighet her er Sjøfartsdirektoratet.

Fremtidens skipsfart vil bli kraftig påvirket av de store endringene som skjer innenfor digitalisering og automatisering. Maritime myndigheter må bidra til utvikling, godkjenning og implementering av nye løsninger, og IKT-sikkerhet vil være et viktig hensyn. Som et eksempel nevnes samarbeidet mellom Sjøfartsdirektoratet, Kystverket og andre aktører om et pilotprosjekt for førerløse/autonome fartøy i Trondheimsfjorden.

Etablere helhetsoversikt over IKT-sikkerheten i maritime verdikjeder

Samferdselsdepartementet vil vurdere mulige tiltak for å redusere den digitale sårbarheten innenfor sjøtransport. Dette innebærer blant annet at tiltakenes potensielle risikoreduserende effekt sammenholdes med kostnadene ved gjennomføring.

Lysneutvalgets anbefaling om å gi Kystverket et overordnet ansvar for å ha helhetsoversikt over IKT-sikkerheten i den maritime verdikjeden vil kunne komme i konflikt med dagens ansvarsfordeling mellom Kystverket og Sjøfartsdirektoratet.

Det som omhandler land, farleder eller logistikk som er basert på landinfrastruktur, ligger under Kystverket, mens det som omhandler skip, miljø, sjøfolk og passasjerer ligger under Sjøfartsdirektoratet. En nasjonal ansvarsfordeling for IKT-sikkerheten i den maritime verdikjeden bør følge samme lest.

Samferdselsdepartementet vil i samarbeid med Nærings- og fiskeridepartementet gjennomføre en nærmere kartlegging av Kystverkets og Sjøfartsdirektoratets ansvar og oppgaver, mandater, eksisterende krav og retningslinjer for IKT-sikkerheten, jf. status på tiltaket «styrke IKT-tilsyn og samarbeid mellom transportformene» (se punkt 17.1). Når denne kartleggingen er gjort, vil vi ha et bedre grunnlag for å vurdere hvorvidt det overordnede ansvaret for å ha helhetsoversikt over IKT-sikkerheten i maritime verdikjeder bør tillegges Kystverket, Sjøfartsdirektoratet eller en annen myndighet.

Tilrettelegge for å sikre identitet

Gjennom våre internasjonale forpliktelser stilles det krav til rapportering fra skip til land. Oversendelse av skipets pliktige ankomst- og avgangsopplysninger til norske myndigheter og havner skjer i all hovedsak gjennom SafeSeaNet. Informasjonen som registreres i meldingssystemet, gjøres tilgjengelig for ulike nasjonale myndigheter. Dette er blant annet tollmyndigheter, politi, Forsvaret, Sjøfartsdirektoratet og Kystverket.

Fremover vil stadig flere av systemene om bord på skipene ha en forbindelse til landsiden, og IKT-sikkerhet vil bli aktualisert i utviklingen av dette. I ytterste konsekvens kan man fremover oppleve at skip kan overstyres fra land, og dersom noen klarer å komme seg inn på disse systemene, vil det kunne få alvorlige konsekvenser. Internasjonalt er det av Den internasjonale sjøfartsorganisasjonen (IMO) utarbeidet en overordnet retningslinje omkring emnet «*cybersecurity management*».

Effektiv sikring av digital utveksling av informasjon mellom skip og land forutsetter at det vedtas en internasjonal standard. Samferdselsdepartementet vil be Kystverket vurdere nærmere hvordan sikring av identitet kan løses. Dette bør vurderes i samråd med Sjøfartsdirektoratet og andre berørte myndigheter.

18 Kompetanse

18.1 Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 19.8)

IKT-sikkerhetskompetanse er mangelvare i Norge, og det er nødvendig å iverksette både langsiktige og kortsiktige tiltak. I dag utdannes det for få innenfor IKT-fagene, spesielt innenfor IKT-sikkerhet. En nasjonal kompetansestrategi innenfor IKT-sikkerhet er nødvendig for å få langsiktighet i finansieringen og på den måten sørge for å bygge opp varige kompetansemiljøer. Skal Norge som nasjon være rustet til å møte den økende digitale sårbarheten i samfunnet, må kompetansen innenfor IKT-sikkerhet bygges gjennom hele utdanningsløpet.

Status på tiltak

Anbefalingen fra Lysneutvalget har bred støtte i høringsuttalelsene. Vektlegging av kompetansebehov for IKT og IKT-sikkerhet er også i tråd med regjeringens overordnede IKT-politikk slik denne er lagt fram i Meld. St. 23 (2015–2016) *Digital agenda for Norge* og Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*.

Regjeringen vil i tiden fremover sette i verk flere tiltak for å styrke IKT-sikkerhetskompetansen i Norge, herunder utarbeide en nasjonal kompetansestrategi innenfor IKT-sikkerhet. Strategien vil legge føringer for kommende tiltak. Se en bredere omtale av tiltaket i punkt 8.1.

19 Styring og kriseledelse

19.1 Øke IKT-sikkerhetskompetansen på lokalt og regionalt nivå

Problembeskrivelse (NOU 2015: 13, punkt 20.3.1)

Digitaliseringen av samfunnet fører til mange utfordringer på regionalt og lokalt nivå. Kommunene har ansvar for mange viktige systemer og tjenester, og særlig for små kommuner kan det være en utfordring å ha tilstrekkelig IKT-sikkerhetskompetanse. Det er behov for økt veiledning av kommunene, slik at de settes i stand til å gjennomføre gode ROS-analyser og utvikle styringssystemer som ivaretar IKT-sikkerheten.

Utvalget anbefaler at Justis- og beredskapsdepartementet i samarbeid med Kommunal- og moderniseringsdepartementet tar initiativ til å etablere en felles arena for IKT-sikkerhet for lokalt og regionalt nivå. Utvalget mener videre at det er behov for å tydeliggjøre hvilke krav og forventninger til IKT-sikkerhet som legges til lokalt og regionalt nivå.

Status på tiltak

Kommunal- og moderniseringsdepartementet har i lengre tid rettet oppmerksomhet mot hvordan fylkesmannsembetet ivaretar informasjonssikkerheten. Kommunal- og moderniseringsdepartementet har etablert et eget fagutvalg for informasjonssikkerhet, og det har vært avholdt egne seminarer de siste årene. Kommunal- og moderniseringsdepartementet har overfor embetsledelsen understreket ansvaret de har på dette området.

Kommunal- og moderniseringsdepartementet har også iverksatt egne krav til fylkesmannsembetene når det gjelder informasjonssikkerhet. Alle embeter er nå pliktig til å bruke et eget styringsverktøy for å dokumentere oppfølging av krav og rapportering innenfor informasjonssikkerhet. Kravet innebærer at alle embetene skal ha tatt dette verktøyet i bruk innen utgangen av 2017.

Justis- og beredskapsdepartementet har foreløpig ikke vurdert å etablere en felles arena for IKT-sikkerhet for lokalt og regionalt nivå. DSB følger opp fylkesmennenes arbeid med samfunnssikkerhet, herunder sikkerhet knyttet til kritiske samfunnsfunksjoner, der IKT-sikkerhet inngår. Der det er relevant, vil spørsmål om IKT-sikkerhet inngå i DSBs oppfølging av fylkesmennenes arbeid regionalt og rettet mot kommunene.

19.2 Styrke beredskapen på regionalt og lokalt nivå

Problembeskrivelse (NOU 2015: 13, punkt 20.3.2)

Det er behov for å styrke evnen til å oppdage og håndtere IKT-sikkerhetshendelser på regionalt og lokalt nivå. Fylkesmannen og kommunene har ikke definerte rapporteringslinjer ved IKT-sikkerhetshendelser eller noe responsmiljø som kan håndtere dem.

Lysneutvalget mener det bør vurderes om Fylkesberedskapsrådet bør utvides med representanter fra andre infrastrukturer og viktige leverandører. Utvalget mener videre at det må etableres en mekanisme for å avdekke og håndtere IKT-sikkerhetshendelser for kommunesektoren, og viser til viktigheten av at det gjennomføres tverrsektorielle øvelser på lokalt og regionalt nivå som har IKT-sikkerhet som øvelsesmål.

Status på tiltak

I tillegg til håndtering av digitale hendelser mot egne virksomheter har kommuner og fylkesmenn en sentral rolle ved håndtering av alvorlige samfunnsmessige konsekvenser av digitale hendelser. I november 2016 deltok fylkesmannen i Hordaland og fylkesmannen i Rogaland på den nasjonale sikkerhetsøvelsen IKT16. Fylkesmennene og kommunene er ikke som virksomhet knyttet opp mot et sektorvist responsmiljø. De er heller ikke knyttet opp til et sektorvist responsmiljø i kraft av å ha den lokale og regionale samordningsrollen. Justis- og beredskapsdepartementet vil sette i gang en prosess for å få på plass en struktur for kommunenes og fylkesmennenes rolle i responsmiljøene og i nasjonalt rammeverk for digital hendelseshåndtering.

Regionalt og lokalt nivå må sikres tilgang til like og alternative kommunikasjonskanaler (som backup) ved et eventuelt bortfall av ekom. Dette kan være Nødnett, men også satellittelefoner og lignende. I tillegg til Fylkesmannen og kommunene gjelder dette også blant annet Sivilforsvaret, som ved hendelser og kriser i stor grad samvirker i krisehåndteringen og kriseledelsen.

19.3 Etablere felles gradert IKT-infrastruktur

Problembeskrivelse (NOU 2015: 13, punkt 20.3.3)

Justis- og beredskapsdepartementet bør tydeliggjøre hvilket departement som skal ha det overordnede ansvaret for å etablere en felles gradert IKT-infrastruktur for sentralforvaltningen, og klargjøre hvilke roller og hvilket ansvar Kommunal- og moderniseringsdepartementet og Forsvarsdepartementet har i dette bildet.

Status på tiltak

Regjeringen har gitt Forsvarsdepartementet i oppdrag å stå for utvikling og drift av Nasjonalt BEGRENSET nett (NBN) og Nasjonalt HEMMELIG nett (NHN) for sentralforvaltningen og andre utvalgte brukere. Det er viktig at disse informasjonssystemene brukes også i en normalsituasjon, slik at personellet som skal bruke løsningene, har øvelse og kjenner systemet dersom det skal tas i bruk i forbindelse med en eventuell krise eller krig. I tillegg utreder Kommunal- og moderniseringsdepartementet mulighetene for en felles ugradert/lavgradert løsning for alle i det nye regjeringskvartalet som er under planlegging.

Justis- og beredskapsdepartementet iverksatte i fjerde kvartal 2016 et arbeid med å klargjøre departementenes lokaler til å motta en høygradert IKT-løsning gjennom installasjon av fiberkabler, kryptoutstyr med mer. Arbeidet resulterte i at alle departement kan ta imot en høygradert IKT-løsning så snart en løsning er klar. Foreløpige estimater tilsier at NHN kan være klar til innføring medio 2018.

Justis- og beredskapsdepartementet skal sammen med Forsvarsdepartementet og Kommunal- og moderniseringsdepartementet vurdere eksisterende ansvarsfordeling på departementsnivå knyttet til videre initiering, innføring, drift og forvaltning av graderte IKT-løsninger, samt tjenester på de enkelte plattformene.

19.4 Vurdere virkemidler for kommunikasjon med befolkningen

Problembeskrivelse (NOU 2015: 13, punkt 20.3.4)

Ved større kriser og hendelser må myndighetene kunne nå befolkningen med informasjon og varsling. Felles for de fleste virkemidler og kanaler for kommunikasjon er at de er avhengige av tilgjengelig ekominfrastruktur. Utvalget anbefaler at DSB vurderer bruken av virkemidler for kommunikasjon med befolkningen i kriser og i den sammenheng også vurderer beredskapsrollen til NRK i samarbeid med Kulturdepartementet.

Status på tiltak

Sivilforsvarets varslingsanlegg (tyfoner) består av 1250 lydgivere og er et viktig virkemiddel for myndighetene i varsling av akutte faresituasjoner. Varsling har hittil blitt utløst ved hjelp av signaler formidlet over FM-nettet. Når FM-nettet i løpet av 2017 slukkes over hele landet, vil Nødnett overta denne rollen.

I en krisesituasjon vil myndighetenes mulighet til å informere befolkningen kunne ha stor betydning. I dag foreligger det tre parallelle kanaler for fremføring av myndighetsinformasjon: radio, tv og internett. De tre kanalene kan i noen grad erstatte hverandre som informasjonsbærere. Det vil si at dersom for eksempel radiosendinger skulle falle ut, så vil informasjonen fortsatt kunne formidles gjennom tv og over internett og vice versa. DSB har på oppdrag fra Justis- og beredskapsdepartementet iverksatt en utredning av supplerende varslingsmetoder. Et alternativ kan være et mobilbasert befolkningsvarslingssystem hvor det er mulig å motta varsel om uønskede, potensielt farlige hendelser på mobiltelefonen.

Regjeringens strategi for å opprettholde og styrke evnen til kommunikasjon med befolkningen har tre elementer: For det første å styrke robustheten innenfor hver av de tre kanalene. For det andre å tilstrebe en stor grad av autonomi for hver av kanalene, slik at ikke én feil kan medføre svikt i alle. For det tredje å legge planer for hvordan en slik svikt likevel skal kunne håndteres. I Meld. St. 15 (2016–2017) *Eit moderne og framtidsretta NRK* understreker regjeringen at NRK fortsatt skal ha et særlig beredskapsansvar. Kriseinfo.no er en kanal for myndighetsinformasjon i krisesituasjoner. DSB har ansvaret for at disse nettsidene publiserer verifisert informasjon fra myndighetene.

20 Digitale angrep

20.1 Etablere og øve et helhetlig rammeverk for digital hendelseshåndtering

Problembeskrivelse (NOU 2015: 13, punkt 21.11.1)

Nasjonal sikkerhet avhenger av sikkerheten til de enkelte virksomheter, og en effektiv bekjempelse av digitale angrep krever godt samarbeid mellom myndighetene og mellom myndighetene og private aktører. I dag meldes det om usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for bekjempelsen av digitale angrep. Det er viktig å maksimere mulighetene innenfor det handlingsrommet som finnes for deling av informasjon. Det bør tas initiativ til å etablere og øve på et helhetlig rammeverk for håndtering av digitale hendelser på nasjonalt plan for å avklare og tydeliggjøre innsatsen mellom relevante aktører innenfor hendelseshåndtering og straffeforfølging. Utvalget foreslår en punktliste for et ambisjonsnivå til myndighetenes operative evne til å avdekke, håndtere og etterforske alvorlige hendelser.

Status på tiltak

Til grunn for nasjonal hendelseshåndtering ligger i dag føringer gitt i *Nasjonal strategi for informasjonssikkerhet med handlingsplan* (2012), *Retningslinjer for samarbeid mellom EOS-tjenestene om forebygging og håndtering av alvorlige cyberhendelser* (2013), *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner* (2014), *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer* (2014) samt relevante tiltak i lovverk og i det nasjonale beredskapsplanverket.

Høringssvarene viser at det er bred støtte for tiltaket med å etablere et nasjonalt rammeverk for håndtering av digitale hendelser. I 2016 fikk NSM i oppdrag å utarbeide, i samarbeid med berørte aktører, et utkast til et slikt rammeverk. Formålet er å avklare og tydeliggjøre innsatsen fra relevante aktører innenfor hendelseshåndtering og følge opp Lysneutvalgets anbefalinger knyttet til dette rammeverket. Et utkast til rammeverk ble øvet under den nasjonale IKT-øvelsen i november 2016. Evalueringen av øvelsen skal fullføres og rammeverket ferdigstilles i løpet av 2017 (se punkt 7.2 og 8.7).

Utvalgets punkter til ambisjonsnivå dekkes, etter Justis- og beredskapsdepartementets vurdering, av andre tiltak i denne meldingen.

20.2 Forbedre den nasjonale operative evnen gjennom samlokalisering (flertall og mindretall)

Problembeskrivelse (NOU 2015: 13, punkt 21.11.2)

Lysneutvalget tar særlig opp to problemstillinger: 1) bruken av samlokalisering som virkemiddel for å få til god samhandling, deling av informasjon og bedre ressursutnyttelse, og 2) om det er politiet eller NSM som bør koordinere håndteringen av digital hendelser og stå som vert for en eventuell samlokalisering.

Det er flere små operative miljøer i Norge i dag som skal samhandle med hverandre under en digital hendelse. Et sentralt spørsmål er om Norge evner å utnytte den samlede nasjonale kapasiteten til å forebygge, avdekke og håndtere digitale angrep, både på offentlig og på privat side. Private og offentlige aktører bør dele informasjon fra åpne kilder og lovlig delbar informasjon i langt større grad. Samlokalisering kan være et sentralt virkemiddel for å få til god samhandling og ressursutnyttelse. Utvalget foreslår at det legges bygningsmessig til rette for at de som ønsker samlokalisering, kan gå sammen om ett felles bygg.

Flertallet i utvalget anbefaler at samlokalisering bør ta utgangspunkt i det miljøet som både har tradisjon for offentlig–privat samarbeid og er en del av EOS-miljøet, og som i dag har det koordinerende ansvaret for håndtering av digitale hendelser. Flertallet anser NSM som den mest naturlige verten for samlokalisering. Justis- og beredskapsdepartementet må følge opp, særlig overfor de sivile aktørene i samarbeidet, og definere klare, målbare suksesskriterier for samarbeidet, som skal evalueres innenfor henholdsvis to og

fem år. Mindretallet i utvalget anbefaler at det legges til et «Cyber Crime Center» hos politiet hvor det samtidig vektlegges likeverdig samarbeid mellom offentlig og private sektor.

Status på tiltak

Flere av høringssvarene understreker viktigheten av rask informasjonsdeling, godt og tydeliggjort samarbeid og god oversikt over hverandres kompetanse og kapasitet.

Det er ikke etablert et nasjonalt «Cyber Crime Center», se punkt 20.5. Modellen for hendelseshåndtering i Norge har vært bygget opp og styrket gjennom flere år, og det er et mulighetsrom i dagens struktur. Regjeringen ønsker å benytte handlingsrommet i dagens struktur, med NSM som det nasjonale navet, og har derfor prioritert arbeidet med et nasjonalt rammeverk for digital hendelseshåndtering og gjennomføring av den nasjonale øvelsen IKT16. Gjennom arbeidet med et helhetlig rammeverk for hendelseshåndtering styrkes og videreutvikles et godt samarbeid mellom virksomheter, sektorvise responsmiljøer, nasjonalt responsmiljø og politiet. Erfaringer fra øvelsen vil være viktig for å videreutvikle og forbedre dagens modell.

Annen oppfølging knyttet til dette punktet er omtalt under punkt 6.1, punkt 6.2, punkt 7.3 og punkt 7.6.

20.3 Øke deteksjonsevnen og sammenstille et felles situasjonsbilde

Problembeskrivelse (NOU 2015: 13, punkt 21.11.3)

For å få til en effektiv avdekking av digitale angrep trengs det gode deteksjonsmekanismer som dekker de kanalene angrepene gjennomføres gjennom. Dette innebærer mer enn teknologiske tiltak. Informasjonsdeling i forbindelse med hendelser bør starte tidligere enn i dag.

Hovedanbefalingene omfatter følgende områder:

1. Aktiv og rettidig informasjonsdeling ved å etablere en hensiktsmessig teknisk plattform. NSM må etablere en teknisk informasjonsdelingsplattform for ugradert informasjon mot virksomheter for å kunne dele informasjon raskt og sikkert.
2. Å styrke deteksjonsevnen gjennom tilpasset monitorering i den enkelte sektor.
3. Å etablere et felles situasjonsbilde og automatisert informasjonsdeling.

Status på tiltak

Høringssvarene gir bred støtte til tiltaket. Det er igangsatt flere tiltak for å imøtekomme hovedanbefalingene. Regjeringens beslutning om å utrede og konkretisere hvordan en form for digitalt grenseforsvar kan etableres og lovreguleres, er omtalt i punkt 7.4. I tillegg har NSM utarbeidet et ugradert nasjonalt situasjonsbilde, tilgjengelig via en portal med påloggingsmulighet for de sektorvise responsmiljøene og nasjonale beslutningstakere. NSM vil også etablere en plattform for deling av teknisk informasjon. Plattformen skal raskt og sikkert motta og dele strukturerte data om trusler og andre tekniske indikatorer med de sektorvise responsmiljøene. Se også punkt 7.3.

Regjeringen ønsker å videreutvikle VDI for å styrke deteksjonsevnen i den enkelte sektor. Sensorteknologien skal oppgraderes. VDI er nærmere omtalt i punkt 7.1.

20.4 Styrke kapasitet og kompetanse knyttet til håndtering av digitale angrep

Problembeskrivelse (NOU 2015: 13, punkt 21.11.4)

Det er kapasitets- og kompetanseutfordringer knyttet til håndtering av digitale angrep. Det er viktig at fagmiljøene har en aktiv rolle overfor akademia for å tilføre praktisk erfaring som har verdi for kunnskapsutviklingen, og for å sikre rekruttering. To sentrale områder er omfattet av tiltaket:

1. Evaluere ordningen med sektorvise responsmiljøer sett opp mot det tverrsektorielle behovet for hendelseshåndtering. Dette bør gjøres i etterkant av øvelse IKT16. Det er en forutsetning at de sektorvise responsmiljøene involveres tett i evalueringen. I evalueringen bør det blant annet ses på om inndelingen i sektorvise responsmiljøer er hensiktsmessig, eller om responsmiljøer for sektorer med tilsvarende utfordringer bør slås sammen.
2. Utrede en nasjonal cyberreserve for håndtering av digitale hendelser, en reserve som skal kunne skalere innsatsen ved store hendelser og kriser.

Status på tiltak

Høringssvarene viser at det er bred enighet om å styrke den nasjonale kapasiteten og kompetansen knyttet til håndtering av digitale angrep og å opprette en nasjonal cyberreserve.

Regjeringen følger opp den nasjonale modellen for hendelseshåndtering og anbefalingen fra Lysneutvalget gjennom evalueringen av øvelse IKT16 og utviklingen av et nasjonalt rammeverk for håndtering av digitale hendelser (se punkt 7.2). Dette inkluderer gjennomgang av etableringen og innretningen av sektorvise responsmiljøer. Evalueringen av øvelsen og utviklingen av rammeverket skjer i tett samarbeid med berørte aktører.

Forsvarsdepartementet og Justis- og beredskapsdepartementet har bedt NSM, i løpet av langtidsplanperioden 2017–2020, om å vurdere en tverrsektoriell cyberreserve for hendelseshåndtering ved spesielt store kriser som krever innsats utover ordinær bemanning. I utredningen skal det sees på hvilke krav som må stilles til personell i en slik modell, og hvilke miljøer eller personer det er naturlig å knytte til et slikt tiltak. Andre momenter som må avklares er blant annet juridiske forhold, behov for klarering av personell, og øvelser og trening for å opprettholde kompetanse.

NSM har etablert et pilotprosjekt med en kvalitetsordning for leverandører i markedet som tilbyr tjenester innenfor håndtering av digitale angrep. Formålet med ordningen er todelt: For det første skal ordningen bidra til at virksomheter som opplever en IKT-sikkerhetshendelse, kan velge en tjenesteleverandør som tilfredsstiller NSMs faglige krav på søknadstidspunktet. For det andre skal ordningen bidra til å heve den sikkerhetsfaglige kompetansen innenfor hendelseshåndtering i Norge. Ordningen kan, dersom den får en god utbredelse, også representere en nasjonal kapasitetsøkning innenfor nasjonal hendelseshåndtering.

20.5 Etablere et nasjonalt «Cyber Crime Center»

Problembeskrivelse (NOU 2015: 13, punkt 21.11.5)

Det er utvalgets oppfatning at politiets beredskapsevne og oppgaveløsning i det digitale rommet langt fra er tilstrekkelig og ikke tilpasset samfunnets forventninger og den risikoen samfunnet står overfor. Utvalget støtter forslaget i Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet fra 2015 om å opprette et nytt nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet. Senteret bør organiseres under Kripos. Særorganutvalget bør vurdere om alternative organisasjonsformer er mer hensiktsmessige enn kapasitetsoppbygging.

Status på tiltak

Det er ikke etablert et nasjonalt «Cyber Crime Center». POD har utarbeidet et konkret forslag om hvordan det i politiet kan etableres et slikt senter for å forebygge og bekjempe IKT-kriminalitet, herunder hvilke oppgaver som skal legges til et slikt senter, organisatorisk forankring og ressursbehov. Forslaget innebærer at politiet må avsette betydelige ressurser som for noen funksjoner må dekkes opp ved ekstern rekruttering av kompetanse politiet ikke har i dag. Forslaget må derfor tas inn i det ordinære budsjettarbeidet og vurderes opp mot andre viktige tiltak.

Justis- og beredskapsdepartementet nedsatte i 2016 et utvalg for å se på funksjon og kapasitet blant politiets særorganer. Utvalget omtaler bekjempelse av IKT-kriminalitet som en hovedutfordring for politiet. Utvalget overleverte sin utredning til Justis- og beredskapsdepartementet i mai 2017, og utredningen sendes på bred høring.[2]

20.6 Sikre sterke fagmiljøer for IKT-kriminalitet i politidistriktene

Problembeskrivelse (NOU 2015: 13, punkt 21.11.6)

Digital kompetanse i politiet må bygges i bredden, det vil si i alle politidistrikt. I politidistriktene er det behov for bedre og mer spesialisert kompetanse og ferdigheter og økt kvalitet på politiarbeidet. Utvalget anbefaler at det gjennomføres et stort løft innenfor etter- og videreutdanning for allerede uteksaminerte tjenestemenn og -kvinner. Utvalget mener også at Justis- og beredskapsdepartementet bør gi klare føringer til politidistriktene for å sikre nødvendig tverrfaglig kompetanse i politiet, herunder sivilt ansatte med teknisk bakgrunn.

Utvalget anbefaler at politidistriktenes fagmiljøer styrkes betraktelig. Ved politiets arbeid på internett bør den åpne tilstedeværelsen, herunder «politistasjon og patruljering på nett», ligge til det enkelte politidistrikt. Utvalget mener at et klart grensesnitt mellom hva et Cyber Crime Center håndterer, og hva politidistriktene selv forventes å håndtere, er avgjørende.

Nåværende styringsmodell i politiet må ikke være til hinder for å vurdere ulike modeller for organisering av IKT-kriminalitetsbekjempelsen, blant annet i særorganutredningen.

---

[2] NOU 2017: 11 *Bedre bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer.*

Status på tiltak

Politidistriktene skal settes bedre i stand til å operere i det digitale landskapet. Politiets digitale kompetanse og kapasitet skal styrkes i alle politidistrikt. I henhold til Justis- og beredskapsdepartementets strategi av 2015 for å bekjempe IKT-kriminalitet er det utarbeidet en plan for å styrke etterforskningskapasiteten. Politiet skal prioritere ressurser til bekjempelsen av IKT-kriminalitet og i større grad enn i dag utnytte digitale spor.

Gjennom nærpolitireformen legges det grunnlag for sterkere fagmiljøer på IKT i politidistriktene. Som en del av reformen er det utarbeidet en funksjonsbeskrivelse for digitalt politiarbeid. Funksjonen digitalt politiarbeid skal ivareta en bred, effektiv og hensiktsmessig bruk av digital informasjon og elektroniske spor i politiarbeidet, herunder etterretning, forebygging, stansing av straffbare forhold, bistand til befolkningen, tilbakeføring til normalsituasjonen, etterforskning og iretteføring. Gjennom utnyttelse av teknologi og elektroniske spor skal funksjonen sikre at flere straffesaker kan etterforskes raskt og med god kvalitet i metodebruk, bevissikring og analyse.

POD har utarbeidet en strategi for digital kompetanseheving i politiutdanningen. Strategien omfatter både grunnutdanningen og etter- og videreutdanningen og tar utgangspunkt i arbeidet som er gjort ved Politihøgskolen.

20.7 Sikre en IKT-infrastruktur til støtte for politiets kriminalitetsbekjempelse

Problembeskrivelse (NOU 2015: 13, punkt 21.11.7)

Utvalget opplever at IKT-situasjonen i politiet er kritisk. Det er behov for langsiktige og omfattende løft med tanke på stabilitet i grunnleggende infrastruktur og sikkerhet i applikasjoner og tjenester. I tillegg er det behov for å etablere felles nasjonale løsninger som erstatning for ulike lokale løsninger.

Justis- og beredskapsdepartementet bør iverksette tiltak for å sikre politiet et teknologiløft, med fokus på IKT-ledelsen og -styringen, øke bestillerkompetansen og gi klare prioriteringer for ressursutnyttelse i et langsiktig perspektiv.

Status på tiltak

Politiets grunnleggende IKT-infrastruktur er gradvis modernisert de siste årene, men fortsatt er det etterslep og mangler på flere områder. De siste årene har det vært flere alvorlige hendelser hvor politiets operative evne har blitt påvirket av feil i IKT-systemene. I tillegg skjer det for ofte at ansatte i politietaten opplever at de ikke får gjort det de skal, eller blir svært forsinket, på grunn av systemene.

Å styrke politiets IKT-infrastruktur er et prioritert område for Justis- og beredskapsdepartementet. En god IKT-infrastruktur er nødvendig for at politiet skal kunne realisere gevinster knyttet til nærpolitireformen, arbeide effektivt med å bekjempe IKT-kriminalitet og nyttiggjøre seg av hensiktsmessige applikasjoner og utstyr.

20.8 Sikre balansen mellom personvern og et sikrere samfunn

Problembeskrivelse (NOU 2015: 13, punkt 21.11.8)

For å få et sikrere samfunn foreslås det ofte inngripende metoder uten at det er tatt tilstrekkelig stilling til eller redegjort for balansen mot personvern og ytringsfrihet. Utvalget mener det er behov for å ivareta balansen mellom personvern og et sikrere samfunn gjennom utredninger og offentlig debatt. Utvalget pekte spesielt på to områder der det må foretas viktige avveininger for å finne den rette balansen mellom motstridende hensyn:

1. Utrede innføring av digital grenseovervåking ved en NOU eller annen offentlig utredning
2. Utrede politiet og PSTs skjulte metodebruk på internett

Status på tiltak

Høringssvarene viser at det er bred enighet om disse anbefalingene. Spesielt Datatilsynet er kritisk til masseovervåking av alminnelige borgere og mener at nye og inngripende metoder alltid bør utredes. Se også nærmere omtale av personvern i kapittel 4.

Utredning av digital grenseovervåking

Som en oppfølging av anbefalingen fra Lysneutvalget nedsatte Forsvarsdepartementet et utvalg for å utrede sentrale problemstillinger knyttet til digitalt grenseovervåking. Utvalget avga sin rapport til Forsvarsdepartementet 26. august 2016. Rapporten anbefaler at det etableres et digitalt grenseforsvar som gir Etterretningstjenesten innsyn i digitale datastrømmer som krysser landegrensen i fiberoptiske kabler. Forutsetningen for anbefalingen er at det etableres et strengt kontrollregime

bestående av både teknologiske og menneskelige kontrollmekanismer.

Regjeringen støtter konklusjonen fra utvalget og mener det er behov for å etablere en form for digitalt grenseforsvar. Regjeringen vil utrede nærmere hvordan et slikt grenseforsvar kan etableres og lovreguleres. Se nærmere omtale av dette i punkt 7.4.

Utredning av politiets skjulte metodebruk på internett

Regjeringen er enig i utvalgets anbefaling om å utrede nærmere PSTs og det øvrige politiets skjulte metodebruk på internett for det tilfellet at PST foreslår å registrere ytringer på sosiale medier og analysere informasjon fra åpne kanaler.

21 Felleskomponenter

21.1 Følge utviklingen av IKT-utsetting for felleskomponenter

Problembeskrivelse (NOU 2015: 13, punkt 22.6.1)

Offentlig sektor har etablert en rekke åpne, gjenbrukbare løsninger som dekker typiske behov på digitaliseringsfeltet, slik som innlogging, autentisering, registre og lignende. Dette gjelder for eksempel ID-porten, som gir innbyggerne den samme innloggingsfunksjonaliteten uansett hvilken etat eller kommune man logger inn hos.

Det er rimelig å tro at det vil bli færre datasentre, at flere av datasentrene vil bli drevet av eksterne, og at flere samfunnsfunksjoner vil dele infrastruktur som datasentre. Dette kan endre sårbarhetsbildet. Kommunal- og moderniseringsdepartementet bør følge med på sårbarhetsutviklingen knyttet til utsetting av IKT-tjenester for offentlige registre og fellestjenester.

Status på tiltak

Kommunal- og moderniseringsdepartementet følger arbeidet i dialogmøter med øvrige departementer som er felleskomponenteiere, men har ingen aktiviteter utover dette, da det er sektordepartementenes ansvar. Kommunal- og moderniseringsdepartementet følger opp egne felleskomponenter i dialog med Difi og foretar løpende vurderinger av sikkerhet, drift og forvaltning. Se også punkt 6.4 og 22.10 om tjenesteutsetting og punkt 22.1 om å ivareta en helhetsvurdering av verdikjeder.

21.2 Utvikle felles beskyttelsestiltak mot sofistikerte IKT-angripere

Problembeskrivelse (NOU 2015: 13, punkt 22.6.2)

Det krever ekspertkompetanse å identifisere og håndtere sofistikerte angripere. Dagens evne og kapasitet til å oppdage disse aktørene er ikke tilstrekkelig i norske virksomheter. Det er behov for å starte utvikling av mekanismer som eierne kan bruke for å sikre fellesfunksjoner mot sofistikerte angripere. Difi bør ta en koordinerende rolle i dette arbeidet, og det bør gjøres i samarbeid med forskningsmiljøene og med bistand fra NSM.

Status på tiltak

Utvalget foreslår at Difi tar en koordinerende rolle i arbeidet med å utvikle mekanismer som virksomhetseierne kan bruke for å sikre fellesfunksjoner mot sofistikerte angrep. Dette er Kommunal- og moderniseringsdepartementet uenig i. Ifølge ansvarsprinsippet er det virksomheten og sektordepartementet som skal beskytte (nasjonale) felleskomponenter. Alle felleskomponenter kan knytte seg til NSMs varslingssystem for digital infrastruktur (VDI). Dette er ett av flere tiltak som er tilgjengelige for virksomhetene som er ansvarlige for nasjonale felleskomponenter. Andre tiltak er verdivurdering og risikoanalyse, sikkerhetsrevisjon, samarbeid om sterke IKT-sikkerhetsmiljøer og inntrengingstesting. Difis rolle i denne sammenheng er å gi råd og veiledning til virksomhetene om hvordan de skal tilnærme seg arbeidet, og å legge til rette for erfaringsutveksling. Dette gjøres i samarbeid med forskningsmiljøene og med bistand fra NSM.

21.3 Regulere elektronisk identitet

Problembeskrivelse (NOU 2015: 13, punkt 22.6.3)

Lysneutvalget skriver at e-ID-feltet har vært preget av noe ubesluttsomhet siden arbeidet begynte rundt årtusenskiftet. Gjentatte ganger har et offentlig ID-kort med tilhørende e-ID vært på trappene, uten at det har blitt noe av. Det er i dag flere private aktører som utsteder e-ID, og det er ulike behov for e-ID mellom virksomheter og sektorer. Utvalget anbefaler følgende fem tiltak vedrørende e-ID:

1. Kartlegge personinformasjon som tilflyter e-ID-leverandørene ved bruk. Løsninger med tiltrodde tredjeparter innebærer at e-ID-leverandøren får vite hva brukere gjør med sin elektroniske identitet på nettet. Nkom bør sammen med utstederne lage en samlet oversikt over

hvor mye personinformasjon som tilflyter de forskjellige e-ID-leverandørene ved bruk av e-ID-en, og hvordan denne informasjonen lagres. Videre bør Kommunal- og moderniseringsdepartementet gjennomgå reguleringen på området, slik at e-ID-leverandørene ikke tvinges til å oppbevare unødvendig personinformasjon.

2. Kommunal- og moderniseringsdepartementet bør utarbeide én tydelig definisjon av sikkerhetsnivåene. Den bør ta utgangspunkt i kombinasjoner av angriperens evne og konsekvensen av angrepet. Det må være enkelt å avgjøre om en e-ID når et sikkerhetsmål. Dette bør gjøres samtidig med tilpasningene i forbindelse med den nye EU-forordningen.[1]
3. Bruken av innloggingsportaler til engangspålogging bør begrenses, da slike portaler observerer all innlogging til svært mange tjenester, og feilaktig integrasjon av e-ID-ene kan svekke sikkerheten.
4. Man bør forbedre eksisterende e-ID-løsninger fremfor å vente på det nasjonale ID-kortet. Difi bør videreutvikle den eksisterende MinID-løsningen, blant annet ved å tilby en sikrere utstedelse av identiteter, tilsvarende «kvalifiserte sertifikater», og bedre tekniske løsninger. Difi og Nkom bør sammen oppmuntre til og kreve økt sikkerhet og åpenhet hos private leverandører, fortrinnsvis basert på standard tekniske løsninger.
5. Myndighetene bør utvise varsomhet med å tilby tjenester med sensitive personopplysninger til hele befolkningen.

Status på tiltak

Elektronisk identitet reguleres gjennom *Lov om elektronisk signatur* (2001), *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor* (2008) og gjennom *Kravspesifikasjon for PKI i offentlig sektor* (2010). Lov om elektronisk signatur sorterer under Nærings- og fiskeridepartementet. Kravspesifikasjonen er hjemlet i eForvaltningsforskriften § 27. Både rammeverket og kravspesifikasjonen sorterer under Kommunal- og moderniseringsdepartementets ansvarsområde og er en del av gjeldende strategi for bruk av e-ID.

Det foregår nå flere prosesser som vil berøre reguleringen av elektronisk identitet og Lysneutvalgets fempunktsliste med anbefalinger. Regjeringen har vedtatt at nasjonalt ID-kort skal utstyres med en e-ID, og at denne e-ID-en skal være et supplement til dagens markedsløsninger som benyttes for pålogging i ID-porten. Lanseringen vil skje i 2018.

Regjeringen ønsker at Norge skal være en del av det digitale indre markedet i Europa. Et hovedelement i dette er at de europeiske landene skal godkjenne hverandres løsninger for elektronisk identifisering, e-ID, og en rekke såkalte tillitstjenester som legger til rette for elektronisk samhandling. EU-forordningen om e-ID og elektroniske tillitstjenester (eIDAS) vil bli implementert som egen lov og erstatte dagens lov om elektronisk signatur (esignaturloven). Nærings- og fiskeridepartementet har ansvaret for gjennomføring av forordningen i samarbeid med Kommunal- og moderniseringsdepartementet. Justis- og beredskapsdepartementet vil følge opp at samfunnssikkerhetsperspektivet ivaretas i arbeidet.

Formålet med endringene er å legge til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS og dermed bidra til sterkere økonomisk vekst i det indre marked.

[1] Electronic identification and trust services (eIDAS).

22 Tverrsektorielle tiltak

22.1 Etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder

Problembeskrivelse (NOU 2015: 13, punkt 23.1)

Lange og kompliserte verdikjeder gjør det utfordrende å få oversikt over digitale sårbarheter. Verdikjedene kan spenne over flere aktører og sektorer som kan være underlagt forskjellige lovverk og tilsynsregimer. Et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder kan bidra til verdivurdering av informasjonen som bæres i verdikjedene, og til å fastsette akseptabelt risikonivå for digital sårbarhet.

Utvalget foreslår tiltak som gir en prinsipiell tilnærming til å få grep om hvordan digital sårbarhet oppstår og utvikler seg i verdikjedene. Utvalget mener at Justis- og beredskapsdepartementet bør utvikle et rammeverk for å ivareta helhetsperspektiver i verdivurderinger og sårbarhetsvurderinger. Utvalget foreslår videre å benytte dette rammeverket til ytterligere tiltak som bidrar til størst mulig åpenhet om hvilken restsårbarhet man har akseptert som bruker av utstyr og tjenester, og hvilke verdier man betror sin underleverandører.

Status på tiltak

I DSBs rapport *Samfunnets kritiske funksjoner* (2016) pekes det på at alle virksomheter som har ansvar for kritiske samfunnsfunksjoner, må planlegge for å kunne opprettholde sin virksomhet. Kartlegging av egen sårbarhet og iverksettelse av tiltak for å redusere denne sårbarheten inngår i dette. Rapporten slår fast at det er eierne og operatørene av infrastrukturene som er ansvarlig for sikkerheten og funksjonsdyktigheten i systemene. Myndighetenes rolle i denne sammenheng er å være pådriver, veilede, stille krav og føre tilsyn.

Justis- og beredskapsdepartementet vil be DSB utrede spørsmålet om å etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder, og om det bør utarbeides et sett med standardformuleringer som definerer ulike robusthetsnivåer.

22.2 Tydeliggjøre krav til virksomhetsstyringssystemer

Problembeskrivelse (NOU 2015: 13, punkt 23.2)

Virksomhetsstyringssystemene må kunne synliggjøre et sårbarhetsbilde basert på en risikovurdering av tilsiktede og utilsiktede IKT-hendelser. Virksomhetsstyringssystemene bør videre gi grunnlag for å vurdere effekten av ulike forebyggende tiltak på IKT-sikkerhetsområdet og hvilke konsekvenser svikt vil ha for samfunnet. Dette vil gi et bedre grunnlag for å prioritere ulike kostnadsdrivende forebyggende tiltak.

Utvalget anbefaler at de ulike departementene tydeliggjør krav og føringer i virksomhetsstyringssystemene, både på sentralt nivå og ute i de ulike sektorene. Tilsynsmyndighetene må følge opp at dette blir ivaretatt. Utvalget anbefaler at Justis- og beredskapsdepartementet utarbeider et sett med minimumskrav til hvilke elementer som skal inkluderes i virksomhetsstyringssystemene, og det bør utarbeides veiledningsmateriell som kan øke kompetansen på området.

Status på tiltak

Utvalgets anbefaling peker først og fremst på departementene og at de skal tydeliggjøre krav og føringer for virksomhetsstyringssystemer i egen sektor. Høringssvarene viser at det er bred enighet om denne anbefalingen.

Det stilles krav om bruk av styringssystem for informasjonssikkerhet i eForvaltningsforskriften § 15. Alle forvaltningsorgan som benytter elektronisk kommunikasjon, skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. Kommunal- og moderniseringsdepartementet har pekt ut Difi til det organet som skal gi anbefalinger på området til statsforvaltningen. I 2016 lanserte Difi veilederen *Internkontroll i praksis – informasjonssikkerhet*.[1] Veilederen er først og fremst myntet på offentlige virksomheter, men er

tilgjengelig for alle fra Difis nettsider. NSM forvalter også en veileder i sikkerhetsstyring (sist oppdatert i 2015).[2] Formålet er å gi råd til virksomheter om hvordan et styringssystem for sikkerhet kan etableres og videreutvikles.

NSM arbeider med å etablere et helhetlig og systematisk sett med de viktigste minimumskrav og tiltak for å sikre samfunnsviktige IKT-løsninger gjennom grunnprinsipper for IKT-sikkerhet. Grunnprinsippene vil legge til rette for gjenbruk i og på tvers av ulike sektorer ved å bygge på etablerte internasjonale standarder. Prinsippene skal gjøre det enklere for sektorer og virksomheter å oppfylle krav i ulike regelverk og på den måten legge til rette for felles tekniske løsninger. Hensikten er å gi beslutningstakere i offentlige og private virksomheter en tiltakspakke for sikring av sin virksomhet og sine informasjonssystemer. Den første tiltakspakken vil bli publisert i løpet av 2017, med påfølgende jevnlige revisjoner og oppdateringer.

22.3 Bevisst bruk av standarder

Problembeskrivelse (NOU 2015: 13, punkt 23.2.1)

Kravene til IKT-sikkerhet i offentlig sektor er ofte funksjonsbaserte og har definerte overordnede mål. Det er ofte henvist til bruk av standarder på områder der det eksisterer et funksjonsbasert regelverk. Norge bør i stor grad implementere standarder som er internasjonalt anerkjent, og på IKT-området er det i liten grad hensiktsmessig eller nødvendig å produsere særnorske standarder. Det er imidlertid viktig at Norge bidrar og er aktiv i utarbeidelsen av standarder internasjonalt. Justis- og beredskapsdepartementet har et særskilt ansvar for de standardene som omhandler IKT-sikkerhet, og som ikke er direkte relatert til en bestemt sektor. Utvalget anbefaler at Justis- og beredskapsdepartementet har en strategisk tilnærming til hvordan det skal bidra i standardiseringsarbeidet.

Status på tiltak

Høringssvarene gir bred støtte til tiltaket og poengterer at standarder bidrar til felles begrepsbruk og definisjoner. Internasjonalt er det utviklet gode standarder som revideres jevnlig i takt med den teknologiske utviklingen. Å utvikle egne norske standarder innenfor IKT-sikkerhet er derfor ikke hensiktsmessig.

Regjeringen ønsker at Norge skal være til stede på internasjonale arenaer hvor IKT-sikkerhetsstandarder utvikles. Justis- og beredskapsdepartementet har inngått et samarbeid med Standard Norge med dette formålet, og departementet har i 2016 gitt Standard Norge tilsagn om bevilgning til arbeidsprogrammet *standardisering innen IKT-sikkerhet*.

Standard Norge organiserer arbeidet for internasjonal påvirkning med relevante aktører for å sikre norske interesser i utviklingen av internasjonale IKT-sikkerhetsstandarder. Reetablering av en norsk speilkomité skal bidra til å avklare behov for standarder innenfor IKT-sikkerhetsområdet. Den skal utvikle et eget arbeidsprogram med oversikt over hvilke arbeider som skal følges opp fra norsk side. Arbeidsprogrammet har langsiktig varighet og skal være i tråd med Norges digitale satsing, men også europeiske arbeider og EU-kommisjonens plan for IKT-sikkerhet.[3]

Kommunal- og moderniseringsdepartementet gir også Standard Norge et årlig tilskudd via Difi. Formålet med bevilgningen er å støtte Standard Norge i arbeidet med IKT-standardisering generelt og oppfølgingsarbeid innenfor IKT-sikkerhetsstandardisering og å bidra til kompetanseoverføring på området mellom Standard Norge og forvaltningen. Flere statlige etater bidrar også i standardiseringsarbeidet.

22.4 Tydeliggjøre Justis- og beredskapsdepartementets rolle og ansvarsområde

Problembeskrivelse (NOU 2015: 13, punkt 23.3.1)

Justis- og beredskapsdepartementets samordningsansvar for forebyggende IKT-sikkerhet i sivil sektor omfatter etter Lysneutvalgets oppfatning både offentlig og privat sektor. Det enkelte fagdepartement har ansvar innenfor egen sektor. Utvalget anbefaler å konkretisere ansvaret for IKT-sikkerhet ytterligere, slik at det går klart frem at Justis- og beredskapsdepartementets samordningsansvar gjelder både offentlig og privat sektor. Om nødvendig kan en slik klargjøring komme i form av en revisjon av kongelig resolusjon 22. mars 2013.

---

1 Difis veiledningsmateriell «Internkontroll i praksis»: http://internkontroll.infosikkerhet.difi.no/.

2 Veileder i sikkerhetsstyring, NSM (2015).

3 *Rolling Plan for ICT Standardisation*, European Commision (2017).

Status på tiltak

Justis- og beredskapsdepartementet har samordningsansvaret for IKT-sikkerhet i sivil sektor. Roller og ansvar er presisert i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* og kongelig resolusjon av 10. mars 2017 om ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innenfor samfunnssikkerhet og IKT-sikkerhet.

For å skape en felles tilnærming til IKT-sikkerhet i statsforvaltningen må fagmyndighetene gi anbefalinger som er koordinerte. Justis- og beredskapsdepartementet, Kommunal- og moderniseringsdepartementet, NSM og Difi møtes jevnlig for å samordne innsatsen og dra nytte av hverandres kompetanse.

22.5 Styrke Justis- og beredskapsdepartementets virkemidler

Problembeskrivelse (NOU 2015: 13, punkt 23.3.2)

Justis- og beredskapsdepartementet må gjøre ytterligere grep for å få oversikt over digitale sårbarheter på tvers av sektorer. Det anbefales at departementet ber NSM og DSB i samarbeid utarbeide et felles metodisk rammeverk som kan ligge til grunn for en helhetlig årlig oversikt over digital sårbarhet. Videre at Justis- og beredskapsdepartementet utarbeider en helhetsoversikt over digitale sårbarheter. Oversikten skal bidra til komparative tverrsektorielle sammenligninger og gi et kunnskapsgrunnlag for virkemiddelbruk og prioriteringer på tvers av sektorer.

Justis- og beredskapsdepartementets samordningsansvar bør omfatte samordning av minstekrav til IKT-sikkerhet i sivil sektor. Justis- og beredskapsdepartementet anbefales aktivt å følge opp prosessen rundt EUs NIS-direktiv og vurdere hvilke konsekvenser direktivet kan få for Norge, og hvordan dette kan påvirke Justis- og beredskapsdepartementets samordningsrolle på området, særlig med tanke på å gi føringer og stille krav til andre departementer og forberede sektorene på å implementere direktivet.

Samfunnets teknologiske avhengighet gjør at teknologiskifter og større strukturelle endringer har konsekvenser for den digitale sårbarheten. Utvalget anbefaler å se hen til hvordan Konkurransetilsynet ivaretar konkurransehensyn ved organisatoriske og strukturelle endringer i markedet. Ordningen bør ivaretas av Justis- og beredskapsdepartementet.

Utvalget peker særlig på viktigheten av samarbeid med privat sektor. Utvalget anbefaler at Justis- og beredskapsdepartementet vurderer hvorvidt det offentlige–private samarbeidet på IKT-sikkerhetsområdet er tilstrekkelig ivaretatt og hensiktsmessig, og hvorvidt det er behov for en strategisk arena for samarbeid med eiere av kritisk infrastruktur og kritisk informasjon og med akademia, under ledelse av Justis- og beredskapsdepartementet.

Status på tiltak

Utarbeide et felles metodisk rammeverk for, og en årlig helhetsoversikt over, digitale sårbarheter

I 2015 utarbeidet NSM rapporten *Helhetlig IKT-risikobilde* for første gang. Hensikten med rapporten er å etablere et felles situasjonsbilde som gjør virksomheter og myndigheter i stand til å treffe riktige tiltak. I tillegg skal den være et verktøy for virksomheter i deres arbeid med å utarbeide risikovurderinger. Rapporten utgis årlig. NSM har fått i oppdrag å videreutvikle rapporten i samarbeid med andre relevante virksomheter, blant annet DSB. Mer informasjon om dette finnes i punkt 6.6.

Samordning av minstekrav til IKT-sikkerhet i sivil sektor og oppfølging av NIS-direktivet

Den 6. juli 2016 ble Europaparlamentet og Det europeiske råds direktiv (EU) 2016/1148 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet), vedtatt i EU. Regjeringen mener at NIS-direktivet er EØS-relevant og akseptabelt.

Formålet med direktivet er å forbedre det indre markeds funksjon. Et høyt felles IKT-sikkerhetsnivå skal styrke europeiske virksomheters konkurransedyktighet i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa. Videre vil et økt sikkerhetsnivå redusere kostnadene forbundet med sikkerhetsbrudd og IKT-kriminalitet.

Direktivet pålegger medlemsstatene å sørge for et minimumsnivå for den nasjonale IKT-sikkerheten ved at de plikter å utarbeide en nasjonal strategi for IKT-sikkerhetsarbeidet, å etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og å pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. Direktivet etablerer to internasjonale samarbeidsgrupper – én på strategisk nivå og én på CSIRT-nivå.

Justis- og beredskapsdepartementet har ansvaret for å følge opp NIS-direktivet. Det er ikke formelt avgjort at direktivet vil bli norsk rett. Norge deltar likevel som observatør i NIS' ekspertgruppe, NIS-komiteen og NIS' samarbeidsgruppe. Gjennom Justis- og beredskapsdepartementets deltakelse i disse gruppene bidrar Norge til å drive det videre arbeidet med direktivet fremover. Den internasjonale deltakelsen legger et godt grunnlag for en eventuell gjennomføring av direktivet i norsk rett. En gjennomføring vil innebære at det gjennom lov innføres et minimumsnivå for virksomheters IKT-sikkerhet og krav om varsling. Myndighetene skal kontrollere at direktivet etterleves som forutsatt.

Ivareta hensyn til IKT-sikkerhet ved teknologiskifter og strukturelle samfunnsendringer

I punkt 6.4 i Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* fremgår det at alle departementer i sivil sektor har ansvar for å følge opp krav og anbefalinger gitt av Justis- og beredskapsdepartementet for egen virksomhet og i egen sektor. Departementene skal involvere Justis- og beredskapsdepartementet i prosesser hvor IKT-sikkerhetshensyn er av nasjonal betydning, særlig ved større teknologiske og strukturelle endringer i samfunnet.

Etablere en arena for offentlig–privat samarbeid

Regjeringen er opptatt av å styrke offentlig–privat samarbeid, og det skal opprettes et eget forum for å støtte opp under det nasjonale arbeidet med IKT-sikkerhet. Se en nærmere omtale av dette under punkt 5.1.

22.6 Øke kapasiteten innen IKT-sikkerhet i Justis- og beredskapsdepartementet

Problembeskrivelse (NOU 2015: 13, punkt 23.3.3)

Utvalget anbefaler å styrke Justis- og beredskapsdepartementets ressurser vesentlig på IKT-sikkerhetsområdet for å ivareta departementets rolle og gjennomføre tiltakene som følger av Lysneutvalgets utredning.

Status på tiltak

Justis- og beredskapsdepartementet støtter Lysneutvalgets vurdering knyttet til behov for styrking av departementet på dette området. Justis- og beredskapsdepartementet opplever en stadig økning i oppgavetilfang, forventinger og behov innenfor oppfølging av nasjonal IKT-sikkerhet, herunder også knyttet til oppfølgingen av Lysneutvalgets utredning.

Justis- og beredskapsdepartementet har hatt en vesentlig styrking på området siden departementet overtok samordningsansvaret i 2013. Det er viktig å merke seg at denne styrkingen i seg selv skaper utfordringer hos samarbeidspartnere som ikke har opplevd den samme styrkingen, og som merker økt oppgavetilfang som følge av Justis- og beredskapsdepartementets økte aktivitet. Etter Justis- og beredskapsdepartementets vurdering må kapasitetsbehovene innenfor IKT-sikkerhet i sentrale departement og fagmiljøer sees i sammenheng.

22.7 Tilpasse tilsynsvirksomheten til å omfatte IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 23.4)

Utvalget anbefaler at når tilsynsmyndighetene skal utforme nye krav og føringer til regulerte virksomheter, må de ta hensyn til vurderingene av funksjonsbasert regelverk. Når det skal stilles krav til IKT-sikkerhet, bør funksjonsbasert regelverk og tilsyn vurderes – dette for å kunne følge med på raske teknologiske endringer og legge til rette for sikkerhetstiltak som er tilpasset den enkelte virksomheten.

Etter utvalgets vurderinger er det behov for å styrke IKT-sikkerhetskompetansen innenfor flere sektortilsyn. På kort sikt kan det være hensiktsmessig med felles ressurser, slik at ulike sektortilsyn kan tilføres kompetanse fra for eksempel NSM i enkelttilfeller. På lengre sikt tilsier utviklingen at tilsynsmyndighetene må etablere egen kompetanse. Utvalget anbefaler at Justis- og beredskapsdepartementet tar initiativ til å etablere en fellesarena for tilsynssamarbeid på IKT-sikkerhetsområdet.

Status på tiltak

Høringssvarene viser at dette er et viktig tiltak, og det jobbes godt med kompetanseheving i flere sektortilsyn. For eksempel har NVE oppbemannet, og en tilsvarende prosess pågår i Ptil. Allikevel er det slik at knappheten på IKT-sikkerhetskompetanse i samfunnet gjør det utfordrende å bemanne opp alle sektortilsyn med tilstrekkelig kompetanse på området.

For å styrke IKT-sikkerheten og kvaliteten på IKT-sikkerhetstilsyn som gjennomføres i de ulike sektorene, ønsker Justis- og beredskapsdepartementet og Forsvarsdepartementet at det etableres en felles arena for de ulike sektorenes mest sentrale tilsynsmyndigheter. Hensikten er å sikre informasjonsutveksling og kompetanseoverføring og på den måten øke kvaliteten på sektorenes tilsyn med IKT-sikkerhet. Departementene har bedt NSM om å etablere og lede en slik arena.

Difi og FFI har på oppdrag fra Justis- og beredskapsdepartementet evaluert tilsynene som DSB utfører på vegne av Justis- og beredskapsdepartementet. Innenfor IKT-sikkerhetsområdet viser evalueringen at mer enn halvparten av departementene ser et behov for inntrengingstesting som et tillegg til, eller alternativ til, dagens tilsyn. Bruk av inntrengingstesting kan være et effektivt virkemiddel for å avdekke sårbarheter ved et informasjonssystem. Det er imidlertid viktig at bruk av slik testing kommer i tillegg til og ikke som erstatning for, systematisk arbeid med IKT-sikkerhet i virksomhetene. Punkt 6.5 gir en nærmere omtale av inntrengingstesting. Punkt 8.6 gir en nærmere omtale av kompetanse i tilsyn.

22.8 En redegjørelse for IKT-sikkerhet bør inngå i årsmeldinger

Problembeskrivelse (NOU 2015: 13, punkt 23.5)

Ansvaret for IKT-sikkerhet ligger hos den øverste ledelsen både i offentlig og i privat virksomhet. Utvalgets undersøkelser tyder på at arbeidet med IKT-sikkerhet ikke alltid får den prioriteten det bør ha. For å sikre at arbeidet med IKT-sikkerhet prioriteres høyere, bør det innføres et krav om at ivaretakelse av IKT-sikkerhet beskrives i virksomhetenes årsmelding. Utvalget oppfordrer Nærings- og fiskeridepartementet og Kommunal- og moderniseringsdepartementet til å utarbeide en regelendring i lovverket for henholdsvis offentlig og privat sektor.

Status på tiltak

Høringssvarene er noe delte i synet på dette tiltaket. Rapporteringsplikter i årsrapporten bør vurderes ut fra om det gir god nok gevinst holdt opp mot kostnadene og tidsbruken på rapporteringen.

Finansdepartementet har fastsatt krav til statlige virksomheters årsrapport i økonomiregelverket. Det er et uttalt mål at rapporteringen skal holdes på et moderat nivå. Krav til innhold i årsregnskap og årsberetninger for regnskapspliktige foretak er regulert i lov om årsregnskap mv. kapittel 3 (regnskapsloven). Denne loven hører inn under Finansdepartementets ansvarsområde, men andre krav til avleggelse av årsregnskap finnes også i annet lovverk. Kravene bør harmoniseres, men det enkelte departement har ansvar for å følge opp regelverket innenfor sitt ansvarsområde, herunder også i medhold av de sentrale føringer som gis.

22.9 Næringsutvikling og IKT-sikkerhet

Problembeskrivelse (NOU 2015: 13, punkt 23.6)

En sterk IKT-sikkerhetsindustri i Norge vil være et positivt bidrag til å redusere digitale sårbarheter. Dette vil sikre kompetanse og bidra til oppmerksomhet og kunnskapsspredning i hele det norske samfunnet. Utvalget anbefaler derfor at regjeringen forsterker arbeidet med å se etter virkemidler for å stimulere til næringsutvikling på dette området, for eksempel gjennom skattepolitikk, tilskuddsordninger og kompetansebygging i dialog med næringslivet.

Status på tiltak

Hovedmålet i næringspolitikken er å legge til rette for størst mulig samlet verdiskaping i norsk økonomi, innenfor bærekraftige rammer. Næringspolitikken skal legge til rette for at ressurser brukes der de har sin beste anvendelse, slik at verdiskapingen blir størst. Næringspolitikken har derfor som mål å legge til rette for gode rammebetingelser og virkemidler som favner bredt, og søker aktivt å legge til rette for velfungerende markeder ved å korrigere for markedssvikt der det er hensiktsmessig. Regjeringens politikk for skatter og avgifter, og forskning, utvikling og innovasjon skal legge til rette for konkurransedyktig utvikling innenfor alle næringer, også IKT-sikkerhetsnæringen. Regjeringen vil legge til rette for fremtidens næringsliv ved å sikre tilgang på kompetanse og satse videre på forskning, innovasjon og teknologiutvikling.

I tillegg legges det til rette for nyskaping i næringslivet gjennom Forskningsrådets og Innovasjon Norges ordninger. Næringsstimulerende virkemidler som kan nyttiggjøres innenfor IKT-sikkerhetsindustrien, er de generelle ordningene Skattefunn og Brukerstyrte innovasjonsarena (BIA) fra Forskningsrådet.

22.10 Utkontraktering og skytjenester

Problembeskrivelse (NOU 2015: 13, punkt 23.7)

Bruk av utkontraktering og skytjenester i både offentlig og privat virksomheter er forventet å øke i årene fremover. Selv om utkontraktering og bruk av skytjenester kan bidra til økt teknisk IKT-sikkerhet, fritas ikke virksomheten for IKT-sikkerhetsansvaret og -arbeidet.

Lysneutvalget mener regjeringens påbegynte arbeid for å fjerne unødige hindringer, rydde opp i lovtekniske hindringer og legge til rette for sikre løsninger er viktig. Særlig bør arbeidet som omhandler hva slags informasjon som kan lagres hvor, herunder arkivlovens og bokføringslovens bestemmelser, belyses. Det bør også gjennomføres en felles utredning på tvers av sektorene, slik at det etableres en felles tilsynspraksis for data lagret i skytjenester. Dette inkluderer bruk av tredjepartsrevisorer.

I en særmerknad fra et av utvalgsmedlemmene legges det vekt på at Justis- og beredskapsdepartementet i politikkutformingen knyttet til digitale sårbarheter og skytjenester også må se muligheten teknologien gir for å øke sikkerheten. Dette bør utføres i samråd med Nærings- og fiskeridepartementet og Kommunal- og moderniseringsdepartementet.

Status på tiltak

I 2016 la Kommunal- og moderniseringsdepartementet fram en nasjonal strategi for bruk av skytjenester. Målet med strategien er å synliggjøre hvordan offentlige og private virksomheter kan ha utbytte av å bruke skytjenester, og når slike tjenester er egnet for bruk i offentlig sektor. Departementet har gitt Difi i oppdrag å etablere et kompetansemiljø og veiledningsressurser knyttet til anskaffelse av skytjenester. Dette inkluderer vurderinger knyttet til sikkerhet og risiko, herunder verdivurdering av informasjon, og å samle anbefalinger fra de ulike sektorene på dette området.

Kommunal- og moderniseringsdepartementet vurderer også om det skal utvikles en markedsplass eller andre mekanismer som gjør vurdering og anskaffelse av skytjenester enklere for virksomhetene.

Kommunal- og moderniseringsdepartementet har startet et arbeid med å harmonisere måten ulike tilsyn jobber på når de fører tilsyn med informasjonssikkerhet i skytjenester. Erfaringen så langt er at ulikhetene i tilsynspraksis er mindre enn man tidligere har fått inntrykk av. Kommunal- og moderniseringsdepartementet opplever at tilsynene er interessert i å dele erfaringer og lære av hverandre på dette området.

Kommunal- og moderniseringsdepartementet har diskutert bruk av tredjepartsrevisjoner med tilsyn. Det er få tilsyn som har konkrete erfaringer med dette, men de som har det, har gjennomgående positive erfaringer. Dette er også et område som er viktig for EU-kommisjonen, og Kommunal- og moderniseringsdepartementet både deltar i og følger med på det arbeidet som skjer innenfor skytjenester og fri flyt av data i EU. Regjeringen vurderer det slik at det ikke vil være hensiktsmessig å sette i gang en egen utredning på dette området, men man fortsetter med å vurdere status og å delta i relevant EU-arbeid på området.

Kulturdepartementet har hatt revidert arkivforskrift på høring. Høringsfrist var 15. januar 2017. Den reviderte forskriften åpner for lagring av digitale offentlige arkiv i utlandet (§ 22), gitt at leverandøren tilfredsstiller de krav som stilles for oppbevaring av arkivmateriale. Kommunal- og moderniseringsdepartementet vil nå også se på en mulig utvidelse i hvor man kan lagre bokføringsdata. I dag er det kun tillatt å lagre dette i Norden.

Justis- og beredskapsdepartementet, Forsvarsdepartementet og Kommunal- og moderniseringsdepartementet vurderer muligheten for å etablere en skyløsning med høyt sikkerhetsnivå. Et viktig formål er å vurdere hvordan sentrale myndigheter med særskilte sikkerhetsbehov også kan utnytte de effektiviseringsmulighetene som skytjenester gir. NSM og Difi gjennomfører vurderingen.

Se nærmere omtale av tjenesteutsetting under punkt 6.4.

22.11 Regulering av kryptografi

Problembeskrivelse (NOU 2015: 13, punkt 23.8)

Kryptografi er teknikker som skal sikre informasjonens opphav, hindre innsyn og avdekke endring. Bruk av kryptografiske mekanismer har stor betydning for IKT-sikkerhet og er en forutsetning for sikker elektronisk kommunikasjon. Lysneutvalget er av den oppfatning at bruk av kryptografi ikke skal reguleres eller forbys i Norge. Norske myndigheter bør arbeide aktivt mot regulering eller forbud internasjonalt. Ved økt bruk av kryptografiske mekanismer for å beskytte informasjon og kommunikasjon bør nye etterforskningsmetoder utvikles for å sikre effektivt politi- og etterretningsarbeid.

Status på tiltak

Bruk av kryptering skal ikke forbys eller reguleres

Regjeringen legger til grunn at utvalget mener at kryptering ikke skal forbys eller begrenses gjennom lov. Dette berører ikke dagens regulering av kryptosikkerhet i sikkerhetsloven. Regjeringen legger dessuten til grunn at når utvalget skriver «ikke reguleres» / «arbeide aktivt mot regulering», mener det ikke regulering i form av pålegg om kryptering gjennom lov, slik det blant annet er krav om gjennom de ulike regelverkene for sikring av personopplysninger.

Regjeringen slutter seg generelt til utvalgets konklusjoner om ikke å forby eller regulere bruk av kryptografi. Kryptering og tilgang til robuste krypteringsmetoder er en forutsetning for å kunne kommunisere med trygghet for at kommunikasjonsinnholdet ikke fanges opp.

Norske myndigheter bør arbeide aktivt mot regulering eller forbud internasjonalt

Myndighetene fremholder sine synspunkter i relevante internasjonale fora, for eksempel EU og OECD.

Utvikling av nye etterforskningsmetoder

Behovet for utvikling av nye etterforskningsmetoder henger tett sammen med punktet over om utbredelsen av kryptering. Økt bruk av kryptering skaper utfordringer for politi og påtalemyndighet.

Regjeringen foreslo i Prop. 68 L (2015–2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)* lovendringer som skulle gi politiet utvidet adgang til å benytte skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd. Blant annet ble det foreslått å innføre dataavlesing som et nytt, skjult tvangsmiddel med hjemmel i straffeprosessloven nye §§ 216 o og 216 p. Forslaget var begrunnet i «et stort og udekket behov for effektiv tilgang til elektronisk lagret og kommunisert informasjon. Informasjon produseres, bearbeides, kommuniseres og lagres i dag ofte elektronisk og ved bruk av mobile tjenester. Samtidig øker bruken av krypteringsløsninger og andre metoder for beskyttelse av slik informasjon». Forslaget ble vedtatt med bred støtte i Stortinget, med enkelte mindre endringer. Lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler) trådte delvis i kraft 17. juni 2016, med unntak av bestemmelsene om dataavlesning, som på grunn av forskriftsendringer først trådte i kraft 9. september 2016.

For øvrig vil regjeringen påpeke at ved vurdering av nye etterforskningsmetoder er det helt avgjørende å vurdere personvernkonsekvenser ved de nye metodene grundig og å se inngrepet de nye metodene representerer, i sammenheng med allerede eksisterende personverninngrep.

Norsk kryptopolitikk

NSM har et tett samarbeid med norsk kryptoindustri for å utvikle høygraderte kryptoløsninger. Det er en langsiktig prosess å bygge opp kompetanse- og forskningsmiljøer, og kunnskap om kryptering må vedlikeholdes dersom den skal være relevant. Uten kompetente nasjonale fagmiljøer vil norske myndigheter og bedrifter måtte forholde seg til utenlandske aktører for å innhente kvalifiserte vurderinger og råd om kryptografiske systemer. Dette vil være uheldig sett fra et nasjonalt sikkerhetsperspektiv.

For å bidra til å sikre nødvendig nasjonal kryptokompetanse og stimulere til innovasjon og produktutvikling vil Forsvarsdepartementet og Justis- og beredskapsdepartementet revidere nasjonal kryptopolitikk.[4]

---

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

Del IV
Økonomiske og administrative konsekvenser

23 Økonomiske og administrative konsekvenser

I regjeringens politiske plattform er *trygghet i hverdagen og styrket beredskap* løftet frem som et av åtte viktige satsingsområder. Denne stortingsmeldingen redegjør for regjeringens politikk for arbeidet med IKT-sikkerhet.

IKT-sikkerhet er et bredt fagområde som berører de fleste sektorer og mange ulike samfunnsområder. Meldingen tar ikke sikte på å gi en uttømmende redegjørelse for alt som gjøres av betydning for IKT-sikkerhet, men fremhever noen viktige prioriterte områder.

Vesentlige deler av IKT-sikkerhetsarbeidet skjer i hver enkelt sektor, basert på relevant sektorlovgivning samt spesifikke krav til departementenes samfunnssikkerhetsarbeid og arbeid med IKT-sikkerhet. Arbeidet skal være en integrert del av den ordinære styringen. Hvis risiko- og sårbarhetsbildet endrer seg, er det viktig at tiltakene og virkemiddelapparatet justeres deretter. Endring i virkemiddelbruk, og eventuelle tiltak som iverksettes som et resultat av endringer i risiko- og sårbarhetsbildet, skal dekkes innenfor gjeldende budsjettrammer. Hvis tiltak medfører utgiftsøkninger over statsbudsjettet, vil regjeringen komme tilbake til dette i forbindelse med de årlige budsjettforslagene.

Regjeringen har ambisjon om å styrke IKT-sikkerhetsarbeidet på flere sentrale områder. I meldingen vises det blant annet til strategier, handlingsplaner og annet for de nærmeste årene som vil kunne innebære merutgifter. Tiltakene skal i utgangspunktet dekkes innenfor gjeldende budsjettrammer. Eventuelle utgifter eller innsparinger som går ut over gjeldende budsjettrammer, vil regjeringen komme tilbake til i forbindelse med de årlige budsjettforslagene. Det kan derfor ikke tidfestes når tiltakene eventuelt kan gjennomføres.

Justis- og beredskapsdepartementet

t i l r å r :

Tilråding fra Justis- og beredskapsdepartementet 9. juni 2017 om IKT-sikkerhet – Et felles ansvar blir sendt Stortinget.

Bestilling av publikasjoner

Offentlige institusjoner:
Departementenes sikkerhets- og serviceorganisasjon
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 00 00

Privat sektor:
Internett: www.fagbokforlaget.no/offpub
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Omslagsillustrasjon: M. Sylstad, NSM. Bilder hentet fra Colourbox og Earth Science and Remote Sensing Unit, NASA Johnson Space Center

Trykk: 07 PrintMedia AS – 06/2017