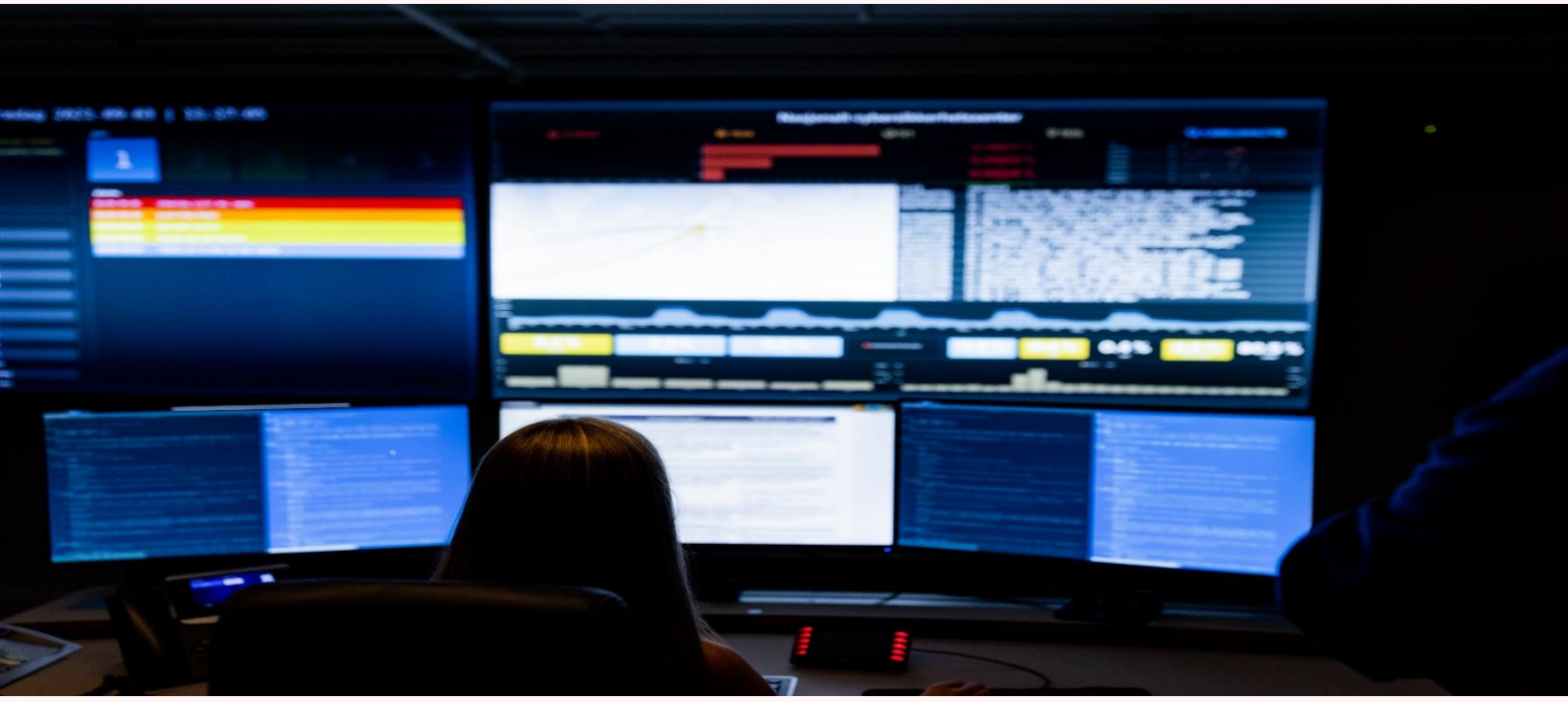
Riksrevisjonen

Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor

Dokument 3:7 (2022–2023)



Riksrevisjonen

Til Stortinget

Riksrevisjonen legger med dette fram Dokument 3:7 (2022–2023) *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*

Dokumentet har følgende inndeling:

- Riksrevisjonens konklusjoner, utdyping av konklusjoner, anbefalinger, statsrådens svar og Riksrevisjonens uttalelse til statsrådens svar
- Vedlegg 1: Riksrevisjonens brev til statsråden
- Vedlegg 2: Statsrådens svar
- Vedlegg 3: Forvaltningsrevisjonsrapport med vurderinger

Riksrevisjonen, 2. februar 2023

for riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
riksrevisor

Forsidebilde: Nasjonal sikkerhetsmyndighet / Oda Hveem
ISBN-978-82-8229-555-0

Innhold

Tabelloversikt

Faktaboksoversikt

Riksrevisjonen benytter følgende begreper for kritikk, med denne rangeringen etter høyest alvorlighetsgrad:

1. **Sterkt kritikkverdig** er Riksrevisjonens sterkeste kritikk. Vi bruker dette kritikknivået når vi finner alvorlige svakheter, feil og mangler. Ofte vil disse kunne få svært store konsekvenser for enkeltmennesker eller samfunnet.

2. **Kritikkverdig** bruker vi når vi finner betydelige svakheter, feil og mangler som ofte vil kunne få moderate til store konsekvenser for enkeltmennesker eller samfunnet.

3. **Ikke tilfredsstillende** bruker vi når vi finner svakheter, feil og mangler, men som i mindre grad får direkte konsekvenser for enkeltmennesker eller samfunnet.

1 Innledning

I den siste *samfunnssikkerhetsmeldingen* fra 2020 går det fram at digital sikkerhet er helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser.[1]

De nasjonale etterretnings- og sikkerhetstjenestene har over flere år vurdert etterretningstrusselen som den største trusselen mot Norge. Politiets sikkerhetstjeneste viser til at digitale operasjoner har blitt en integrert del av andre lands etterretningstjenester. Det vises også til at statlige etterretningsaktører i andre land har gjennomført sabotasje ved hjelp av digitale angrep.[2] Ifølge Nasjonal sikkerhetsmyndighet har det i perioden 2019 til 2021 vært en tredobling i antall alvorlige digitale hendelser og angrep mot offentlige og private virksomheter i Norge.[3] Både Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste rapporterer om økt digital trusselaktivitet i Norge som følge av krigen i Ukraina.[4]

Digitale operasjoner og digitale angrep

En prosess der en trusselaktør søker å skaffe seg urettmessig tilgang til et digitalt nettverk hos en spesifikk virksomhet. Formålet med en digital operasjon kan være etterretnings-innsamling, forberedelser til potensiell sabotasje, tyveri eller manipulasjon av data. Ved et digitalt angrep er formålet å stjele, sabotere eller manipulere data.

En økende grad av digitalisering og samarbeid på tvers av sektorer og landegrenser gjør samfunnet vårt mer sårbart for digitale trusler. Et digitalt angrep kan få store negative konsekvenser for Norge ved at funksjoner som er kritiske for stat og samfunn rammes. Dette kan for eksempel være betalingssystemer, helsevesenet, kraftforsyningen, elektronisk kommunikasjon eller transport.

Arbeidet med digital sikkerhet berører hele samfunnet, og krever derfor samordning av aktører og virkemidler på tvers av sektorene. Det er Justis- og beredskapsdepartementet som siden 2013 har hatt ansvar for samordningen av samfunnssikkerhetsarbeidet og digital sikkerhet i sivil sektor.[5] Departementet har videre et overordnet ansvar for det forebyggende sikkerhetsarbeidet i sivil sektor.[6]

I 2018 pekte IKT-sikkerhetsutvalget på at styringen av den digitale sikkerheten er sterk i flere sektorer, men at samordningen og oversikten på tvers av sektorer er mangelfull.[7] Dårlig samordning kan føre til overlapp mellom ansvarsområder og blindsoner i regulering, oversikter og oppfølging. Effektiv samordning kan på sin side redusere ressursbruken og forbedre effekten av tiltak og virkemidler.[8]

---

[1] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden* (*samfunnssikkerhetsmeldingen*)
[2] Politiets sikkerhetstjeneste (2021) *PSTs trusselvurdering 2021;* Politiets sikkerhetstjeneste (2022) *PSTs trusselvurdering 2022*.
[3] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022*, s. 9.
[4] Politiets sikkerhetstjeneste, *Pressemelding: PST vurderer etterretningstrusselen fra Russland i Norge som økt*, 18. mars 2022. VG, *PST: Forhøyet sabotasjetrussel mot Norge*. 18. oktober 2022. Nettartikkel. [Hentet: 25. oktober 2022].
[5] Kgl. res. av 10. mars 2017 nr. 312 *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*
[6] Kgl. res. av 1. april 2013 *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*; Kgl.res. 20. desember 2018 *Ikraftsetting av lov 1. juni 2018 nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.*
[7] NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*
[8] Trondal, Jarle (2017) *The Rise of Common Political Order.* Storbritannia: Edward Elgar Publishing.

Riksrevisjonens undersøkelse har tatt utgangspunkt i blant annet følgende vedtak og forutsetninger fra Stortinget:

- Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020−2021)
- Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar*, jf. Innst. 187 S (2017−2018)
- kgl.res. av 10. mars 2017 nr. 312: *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*
- *instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen), 2017
- *lov om nasjonal sikkerhet* (sikkerhetsloven), 2019

Målet med undersøkelsen har vært å vurdere hvorvidt Justis- og beredskapsdepartements samordning av arbeidet med å ivareta den digitale sikkerheten i sivil sektor er effektiv og i tråd med Stortingets vedtak og forutsetninger. Undersøkelsesperioden er i hovedsak 2018−2021, men vi har også tatt med relevante data fra 2022 når disse har vært tilgjengelige.

I undersøkelsen ser vi nærmere på arbeidet med digital sikkerhet i flere sektorer, der ansvaret i hver enkelt sektor ligger hos det enkelte sektordepartement. Vi påpeker svakheter og utfordringer i enkelte virkemidler og tiltak som disse departementene har ansvar for. Når det er svakheter i samordningen av disse tiltakene, retter vi imidlertid kritikken mot Justis- og beredskapsdepartementet på grunn av departementets samordningsansvar for den digitale sikkerheten nasjonalt.

Store deler av undersøkelsesperioden har vært preget av koronapandemien, som kom til Norge i februar 2020. Pandemien har påvirket både myndighetene og samfunnet for øvrig på mange forskjellige måter. Nasjonal sikkerhetsmyndighet viser for eksempel til at utstrakt bruk av hjemmekontorløsninger har skapt nye digitale sårbarheter.[9] Pandemien økte presset mot enkelte sektorer og samfunnsfunksjoner som hadde sentrale oppgaver i pandemihåndteringen. Justis- og beredskapsdepartementet viser til at departementet og underliggende etater over en lengre periode har stått i en ekstraordinær situasjon der sikkerhets- og beredskapsressurser har måttet bistå i pandemihåndteringen. Departementet står nå i en tilsvarende situasjon, med krig i Ukraina og samordning av sivile behov.[10] Andre etater som omfattes av undersøkelsen, har også pekt på at restriksjonene som fulgte av pandemien, har påvirket arbeidet samfunnssikkerhet og digital sikkerhet. Riksrevisjonen bemerker at konsekvensene av svakheter og mangler i arbeidet med digital sikkerhet like fullt er de samme, og at det ofte vil være nødvendig å håndtere flere ulike risikoer og hendelser samtidig.

Rapporten ble forelagt Justis- og beredskapsdepartementet ved brev 13. oktober 2022. Departementet har i brev 11. november 2022 gitt

[9] Nasjonal sikkerhetsmyndighet (2021) *Nasjonalt digitalt risikobilde 2021*.
[10] Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet*. Brev til Riksrevisjonen, 11. november 2022.

kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

Rapporten, riksrevisorkollegiets oversendelsesbrev til departementet 30. november 2022 og statsrådens svar 16. desember 2022 følger som vedlegg.

2 Konklusjoner

- Svak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene.
- Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden.
- Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av *Nasjonal strategi for digital sikkerhet*.
- Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering.

3 Overordnet vurdering

Kritikkverdig

Samlet sett er det kritikkverdig at Justis- og beredskapsdepartementet med underliggende etater ikke har ivaretatt samordnings- og pådriveransvaret godt nok til å møte utfordringene på det digitale sikkerhetsområdet.

Det er videre kritikkverdig at

- Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar for å bidra til tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov
- Justis- og beredskapsdepartementet ikke har lagt godt nok til rette for tverrsektoriell hendelseshåndtering
- det gjennomføres få tilsyn med digital sikkerhet og tilsynsmyndighetene er lite samordnet

4 Utdyping av konklusjoner

Justis- og beredskapsdepartementets samordnings- og pådriveransvar på samfunnssikkerhetsområdet innebærer blant annet å initiere og koordinere prosesser på tvers av departementer, veilede departementene i arbeidet de gjør på området, og sørge for at problemstillinger på tvers av sektorer blir håndtert. Videre skal Justis- og beredskapsdepartementet utforme regjeringens politikk for den digitale sikkerheten nasjonalt, blant annet nasjonale strategier. Justis- og beredskapsdepartementet har fullmakt til å stille krav til departementenes samfunnssikkerhetsarbeid, etablere nasjonale krav til den digitale sikkerheten og gi nærmere bestemmelser om sin egen samordningsrolle og tilsynsfunksjon.[11] Samordningsansvaret innebærer også å sørge for at myndighetene har en helhetlig tilnærming til digital sikkerhet, og at kompetansen på digital sikkerhet møter framtidens behov.[12] Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap utøver viktige samordningsoppgaver for departementet på samfunnssikkerhetsområdet.

Samordning

En prosess der formålet er at ulike mål, verdier, aktiviteter, ressurser eller andre premisser blir sett i sammenheng, prioritert, avveid og tilpasset til hverandre.

Ifølge Justis- og beredskapsdepartementet har samordningen mellom etatene innenfor området digital sikkerhet hatt en positiv utvikling, både på departements- og etatsnivå. Departementet viser samtidig til at sektorprinsippet, varierende prioritering av sikkerhetsarbeidet i departementene og samarbeidsutfordringer mellom departementene gjør samordningen krevende.

Undersøkelsen viser at det er flere utfordringer med samordningen av arbeidet med digital sikkerhet som ikke har blitt håndtert. Justis- og beredskapsdepartementet har ikke sørget for at samordningen av roller, ansvar og krav er god nok når det gjelder dette arbeidet. Vi finner også at Justis- og beredskapsdepartementet ikke har tilstrekkelig oversikt over den nasjonale digitale sikkerhetstilstanden, særlig fordi departementenes arbeid med å kartlegge virksomheter som understøtter grunnleggende nasjonale funksjoner, går for sakte. Justis- og beredskapsdepartementet følger i liten grad opp hvilken effekt tiltakene i nasjonale strategier på det digitale sikkerhetsområdet har, og siden 2016 har de ikke sørget for at det på nasjonalt nivå har blitt øvd godt nok på å håndtere alvorlige digitale angrep som treffer flere sektorer.

Det er Riksrevisjonens vurdering at Justis- og beredskapsdepartementet med underliggende etater ikke ivaretar pådriver- og samordningsansvaret godt nok til å møte utfordringene på det digitale sikkerhetsområdet. Dette medfører risiko for at funksjoner som er kritiske for både stats- og samfunnssikkerheten, ikke er godt nok beskyttet mot digitale angrep, og at alvorlige digitale angrep ikke håndteres effektivt. Samlet sett vurderer vi at dette er **kritikkverdig**.

[11] *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen) (1. september 2017).

[12] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*.

4.1 Svak samordning av roller, ansvar og krav gjør arbeidet med forebyggende digital sikkerhet krevende for virksomhetene

Den nasjonale digitale sikkerheten reguleres av flere forskjellige regelverk. Regelverkene forvaltes av en rekke ulike aktører som har ansvar for at det føres tilsyn etter regelverkene, og for at det gis veiledning i hvordan regelverkene skal etterleves.

Ifølge *samfunnssikkerhetsmeldingen* er det satt et mål om at all rådgivning og veiledning om digital sikkerhet fra myndighetene skal være harmonisert og ensrettet. Justis- og beredskapsdepartementet skal bidra til at rådgivnings- og veiledningsaktiviteter innenfor digital sikkerhet blir bedre koordinert.[13]

Riksrevisjonens undersøkelse viser imidlertid at myndighetenes samordning av arbeidet med veiledning og tilsyn er svak, og at potensialet i sentrale samordningsarenaer ikke utnyttes fullt ut. Den svake samordningen gjør det forebyggende sikkerhetsarbeidet krevende for offentlige og private virksomheter.

4.1.1 Sentrale samordningsarenaer er lite forpliktende for deltakerne og bidrar i varierende grad til samordning

Det er etablert en rekke ulike samordningsarenaer som på forskjellige måter skal bidra til å samordne aktører med roller og ansvar knyttet til digital sikkerhet. Undersøkelsen viser imidlertid at disse arenaene i varierende grad bidrar til samordning av aktørene.

Samordningsarena

En fysisk eller digital møteplass der autonome aktører kan møtes for å utveksle informasjon, kunnskap og erfaringer med formål om å løse spesifikke komplekse utfordringer.

I tiltaksoversikten tilhørende *Nasjonal strategi for digital sikkerhet* (2019) trekkes det fram seks samordningsarenaer som skal understøtte målet om styrket samordning mellom aktørene og målet om å skape et felles situasjonsbilde på det digitale sikkerhetsområdet. De seks arenaene er: *Felles cyberkoordineringssenter*, *Forum for digital sikkerhet*, *Forum for IKT-tilsyn*, *Nasjonalt cybersikkerhetssenter*, *Nettverk for nasjonal IKT-sikkerhet* og *Nettverk for veiledningsaktører innen styring og kontroll*. I tillegg trekkes *Samhandlingsarena for sektortilsyn etter sikkerhetsloven* i *samfunnssikkerhetsmeldingen* fram som en sentral for samordning av myndigheter med ansvar for å føre tilsyn etter sikkerhetsloven. Tabell 1 viser deltakere og formål for de nevnte samordningsarenaene (unntatt *Felles cyberkoordineringssenter* som omtales i kapittel 4.4).

[13] Meld. St. 5 (2020−2021) S*amfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020–2021).

Tabell 1 Samordningsarenaer innenfor forebyggende digital sikkerhet – deltakere og formål

Navn og deltakere	Formål
Forum for digital sikkerhet *Representanter fra myndighetene, næringslivet, organisasjoner og akademia. Ledes av Nasjonal sikkerhetsmyndighet.*	Skal legge til rette for diskusjon av strategiske spørsmål knyttet til digital sikkerhet mellom private og offentlige aktører og myndigheter.
Forum for IKT-tilsyn *Digitaliseringsdirektoratet, Direktoratet for strålevern og atomsikkerhet, Finanstilsynet, Kystverket, Luftfartstilsynet, Mattilsynet, Nasjonal kommunikasjonsmyndighet, Norges vassdrags- og energidirektorat, Petroleumstilsynet, Sjøfartsdirektoratet og Statens jernbanetilsyn. Ledes av Nasjonal sikkerhetsmyndighet.*	Skal koordinere arbeidet mellom myndigheter som fører tilsyn med digital sikkerhet.
Nasjonalt cybersikkerhetssenter *Virksomheter fra offentlig og privat sektor. Ledes av Nasjonal sikkerhetsmyndighet.*	Skal fungere som er nasjonalt responsmiljø for håndtering av digitale hendelser, og som et knutepunkt mellom privat og offentlig sektor i arbeidet med digital sikkerhet.
Nettverk for nasjonal IKT-sikkerhet *Alle departementer. Ledes av Justis- og beredskapsdepartementet.*	Skal sørge for at strategiske spørsmål knyttet til internasjonalt samarbeid og digitale sikkerhetsutfordringer blir diskutert og koordinert mellom departementene.
Nettverk for veiledningsaktører innen styring og kontroll *Datatilsynet, Direktoratet for e-helse, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, Kommunesektorens organisasjon og Foreningen Kommunal Informasjonssikkerhet. Ledes av Digitaliseringsdirektoratet.*	Skal legge til rette for informasjonsutveksling om pågående samordningsprosjekter og samarbeide om ulike tema under styring og kontroll.
Samhandlingsarena for sektortilsyn etter sikkerhetsloven *Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet (leder) og Norges vassdrags- og energidirektorat.*	Skal legge til rette for kunnskaps- og erfaringsutveksling for å sikre kvalitet og enhetlig praksis i tilsynsvirksomhet etter sikkerhetsloven.

Nasjonalt cybersikkerhetssenter har oppgaver knyttet til både forebyggende sikkerhetsarbeid og hendelseshåndtering. Senterets oppgaver knyttet til hendelseshåndtering omtales i kapittel 4.4. Basert på undersøkelsen vurderer vi *Nasjonalt cybersikkerhetssenter* som en velfungerende samordningsarena innenfor forebyggende sikkerhetsarbeid. Senteret arrangerer jevnlige og hyppige møter med relevante tema og legger til rette for erfaringsutveksling mellom deltakerne. Deltakerne opplever begge deler som nyttig.

Når det gjelder *Nettverk for nasjonal IKT-sikkerhet*, *Forum for digital sikkerhet, Forum for IKT-tilsyn* og *Nettverk for veiledningsaktører innen styring og kontroll,* viser undersøkelsen at deltakerne i hovedsak bruker arenaene for å dele informasjon og orientere hverandre om pågående

arbeid. Møteaktiviteten har dessuten vært lav. For eksempel har det i *Nettverk for veiledningsaktører innen styring og kontroll* kun blitt avholdt fire møter siden desember 2020.

Videre har sammensetningen av deltakere i arenaene og deltakernes engasjement og erfaringsgrunnlag vært gjenstand for diskusjon. Da *Forum for digital sikkerhet* og *Nettverk for IKT-sikkerhet* ble evaluert i henholdsvis 2019 og 2020, kom det fram at de deltakende virksomhetene varierer med hensyn til hvor forpliktet og engasjert de er i arbeidet, og at deltakerne i *Forum for digital sikkerhet* i mindre grad evner å diskutere nasjonale sikkerhetsspørsmål på strategisk nivå. Evalueringene påpekte også at sammensetningen av deltakere i forumet ikke var ideell.

Det er positivt at Justis- og beredskapsdepartementet har endret *Forum for digital sikkerhets* sammensetning og mandat på bakgrunn av evalueringen. Det er også positivt at det i *Nettverk for veiledningsaktører innen styring og kontroll* har vært gjort en systematisk gjennomgang av deltakerne, og at flere nye, relevante aktører har kommet inn i nettverket siden etableringen.

Basert på evalueringen av *Nettverk for nasjonal IKT-sikkerhet* ble det besluttet å slå nettverket sammen med *Departementenes samordningsråd for samfunnssikkerhet,* men sammenslåingen er som følge av pandemien per november 2022 ikke gjennomført.

Slik samordningsarenaenes mandater er utformet i dag, med formål om kunnskaps- og erfaringsutveksling, er det ikke å forvente at deltakerne i arenaene skal drive operativt arbeid for økt samordning av det digitale sikkerhetsarbeidet. Det foregår dessuten mye samarbeid mellom deltakerne i arenaene, utover de planlagte møtene. Det er likevel Riksrevisjonens vurdering at de nevnte arenaene i større grad kunne vært benyttet til å styrke samordningen av det forebyggende digitale sikkerhetsarbeidet på nasjonalt nivå gjennom større grad av forpliktelse blant deltakerne og systematikk i arbeidet.

4.1.2 Tilsynsmyndighetene er lite samordnet, og arbeidet med felles tilsynsmetodikk er ikke kommet i gang

Tilsyn er et sentralt virkemiddel som Justis- og beredskapsdepartementet og øvrige myndigheter kan bruke til å kontrollere at regelverket på det digitale sikkerhetsområdet implementeres og overholdes. Allerede i 2005 pekte Koordineringsutvalget for informasjonssikkerhet på at det var behov for å samordne tilsyn og tilsynsmetodikken på området.

På oppdrag fra Justis- og beredskapsdepartementet skal Nasjonal sikkerhetsmyndighet legge til rette for hensiktsmessig samhandling mellom myndigheter som fører tilsyn med digital sikkerhet. Nasjonal sikkerhetsmyndighet har derfor etablert to ulike samordningsarenaer på tilsynsområdet. *Forum for IKT-tilsyn* hadde oppstartsmøte i mars 2021, mens *Samhandlingsarena for sektortilsyn etter sikkerhetsloven* ble etablert i 2019.

Deltakerne i *Samhandlingsarena for sektortilsyn etter sikkerhetsloven* har inngått samarbeidsavtaler om tilsyn. Det har vært avholdt møter for å legge

til rette for mer enhetlige tilsyn etter sikkerhetsloven, og Nasjonal sikkerhetsmyndighet har utarbeidet en veileder, *Veileder for tilsyn med forebyggende sikkerhetsarbeid*, og nettkurs om hvordan virksomheter skal gjennomføre tilsyn. Ettersom Norges vassdrags- og energidirektorat og Nasjonal kommunikasjonsmyndighet ennå ikke har gjennomført tilsyn etter sikkerhetsloven, foreligger det ingen informasjon om hvordan arbeidet i samhandlingsarenaen påvirker tilsynspraksisen.

I *Forum for IKT-tilsyn* har ikke arbeidet med å utarbeide en enhetlig tilsynsmetodikk kommet ordentlig i gang. Det har kun vært avholdt noen få møter, og arbeidet framstår som lite målrettet. Vi merker oss at det ikke har vært gjort noen systematisk gjennomgang av deltakerne,[14] verken ved etableringen av arenaen eller i ettertid, og at Datatilsynet ikke er representert i forumet.

Mangelen på samordning mellom tilsynsmyndighetene på det digitale sikkerhetsområdet kan føre til ulike oppfatninger av hva som er godt nok for å etterleve samme type regelverkskrav. Dette kan føre til ulike oppfatninger av hva som er godt nok hos tilsynsobjektene, ulik eller manglende etterlevelse av regelverkskrav og dermed ulik grad av digital sikkerhet mellom sektorene.

4.1.3 Brukere opplever det krevende å holde oversikt over regelverk og veiledning

Sikkerhetsloven og samfunnssikkerhetsinstruksen legger grunnlaget for arbeidet med nasjonal sikkerhet og samfunnssikkerhet, der digital sikkerhet er en integrert del.

Faktaboks 1 Samfunnssikkerhet, statssikkerhet og nasjonal sikkerhet

Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier som setter liv og helse i fare.

Statssikkerhet er å ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet.

Samfunnssikkerheten og statssikkerheten er gjensidig avhengig av hverandre. Framveksten av nye sikkerhetsutfordringer kan utfordre både samfunnssikkerheten og statssikkerheten, og skille mellom dem blir stadig mer utydelig.

Nasjonal sikkerhet er definert som statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Kilde: Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden.

I tillegg til disse er det mange andre regelverk som på ulike måter og i ulik grad omfatter digital sikkerhet. Tabell 2 gir en oversikt over aktuelle regelverk. Regelverkene forvaltes av ulike aktører, som blant annet er ansvarlige for å tilby veiledning i hvordan regelverkene skal etterleves.

[14] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.

Tabell 2 Oversikt over regelverk som omfatter digital sikkerhet

Generelt lovverk	Sektorspesifikt lovverk
• instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) • lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og sivilforsvaret • lov om nasjonal sikkerhet (sikkerhetsloven) • lov om behandling av personopplysninger (personopplysningsloven) • lov om behandlingsmåten i forvaltningssaker* • lov om arkiv* • lov om arbeidsmiljø, arbeidstid og stillingsvern mv.**	• lov om behandling av opplysninger i politiet og påtalemyndigheten • lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. • lov om tilsynet med finansforetak mv. • lov om betalingssystemer m.v. • lov om behandling av helseopplysninger ved ytelse av helsehjelp • lov om helseregistre og behandling av helseopplysninger • lov om medisinsk og helsefaglig forskning • lov om helsemessig og sosial beredskap • lov om elektronisk kommunikasjon • lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked • lov om luftfart • lov om petroleumsvirksomhet • lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. • lov om skipssikkerhet • lov om matproduksjon og mattrygghet m.v. • lov om arbeids- og velferdsforvaltningen

***** Viser til forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

** Viser til forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften)

Det har gjennom årene har vært nedsatt flere utvalg som har undersøkt lovgivningen på det digitale sikkerhetsområdet. Omfang og overlapp i regelverk har vært trukket fram som en utfordring av flere av utvalgene.[15] Og i 2018 pekte IKT-sikkerhetsutvalget også på overlapp mellom veiledere fra ulike aktører innenfor arbeidet med digital sikkerhet som en utfordring.[16]

[15] NOU 1986: 12 *Datateknikk og samfunnets sårbarhet* (Seip-utvalget); Rapport fra styrings- og arbeidsgruppene for samordning av regelverk for beskyttelse av informasjon, nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet (1991); NOU 2000: 24 *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeid i samfunnet* (Willoch-utvalget); NOU 2018: 14 *IKT-sikkerhet i alle ledd.*

[16] NOU 2018: 14 *IKT-sikkerhet i alle ledd.*

Regelverkene på det digitale sikkerhetsområdet, inkludert den nye sikkerhetsloven fra 2019, er endret: Tidligere ble det stilt konkrete krav til hvordan virksomhetene skulle oppnå forsvarlig sikkerhet, mens det i dag hovedsakelig stilles funksjonskrav. Det krever mer kompetanse og kapasitet å etterleve et funksjonsbasert regelverk fordi virksomhetene selv må vurdere risikoen og finne fram til sikkerhetsløsninger som innfrir funksjonskravene. Da er det – fra et brukerperspektiv – desto viktigere at veiledningen er god og tilgjengelig.

Funksjonsbasert sikkerhetsregelverk

Et regelverk som slår fast hvilket sikkerhetsnivå som skal oppnås, men ikke hvordan det skal oppnås. Det er opp til virksomhetene selv å innfri kravene på den måten de anser som den beste. Dette skal legge til rette for fleksibilitet i valg av metoder, framgangsmåter og teknologiutvikling

Undersøkelsen viser at omfanget av regelverk fortsatt er stort og at flere av regelverkene og veilederne på det digitale sikkerhetsområdet overlapper tematisk. Undersøkelsen viser også at det i veiledningsmateriellet brukes ulike standarder og begreper og gir ulike anbefalinger om de samme emnene. Digitaliseringsdirektoratet har søkt å løse noe av utfordringen ved å samle veiledere om regelverk for digital sikkerhet i offentlig sektor på en egen nettside. Fra et brukerperspektiv er det likevel vanskelig å finne fram, og veilederne framstår ikke som samordnet. Direktoratets nettside inneholder kun et utvalg veiledere, og det er ikke gjort noe for å samordne innholdet i veilederne.

Den svake samordningen av roller, ansvar og krav fører til at det er krevende for virksomhetene å avklare hvilke regelverk de omfattes av, hvilke myndighetsaktører de skal forholde seg til, og hvilke veiledere de skal benytte i det forebyggende digitale sikkerhetsarbeidet. Dette gjør at implementeringen av relevant regelverk blir forsinket og mangelfull. I verste fall kan det føre til at viktige verdier ikke sikres tilstrekkelig.

Riksrevisjonen mener myndighetene ikke har lagt godt nok til rette for at virksomhetene kan etterleve regelverket som gjelder digital sikkerhet, gjennom ensartet og tilgjengelig veiledning og veiledningsmateriell.

4.2 Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden

Som en del av samordningsansvaret på samfunnssikkerhetsområdet skal Justis- og beredskapsdepartementet ha oversikt over den nasjonale sikkerhetstilstanden, herunder den nasjonale digitale sikkerhetstilstanden.[17] Denne oversikten er blant annet en forutsetning for at departementet skal kunne identifisere tverrsektorielle sikkerhetsutfordringer, og for at det skal kunne iverksettes sikkerhetstiltak som reduserer risikoen knyttet til disse.

Justis- og beredskapsdepartementet benytter en rekke ulike kilder for å holde oversikt over den nasjonale digitale sikkerhetstilstanden. Departementenes rapportering på arbeidet som følger av den nye sikkerhetsloven, og arbeidet som følger av samfunnssikkerhetsinstruksen, trekkes blant annet fram som viktige kilder. Andre viktige informasjonskilder er rapporter fra Nasjonal sikkerhetsmyndighet, Direktoratet for

[17] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) (1. september 2017).

samfunnssikkerhet og beredskap og de nasjonale etterretnings- og sikkerhetstjenestene.

Justis- og beredskapsdepartementet mener at de har tilstrekkelig oversikt til å identifisere behov på nasjonalt nivå og til å kunne sette retning og prioritere tverrsektorielle tiltak. Denne undersøkelsen viser imidlertid at det er flere utfordringer med disse kildene, og at det derfor er mangler i departementets informasjonsgrunnlag

4.2.1 Det er ikke etablert en fullstendig oversikt over hvilke verdier og avhengigheter som skal sikres etter sikkerhetsloven

Ny sikkerhetslov trådte i kraft 1. januar 2019. I henhold til denne loven er departementene ansvarlig for å identifisere og holde oversikt over *grunnleggende nasjonale funksjoner* innenfor sine ansvarsområder. Det enkelte departement er også ansvarlig for å identifisere og holde oversikt over *avhengigheter,* det vil si virksomheter som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. Det er disse funksjonene, og virksomhetene som understøtter dem, som skal sikres i henhold til sikkerhetsloven. Departementene skal melde inn oversikt til Nasjonal sikkerhetsmyndighet, som rapporterer dette til Justis- og beredskapsdepartementet årlig.

Grunnleggende nasjonale funksjoner

Tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Justis- og beredskapsdepartementet utarbeidet og fastsatte i 2019 en milepælsplan for implementering av den nye loven. I henhold til planen skulle alle departementene i løpet av august 2020 ha identifisert grunnleggende nasjonale funksjoner innenfor sitt ansvarsområde. Allerede ved første milepæl ble arbeidet forsinket, og først høsten 2021 hadde alle departementene meldt inn sine identifiserte grunnleggende nasjonale funksjoner.

Digitale verdikjeder

En digital verdikjede er en struktur av leveranser mellom virksomheter, der hver leveranse enten er en digital tjeneste, programvare eller maskinvare. Verdikjeden representerer en avhengighet mellom virksomheter, med tanke på å få levert tjenester/produkter.

Fordi identifiseringen av disse funksjonene er en forutsetning for den videre implementeringen, ble også arbeidet ellers forsinket. I henhold til planen skulle kartleggingen av avhengigheter være ferdig i juli 2021, men høsten 2022 arbeider departementene fortsatt med å kartlegge avhengigheter. Myndighetene har heller ikke oversikt over alle avhengighetene mellom de ulike funksjonene.

At myndighetene ikke har denne oversikten, og at det derfor ikke blir stilt krav til sikkerhet gjennom hele verdikjeden til en grunnleggende funksjon, medfører risiko for at virksomheter, systemer og infrastruktur som denne funksjonen er avhengig av, ikke er tilstrekkelig sikret. Grunnleggende nasjonale funksjoner kan dermed settes ut av spill, for eksempel ved at digitale angrep rettes mot sårbare virksomheter, informasjonssystemer eller infrastruktur som befinner seg lenger ut i den digitale verdikjeden.

Både Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at arbeidet som følger av ny sikkerhetslov går sakte. Manglende kapasitet og sikkerhetskompetanse i departementer og virksomheter som omfattes av sikkerhetsloven trekkes fram som en medvirkende årsak. Ifølge Justis- og beredskapsdepartementet kan dette medføre at viktige verdier ikke er tilstrekkelig sikret.

Det er det enkelte departement som har ansvar for samfunnssikkerhet i egen sektor. Samtidig må det være slik at når fremdriften i departementenes arbeid som følger av ny sikkerhetslov går tregt, må Justis- og beredskapsdepartementet følge dette tydelig opp. Riksrevisjonen vil her peke på de alvorlige konsekvensene tregheten i arbeidet kan ha for nasjonal sikkerhet. På grunn av sakens alvorlige karakter er det **kritikkverdig** at Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar mer aktivt, for eksempel gjennom nye krav og frister, for å sikre framdriften i arbeidet som følger av ny sikkerhetslov.

4.2.2 Justis- og beredskapsdepartementet har ikke sørget for at sentral rapportering fra departementene kan brukes til å holde oversikt over sikkerhetstilstanden

Som en del av samordningsansvaret for samfunnssikkerhetsområdet skal Justis- og beredskapsdepartementet definere hvilke samfunnsfunksjoner som i et tverrsektorielt perspektiv er å anse som kritiske, og hva som inngår i disse funksjonene. På oppdrag fra departementet har Direktoratet for samfunnssikkerhet og beredskap definert totalt 16 kritiske samfunnsfunksjoner.[18] I henhold til samfunnssikkerhetsinstruksen skal departementet med hovedansvar for en samfunnskritisk funksjon gjennomføre status- og tilstandsvurderinger for funksjonen. Det går også fram at disse status- og tilstandsvurderingene skal være en kilde til Justis- og beredskapsdepartementets oversikt over den nasjonale sikkerhetstilstanden. Justis- og beredskapsdepartementet oppgir vurderingene som en sentral kilde til informasjon om den nasjonale sikkerhetstilstanden, som også omfatter den digitale sikkerheten.

Samfunnets kritiske funksjoner

En samfunnsfunksjon defineres som kritisk hvis bortfall av den får konsekvenser som truer befolkningens og samfunnets grunnleggende behov, herunder ivaretakelse av grunnleggende samfunnsverdier som liv og helse, natur og miljø, økonomi, samfunnsstabilitet, styringsevne og kontroll.

Undersøkelsen viser imidlertid at status- og tilstandsvurderingene er av varierende omfang og kvalitet. I vurderingene framheves det som fungerer bra, men det rettes lite oppmerksomhet mot sårbarhetene i funksjonene som er vurdert. En annen utfordring med vurderingene er at de er overordnede og i liten grad gir konkrete forslag til forbedringer og tiltak. Samlet sett fører dette til at vurderingene ikke gir en tilstrekkelig oversikt over den digitale sikkerhetstilstanden for kritiske samfunnsfunksjoner. En mer enhetlig gjennomføring og rapportering av vurderingene ville gjort dem mer relevante og tilgjengelige. Justis- og beredskapsdepartementet har som mål å komme fram til en ny, enhetlig måte å gjennomføre og rapportere status- og tilstandsvurderinger på. Dette arbeidet er satt i gang, men det er ennå ikke fullført.

I tillegg til de overnevnte status- og tilstandsvurderingene skal alle departementene i henhold til samfunnssikkerhetsinstruksen gjennomføre risiko- og sårbarhetsanalyser for eget ansvarsområde. Dette inkluderer risiko knyttet til digital sikkerhet. Justis- og beredskapsdepartementet bruker imidlertid ikke disse risiko- og sårbarhetsanalysene for å få oversikt over den nasjonale digitale sikkerhetstilstanden. Ifølge departementet er det fordi de utføres på ulike måter og etter ulik metodikk, noe som gjør en sammenstilling av analysene mer ressurskrevende enn den antatte nytten.

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

Gjennom samordningsansvaret for samfunnssikkerheten kan Justis- og beredskapsdepartementet gi føringer for hvordan departementene skal gjennomføre risiko- og sårbarhetsanalyser. Departementet har imidlertid valgt å ikke gi slike føringer.

Etter Riksrevisjonens vurdering har ikke Justis- og beredskapsdepartementet sørget for at arbeidet med status- og tilstandsvurderinger og risiko- og sårbarhetsanalyser blir gjennomført på en enhetlig måte. Dersom rapporteringen fra departementene var mer enhetlig, ville det ha vært mulig å sammenstille informasjon og få en bedre oversikt over sikkerhetstilstanden. Det ville også ha gitt et større utbytte av ressursbruken knyttet til analysearbeidet i departementene.

4.2.3 Det gjennomføres få tilsyn med digital sikkerhet sett opp mot antall virksomheter det skal og kan føres tilsyn med

Arbeidet med digital sikkerhet er regulert gjennom en rekke regelverk, berører de fleste virksomheter og kontrolleres av flere ulike tilsynsmyndigheter. Tilsyn er et sentralt virkemiddel som Justis- og beredskapsdepartementet og øvrige myndigheter kan bruke til å kontrollere at regelverket på det digitale sikkerhetsområdet implementeres og overholdes. Tilsyn skal bidra til å forbedre arbeidet med digital sikkerhet i virksomhetene. For myndighetene er tilsynsrapportene også en viktig kilde til innsikt i arbeidet på området – i hver enkelt sektor og i samfunnet som helhet. Mangelfull tilsynsvirksomhet kan føre til at den digitale sikkerheten får for lite oppmerksomhet i virksomheter og departementer. Dette kan svekke den digitale sikkerheten i samfunnet. Undersøkelsen viser at det gjennomføres forholdvis få tilsyn med digital sikkerhet som tema.

Det er et stort antall tilsynsobjekter som omfattes av de generelle regelverkene, som sikkerhetsloven og personvernregelverket. Justis- og beredskapsdepartementet har gitt Nasjonal sikkerhetsmyndighet det overordnede ansvaret for å sørge for at sikkerhetstilstanden i alle sektorer kontrolleres, og at virksomhetene oppfyller pliktene de har etter sikkerhetsloven. I kontrollmeldingen for 2020 peker Nasjonal sikkerhetsmyndighet på at antall tilsyn per år er begrenset sammenlignet med antall tilsynsobjekter. Det begrensede antallet tilsyn i 2019 og 2020 skyldes imidlertid sikkerhetsmyndighetenes beslutning om å være tilbakeholdne med undersøkelser så kort tid etter innføringen av den nye sikkerhetsloven. I 2022 har antallet tilsyn økt, og sikkerhetsmyndighetene antar at det vil fortsette å øke framover. I 2019 ble Nasjonal kommunikasjonsmyndighet og Norges vassdrags- og energidirektorat utpekt som sektortilsyn for tilsyn etter sikkerhetsloven. Dette skulle bidra til at tilsynene ble bedre tilpasset de ulike sektorene, og til at antall tilsyn etter sikkerhetsloven økte. Verken Nasjonal kommunikasjonsmyndighet eller Norges vassdrags- og energidirektorat har imidlertid kommet i gang med slike tilsyn.

Datatilsynet gjennomfører tilsyn etter personvernregelverket. I 2021 planla Datatilsynet å gjennomføre 14 egeninitierte tilsyn, men bare 5 ble startet opp og kun 3 ble gjennomført.

Samfunnssikkerhetsinstruksen og sivilbeskyttelsesloven stiller krav til henholdsvis departementenes og kommunenes samfunnssikkerhetsarbeid, inkludert arbeidet med digital sikkerhet. Ansvaret for å føre tilsyn med departementene er delegert fra Justis- og beredskapsdepartementet til Direktoratet for samfunnssikkerhet og beredskap, mens statsforvalterne fører tilsyn med kommunene. Temaene for tilsynene skal velges ut fra en risiko- og vesentlighetsvurdering. I en tilsynsrapport om Justis- og beredskapsdepartements gjennomføring av tilsyn på området fra 2013 går det fram at tilsynene i større grad framstår som brede gjennomganger enn som tilsyn som er spisset mot risiko og vesentlighet.[19] Også Riksrevisjonens undersøkelse viser at tilsynene av departementene og kommunene omfatter samfunnssikkerhetsarbeid generelt og ikke arbeidet med digital sikkerhet spesielt. Tilsynsrapportene gir dermed ikke informasjon om statusen for arbeidet med digital sikkerhet i departementene og kommunene.

Nasjonal sikkerhetsmyndighet har framhevet at det er betydelige trusler i det digitale rom, og at antallet digitale angrep øker. Konsekvensen av at det gjennomføres få tilsyn med digital sikkerhet er en økt risiko for at sårbarheter ikke fanges opp. Riksrevisjonen vurderer det derfor som **kritikkverdig** at det gjennomføres få tilsyn med digital sikkerhet, og at tilsynsmyndighetene på området er lite samordnet (jf. kapittel 4.1).

4.3 Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av *Nasjonal strategi for digital sikkerhet*

I 2019 utga Justis- og beredskapsdepartementet *Nasjonal strategi for digital sikkerhet* og delstrategien *Nasjonal strategi for digital sikkerhetskompetanse*. Strategiene er utarbeidet i samarbeid med Forsvarsdepartementet og Kunnskapsdepartementet. Dette er fjerde gang det har blitt utgitt en nasjonal strategi for digital sikkerhet (strategier er tidligere utgitt i 2003, 2007 og 2012), og første gang det er utgitt en egen delstrategi for digital sikkerhetskompetanse. I *samfunnssikkerhetsmeldingen* trekkes strategien fram som et sentralt virkemiddel i myndighetenes arbeid med digital sikkerhet. Etter Riksrevisjonens vurdering utnytter ikke Justis- og beredskapsdepartementet potensialet som ligger i dette virkemiddelet, godt nok til å forbedre samordningen av arbeidet med digital sikkerhet nasjonalt.

4.3.1 Justis- og beredskapsdepartementets oppfølging av strategien gir ikke grunnlag for å løpende vurdere effekt av tiltakene

Justis- og beredskapsdepartementet viser til at en systematisk og kunnskapsbasert tilnærming ligger til grunn for utarbeidelsen av *Nasjonal strategi for digital sikkerhet* (2019). Etter at Justis- og beredskapsdepartementet overtok ansvaret for den digitale sikkerheten i 2013, er det utarbeidet flere utredninger og styrende dokumenter (se

[19] Helsetilsynet (2014) *Rapport fra tilsyn med samfunnssikkerhets- og beredskapsarbeidet i Justis- og beredskapsdepartementet. Inkludert undersøkelser i Direktoratet for samfunnssikkerhet og beredskap, Politidirektoratet og to politidistrikter*.

faktaboks 2). Blant annet har det vært nedsatt to nasjonale utvalg for å utrede særskilte forhold knyttet til den digitale sikkerheten nasjonalt, og i 2017 kom den første stortingsmeldingen som utelukkende omhandler digital sikkerhet. Justis- og beredskapsdepartementet viser også til at det i forkant av utgivelsen av *Nasjonal strategi for digital sikkerhet* (2019) ble gjennomført en omfattende prosess for å få innspill til strategien fra et så bredt utvalg av aktører som mulig. Riksrevisjonen vurderer dette arbeidet som positivt.

Faktaboks 2 Utredninger om og styrende dokumenter for digital sikkerhet

- NOU (2015: 13) *Digital sårbarhet – sikkert samfunn* (Digitalt sårbarhetsutvalg, også omtalt som Lysneutvalget)
- *Nasjonalt digitalt risikobilde,* rapport som utgis årlig av Nasjonal sikkerhetsmyndighet, og som ble utgitt for første gang i 2015
- Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*
- *Internasjonal cyberstrategi for Norge* (2017)
- *Nasjonal strategi for digital sikkerhet* (2019)
- *Nasjonal strategi for digital sikkerhetskompetanse* (2019)
- NOU (2018: 14) *IKT-sikkerhet i alle ledd* (Holteutvalget)
- *Risikostyring i digitale verdikjeder* (2019), Direktoratet for samfunnssikkerhet og beredskap
- *Evaluering av hendelseshåndteringen av IKT-sikkerhetshendelsene hos Helse Sør-Øst Regionalt helseforetak og fylkesmannsembetene 2018* (2020), Forsvarets forskningsinstitutt
- *Norsk kryptopolitikk* (2020)

Kilde: Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden*, s. 89.

Med strategien fra 2019 følger en oversikt over sentrale tiltak som skal understøtte strategiens målsettinger, og som skal revideres ved behov. Justis- og beredskapsdepartementet har imidlertid besluttet at tiltaksoversikten ikke vil bli oppdatert med nye tiltak eller endringer i eksisterende tiltak, til tross for at det er identifisert behov for nye tiltak på det digitale sikkerhetsområdet. Nye tiltak vil i stedet bli presentert på annen måte, for eksempel gjennom proposisjoner til Stortinget.

Våren 2021 innhentet Justis- og beredskapsdepartementet rapportering på ansvarlige departementers og virksomheters arbeid med gjennomføringen og oppfølgingen av tiltakene som tilhørte strategien. I en oppsummering av rapporteringen påpeker Justis- og beredskapsdepartementet at kvaliteten på rapporteringen er varierende, og at den sier lite om tiltakenes effekt på den digitale sikkerheten. Justis- og beredskapsdepartementet har likevel ikke etterspurt ytterligere informasjon fra virksomhetene. Til tross for at de samme utfordringene ble påpekt i forbindelse med oppfølgingen av tiltak som tilhørte strategien fra 2012, har departementet altså ikke endret metoden for statusrapportering.

I henhold til *Nasjonal strategi for digital sikkerhetskompetanse* (2019) skal Justis- og beredskapsdepartementet og Kunnskapsdepartementet sørge for at det foreligger oppdaterte tall og statistikk, slik at det er mulig å følge med på forholdet mellom samfunnets tilgang til og behov for digital

sikkerhetskompetanse. Det er imidlertid ikke innhentet oppdaterte data og analyser om kompetansegapet på det digitale sikkerhetsområdet siden 2017. Grunnen til dette er at departementene mener det er for tidlig å vurdere effekten av tiltakene i kompetansestrategien. Det har for øvrig vist seg å være en risiko for at enkelte tiltak ikke oppfyller målene i strategien. Dette gjelder for eksempel rekruttering til utdanning og forskning innenfor digital sikkerhet. Til tross for dette har ikke de ansvarlige departementene innhentet nok informasjon til å foreta en løpende vurdering av effekten av tiltak i kompetansestrategien der dette hadde vært mulig.

Etter Riksrevisjonens vurdering har ikke Justis- og beredskapsdepartementet sørget for å tilegne seg god nok informasjon om virkningen av *Nasjonal strategi for digital sikkerhet* (2019) med tilhørende tiltak. Bedre informasjon om statusen for og effekten av tiltakene kunne ha dannet grunnlag for nye tiltak eller endringer i pågående tiltak, slik at man kunne oppfylle strategiens mål i lys av dagens behov.

4.3.2 Satsingen på kompetanse er mindre målrettet enn beskrevet i *Nasjonal strategi for digital sikkerhet*

Behovet for økt digital sikkerhetskompetanse er trukket fram som en av de største utfordringene på det digitale sikkerhetsområdet. Å styrke den digitale sikkerhetskompetansen i samfunnet er derfor et av fem overordnende mål i *Nasjonal strategi for digital sikkerhet* (2019). Kompetansemålene utdypes i *Nasjonal strategi for digital sikkerhetskompetanse* fra samme år. Som følge av at de fleste av tiltakene i kompetansestrategien er rettet mot forsknings- og utdanningsinstitusjoner, er det Kunnskapsdepartementet som har hovedansvaret for gjennomføringen og oppfølgingen av tiltakene.

Undersøkelsen viser at satsingen på digital sikkerhetskompetanse er mindre målrettet enn det som er beskrevet i strategidokumentet. I tiltaksoversikten til *Nasjonal strategi for digital sikkerhet* (2019) vises det til prioriteringer på kompetanseområdet på over 800 millioner kroner. Også i *samfunnssikkerhetsmeldingen* vises det til at 800 millioner kroner er satt av til å styrke den digitale sikkerhetskompetansen. Flere av tiltakene i strategien er imidlertid ikke rettet mot å øke den digitale *sikkerhetskompetansen*, men den digitale kompetansen i samfunnet generelt, og de omtaler i ulik grad digital sikkerhetskompetanse.

4.4 Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering

I *samfunnssikkerhetsmeldingen* trekkes *Nasjonalt cybersikkerhetssenter* og *Felles cyberkoordineringssenter* fram som sentrale arenaer for å avdekke, håndtere og koordinere innsatsen ved alvorlige digitale angrep. Riksrevisjonens undersøkelse viser at det er utfordringer knyttet til arbeidet i de to arenaene.

En annen del av Justis- og beredskapsdepartementets samordningsrolle på samfunnssikkerhetsområdet går ut på å gjennomføre nasjonale øvelser og

sørge for at utfordringer på tvers av flere sektorer blir håndtert. Sentrale tiltak omfatter blant annet å få på plass et felles rammeverk for digital hendelseshåndtering og tekniske systemer for varsling av uønsket aktivitet og kommunikasjon mellom beredskapsaktører. Undersøkelsen viser at gjennomføringen av flere av disse tiltakene er forsinket og at viktige elementer av tverrsektoriell hendelseshåndtering ikke har blitt øvet som planlagt.

Med tanke på utfordringene som er knyttet til å avdekke, håndtere og koordinere innsatsen ved alvorlige digitale hendelser, mener Riksrevisjonen at dette samlet sett er **kritikkverdig.** Detaljer om utfordringene er omtalt i et eget sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

4.4.1 Nasjonal sikkerhetsmyndighets evne til å oppdage og håndtere digitale hendelser har svakheter

I henhold til sikkerhetsloven skal Nasjonal sikkerhetsmyndighet drive en nasjonal responsfunksjon for alvorlige angrep og et nasjonalt varslingssystem for digital infrastruktur. Som en del av den nasjonale responsfunksjonen skal Nasjonal sikkerhetsmyndighet ved behov og basert på samtykke bistå virksomheter i håndteringen av alvorlige digitale angrep. Nasjonal sikkerhetsmyndighet opprettet i 2019 *Nasjonalt cybersikkerhetssenter* for å ivareta denne funksjonen. Senteret drifter og organiserer sensornettverket *Varslingssystem for digital infrastruktur* (VDI), som skal oppdage og varsle om digitale trusler. Nasjonal sikkerhetsmyndighet tilbyr også gratistjenesten Allvis NOR, som virksomheter kan abonnere på. Verktøyet skanner de av virksomhetenes datatjenester som er eksponert for sårbarheter gjennom internett.

Faktaboks 3 Nasjonalt cybersikkerhetssenter

Nasjonalt cybersikkerhetssenter ble etablert for å styrke Norges robusthet i det digitale rom. Senterets viktigste oppgaver er å overvåke og reagere på digitale trusler. Ved alvorlige digitale hendelser bistår *Nasjonalt cybersikkerhetssenter* ved behov den aktuelle virksomheten i håndteringen av hendelsene. Bistanden gis enten direkte til virksomheten eller indirekte via det sektorvise responsmiljøet.

Ved alvorlige digitale hendelser sender *Nasjonalt cybersikkerhetssenter* også ut varsler og informasjon til departementer, sektorvise responsmiljøer eller andre relevante virksomheter som deltar i senterets nettverk. Dette kan for eksempel være informasjon om hvilke tiltak som bør iverksettes for å hindre hendelser.

Kilde: Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT.* Nettartikkel [Hentedato: 4. februar 2022]; verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.

Riksrevisjonen har intervjuet et utvalg private og offentlige virksomheter som ved hendelser har fått bistand fra *Nasjonalt cybersikkerhetssenter*. Virksomhetene understøtter en grunnleggende nasjonal funksjon. Disse opplyser til Riksrevisjonen at de gjennomgående har vært fornøyd med bistanden. *Nasjonalt cybersikkerhetssenter* beskrives av virksomhetene som

en aktør som har bidratt til økt informasjonsdeling mellom norske virksomheter forut for, under og i etterkant av alvorlig digitale hendelser.

De intervjuede virksomhetene er tildelt en fast kontaktperson i *Nasjonalt cybersikkerhetssenter*. Det er imidlertid ikke alle virksomhetene som har en slik kontaktperson. Representanter for kommunesektoren, som understøtter flere kritiske samfunnsfunksjoner, uttaler til Riksrevisjonen at noen kommuner opplever at det er vanskelig å komme i kontakt med og få bistand fra *Nasjonalt cybersikkerhetssenter*, også ved digitale hendelser.

Undersøkelsen avdekker også at det er utfordringer med Nasjonal sikkerhetsmyndighets tekniske systemer VDI og Allvis NOR. Allvis NOR tilbys virksomheter som er underlagt sikkerhetsloven, og eiere og forvaltere av samfunnskritiske funksjoner. Allvis NOR skanner som nevnt ovenfor tjenester som er eksponert for sårbarheter gjennom internett. Undersøkelsen viser imidlertid at Allvis NOR har begrenset evne til å fange opp sårbarheter. Skanningen gir dermed ikke et fullstendig bilde av en virksomhets digitale sårbarheter. Dette kan potensielt få store konsekvenser for virksomhetene som benytter tjenesten.

VDI består av nettverkssensorer som er utplassert hos virksomheter som anses som en del av norsk kritisk infrastruktur. Sensorene overvåker internettrafikken for å oppdage mistenkelig trafikk. Det er avdekket flere utfordringer knyttet til sensornettverket. Blant annet vil ikke nye og ukjente angrepsmønstre oppdages av VDI, da sensorene kun fanger opp kjente mønstre. I tillegg er mesteparten av dagens nettverkstrafikk kryptert. Sensorene er ikke i stand til å overvåke denne typen trafikk. Flere og flere virksomheter bruker dessuten skyløsninger, men sensorene overvåker heller ikke trafikk som går direkte fra datamaskiner og mobiltelefoner til servere i skyen. Det er både tekniske og regulatoriske utfordringer med å få på plass slik funksjonalitet. Det er dermed en stor del av nettverkstrafikken som ikke overvåkes av VDI. Det er også en utfordring at det ikke er utplassert VDI-sensorer i alle relevante virksomheter. Ytterligere detaljer om utfordringene knyttet til VDI og konsekvensene av disse utdypes i et sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

De påpekte svakhetene i VDI gjør i sum at sensornettverket har store blindsoner. Det pågår derfor et større prosjekt der målet er å oppgradere og videreutvikle funksjonaliteten og kapasiteten i sensornettverket. Prosjektet skal etter planen ferdigstilles i 2023. I forbindelse med utbruddet av krigen i Ukraina ble det bevilget ekstra midler til å øke dekningen og analysekapasiteten i VDI.[20] Justis- og beredskapsdepartementer opplyser imidlertid at midlene til å øke omfanget av VDI-sensorer ikke ble videreført for 2023.[21]

Allvis NOR

Allvis NOR kartlegger og tester tjenester som er eksponert mot internett. Deretter gjennomføres automatiserte sårbarhetsskanninger mot spesifikke protokoller eller programvarer i disse tjenestene. Skanningen gjøres jevnlig, og oppdateres på bakgrunn av sårbarheter som Nasjonal sikkerhetsmyndighet er kjent med.

Varslingssystem for digital infrastruktur (VDI)

VDI-sensorene lytter til trafikken som går til og fra virksomhetene. Basert på kjente mønstre skal sensorene oppdage mistenkelig aktivitet og trusler. Dersom slik aktivitet oppdages varsles øvrige deltakerne i VDI-nettverket av Nasjonal sikkerhetsmyndighet ved Nasjonalt cybersikkerhetssenter.

[20] Prop. 78 S (2021–2022) *Endringer i statsbudsjettet 2022 under Kunnskapsdepartementet, Kultur- og likestillingsdepartementet, Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet, Arbeids- og inkluderingsdepartementet, Helse- og omsorgsdepartementet, Barne- og familiedepartementet, Nærings- og fiskeridepartementet, Finansdepartementet og Forsvarsdepartementet (økonomiske tiltak som følge av krigen i Ukraina).*

[21] Justis- og beredskapsdepartementet (2022) Hovedanalyserapport Samordning av digital sikkerhet, JDs innspill. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet*. Brev til Riksrevisjonen, 11. november 2022.

Riksrevisjonen vurderer det som positivt at det er satt i gang tiltak for å oppgradere og videreutvikle de tekniske verktøyene VDI og Allvis NOR, men påpeker samtidig at det kreves en betydelig innsats for å løse utfordringene med systemene.

4.4.2 Vedvarende utfordringer i Felles cyberkoordineringssenter har ikke blitt godt nok fulgt opp av Justis- og beredskapsdepartementet

På oppdrag fra Justis- og beredskapsdepartementet og Forsvarsdepartementet ble *Felles cyberkoordineringssenter* etablert i 2017. *Felles cyberkoordineringssenter* er et permanent, samlokalisert fagmiljø med representanter fra Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos. Det er Nasjonal sikkerhetsmyndighet som er gitt ansvaret for å lede senterets arbeid.

Felles cyberkoordineringssenter skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep, understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom. I henhold til *Retningslinjer for cybersamarbeid* (2022) skal dette oppnås gjennom senterets åtte hovedoppgaver. Partene i senteret har i hovedsak prioritert fire av disse oppgavene.

Hovedoppgavene til Felles cyber-koordineringssenter

a. Tidsriktige og relevant informasjonsutveksling

b. Operativ koordinering og hendelseshåndtering

c. Samarbeid om analyser og vedlikeholdelse et felles situasjonsbilde

d. Utarbeide og sammenstille strategiske analyser

e. Utarbeide, vedlikeholde og øve krise- og beredskapsplaner

f. Koordinert samvirke med nasjonale og internasjonale partnere

g. Felles kompetanseheving

h. Samvirke og koordinert utvikling av kapasiteter og evner

Undersøkelsen har blant annet vist at det er utfordringer knyttet til ressurssituasjonen og bemanningen i *Felles cyberkoordineringssenter*. Utfordringer knyttet til senterets arbeid beskrives mer inngående i et sikkerhetsgradert vedlegg til Riksrevisjonens rapport.

Utfordringene som er identifisert i denne undersøkelsen, kom også fram i partenes egen evaluering av *Felles cyberkoordineringssenter* i 2019. Partene utarbeidet da en handlingsplan for å håndtere utfordringene, men flere av dem vedvarer. En evalueringsrapport ble sendt til Justis- og beredskapsdepartementet og Forsvarsdepartementet i etterkant av evalueringen. Rapporten inneholdt imidlertid ingen informasjon om utfordringer knyttet til arbeidet eller tiltak for å imøtekomme utfordringene. Justis- og beredskapsdepartementet opplyser at de etterspurte mer informasjon om resultatene av evalueringen, men at enkelte av partene ikke ønsket å dele denne med departementet. Justis- og beredskapsdepartementet fulgte ikke dette opp videre, og er ikke blitt gjort kjent med senterets utfordringer.

Justis- og beredskapsdepartementet viser til at det er partene selv som er ansvarlige for ressurssetting av senteret. Videre viser departementet til at Nasjonal sikkerhetsmyndighet er gitt en lederfunksjon for *Felles cyberkoordineringssenter*. Departementet mener det følger av denne funksjonen blant annet å sørge for at senteret har gode rutiner for hendelseshåndtering.

Det er Riksrevisjonens vurdering at de identifiserte utfordringene begrenser måloppnåelsen med etableringen av *Felles cyber koordineringssenter*. Videre mener Riksrevisjonens at Justis- og beredskapsdepartementet skulle ha gjort mer for å sikre seg relevant informasjon om måloppnåelsen i *Felles cyberkoordineringssenter*.

4.4.3 Det er behov for mer øving av tverrsektoriell håndtering av hendelser på nasjonalt nivå

Justis- og beredskapsdepartementet skal som en del av samordningsansvaret planlegge, gjennomføre og evaluere nasjonale øvelser i sivil sektor. Formålet er å sørge for at aktører ved en reell hendelse vet hva de skal gjøre, og hvem de skal samarbeide med.

Høsten 2020 skulle Øvelse Digital 2020 avholdes, men på grunn av koronarestriksjoner ble den nedskalert. Spilløvelsen, som opprinnelig var en del av et tredelt konsept, ble gjennomført med redusert deltakelse, begrensede scenarioer og kortere varighet. Nedskaleringen innebar at tverrsektoriell hendelseshåndtering på nasjonalt nivå ikke ble øvet.

Direktoratet for samfunnssikkerhet og beredskap var ansvarlig for å evaluere øvelsen. I evalueringsrapporten konkluderer direktoratet med at prosjektet som helhet har oppfylt hensikten med Øvelse Digital 2020, til tross for at nedskaleringen førte til at ikke alle øvingsmålene ble innfridd. Direktoratet viser imidlertid til at det fortsatt er behov for bedre oversikt over aktørbildet, økt samhandling på tvers av sektorer og mer koordinert kommunikasjonshåndtering. Direktoratet ser også at det er behov for flere og hyppigere nasjonale øvelser innenfor digital sikkerhet. Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at det var uheldig at øvelsen ble nedskalert og at viktige elementer ikke ble øvet.

Det er ikke planlagt å gjennomføre en ny spilløvelse som erstatning for den delen av Øvelse Digital 2020 som ble nedskalert. Justis- og beredskapsdepartementet viser til at det øves på digitale hendelser internt i sektorene, og at Norge deltar i en rekke internasjonale øvelser på det digitale området. De sentrale hendelseshåndteringsmiljøene håndterer dessuten jevnlig reelle digitale hendelser, og har gjennom det fått god erfaring med håndtering av slike hendelser. Videre bemerker departementet at det generiske systemet for sentral krisehåndtering øves ofte, selv om disse øvelsene ikke alltid er knyttet spesifikt til digital sikkerhet.

Det er positivt at Norge deltar i internasjonale øvelser på det digitale området, og at det øves på krisehåndtering på strategisk nivå. Dette er svært viktig for den nasjonale sikkerheten. Undersøkelsen viser imidlertid at scenarioer som omhandler digital sikkerhet, ofte blir nedprioritert ved gjennomføring av øvelser. Dette gjelder særlig i kommunene. Til tross for at Justis- og beredskapsdepartementet uttaler at det gjennomføres en rekke sektorinterne øvelser knyttet til digital sikkerhet, har ikke departementet noen oversikt over dette. Det er derfor usikkerhet knyttet til hvor ofte disse øvelsene faktisk gjennomføres. Sentrale aktører innenfor det digitale sikkerhetsområdet har også etterlyst flere tverrsektorielle øvelser på området.

Øvelse Digital 2020

Øvelsen bestod opprinnelig av følgende elementer:

- gjennomføring av kompetansehevingsløp for relevante virksomheter
- planlegging, gjennomføring og evaluering av en to-dagers spilløvelse
- utarbeide diskusjonsøvelser (øvingspakker)

4.4.4 Viktige tverrsektorielle tiltak for å håndtere digitale angrep er forsinket

Flere av tiltakene som tilhører *Nasjonal strategi for digital sikkerhet* (2019), er iverksatt for å øke den nasjonale evnen og kapasiteten til å forebygge, avdekke og håndtere digitale angrep. Undersøkelsen viser imidlertid at

arbeidet har gått tregt, og at det er forsinkelser i gjennomføringen av flere av tiltakene. Forsinkelsene medfører økt risiko for at digitale hendelser ikke håndteres effektivt.

I 2012 ble det bestemt at alle sektorer skulle etablere egne sektorvise responsmiljøer. De sektorvise responsmiljøene skal blant annet fungere som bindeledd mellom *Nasjonalt cybersikkerhetssenter* og virksomhetene i sektoren. Undersøkelsen viser imidlertid at responsmiljøene i enkelte sektorer bidrar til forsinkelser i håndtering og informasjonsflyt. En evaluering av ordningen med sektorvise responsmiljøer som ble utført av KPMG i 2022, viser til flere utfordringer med ordningen, blant annet uklar ansvars- og rolleforståelse og mangel på tilgang på relevant kompetanse. Riksrevisjonen ser det som positivt at Justis- og beredskapsdepartementet sommeren 2022 satte i gang en prosess for å evaluere og forbedre ordningen med sektorvise responsmiljøer.

Rammeverk for håndtering av IKT-sikkerhetshendelser skal bidra til effektiv håndtering av alvorlige IKT-sikkerhetshendelser.[22] Rammeverket ble utformet i 2017 og skal revideres annethvert år, men har ikke blitt revidert siden 2017. Etter planen skulle bruken av rammeverket øves under Øvelse Digital 2020*,* og målet var at øvelsen skulle gi innspill til revisjonen av rammeverket. Siden øvelsen ikke ble gjennomført som planlagt, fikk imidlertid ikke Nasjonal sikkerhetsmyndighet noen innspill om hvordan rammeverket fungerer ved håndtering av hendelser. Nasjonal sikkerhetsmyndighet jobber for tiden med en revisjon av rammeverket.

For å øke den nasjonale kapasiteten til å håndtere alvorlige digitale angrep skal Nasjonal sikkerhetsmyndighet utrede mulighetene for en tverrsektoriell cyberreserve. Dette skal være en nasjonal kapasitet bestående av operativt personell som kan bistå ved spesielt store kriser som krever innsats utover ordinær bemanning. Utredningen skulle etter planen ha blitt gjennomført i perioden 2018−2019, men arbeidet er ennå ikke ferdigstilt. Justis- og beredskapsdepartementet forventer en utredning fra Nasjonal sikkerhetsmyndighet i løpet av høsten 2022.

Det har siden 2012 vært iverksatt tiltak for å utvikle et system for høygradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører.[23] Manglende muligheter til å kommunisere via sikkerhetsgraderte informasjonssystemer har blitt pekt på som et hinder for effektiv hendelseshåndtering både av Digitalt sårbarhetsutvalg (Lysneutvalget) i 2015 og Forsvarets forskningsinstitutt i 2020.[24] I henhold til *Nasjonal strategi for digital sikkerhet* (2019) skal Forsvarsdepartementet utvikle og drifte Nasjonalt BEGRENSET nett for lavgradert kommunikasjon og Nasjonalt HEMMELIG nett for høygradert kommunikasjon. Ifølge strategien skulle tiltaket ha blitt gjennomført i 2019. Nasjonalt BEGRENSET nett er etablert og tatt i bruk. Nasjonalt HEMMELIG nett er ikke rullet ut til beredskapsaktørene ennå.

[22] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser.*
[23] Justis- og beredskapsdepartementet (2012) *Handlingsplan − Nasjonal strategi for informasjonssikkerhet.*
[24] NOU 2015:13 *Digital sårbarhet – sikkert samfunn;* Forsvarets forskningsinstitutt (2020) *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene.*

5 Anbefalinger

Riksrevisjonen anbefaler at Justis- og beredskapsdepartementet

- tar en tydeligere samordnings- og pådriverrolle for nasjonal digital sikkerhet i sivil sektor
- sørger for at Nasjonal sikkerhetsmyndighet i samarbeid med de andre veiledningsaktørene gjør veiledningen på det digitale sikkerhetsområdet mer samordnet og tilgjengelig
- sørger for bedre utnyttelse og koordinering av de etablerte arenaene for samordning
- gjennom pådriverrollen bidrar til at alle departementer har tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov
- sikrer et bedre kildegrunnlag for å holde oversikt over den nasjonale digitale sikkerhetstilstanden
- sørger for bedre informasjon om resultater av iverksatte tiltak for å kunne vurdere behovet for endringer og nye tiltak på det digitale sikkerhetsområdet
- styrker arbeidet med å avdekke, håndtere og koordinere innsatsen mot alvorlige digitale hendelser

6 Statsrådens svar

Dokument 3:7 (2022–2023) *Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor* ble oversendt statsråden i Justis- og beredskapsdepartementet. Statsrådens svar følger i vedlegg 2.

7 Riksrevisjonens uttalelse til statsrådens svar

Riksrevisjonen har ingen ytterligere merknader.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 19. januar 2023.

Karl Eirik Schjøtt-Pedersen Tom-Christer Nilsen

Helga Pedersen Anne Tingelstad Wøien Arve Lønnum

Jens A. Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Justis- og beredskapsdepartementet

Riksrevisjonen

Vår saksbehandler
Morten Fosaas 22241374
Vår dato
30.11.2022
Vår referanse
2021/00886-66
Deres dato
Deres referanse

Utsatt offentlighet jf. rrevl § 18 (2)

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Attn: Statsråd Emilie Enger Mehl

Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor

Vedlagt oversendes utkast til Dokument 3:7 (2022-2023) *Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.*

Dokumentet er basert på rapport oversendt Justis- beredskapsdepartementet ved vårt brev 13. oktober 2022, og på departementets svar 11. november 2022.

Statsråden bes redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Statsrådens svar vil i sin helhet bli vedlagt dokumentet. Det bes om at svaret oversendes som PDF lagret fra Word, ikke skannet som bilde, slik at innholdet kan gjøres tilgjengelig for alle i samsvar med krav til universell utforming.

Svarfrist: 15. desember 2022

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
riksrevisor

Brevet er godkjent og ekspedert digitalt.

Vedlegg: Utkast til Dokument 3:7 (2022–2023) *Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Justis- og beredskapsministeren

Riksrevisjonen
Postboks 6835 St Olavs plass
0130 Oslo

Deres ref.	Vår ref.	Dato
2021/00886-66	21/1996 -	16.12.2022

Justis- og beredskapsministerens tilbakemelding på Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet

1. BAKGRUNN

Jeg viser til Riksrevisjonens brev av 30. november og 9. desember i år hvor jeg blir bedt om å redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner og anbefalinger fra undersøkelsen av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Undersøkelsesperioden er 2018-2021, men der det er relevante og tilgjengelige data for 2022 er dette også inkludert.

2. INNLEDNING

Jeg vil innledningsvis gjøre oppmerksom på at jeg tiltrådte som statsråd 14. oktober 2021. Det alt vesentlige av Riksrevisjonens undersøkelsesperiode ligger forut for denne tid. Av naturlige årsaker er jeg ikke kjent med ulike avveininger som ble tatt forut for denne tid.

Etter at jeg tiltrådte som statsråd fant jeg det nødvendig raskt å iverksette en rekke tiltak for å bedre vår digitale motstandskraft. Dette i form av både økte bevilgninger og andre tiltak.

Postadresse: Postboks 8005 Dep, 0030 Oslo
Kontoradresse: Gullhaug Torg 4A Telefon: 22 24 90 90
Org. nr.: 972 417 831

Gjennom Prop. 78 S (2021-2022) som ble fremlagt 1. april 2022 har regjeringen styrket den sivile beredskapen innenfor cyberområdet, hvorav følgende utvalgte tiltak er relevante opp mot denne undersøkelsen:

Tiltak	Prop.	Beløp i mill. kroner i 2022	Beløp i mill. kroner i 2023
Informasjonskampanje om digital sikkerhet (NorSIS)	Prop. 78 S	3	0
Flere stillinger i nasjonalt cybersikkerhetssenter og økt analysekapasitet i Varslingssystem for digital infrastruktur	Prop. 78 S	28,3	24,3
Investeringer i teknisk utstyr for bruk av graderte systemer i Varslingssystem for digital infrastruktur	Prop. 78 S	17	23,9
Myndighetsportal og støtteverktøy for digital sikkerhet i 2022	Prop. 78 S	7	0
Kommune-CERT	Prop. 78 S	50	0

Disse styrkingene som særlig materialiserte seg gjennom Prop. 78 S (2021-2022) representerer et taktskifte som vil sette oss bedre i stand til å kunne håndtere og avdekke digitale trusler.

Regjeringen har nylig fremmet Meld. St. 9 (2022-2023) om nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet. Lagt fram 9. desember 2022. Meldingen belyser regjeringens tiltak for å styrke innsatsen og arbeidet med digital sikkerhet. Dette er tiltak som vil gi økt digital sikkerhet innenfor forebygging, avdekking og håndtering, både på lokalt, regionalt og nasjonalt nivå. Jeg mener tiltakene svarer ut flere av Riksrevisjonens konklusjoner og anbefalinger, hvilket jeg redegjør for i det videre.

Jeg opplever at både myndigheter og virksomheter tar arbeidet med digital sikkerhet på største alvor. I forbindelse med Nasjonal sikkerhetsmåned 2022 gjennomførte rekordmange sikkerhetskurset «Grunnprinsipper for IKT-sikkerhet», som Nasjonal sikkerhetsmyndighet (NSM) tilbøy gratis som del av sikkerhetsmåneden.

3. DEPARTEMENTETS KOMMENTARER

Riksrevisjonen har gjort en grundig undersøkelse, og kommet med anbefalinger som jeg vil sørge for blir fulgt opp i samhandling med andre departementer. Undersøkelsen synliggjør at dette er et omfattende og krevende felt med mange aktører. I perioden for undersøkelsen har store deler av samfunnet vært stengt ned som en følge av pandemien, - noe som kan ha hatt innvirkning på prioriteringene av ressurser. Jeg vil i det følgende kommentere de ulike delene av rapporten.

3.1 Svak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene

Riksrevisjonens undersøkelse bekrefter en kjent utfordring, herunder at området reguleres av flere ulike regelverk som forvaltes av en rekke aktører med tilsyns- og veiledningsansvar. Myndighetene skal i størst mulig grad være samordnet og godt koordinert med entydige råd og anbefalinger.

Regjeringen vurderer å fremme et lovforslag om digital sikkerhet for å bedre samordningen av krav på tvers av ulike samfunnsområder. Forslaget skal ansvarliggjøre virksomheter og sikre gjennomføring av nasjonale råd og anbefalinger. Regjeringen har også besluttet å lansere en nasjonal portal for digital sikkerhet og et støtteverktøy til alle virksomheter for å tilgjengeliggjøre råd og anbefalinger. Portalen skal være en felles inngangsport for ulike brukergrupper, men utformet slik at alle får ensartede råd tilpasset sin brukergruppe. Innholdet skal utarbeides av aktører med roller og ansvar for digital sikkerhet. NSM leder arbeidet og skal forvalte portalen som lanseres i 2023.

Jeg har forståelse for at myndighetenes arbeid utad kan fremstå fragmentert og med behov for større koordinering. Det er derfor besluttet å kartlegge brukerbehov og erfaringer med dagens organisering av veiledning innen digital sikkerhet, for å påse at oppgaver og ansvar er hensiktsmessig fordelt. Kommunal- og distriktsministeren og jeg har fått i ansvar å gjennomføre kartleggingen innen sommeren 2023.

Jeg er enig i at arbeidet i enkelte samordningsarenaer kan bli mer forpliktende enn hva som er tilfellet i dag. Justis- og beredskapsdepartementet (JD) vil fortsette å ha fokus på videreutvikling av møtearenaen for departementene. Vi vil også videreutvikle Nasjonalt cybersikkerhetssenter i NSM for å øke nasjonalt og internasjonalt samarbeid innenfor deteksjon, håndtering, analyse og rådgivning innen digital sikkerhet. I dag deltar nær 50 partnere fra næringsliv, akademia, forsvar og offentlig sektor i partnerprogrammet og stadig flere kommer til. JD vil følge opp bedre samordning av tilsynsmyndigheter og tilsynsmetodikk overfor NSM og Direktoratet for samfunns-sikkerhet og beredskap (DSB). Regjeringen har også styrket kommunesektoren med 50 mill. kroner for å øke kommunenes kompetanse og kapasitet til å forebygge og håndtere digitale hendelser (ref. punkt 2.4 om eget responsmiljø).

3.2 Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om den nasjonale digitale sikkerhetstilstanden

JDs oversikt over sikkerhetstilstanden tar utgangspunkt i aggregert informasjon fra blant annet NSM og DSB. Min vurdering er at departementet har god nok oversikt til å gjøre prioriteringer på nasjonalt nivå, og at den strategiske kursen som myndighetene har satt er riktig. De prioriteringer som gjøres i Norge sammenfaller i stor grad med prioriteringer som gjøres internasjonalt. Norge anses som et land som har kommet langt på dette området og våre vurderinger av utfordringsbildet er gjenkjennelig hos nære allierte. Det er samtidig viktig at vi jobber kontinuerlig med å forbedre kunnskapsgrunnlaget.

Arbeidet med å implementere ny sikkerhetslov har tatt tid. Pandemien påvirket departementenes arbeidssituasjon og gjorde det krevende å nå tidsfristene. Det ble likevel arbeidet aktivt for å nå den overordnede målsettingen om å få etablert den første nasjonale oversikten over grunnleggende nasjonale funksjoner (GNF), og oversikt over virksomheter av betydning for GNF og deres avhengigheter. NSM har nå en samlet oversikt over GNF, skjermingsverdige objekter og infrastrukturer, samt innmeldte vedtak om virksomheter som er underlagt sikkerhetsloven etter § 1-3. Med utgangspunkt i den sikkerhetspolitiske situasjonen har departementet i nært samarbeid med Forsvarsdepartementet og øvrige aktuelle departement nå intensivert arbeidet. JD vil prioritere arbeidet med å kartlegge verdier og avhengigheter, slik at virkemiddelbruken blir så treffsikker som mulig. Sikkerhetsloven er et nyttig verktøy for å beskytte verdiene våre når sikkerhetssituasjonen endrer seg. JD vil forvalte pådriverrollen aktivt.

Regjeringen har i Meld. St. 9 (2022-2023) fremmet flere strategiske grep for å sikre økt oversikt over verdier av betydning for nasjonal og digital sikkerhet. Dette innebærer både å intensivere kartleggingen av verdier i tråd med sikkerhetsloven, men også å få bedre oversikt over virksomheter og verdier som sikkerhetsloven ikke gjelder for, men som likevel kan ha betydning for nasjonal sikkerhet og samfunnskritiske funksjoner. I tillegg vurderer vi en nasjonal skytjeneste for økt kontroll med kritisk IT-infrastruktur og beskyttelsesverdig informasjon. Regjeringen vil videre stille krav til sikkerhet for datasentre og innføre en registreringsplikt for datasenteraktører slik at myndighetene får bedre oversikt over datasenternæringen i Norge.

Når det gjelder status- og tilstandsvurderinger har JD hatt møte med departementene, og bidratt til å legge til rette for gjennomføringen av vurderingene. Den varslede gjennomgangen av ordningen med status- og tilstandsvurderinger er ment å bidra til en mer enhetlig rapportering. JD har utarbeidet en veileder til departementenes arbeid etter samfunnssikkerhetsinstruksen. Denne omfatter også arbeidet med ROS-analyser.

Når det gjelder tilsyn etter sikkerhetsloven vil jeg påpeke at begrenset antall tilsyn i 2019 og 2020 følger av beslutning om å være tilbakeholdne med undersøkelser av et nylig etablert sikkerhetsregelverk. Tilsynsomfanget for NSM vil i 2022 være på om lag 50 tilsyn, hvilket er en jevn stigning. DBSs tilsyn baseres på en vurdering av risiko og

vesentlighet. De omfatter i utgangspunktet alle aspekter ved departementenes arbeid med samfunnssikkerhet etter samfunnssikkerhetsinstruksen, og de er ikke innrettet mot digital sikkerhet spesielt. Det er DSB som har kompetansen til å vurdere hvilke hensyn som skal vektlegges i det enkelte tilsyn, men departementet vil understreke overfor etatene at digital sikkerhet er ansett som en felles utfordring for de fleste virksomheter i Norge med potensielt store konsekvenser. Departementet vil også se på hvordan digital sikkerhet i større grad kan inngå i flere tilsyn utenfor sikkerhetsloven.

3.3 Justis- og beredskapsdepartementet har ikke sørget for god nok oppfølging av Nasjonal strategi for digital sikkerhet

Jeg registrerer at undersøkelsen synliggjør at arbeidet med nasjonal digital sikkerhet er basert på et systematisk og kunnskapsbasert arbeid over tid. Det har vært en vesentlig endring av utøvelsen av samordningsrollen etter at JD overtok ansvaret i 2013, både ved å allokere flere ressurser til arbeidet, og ved å utpeke NSM som nasjonalt fagmiljø. JD har også lagt en bredere definisjon til grunn ut fra identifiserte behov, og lagt større vekt på nasjonale behov i utøvelsen av samordningsrollen. Rollen ble ytterligere styrket da JD fikk ansvaret for sikkerhetsloven og NSM i 2019.

Det har vært særlig viktig å få en uavhengig gjennomgang med konkrete anbefalinger til myndighetene. Lysneutvalgets utredning (NOU 2015: 13) fikk bred støtte i sine funn og anbefalinger. Rapporten har vært en viktig plattform for arbeidet med digital sikkerhet og den strategiske kursen som ble satt i IKT-sikkerhetsmeldingen (2017), og videreutviklet i Nasjonal strategi for digital sikkerhet (2019). Holteutvalgets utredning (NOU 2018: 14) så særlig på organisering og regulering innen digital sikkerhet, og ble fulgt opp blant annet i samfunnssikkerhetsmeldingen (2019).

Jeg er enig i at JD i undersøkelsesperioden ikke har sørget for å få god nok informasjon om virkningen av den nasjonale strategien og tilhørende tiltak, noe som er krevende å måle. I oppfølgingen av strategien har JD prioritert å kartlegge hvordan de 10 anbefalingene i strategien har blitt fulgt opp blant norske virksomheter. Øvrige tiltak i oversikten følges opp av ansvarlig departement som del av den ordinære styringsdialogen. Tiltaksoversikten er ikke et styringsverktøy i seg selv, men skulle i 2019 gi aktørene en oversikt over utvalgte sentrale tiltak innen fem prioriterte områder. Stortingsmeldinger og Prop 1 S benyttes til å gi oppdateringer og synliggjøre prioriteringer på området.

I samråd med Kunnskapsdepartementet skal JD innen mars 2023 innhente oppdaterte tall over kompetansegapet, i tråd med tiltaket i kompetansestrategien. Det vil også bli utredet hva som er arbeidslivets behov for doktorgradskompetanse til stillinger hvor det kreves sikkerhetsklarering, jf. Meld. St. 9 (2022-2023). Jeg vil likevel understreke at intensjonen med strategiene har vært å sette en felles retning, synliggjøre myndighetenes mål og prioriteringer, og få ulike aktører til å understøtte hverandre i arbeidet med digital sikkerhet. Dagens nasjonale strategi er et resultat av langsiktig, systematisk kunnskapsbygging, hvor kursen som er satt har vært bredt forankret.

3.4 Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverrsektoriell hendelseshåndtering

NSM har over tid erfart en kraftig økning av antall registrerte digitale angrep. For å møte disse utfordringene er NSM styrket med 45,3 mill. kroner i 2022. Bevilgningen innebærer en utvidelse av antall stillinger i NSM. Hensikten er å forbedre evnen til koordinering, analyse og håndtering av hendelser og praktisk bistand til rammede virksomheter. Bevilgningen skal også bidra til å øke antallet virksomheter som deltar i VDI-samarbeidet (Varslingssystem for digital infrastruktur) og NSMs analysekapasitet for å håndtere større informasjonsmengder. «Neste generasjon VDI» utvides med flere ulike komponenter som er designet til å fungere sammen og vil totalt sett være mer effektivt enn i dag. Utvidelsen er også et viktig bidrag for å se helheten og arbeidet med et nasjonalt situasjonsbilde i det digitale domenet. I samme budsjettvedtak ble det også gitt midler til å etablere et permanent responsmiljø for kommunene, som skal bistå kommunene med å forebygge, avdekke og håndtere digitale angrep.

Sektorvise responsmiljøer er et viktig tiltak for å sikre deling av informasjon og støtte til håndtering av digitale angrep. På oppdrag fra JD er det utført en ekstern evaluering av ordningen med sektorvise responsmiljø. Det overordnede inntrykket er at samarbeidet mellom aktørene fungerer godt, at det er god utveksling av informasjon, metoder, erfaringer og kompetanse på tvers av miljøene, og at ordningen med sektorvise responsmiljø har gitt et mer samlet sikkerhetshetsmiljø i Norge. En hovedkonklusjon er at den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner. I tillegg bør forebyggende digital sikkerhet i større grad inkluderes i den nasjonale modellen for hendelseshåndtering og balanseres mot operativt arbeid. I Meld. St. 9 (2022-2023) fremgår det at regjeringen vil videreutvikle det nasjonale rammeverket for håndtering av digitale hendelser. Dette for å sikre en bærekraftig hendelseshåndteringsmodell i tråd med samfunnets behov.

På enkelte områder hensyntar undersøkelsen i liten grad at myndighetene over en lang periode har stått i en pandemi, med etterfølgende ny sikkerhetssituasjon som har krevd strenge prioriteringer. Dette gjelder særlig for øvelsesgjennomføring. Digital sikkerhet har fått økt oppmerksomhet og prioritering grunnet økt bruk av hjemmekontor og ny sikkerhetspolitisk situasjon med stadig flere digitale angrep. Verdien av reell hendelseshåndtering, koordinering og samhandling på tvers over en lang periode, gir en kunnskap og erfaring ikke øvelser i seg selv kan gi. Jeg mener det er viktig å vekte prioriteringer opp mot hverandre på et område med knappe ressurser. Det har vært gjennomført en rekke øvelser tross de ekstraordinære situasjonene, men flere viktige oppgaver har også måttet bli utsatt eller nedprioritert. Et eksempel er gjennomføringen av den nasjonale øvelsen «Digital 2020» som måtte nedskaleres under nedstengningen av samfunnet.

4. AVSLUTTENDE KOMMENTAR

Jeg tar Riksrevisjonens anbefalinger (jfr. pkt. 5 i utkast til Dokument 3:7) på alvor, og departementet vil følge opp disse sammen med andre berørte departementer på egnet måte. Jeg mener at flere av de pågående prosessene som jeg her har orientert om langt på vei svarer opp Riksrevisjonens anbefalinger.

Med hilsen

Emilie Mehl

Vedlegg 3:

Forvaltningsrevisjonsrapport med vurderinger

Revisjonen er gjennomført som en forvaltningsrevisjon i henhold til

- **lov om Riksrevisjonen § 9 tredje ledd**
- **instruks om Riksrevisjonens virksomhet § 9**
- **INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000)**
- **Riksrevisjonens faglige retningslinjer for forvaltningsrevisjon**

Innhold

Tabelloversikt

Figuroversikt

Faktaboksoversikt

Ordliste og forkortelser

Alvorlig digital hendelse	Reelle og potensielle uønskede hendelser i det digitale rom som er rettet mot samfunnskritisk infrastruktur eller samfunnets kritiske funksjoner.
CERT/CSIRT	CERT er en forkortelse for *Computer Emergency Response Team.* Begrepet har i den senere tid blitt erstattet med CSIRT, som står for *Computer Security Incident Response Team*. På norsk kan funksjonen omtales som responsmiljø for håndtering av digitale sikkerhetshendelser. Vi bruker responsmiljø i denne rapporten.
Digitale operasjoner og angrep	En prosess der en trusselaktører søker å skaffe seg urettmessig tilgang til et digitalt nettverk hos en spesifikk virksomhet. Formålet med operasjonen kan være etterretningsinnsamling, forberedelser til potensiell sabotasje, tyveri eller manipulasjon av data. Ved et digitalt angrep er formålet å stjele, sabotere eller manipulere data.
Digitale verdikjeder	En struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, programvare eller maskinvare. Virksomhetene i en verdikjede er mer eller mindre avhengige av hverandre for å kunne levere tjenester/produkter, det vil si at det er avhengigheter dem imellom.
Forebyggende sikkerhetsarbeid	Tiltak for å redusere muligheten for en uønsket hendelse eller konsekvensene av en mulig hendelse. Dette omfatter aktiviteter knyttet til beslutninger, utførelse og oppfølging.
Grunnleggende nasjonale funksjoner	Tjenester, produksjon og andre former for virksomhet som i henhold til sikkerhetsloven er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. Virksomheter som grunnleggende nasjonale funksjoner er avhengig av for å opprettholde sin funksjon omtales som *avhengigheter*.
Informasjonssikkerhet	Sikring av både digital og analog informasjon og en utvidelse av fagområdet datasikkerhet. I informasjonssikkerhet legges det større vekt på organisasjonenes overordnede prosesser og rutiner rundt sikring av informasjon og tjenester enn på metodene og verktøyene.
Internkontroll	Et kontroll- og dokumentasjonssystem som bedrifter og virksomheter bruker for å sikre at de oppfyller krav som er fastsatt i lover og forskrifter.
Kritisk infrastruktur	Anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner, som igjen dekker samfunnets grunnleggende behov og ivaretar befolkningens trygghetsfølelse.
Løsepengevirus	En type skadevare som låser eller krypterer hele eller deler av innholdet på datamaskinen. For at brukeren skal få tilgang til innholdet igjen, krever angriperen løsepenger.
Phishing / sosial manipulering	En form for sosial manipulering hvor en angriper forsøker å lure noen til å utføre en handling, for eksempel til å åpne et e-postvedlegg med skadevare eller klikke på en lenke hvor det bes om sensitiv informasjon.

Risiko- og sårbarhetsanalyser / risikovurdering	Et verktøy for å identifisere uønskede hendelser og konsekvensene av disse. Innsikten fra analysene og/eller vurderingen kan brukes som grunnlag for beslutninger om risiko, for eksempel om iverksetting av sikkerhetstiltak.
Samfunnets kritiske funksjoner	Funksjoner som, dersom de faller bort, får konsekvenser som truer befolkningens og samfunnets grunnleggende behov, herunder ivaretakelse av grunnleggende samfunnsverdier som liv og helse, natur og miljø, økonomi, samfunnsstabilitet, styringsevne og kontroll. Virksomheter som samfunnets kritiske funksjoner er avhengig av for å opprettholde sin funksjon omtales som *understøttende virksomheter*.
Sektorvise responsmiljøer	Miljøer med operativt ansvar for å dekke virksomheter innenfor hele eller deler av et departements myndighetsområde eller sektor. Det sektorvise responsmiljøet skal dekke en grunnleggende kapasitet til å koordinere, varsle om og håndtere uønskede digitale hendelser.
Sikkerhetsgradert informasjon	Informasjon som kan skade nasjonale sikkerhetsinteresser dersom den blir kjent for uvedkommende, og som derfor skal sikkerhetsgraderes.
Sikkerhetsstyring	Styring, for eksempel av aktiviteter, som en virksomhet gjør for å sikre en god forebyggende sikkerhet. Målet er å styre arbeidet i virksomheten for å oppnå og opprettholde et forsvarlig sikkerhetsnivå, basert på den risikoen virksomheten er eksponert for. Brukes synonymt med *risikostyring*.
Sikkerhetstiltak	Alle former for tiltak som skal bidra til å øke den digitale sikkerheten, for eksempel tekniske tiltak, som krav til lagring og oppbevaring av digital informasjon. Sikkerhetstiltak kan også være gjennomføring av øvelser og utforming av beredskapsplaner.
Skjermingsverdige objekter og infrastruktur	Objekter og infrastruktur som kan skade grunnleggende nasjonale funksjoner dersom de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.
Skytjenester	En samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelige fra eksterne serverparker tilknyttet internett.
Sårbarheter	Svakheter i et system som kan utnyttes av en angriper og føre til skade og tap. Sårbarheter kan være både organisatoriske, menneskelige, tekniske og fysiske svakheter.
VDI	Varslingssystem for digital infrastruktur

1 Innledning

1.1 Bakgrunnen for undersøkelsen

1.1.1 Økende digital trussel og sårbarhet

I Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden* (*samfunnssikkerhetsmeldingen*) går det fram at digital sikkerhet er helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser.[1] En av myndighetenes hovedprioriteringer er å legge til rette for at både offentlige og private virksomheter skal kunne ta i bruk nye digitale løsninger.[2] Digitaliseringen øker samtidig risikoen for uønskede digitale hendelser og styrker behovet for god digital sikkerhet.

De nasjonale etterretnings- og sikkerhetstjenestene har over flere år vurdert etterretningstrusselen som den største trusselen mot Norge.[3] Politiets sikkerhetstjeneste (PST) beskriver etterretningstrusselen som betydelig og økende og viser til at nettverksoperasjoner[4] har blitt en integrert del av andre lands etterretningstjenester. Videre viser PST til at vi i andre land har sett at statlige aktører har kapasitet til å gjennomføre sabotasje med hjelp av nettverksoperasjoner. I disse landene har både helsevesen, politi, drivstoffleveranser og matforsyning blitt rammet. I lys av den globale utviklingen kan også Norge bli utsatt for digitale nettverksoperasjoner, og i ytterste konsekvens kan grunnleggende nasjonale funksjoner og kritiske samfunnsfunksjoner bli rammet, med forsinkelser og brudd i tjenesteleveranser som resultat.[5]

Nasjonal sikkerhetsmyndighet rapporterte i 2022 om økende digital trusselaktivitet i Norge, både fra statlige og kriminelle aktører. Ifølge Nasjonal sikkerhetsmyndighet har det i perioden 2019–2021 vært en tredobling i antall alvorlige digitale hendelser og angrep.[6] Den samlede statistikken over alle hendelser som er registrert av Nasjonal sikkerhetsmyndighet, viser at teknologibedrifter, forskning og utvikling samt offentlige forvaltningsorganer har vært særlig utsatt.[7] Digitale angrep rammer i økende grad flere mål samtidig, på tvers av sektorer, og angrepene øker i antall, kompleksitet og tid.[8] Gjennomgående beskriver etterretnings- og sikkerhetstjenestene den digitale angrepsflaten og metodikken som stadig mer avansert og treffsikker.[9] I *Helhetlig digitalt risikobilde* for 2020 viser Nasjonal sikkerhetsmyndighet til at hendelseshåndteringen blir stadig mer tid- og ressurskrevende.[10] De siste årene har det vært flere digitale angrep som har rammet offentlige og private virksomheter i Norge. Se faktaboks 1 for utvalgte eksempler.

Faktaboks 1 Eksempler på digitale angrep mot norske mål etter 2020

I løpet av et halvt år i perioden 2020−2021 ble Stortinget utsatt for to digitale angrep. Norske myndigheter anklaget Russland for å ha stått bak det første angrepet, som fant sted i august 2020. Dette er første gang norske myndigheter offentlig har anklaget et annet land for et digitalt angrep mot Norge.[11] Det andre angrepet, som fant sted i mars 2021, var større og mer avansert

[1] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden.*
[2] Meld. St. 27 (2015–2016) *Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet.*
[3] Etterretningstjenesten (2022) *Fokus 2022*; Politiets sikkerhetstjeneste (2018–2022) *Nasjonal trusselvurdering*.
[4] Politiets sikkerhetstjeneste definerer *nettverksoperasjon* som en prosess der trusselaktører søker å skaffe seg urettmessig tilgang til datanettverk hos en spesifikk virksomhet. Nettverksoperasjoner kan ha ulike formål, for eksempel etterretningsinnsamling, forberedelser til potensiell sabotasje eller manipulasjon av data.
[5] Politiets sikkerhetstjeneste (2021) *Nasjonal trusselvurdering 2021;* Politiets sikkerhetstjeneste (2022) *Nasjonal trusselvurdering 2022.*
[6] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022*, s. 9.
[7] Nasjonal sikkerhetsmyndighet (2022) *Nasjonalt digitalt risikobilde 2022*, s. 15.
[8] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022.*
[9] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022*; Politiets sikkerhetstjeneste (2022) *Nasjonal trusselvurdering 2022*; Etterretningstjenesten (2022) *Fokus 2022*.
[10] Nasjonal sikkerhetsmyndighet (2020) *Helhetlig digitalt risikobilde 2020*, s. 5.
[11] Aftenposten (2022) *Regjeringen: Russland stod bak dataangrep på Stortinget.* Nettartikkel, 13. oktober 2020 [Hentedato 7. oktober 2022].

enn det første. Stortingspresidenten omtalte angrepet som «et angrep på vårt demokrati».[12] Begge angrepene medførte tap av sensitive data og informasjon. I januar 2021 ble også Østre Toten kommune rammet av et digitalt angrep som medførte tap av sensitive data. Kommunens systemer ble låst av angriperen og gjort utilgjengelige. Det tok kommunen flere måneder å gjenopprette disse systemene. Videre er det gjort kjent at omfattende digitale angrep den siste tiden har vært rettet mot store norske aktører som blant annet Amedia[13], Nortura[14] og NorDan[15].

Økt bruk av offentlig-privat samarbeid, samarbeid stater imellom og bruk av tjenesteutsetting og underleverandører øker kompleksiteten i digitale systemer og verdikjeder. Dette øker i sin tur den digitale sårbarheten.[16] Utfordringen er i hovedsak at det som følge av dette blir mer krevende for virksomheter å holde oversikt.[17] Trusselaktørene utnytter som regel det svakeste leddet i en verdikjede. Lengre og mer komplekse digitale verdikjeder beskrives derfor i risikovurderingene til etterretnings- og sikkerhetstjenestene som den største digitale sårbarheten i samfunnet.[18]

Faktaboks 2 Digitale verdikjeder

En digital verdikjede eller leverandørkjede er en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, programvare eller maskinvare. Virksomhetene i en verdikjede er mer eller mindre avhengige av hverandre for å kunne levere tjenester/produkter, det vil si at det er avhengigheter dem imellom.

Kilde: Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar.*

«Skyavhengighet» trekkes også fram som en betydelig trussel i de senere årenes nasjonale risikovurderinger. Denne avhengigheten bidrar til å øke kompleksiteten i verdikjedene, blant annet ved at den knytter oss til internasjonale verdikjeder. Dette må ses i sammenheng med utviklingen av 5G-nettet, som øker informasjonsmengden i elektroniske kommunikasjonsnett og muliggjør økt bruk av skytjenester og tingenes internett (gjenstander som kjøleskap, kameraer og belysning tilkoblet Internett).[19]

Ifølge de nasjonale trusselvurderingene har det også vært en betydelig økning i digital kriminalitet som er økonomisk motivert, særlig fra 2020. Risikoen knyttet til løsepenger og kryptovaluta beskrives som større og mer omfattende fra år til år.[20] Løsepengevirus rammer stadig flere sektorer og er i økende grad rettet mot verdikjeder. Telenor omtalte i 2021 løsepengetrusselen som «en reell fare for samfunn, liv og helse».[21] Vår egen gjennomgang av offentliggjorte digitale angrep fra desember 2020 til februar 2022 viser at løsepengevirus (ransomware) var registrert som angrepsmetode i 21 av de 40 angrepene. Selv om løsepengevirus ofte forbindes med vinningskriminalitet, viser PST i trusselvurderingen for 2022 til flere eksempler på at det har vært koblinger mellom løsepengevirus og andre lands etterretningstjenester.[22]

[12] Aftenposten /2021) *Stortinget utsatt for IT-angrep: «Et angrep på vårt demokrati».* Nettartikkel, 10. mars 2021 [Hentedato 7. oktober 2022].
[13] NRK (2021) *Amedia utsatt for alvorlig dataangrep*. Nettartikkel, 28. desember 2021 [Hentedato 7. oktober 2022].
[14] E24 (2021) *Nortura utsatt for dataangrep.* Nettartikkel, 22. desember 2021 [Hentedato 7. oktober 2022].
[15] Nordangruppen (2022) *Bevissthet og åpenhet rundt dataangrep.* Nettartikkel [Hentedato 7. oktober 2022].
[16] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden,* s. 27–28.
[17] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022.*
[18] Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018*; Politiets sikkerhetstjeneste (2018) Politiets sikkerhetstjenestes *trusselvurdering 2018*; Nasjonal sikkerhetsmyndighet (2019) *Helhetlig digitalt risikobilde 2019*; Nasjonal sikkerhetsmyndighet (2019). *Risiko 2019*; Nasjonal sikkerhetsmyndighet (2020) *Risiko 2020*; Telenor (2020) *Digital sikkerhet 2020*; Nasjonal sikkerhetsmyndighet (2021) *IKT-risikobilde 2021*; Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021;* Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022.*
[19] Nasjonal sikkerhetsmyndighet (2020) *Risiko 2020*; Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021.*
[20] Telenor (2018) *Digital sikkerhet 2018*; Nasjonal sikkerhetsmyndighet (2019) *Helhetlig digitalt risikobilde 2019*; Norsk senter for informasjonssikring (2020) *Trusler og trender 2020*; Nasjonal sikkerhetsmyndighet (2020) *Risiko 2020*; Nasjonal sikkerhetsmyndighet (2021) *IKT-risikobilde 2021*; Telenor (2021) *Digital sikkerhet 2021.*
[21] Telenor (2021) *Digital sikkerhet 2021*, s. 28.
[22] Politiets sikkerhetstjeneste (2022) *Nasjonal trusselvurdering 2022.*

1.1.2 Digitalt sikkerhetsarbeid krever samordning av aktører og virkemidler

Myndighetene besitter flere virkemidler for å ivareta den nasjonale digitale sikkerheten. I henhold til *samfunnssikkerhetsmeldingen* (2020) er disse virkemidlene juridiske (lover, forskrifter instrukser og tilsyn), organisatoriske (fordeling av ansvar, roller og oppgaveløsning i forebyggende sikkerhetsarbeid og hendelseshåndtering), økonomiske (for eksempel bevilgninger gjennom statsbudsjettet) og pedagogiske (rundskriv, retningslinjer og veiledere som har som mål å bidra til at lover og forskrifter følges). De ulike virkemidlene må ses i sammenheng, og det må være en bevissthet om når de skal benyttes, for at de skal ha sin tiltenkte effekt.[23]

Det er Justis- og beredskapsdepartementet som har ansvar for å samordne arbeidet med digital sikkerhet i sivil sektor. Departementet har også et pådriveransvar for arbeidet med digital sikkerhet.[24] Arbeidet med digital sikkerhet er imidlertid en kompleks utfordring som krever samordning. Aktørene må utforme og samordne virkemidler og tiltak på tvers av sektorer, fordi ingen aktør har nok kunnskap og informasjon til å løse problemet alene.[25] I Meld. St. 10 (2016−2017) *Risiko i et trygt samfunn* og senere i Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar (IKT-sikkerhetsmeldingen)* og *samfunnssikkerhetsmeldingen* (2020) understrekes viktigheten av at militære og sivile aktører og offentlige og private virksomheter, samarbeider for å ivareta den digitale sikkerheten, slik at samfunnets ressurser kan utnyttes best mulig.

Faktaboks 3 Hva er samordning?

Med *samordning* menes en prosess der selve kjernen er at ulike mål, verdier, aktiviteter, ressurser eller andre premisser blir sett i sammenheng, prioritert, avveid og tilpasset til hverandre.

Kilde: Direktoratet for forvaltning og økonomistyring (2014) *Mot alle odds? Veier til samordning i norsk forvaltning*.

IKT-sikkerhetsutvalget peker i sin utredning NOU (2018: 14) *IKT-sikkerhet i alle ledd* på at styringen av den digitale sikkerheten er sterk i flere sektorer, men at samordningen og oversikten på tvers av sektorer er mangelfull.[26] Dårlig samordning kan føre til overlapp mellom ansvarsområder og blindsoner i regulering, oversikt og oppfølging. Effektiv samordning kan på sin side bidra til å redusere ressursbruken og forbedre effekten av tiltak og virkemidler.[27]

Gjennom tidligere undersøkelser har Riksrevisjonen funnet svakheter i den digitale sikkerheten hos flere statlige virksomheter. Samlet viser undersøkelsene at virksomheter i ulike sektorer har flere av de samme utfordringene knyttet til det digitale sikkerhetsarbeidet.[28] Dette tyder på at det er problemstillinger og utfordringer på tvers av sektorene som ikke er håndtert, og som krever samordning.

1.1.3 Koronapandemiens påvirkning på myndighetenes arbeid med nasjonal digital sikkerhet

Store deler av undersøkelsesperioden har vært preget av koronapandemien. Pandemien var en unntakstilstand som påvirket myndighetene og samfunnet på ulike måter. Pandemien medførte blant

[23] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*.
[24] Kgl.res av 10. mars 2017 nr. 312.
[25] Peters, Guy B. (2018) *The challenge of policy coordination.* I: *Policy Design and Practice*, 1(1), s. 1–11; Kooiman, Jan (1993) *Modern Governance. New Government - Society Interactions*. London: SAGE; Klijn, Erik-Hans (2008) *Governance and Governance Networks in Europe.* I: *Public Management Review*, 10(4), s. 505–525.
[26] NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*
[27] Trondal, Jarle (2017) *The Rise of Common Political Order.* Storbritannia: Edward Elgar Publishing.
[28] Del av Dokument nr. 3:2 (2020–2021) *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer* (15. desember 2020); del av Dokument nr. 3:2 (2020–2021) *Riksrevisjonens undersøkelse av informasjonssikkerhet i Norfund*; Dokument nr. 3:5 (2020–2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT*; Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelse av sikring mot dataangrep i Utenriksdepartementet* (gradert); Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelse av sikring mot dataangrep i Oljedirektoratet*; Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelser av angrep mot IKT-systemer i politiet*.

annet økt digital sårbarhet grunnet omfattende bruk av hjemmekontor. Pandemien har også hatt konsekvenser for planlagte aktiviteter og tiltak på det digitale området. Justis- og beredskapsdepartementet viser i brev til at departementet og underliggende etater over en lengre periode har hatt en ekstraordinær situasjon, hvor sikkerhets- og beredskapsressurser, som vanligvis ville vært benyttet i samordningsarbeidet med digital sikkerhet, har bistått i pandemihåndtering. Departementet står nå i en tilsvarende situasjon, med krig i Ukraina og samordning av sivile behov.[29] Andre etater som omfattes av undersøkelsen har også påpekt at restriksjonene som fulgte av pandemien har påvirket arbeidet på det digitale sikkerhetsområdet.

1.2 Mål og problemstillinger

Målet med denne undersøkelsen er å vurdere om myndighetenes samordning av arbeidet for å ivareta den digitale sikkerheten i sivil sektor er effektiv og i tråd med Stortingets vedtak og forutsetninger. Undersøkelsen omfatter samordningen av arbeidet med å forebygge og håndtere digitale sikkerhetshendelser.

Undersøkelsen har følgende problemstillinger:

Problemstilling 1: *Bidrar myndighetenes samordning av roller, ansvar og krav til å ivareta den digitale sikkerheten?*

Arbeidet med problemstillingen går ut på å kartlegge alle de sentrale aktørene, herunder myndigheter og offentlige og private virksomheter som har et ansvar for å veilede, føre tilsyn med og bistå virksomheter i arbeidet med den digitale sikkerheten og håndtere alvorlige digitale angrep i sivil sektor. Basert på dette undersøker vi om kravene i regelverk og tilhørende veiledning er samordnet og tilgjengelig for de som omfattes av regelverket. Videre undersøker vi om de sentrale aktørene på området har en enhetlig forståelse av roller, ansvar og krav når det gjelder gjennomføring av tilsyn, veiledning av brukere og hendelseshåndtering.

Problemstilling 2: *Har Justis- og beredskapsdepartementet en helhetlig oversikt over den nasjonale digitale sikkerhetstilstanden?*

Det er nødvendig å ha informasjon om den digitale sikkerhetstilstanden for å kunne iverksette og samordne virkemidler og ivareta den digitale sikkerheten på tvers av sektorene. Arbeidet med problemstillingen går derfor ut på å kartlegge om Justis- og beredskapsdepartementet har oversikt over den nasjonale digitale sikkerhetstilstanden. Har departementet for eksempel oversikt over risikobildet og hvilke verdier som skal beskyttes? Vi har som et ledd i dette kartlagt og vurdert kildene departementet benytter for å holde oversikt over den nasjonale digitale sikkerhetstilstanden.

Problemstilling 3: *Ivaretar Justis- og beredskapsdepartementet samordningsrollen for den digitale sikkerheten på samfunnssikkerhetsområdet på en god nok måte?*

Arbeidet med problemstillingen går ut på å kartlegge hvordan Justis- og beredskapsdepartementet jobber med oppfølging av nasjonale strategier og rammeverk, gjennomføring og oppfølging av nasjonale øvelser og hendelser, utveksling av informasjon om felles problemstillinger og tema, kompetanseheving og erfaringsutveksling.

1.2.1 Undersøkelsens omfang

I denne undersøkelsen ser vi på hvordan Justis- og beredskapsdepartementet samordner arbeidet med digital sikkerhet i sivil sektor i fredstid. Vi ser også på hvordan departementet arbeider både med

[29] Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

forebygging og håndtering av digitale angrep. Undersøkelsesperioden har i hovedsak vært 2018 til 2021, men vi har også inkludert data fra 2022 der disse har vært tilgjengelige og relevante. Sentrale styrende dokumenter som er publisert før 2018, og som legger føringer og retning for arbeidet med digital sikkerhet i undersøkelsesperioden, har også blitt inkludert.

Undersøkelsen er rettet mot Justis- og beredskapsdepartementets samordnings- og pådriveransvar. Vi har belyst ulike temaer og tiltak på det digitale sikkerhetsområdet, herunder tilsynsvirksomhet, gjennomføring av nasjonale øvelser og arbeidet i samordningsarenaer på området. Vi har også undersøkt i hvilken grad målet om samordnet veiledning og hendelseshåndtering er oppnådd. Selv om ikke alle undersøkelsens områder direkte omfatter Justis- og beredskapsdepartementets ansvarsområde, har dette samlet sett bidratt til å belyse hvordan Justis- og beredskapsdepartementet ivaretar sin samordnings- og pådriverrolle. Vi har forsøkt å belyse de mulige konsekvensene av en eventuell svak samordning på de enkelte områdene.

I denne undersøkelsen defineres begrepet *digital sikkerhet* på samme måte som det defineres i *Nasjonal strategi for digital sikkerhet*. Der går det fram at digital sikkerhet er *beskyttelse av alt som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi*.[30] Vi bruker *digital sikkerhet* synonymt med begreper som *IKT-sikkerhet* og *cybersikkerhet*. Når andre begreper enn digital sikkerhet brukes i primærkilden, gjengis de slik i undersøkelsen.

Undersøkelsen omfatter informasjon fra dokumenter som er unntatt offentlighet og informasjon som er sikkerhetsgradert etter sikkerhetsloven. Justis- og beredskapsdepartementet har vurdert at informasjonen fra dokumenter som er unntatt offentlighet kan gjengis i denne rapporten. Informasjon som er sikkerhetsgradert etter sikkerhetsloven omtales i et sikkerhetsgradert vedlegg til denne rapporten.

1.2.2 Bruk av ekspertgruppe

Vi har i forbindelse med undersøkelsen nedsatt en ekspertgruppe bestående av Hans Christian Pretorius (partner i KPMG Norge), Nils Kalstad (leder for Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU) og Suhail Mushtaq (fagsjef for informasjonssikkerhet i Kommunesektorens organisasjon (KS). Formålet har vært å sikre at vi har god faglig forståelse av hva arbeidet med digital sikkerhet innebærer. Vi har gjennomført to møter med ekspertgruppen i løpet av undersøkelsesperioden. Ekspertgruppen bidro med kunnskap da vi arbeidet med å planlegge undersøkelsen, og de deltok i en diskusjon om funnene i undersøkelsen. Gruppen har ikke noe ansvar for rapportens innhold eller faglige kvalitet.

[30] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhet*, s. 6.

2 Metodisk tilnærming og gjennomføring

For å besvare problemstillingene har vi benyttet ulike metoder, nærmere bestemt intervjuer, dokumentanalyse, dybdeundersøkelser og skriftlige spørsmål, slik tabellen nedenfor illustrerer.

Tabell 1 Metodene som er brukt for hver problemstilling

Metode	Problemstilling 1	Problemstilling 2	Problemstilling 3
Intervju	X	X	X
Dokumentanalyse	X	X	X
Skriftlige spørsmål til departementene		X	
Dybdeundersøkelse	X	X	X

2.1 Intervjuer

Vi har hentet inn informasjon ved hjelp av intervjuer i arbeidet med alle problemstillingene. Vi har intervjuet Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet, Forsvarsdepartementet, Kunnskapsdepartementet, Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste, Kripos, Direktoratet for samfunnssikkerhet og beredskap, Digitaliseringsdirektoratet, Nasjonal kommunikasjonsmyndighet og Datatilsynet. I tillegg har vi intervjuet sentrale aktører i privat sektor, kommunesektoren og aktørene som inngår i dybdeundersøkelsene (se nedenfor). Skriftlig referat fra intervjuene ble forelagt alle de intervjuede virksomhetene for verifisering.

2.1.1 Gjennomgang av samordningsarenaer

I kapitlet om samordningsarenaer har vi valgt å rette oppmerksomheten mot arenaene som er nevnt som tiltak i *Nasjonal strategi for digital sikkerhet* (2019). Vi har også valgt å se på *Samhandlingsarena for sektortilsyn med sikkerhetsloven* fordi den i *samfunnssikkerhetsmeldingen* (2020) omtales som et viktig tiltak for å øke koordineringen av tilsyn med den digitale sikkerheten.[31] De utvalgte arenaene er alle etablert eller omorganisert relativt nylig. Samtidig har pandemien redusert den planlagte møtehyppigheten og møteformen. Det har derfor ikke latt seg gjøre å måle effektene av samordningsarenaene. Våre vurderinger av samordningsarenaene som tiltak baserer seg på sentrale deltakeres opplevelser av arenaene og gjennomgåtte møtereferater. Vi har ikke intervjuet alle deltakerne i arenaene, men har gjort et utvalg basert på aktørens helhetlige ansvar innenfor myndighetenes arbeid med digital sikkerhet i sivil sektor.

2.2 Dokumentanalyse

Vi har gått gjennom sentrale dokumenter og regelverk som regulerer ansvaret og kravene til aktørene innenfor arbeidet med digital sikkerhet. Dette omfatter lover og forskrifter som regulerer digital sikkerhet, kongelige resolusjoner, budsjettproposisjoner og tildelingsbrev. Videre har *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017), *Retningslinjer for cybersamarbeid* (2022) og

[31] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*.

veiledningene som er utarbeidet for de ulike regelverkene som omfatter digital sikkerhet, vært sentrale i gjennomgangen.

I tillegg har vi gått gjennom kilder til informasjon som myndighetene benytter for å holde en helhetlig oversikt over den digitale sikkerhetstilstanden, blant annet tilsynsrapporter, etterretnings- og sikkerhetstjenestenes risikovurderinger, Nasjonal sikkerhetsmyndighets kontrollmeldinger og årsrapporter, evalueringer fra øvelser og hendelser, rapportering om digital sikkerhet i etatsstyringen og forskning og kartlegginger på temaet. Næringslivets sikkerhetsråd gjennomfører for eksempel jevnlige undersøkelser om sikkerhet, blant annet *Mørketallsundersøkelsen*, hvor den digitale sikkerhetstilstanden både i næringslivet og det offentlige kartlegges. Næringslivets sikkerhetsråd gjennomfører også *Hybridundersøkelsen*, som kartlegger sårbarhet og arbeidet med hybride trusler, og *Kriminalitets- og sikkerhetsundersøkelsen i Norge*, som kartlegger kriminalitets- og sikkerhetstilstanden i privat og offentlig sektor. Samlet tegner disse undersøkelsene et bilde av det digitale sikkerhetsnivået i Norge og samarbeidet mellom næringslivet og ansvarlige myndigheter. Dette har gitt et godt og relevant grunnlag for bedre å forstå truslene og sikkerhetsrisikoen på området.

2.2.1 Gjennomgang av regelverk

For å få oversikt over regelverkskravene for digitale sikkerhet, har vi gått gjennom det generelle regelverket og sektorregelverket på området, og vurdert regelverket etter graden av samordning. Lovene og forskriftene er valgt ut fordi de eksplisitt omhandler krav til digital sikkerhet, informasjonssikkerhet eller IKT-sikkerhet, eller fordi de har krav som indirekte regulerer det digitale sikkerhetsarbeidet, for eksempel om sikkerhetskontroll, risikostyring eller internkontroll. Vi har ikke vurdert lover og forskrifter som omhandler fysisk sikkerhet i denne gjennomgangen.

Av generelt regelverk for digital sikkerhet har vi identifisert og gått gjennom følgende lover og instrukser:

- *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen) (1. september 2017)
- *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv.* (arbeidsmiljøloven) (1. januar 2006)
- *Lov om behandlingsmåten i forvaltningssaker* (forvaltningsloven) (1. januar 1970)
- *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret* (sivilbeskyttelsesloven) (25. juni 2010)
- *Lov om nasjonal sikkerhet* (sikkerhetsloven) (1. januar 2019)
- *Lov om personopplysninger* (personopplysningsloven) (20. juli 2018)

Av relevant sektorspesifikt regelverk for digital sikkerhet har vi identifisert og gått gjennom følgende lover:

- *Lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m.* (jernbaneloven) (1. juli 1993)
- *Lov om arbeids- og velferdsforvaltningen* (arbeids- og velferdsforvaltningsloven) [NAV-loven] (1. juli 2006)
- *Lov om behandling av helseopplysninger ved ytelse av helsehjelp* (pasientjournalloven) (1. januar 2015)
- *Lov om behandling av opplysninger i politiet og påtalemyndigheten* (politiregisterloven) (1. juli 2014)
- *Lov om elektronisk kommunikasjon* (ekomloven) (25. juli 2003)
- *Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (*lov om elektroniske tillitstjenester) (15. juni 2018)
- *Lov om helseregistre og behandling av helseopplysninger* (helseregisterloven) (1. januar 2015)

- *Lov om helsemessig og sosial beredskap* (helseberedskapsloven) (1. juli 2001)
- *Lov om luftfart* (luftfartsloven) (1. april 1994)
- *Lov om matproduksjon og mattrygghet mv.* (matloven) (1. januar 2004)
- *Lov om medisinsk og helsefaglig forskning* (helseforskningsloven) (1. juli 2009)
- *Lov om petroleumsvirksomhet* (petroleumsloven) (1. juli 1997)
- *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energiloven) (29. juni 1990)
- *Lov om skipssikkerhet* (skipssikkerhetsloven) (1. juli 2007)
- *Lov om tilsynet med finansforetak mv.* (finanstilsynsloven) (7. desember 1956)

Listen ovenfor er kryssjekket mot lovverkene IKT-sikkerhetsutvalget identifiserte i 2018. Vi har imidlertid gjort flere selvstendige gjennomganger, både av tilsynsmyndighetenes egne oversikter over regelverk og i form av generelle søk etter lovverk som omhandler tematikken. Oversikten vår er også forelagt Nasjonal sikkerhetsmyndighet, som ikke hadde noen lovverk å tilføye listen.

Vi har gått gjennom og systematisert lovverket etter følgende tematikker:

- *Risiko/risikostyring* (styringssystem for sikkerhet). Dette innebærer organisatoriske tiltak og internkontroll, som krav til strategi for sikkerhet, organisering og ansvarsområder.
- *Risiko- og sårbarhetsanalyse / risikovurdering*. Dette innebærer krav om å utarbeide risiko- og sårbarhetsanalyser knyttet til uønskede hendelser, eller krav om å vurdere risikoen knyttet til uønskede hendelser eller scenarioer.
- *Sikkerhetstiltak.* Dette innebærer alle former for tiltak som skal øke den digitale sikkerheten, for eksempel tekniske tiltak, som krav til lagring og oppbevaring av digital informasjon. Sikkerhetstiltak kan også være personelle og prosessuelle tiltak, som gjennomføring av øvelser og utforming av beredskapsplaner. Tiltakene skal etter regelverket som oftest være i tråd med den identifiserte risikoen for virksomheten.
- *Hendelseshåndtering*. Dette innebærer krav til håndtering av uønskede hendelser, i dette tilfellet knyttet til digitale angrep eller bortfall av kritisk infrastruktur.

2.2.2 Gjennomgang av veiledningsmateriell

Vi har gått gjennom 36 veiledere fra offentlige myndigheter som er relevante for arbeidet med den digitale sikkerheten, og som knytter seg til det gjennomgåtte regelverket. Vi har også gått gjennom 16 sektorspesifikke veiledere. Da vi søkte etter relevant veiledningsmateriell, gikk vi gjennom materiellet til alle tilsynsmyndighetene som forvalter det identifiserte regelverket. Alle veilederne deres ble screenet ved hjelp av søkeordet «sikkerhet» for å fange opp «digital sikkerhet», «informasjonssikkerhet», «IKT-sikkerhet», «cybersikkerhet» o.l.

Ikke alle de gjennomgåtte dokumentene har tittelen «veileder». Noen tar form av en nettside, og flere av dem omtales som håndbøker eller metodehåndbøker. Disse har imidlertid samme type innhold som dokumentene med tittelen «veileder». Vi har derfor valgt å inkludere dem i gjennomgangen. Alle dokumentene vil i fortsettelsen bli omtalt som veiledere eller veiledningsmateriell.

2.2.3 Gjennomgang av kommunale rapporter og planer

For å få et inntrykk av hvordan kommunene vektlegger arbeidet med digital sikkerhet, har vi gått gjennom fire kommunale tilsynsrapporter, tre interne kommunerevisjoner og ni kommunale beredskapsplaner og risiko- og sårbarhetsanalyser. Rapportene og planene ble tilfeldig valgt ut og dekker kommuner av ulik størrelse og med ulik geografisk beliggenhet. Tilsynsrapportene er utformet av ulike tilsynsmyndigheter. De øvrige rapportene og planene er utarbeidet internt i kommunene. Dokumentene er ikke ment å gi et representativt bilde av situasjonen i kommunene. De er snarere

ment som en indikasjon som sammen med et intervju med representanter fra kommunesektoren skal gi et innblikk i hvor mye og hvordan kommunene arbeider med digital sikkerhet.

2.3 Skriftlige spørsmål

For å kartlegge om Justis- og beredskapsdepartementet har et godt nok grunnlag til å få en helhetlig oversikt over det digitale sikkerhetsnivået, har vi sendt skriftlige spørsmål til departementene. Spørsmålene har blant annet handlet om hvilke kilder til informasjon departementene bruker i risiko- og sårbarhetsanalysene sine, hvordan kildene sammenstilles og deles med andre aktører, og om sektorens funksjonsevne. Vi sendte ut og mottok svar fra totalt 13 departementer. Syv av departementene har i tillegg svart på spørsmål om risiko- og sårbarhetsanalysen de har utarbeidet for den kritiske samfunnsfunksjonen de selv er ansvarlige for. Målet med spørsmålene har vært å kartlegge hvordan departementene arbeider med risiko- og sårbarhetsanalysene, hvilke kilder som benyttes i arbeidet, og hvordan arbeidet er organisert og forankret i departementene. Vi har ikke vurdert kvaliteten på risiko- og sårbarhetsanalysene.

Statsministerens kontor og Forsvarsdepartementet ble ikke forespurt. Statsministerens kontor har ikke ansvar for noen av samfunnets kritiske funksjoner slik de er definert av Direktoratet for samfunnssikkerhet og beredskap, og Forsvarsdepartementet faller ikke innunder Justis- og beredskapsdepartementets samordningsansvar for samfunnssikkerhet.

2.4 Dybdeundersøkelser

For å undersøke hvordan sentrale myndighetsaktører arbeider og yter bistand når det oppstår digitale hendelser, har vi sett nærmere på fem virksomheter som i perioden 2018−2022 har blitt utsatt for en alvorlig digital hendelse som har krevd involvering fra en eller flere myndighetsaktører. Med *alvorlig digital hendelse* menes «reelle og potensielle uønskede hendelser i det digitale rom som er rettet mot samfunnskritisk infrastruktur eller samfunnets kritiske funksjoner».[32]

Dybdeundersøkelsene omfatter både offentlige og private virksomheter. Virksomhetene er av ulik størrelse og tilhører ulike sektorer, men har til felles at hele eller deler av virksomheten understøtter en grunnleggende nasjonal funksjon. Av sikkerhetsmessige årsaker og av hensyn til virksomhetssensitiv informasjon har virksomhetene som har deltatt i undersøkelsen, blitt anonymisert.

I dybdeundersøkelsene har vi brukt intervju som metode for informasjonsinnhenting, og vi har intervjuet den enkelte virksomhets sikkerhetsleder og/eller informasjonssikkerhetsleder.

Dybdeundersøkelser får fram kompleksitet og sammenhenger som ikke fanges opp like lett i bredere undersøkelser. Disse undersøkelsene har slik sett gitt oss muligheten til å gå i dybden på konkrete tilfeller av digitale uønskede hendelser. Dybdeundersøkelsene har også gitt oss et brukerperspektiv på hvordan samordningen mellom myndighetsaktørene fungerer, og hvordan myndighetsinnsatsen framstår fra de rammede virksomhetenes perspektiv. Videre har dybdeundersøkelsene belyst virksomhetens interaksjon med sentrale myndigheteraktører i forebyggende aktiviteter, for eksempel informasjonsdeling, veiledning og tilsyn.

[32] Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos (2022) *Retningslinjer for cybersamarbeid.*

3 Revisjonskriterier

Revisjonskriteriene er utledet fra Stortingets behandling av relevante stortingsproposisjoner og stortingsmeldinger. Lover, *bevilgningsreglement vedtatt av Stortinget* (bevilgningsreglementet) og *reglement for økonomistyring i staten* (økonomireglementet) er også kilder til revisjonskriterier.

3.1 Krav til arbeid med digital sikkerhet

Ifølge Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020−2021), er digitale systemer sentrale for alle samfunnsfunksjoner. Det vises til at feil i digitale systemer vil kunne få store konsekvenser på alle nivåer i samfunnet, og at digital sikkerhet derfor er helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser. Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar*, jf. Innst. 187 S (2017−2018), framheves fire viktig områder av særlig betydning for den nasjonale IKT-sikkerheten:

1. Forebyggende IKT-sikkerhet – virksomheters egenevne
2. Avdekking og håndtering av digitale angrep
3. IKT-sikkerhetskompetanse
4. Kritisk IKT-infrastruktur

I Innst. 275 S (2020−2021) til Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden* mener justiskomiteen at det er viktig at myndighetene bidrar til å styrke insentivene til å investere i digital sikkerhet i virksomheter, siden underinvesteringer i digital sikkerhet kan få konsekvenser for større deler av økonomien. Det kan iverksettes gjennom juridiske, pedagogiske, organisatoriske og økonomiske virkemidler. Komiteen mener også det er viktig at myndighetene gjennom samarbeid mellom private og offentlige virksomheter utnytter samfunnets ressurser best mulig. Komiteen framhever at Nasjonalt cybersikkerhetssenter, som ble etablert i 2018, skal være et sentralt verktøy for økt offentlig-privat samarbeid.

Sikkerhetsloven stiller krav til departementenes arbeid med forebyggende sikkerhetsarbeid. Av § 2-1 følger det at departementene skal identifisere og holde oversikt over grunnleggende nasjonale funksjoner og over virksomhetene som har vesentlig betydning for de grunnleggende nasjonale funksjonene, samt melde inn en oversikt over disse til Nasjonal sikkerhetsmyndighet. Departementene skal i tillegg fatte vedtak om hvilke virksomheter loven skal gjelde for innenfor deres virkeområde, jf. § 1-3.

Ifølge sikkerhetsloven § 2-4 skal Nasjonal sikkerhetsmyndighet drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur. Nasjonal sikkerhetsmyndighet har også det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven, blant annet gjennom å se til at det føres tilsyn, gi informasjon, råd og veiledning, innhente relevant informasjon, holde oversikt over grunnleggende nasjonale funksjoner og virksomhetene som er underlagt sikkerhetsloven, jf. § 2-2.

I henhold til sikkerhetsloven skal den enkelte virksomhet kartlegge hvilke andre virksomheter den er avhengig av for å fungere som den skal, § 4-2. *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (virksomhetssikkerhetsforskriften) er en forskrift til sikkerhetsloven og gjelder dermed for virksomheter som omfattes av sikkerhetsloven. Av forskriften går det blant annet fram at en virksomhet som vurderer risiko, skal ta hensyn til hvilken betydning virksomhetens skjermingsverdige verdier har for grunnleggende nasjonale funksjoner, § 12. Dersom virksomheten er avhengig av andre virksomheter for å fungere slik den skal, skal en oversikt sendes til Nasjonal sikkerhetsmyndighet, jf. virksomhetssikkerhetsforskriften § 13 siste ledd.

Gjennom Meld. St. 29 (2011−2012) *Samfunnssikkerhet*, jf. Innst. 426 S (2012−2013), ble det vedtatt at det skulle arbeides for å etablere responsmiljøer i de ulike sektorene. Som en minimumsløsning skal det i hver sektor etableres et kontaktpunkt for alvorlige IKT-hendelser og prosedyrer for varsling, både internt og opp mot Nasjonalt cybersikkerhetssenter (responsfunksjonen i Nasjonalt cybersikkerhetssenter omfatter tidligere NorCERT). Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere IKT-kriser, og hvordan de eventuelt skal skalere opp responsmiljøene sine.

3.2 Mål og krav til myndighetenes samordning av arbeidet med digital sikkerhet

Hvert departement har et overordnet ansvar for å ivareta den digitale sikkerheten i egen sektor. Justis- og beredskapsdepartementet har et samordnings- og pådriveransvar for den digitale sikkerheten i sivil sektor.[33] Departementet skal utforme regjeringens politikk for IKT-sikkerhet, herunder etablere nasjonale krav og anbefalinger på IKT-sikkerhetsområdet for både offentlige og private virksomheter. Berørte fagdepartementer, myndigheter og næringslivet skal involveres i dette arbeidet. Krav skal være hjemlet i lov og forskrift i den grad det er nødvendig.[34]

Justis- og beredskapsdepartementets samordningsrolle er fastsatt ved kgl.res. av 10. mars 2017 nr. 312.[35] Justis- og beredskapsdepartementet har i sivil sektor blant annet fullmakt til å fastsette krav til departementenes arbeid med samfunnssikkerhet, etablere nasjonale krav til IKT-sikkerhet og gi nærmere bestemmelser om egen samordningsrolle og tilsynsfunksjon.[36]

Justis- og beredskapsdepartementet har videre et overordnet ansvar for det forebyggende sikkerhetsarbeidet i sivil sektor, jf. kgl.res. av 20. desember 2018.[37] Pådriver- og samordningsrollen til Justis- og beredskapsdepartementet innebærer blant annet å initiere og koordinere prosesser på tvers av departementer, veilede departementene i deres arbeid på området, sørge for at problemstillinger på tvers av sektorer blir håndtert, og legge fram uenighetssaker for regjeringen eller ved behov for Kongen i statsråd.[38]

I Innst. 326 S (2016–2017) til Meld St. 10 (2016−2017) *Risiko i et trygt samfunn* framhever justiskomiteen det samordningsansvaret som Justis- og beredskapsdepartementet har når det gjelder forebyggende IKT-sikkerhet i sivil sektor. Evnen til å oppdage digitale angrep avhenger av et samspill mellom myndigheter, sektormiljøer og offentlige og private virksomheter samt mellom militære og sivile aktører. For å være godt rustet mot større digitale angrep må roller og ansvar mellom aktørene være avklart, virksomheter må ha tilstrekkelig kompetanse og kapasitet, og de må evne å samvirke. Komiteen understreker hvor viktig det er at IKT som fag prioriteres i større grad, slik at kompetanse og arbeidskraft med kompetanse på IKT-sikkerhetsområdet blir styrket.

I Meld. St. 5 (2020−2021) S*amfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020−2021), går det fram at Justis- og beredskapsdepartementets samordnings- og pådriverrolle innenfor digital sikkerhet skal styrkes. Videre skal samordningen av digital sikkerhet på etatsnivå bli tydeligere. For brukerne er det viktig at de etatene som har ansvar for oppfølgingen av digital sikkerhet, opptrer koordinert, både når det gjelder rådgivning og veiledning og ved tilsyn. Justis- og beredskapsdepartementet skal bidra at rådgivnings- og veiledningsaktiviteter innenfor digital sikkerhet blir bedre koordinert. Målet er at all rådgivning og veiledning som myndighetene tilbyr brukerne, skal

[33] Meld. St. 5 (2020−2021) S*amfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020−2021).
[34] Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar*, jf. Innst. 187 S (2017−2018).
[35] Kgl.res. av 10. mars 2017 nr. 312 *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet* punkt 2.
[36] Kgl. res. av 1 september 2017.
[37] Kgl. res. av 20. desember 2018 *Ikraftsetting av lov 1. juni 2018 nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.*
[38] Prop. 1 S (2020–2021) Justis- og beredskapsdepartementet.

være harmonisert og ensrettet. Nasjonal sikkerhetsmyndighet skal her, i samarbeid med berørte etater, bidra til at utviklingen av rådgivnings- og veiledningsmateriell blir mer koordinert på tvers av sektorene. Justis- og beredskapsdepartementet skal legge til rette for helhetlig koordinering innenfor digital sikkerhet i tildelingsbrevene til Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap, Digitaliseringsdirektoratet og Nasjonal kommunikasjonsmyndighet. Norsk senter for informasjonssikring mottar årlig tilsagnsbrev med føringer fra Justis- og beredskapsdepartementet, og disse føringene vil bli vurdert sammen med føringer i de forannevnte etatenes tildelingsbrev. Samordningsrollen til Justis- og beredskapsdepartementet endrer ikke ansvaret som de enkelte statsrådene har for å styre egne etater. Koordinerte tildelingsbrev forutsetter et godt samarbeid mellom Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet og Forsvarsdepartementet.

Rammeverk for håndtering av IKT-sikkerhetshendelser fastsettes av Justis- og beredskapsdepartementet for sivil sektor og av Forsvarsdepartementet for forsvarssektoren. Rammeverket angir sentrale aktører og deres oppgaver og ansvar ved håndtering av hendelser samt en prosessmodell for hvordan hendelser skal håndteres.[39] Rammeverket gjelder for offentlige og private virksomheter som har betydning for kritisk infrastruktur eller kritiske samfunnsfunksjoner, sektorvise responsmiljøer, relevante myndigheter (blant annet Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten) og departementene. Rammeverket er dynamisk og skal revideres hvert annet år, eller hyppigere ved behov. Nasjonal sikkerhetsmyndighet er ansvarlig for revisjonsprosessen og vurderer behovet for endringer. Det reviderte rammeverket legges fram departementene for godkjenning. Nasjonal sikkerhetsmyndighet skal sikre at sentrale aktører involveres i forbindelse med revisjonen. Innspill om behov for endringer i rammeverket skal sendes til Nasjonal sikkerhetsmyndighet fortløpende. Øvelser er et viktig virkemiddel for å bevisstgjøre bredere målgrupper om digital sikkerhet, og det nåværende rammeverket skal videreutvikles basert på erfaringene fra Øvelse Digital 2020.[40]

3.3 Krav til myndighetenes tilsyn og kontroll med digital sikkerhet

3.3.1 Krav til tilsyn med departementenes arbeid med samfunnssikkerhet

I henhold til samfunnssikkerhetsinstruksen skal Justis- og beredskapsdepartementet føre tilsyn med de andre departementenes etterlevelse av instruksen.[41] Direktoratet for samfunnssikkerhet og beredskap kan utføre tilsynet på vegne av Justis- og beredskapsdepartementet. Tilsynet skal være basert på vesentlighet og risiko. Justis- og beredskapsdepartementets velger hvilke departementer det skal føres tilsyn med, metode og tema på bakgrunn av en vurdering av hvilken betydning det aktuelle området har for samfunnssikkerheten, og av sannsynligheten for og konsekvensene av avvik. Som det går fram av kgl.res. av 10. mars 2017 nr. 312 skal Helse- og omsorgsdepartementet ha ansvar for å føre tilsyn med Justis- og beredskapsdepartementet.

Tilsynet med et departement kan omfatte målrettede og avgrensede undersøkelser i departementet og underlagte virksomheter for å verifisere at departementet etterlever instruksens krav, og at kritiske samfunnsfunksjoner er tilstrekkelig ivaretatt. Alle tilsyn munner ut i en rapport. Dersom tilsynsmyndighetene finner at departementet ikke oppfyller kravene i samfunnssikkerhetsinstruksens kapittel IV («Krav til departementer med hovedansvar for kritiske samfunnsfunksjoner»), kapittel V («Justis- og beredskapsdepartementets samordningsrolle for forebygging og beredskap») og kapittel VI («Tilsyn med departementenes samfunnssikkerhetsarbeid»), skal dette omtales som «brudd på

[39] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser.*
[40] Meld. St. 5 (2020−2021) S*amfunnssikkerhet i en usikker verden*, jf. Innst. 275 S (2020−2021).
[41] *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen), jf. punkt 7.

krav» i rapporten, og det skal angis forbedringstiltak. Også når det ikke foreligger brudd på krav, kan tilsynsmyndighetene peke på forbedringsområder innenfor departementets samfunnssikkerhetsarbeid.

Tilsynsmyndighetenes rapport legger fram de ulike funnene, oppgir frister for uttalelser og beskriver hvordan tilsynet skal følges opp videre. Departementet det er ført tilsyn med, skal utarbeide en oppfølgingsplan som sendes Justis- og beredskapsdepartementet. Justis- og beredskapsdepartementet skal be det departementet det er ført tilsyn med om rapportering på denne planen.

Justis- og beredskapsdepartementet skal rapportere til regjeringen dersom tilsynet avdekker at departementet det er ført tilsyn med, har brutt krav i instruksen, eller ved manglende oppfølging.

3.3.2 Krav til tilsyn med virksomheter som er omfattet av sikkerhetsloven

Nasjonal sikkerhetsmyndighet skal føre tilsyn med virksomheter som er omfattet av sikkerhetsloven, jf. sikkerhetsloven § 3-1. Videre kan Justis- og beredskapsdepartementet bestemme at tilsynsmyndigheter med sektoransvar kan føre tilsyn med virksomheter i egen sektor som er omfattet av sikkerhetsloven. Dette gjelder foreløpig for Nasjonal kommunikasjonsmyndighet og Norges vassdrags- og energidirektorat. Nasjonal sikkerhetsmyndighet skal likevel gjennomføre tilsyn når det følger av internasjonale forpliktelser, eller når det er tvingende nødvendig.

Nasjonal sikkerhetsmyndighet skal i tillegg føre tilsyn med departementene og andre tilsynsmyndigheter som fører tilsyn etter sikkerhetsloven.[42] Kongen kan gi forskrift om tildelingen av tilsynsansvaret og om fordelingen av ansvaret mellom Nasjonal sikkerhetsmyndighet og aktuelle myndigheter med sektoransvar.

Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar etter sikkerhetsloven skal inngå en avtale om samarbeid.[43] Gjennomføringen av tilsyn skal så langt det er mulig, samordnes med andre tilsynsmyndigheter. Sikkerhetsmyndigheten skal utarbeide og utvikle grunnleggende kriterier for tilsyn etter sikkerhetsloven og legge til rette for felles opplæring av tilsynspersonell. Nasjonal sikkerhetsmyndighet kan om nødvendig medvirke i forberedelsene og gjennomføringen av tilsyn som utføres av myndigheter med tilsynsansvar. Myndigheter med tilsynsansvar kan be sikkerhetsmyndigheten om slik bistand. Myndigheter med tilsynsansvar skal orientere sikkerhetsmyndigheten om planlagte tilsyn, redegjøre for gjennomførte tilsyn og informere om eventuelle avvik og pålegg. Kongen kan gi forskrift om samarbeid og informasjonsutveksling mellom sikkerhetsmyndigheten og myndigheter med tilsynsansvar. Dersom myndigheter med tilsynsansvar ikke fører tilsyn i samsvar med krav som er fastsatt i eller følger av loven, kan Nasjonal sikkerhetsmyndighet gi pålegg om å utføre slikt tilsyn.[44]

Tilsynsmyndigheten kan gi virksomheter pålegg om å gjennomføre tiltak som er nødvendige for å ivareta lovens formål.[45] Pålegg om konkrete tiltak kan bare gis dersom kostnadene som påføres virksomheten, framstår som rimelige sett i forhold til det som kan oppnås med tiltaket. Pålegg kan påklages. Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang.

Rådgivende aktiviteter for kontroll av sikkerhet

I tillegg til den overnevnte tilsynsvirksomheten har Nasjonal sikkerhetsmyndighet andre kontrolltiltak. Disse defineres ikke som tilsynsvirksomhet, men som rådgivningsaktivitet knyttet til sikring av systemer og lokaler for høygradert kommunikasjon

[42] Sikkerhetsloven § 3-1.
[43] Sikkerhetsloven § 3-2.
[44] Sikkerhetsloven § 3-6.
[45] Sikkerhetsloven § 3-6.

Tekniske sikkerhetsundersøkelser

Nasjonal sikkerhetsmyndighet kan gjennomføre tekniske sikkerhetsundersøkelser, det vil si de kan undersøke lokaler, bygninger og andre objekter som en virksomhet alene eller sammen med andre råder over, for å fastslå om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting, innsyn eller avlesning av signaler.[46]

Inntrengingstesting av skjermingsverdige informasjonssystemer

Virksomheter kan be sikkerhetsmyndigheten om å forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer. Formålet skal være å kontrollere om sikkerhetstiltakene er tilstrekkelige. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

3.4 Krav til departementenes styring og oppfølging av underliggende virksomheter

Samfunnssikkerhetsinstruksen stiller krav til departementenes arbeid med samfunnssikkerhet. Det følger av instruksen at dette arbeidet skal være basert på systematisk risikostyring. Hvert enkelt departement skal kunne dokumentere at det avklarer og beskriver sentrale roller og ansvarsområder innenfor samfunnssikkerhet i egen sektor, gjør systematiske risiko- og sårbarhetsanalyser av hendelser som kan true sektorens funksjonsevne, iverksetter nødvendige kompenserende tiltak og utarbeider mål for samfunnssikkerhetsarbeidet i sektoren. Det enkelte departement skal ivareta ansvaret for krisehåndteringen i egen sektor. Dette innebærer blant annet å ha et planverk for håndteringen av uønskede hendelser og sørge for at det øves målrettet, både i egen sektor og tverrdepartementalt. Som ansvarlig for kritisk infrastruktur skal departementet også sørge for at det utarbeides risiko- og sårbarhetsanalyser for sektoren, og ha oversikt over tilstanden knyttet til sårbarheter.[47]

Stortinget har i sin behandling av bevilgningsreglementet, jf. Innst. S nr. 187 (2004–2005), fastsatt mål- og resultatstyring i staten som gjeldende prinsipp. De grunnleggende styringsprinsippene er konkretisert i økonomireglementet §§ 4 og 7. Departementene og underliggende virksomheter skal ha tilstrekkelig styringsinformasjon og et forsvarlig beslutningsgrunnlag. Departementene skal i tillegg fastsette overordnede mål og styringsparametere for underliggende virksomheter.

Hvert departement har et overordnet ansvar for at virksomhetene gjennomfører aktiviteter i tråd med Stortingets vedtak og forutsetninger og med departementets fastsatte mål og prioriteringer. Departementet har videre ansvar for at virksomhetene rapporterer pålitelig informasjon, samt at styringsdialogen mellom departementet og virksomheten fungerer på en hensiktsmessig måte, jf. *bestemmelser om økonomistyring i staten* (økonomibestemmelsene) punkt 1.2. Departementets kontroll av underliggende virksomheter skal inngå i den ordinære styringen og oppfølgingen av virksomheten. Departementet skal videre sikre at virksomhetene har tilfredsstillende internkontroll slik at fastsatte mål og resultatkrav følges opp, ressursbruken er effektiv og virksomhetene drives i samsvar med gjeldende lover og regler, jf. økonomireglementet § 15 og økonomibestemmelsene punkt 1.6.2.

Departementet og virksomhetene skal sørge for at det blir gjennomført evalueringer for å skaffe kunnskap om måloppnåelse og resultater på området.[48] Frekvensen og omfanget av evalueringer skal bestemmes ut fra virksomhetens egenart, risiko og vesentlighet. Behovet må vurderes opp mot kvaliteten på og omfanget av øvrig rapportering.

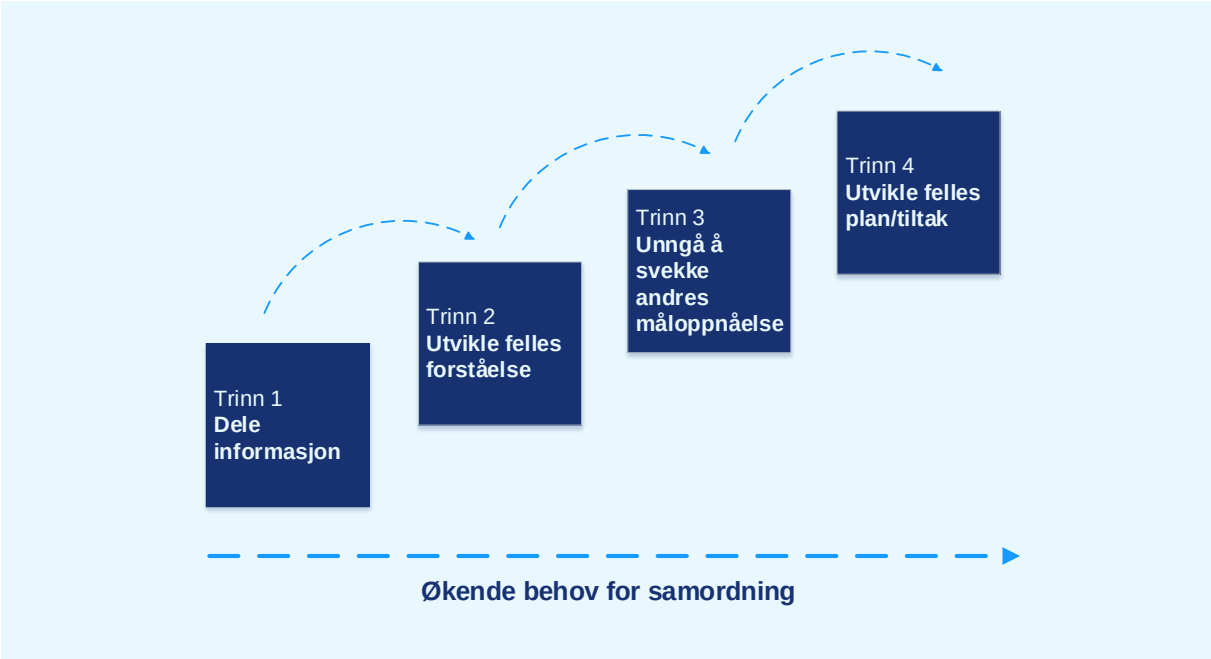
[46] Sikkerhetsloven § 5-5.
[47] Samfunnssikkerhetsinstruksen, del 4 og 5; Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*.
[48] Økonomireglementet § 16; økonomibestemmelsene punkt 2.7.

4 Samordning av roller, ansvar og krav til digital sikkerhet

Det er viktig å samordne roller, ansvar og krav for å unngå duplisering av kompetanse og at andres måloppnåelse svekkes, og for å oppnå mest mulig effektiv bruk av ressurser. I dette kapitlet svarer vi på den første problemstillingen i undersøkelsen: *Bidrar myndighetenes samordning av roller, ansvar og krav til å ivareta den digitale sikkerheten?* Først redegjør vi kort for Direktoratet for forvaltning og økonomistyrings samordningsstige, som vil bli benyttet som analytisk verktøy. Deretter kartlegger vi sentrale aktører med ansvar for tilsyn, veiledning og bistand knyttet til hendelseshåndtering, herunder arenaer som skal bidra til samordning av aktørene. Videre presenterer vi sentrale regelverk for det digitale sikkerhetsarbeidet, før vi går gjennom og analyserer graden av samordning av regelverkene og tilhørende veiledningsmateriell. Til slutt gjør vi en gjennomgang og analyse av tilsynene med det digitale sikkerhetsarbeidet og samordningen av dem.

Direktoratet for økonomistyring beskriver ulike grader av og ambisjonsnivåer for samordning ved hjelp av en stige, slik illustrasjonen i Figur 1 viser.[49]

Figur 1 Ulike grader av samordning (samordningsstigen)



Kilde: Direktoratet for forvaltning og økonomistyring (2021) *Samordning.*

Samordningsstigen er en modell som beskriver ulike grader av og ambisjonsnivåer for samordning. Graden av gjensidig avhengighet og samarbeid øker med trinnene i stigen. For å lykkes med samordning er det viktig å være bevisst på hvor i stigen man er, og hvilket trinn som skal være målet for samordningen.

Første trinn, der ambisjonsnivået er lavest, er begrenset til utveksling av informasjon, erfaringer og kunnskap. På bakgrunn av informasjonen kan aktørene samarbeide om å utvikle problem- og løsningsforslag (trinn to). Trinn tre går ut på at aktørene, på bakgrunn av dialog, endrer planer, retningslinjer eller policyer for å unngå å svekke andres måloppnåelse. Siste trinn i stigen, der ambisjonsnivået er høyest, handler om å utvikle felles planer/tiltak på tvers av sektorene for å oppnå synergieffekter.[50]

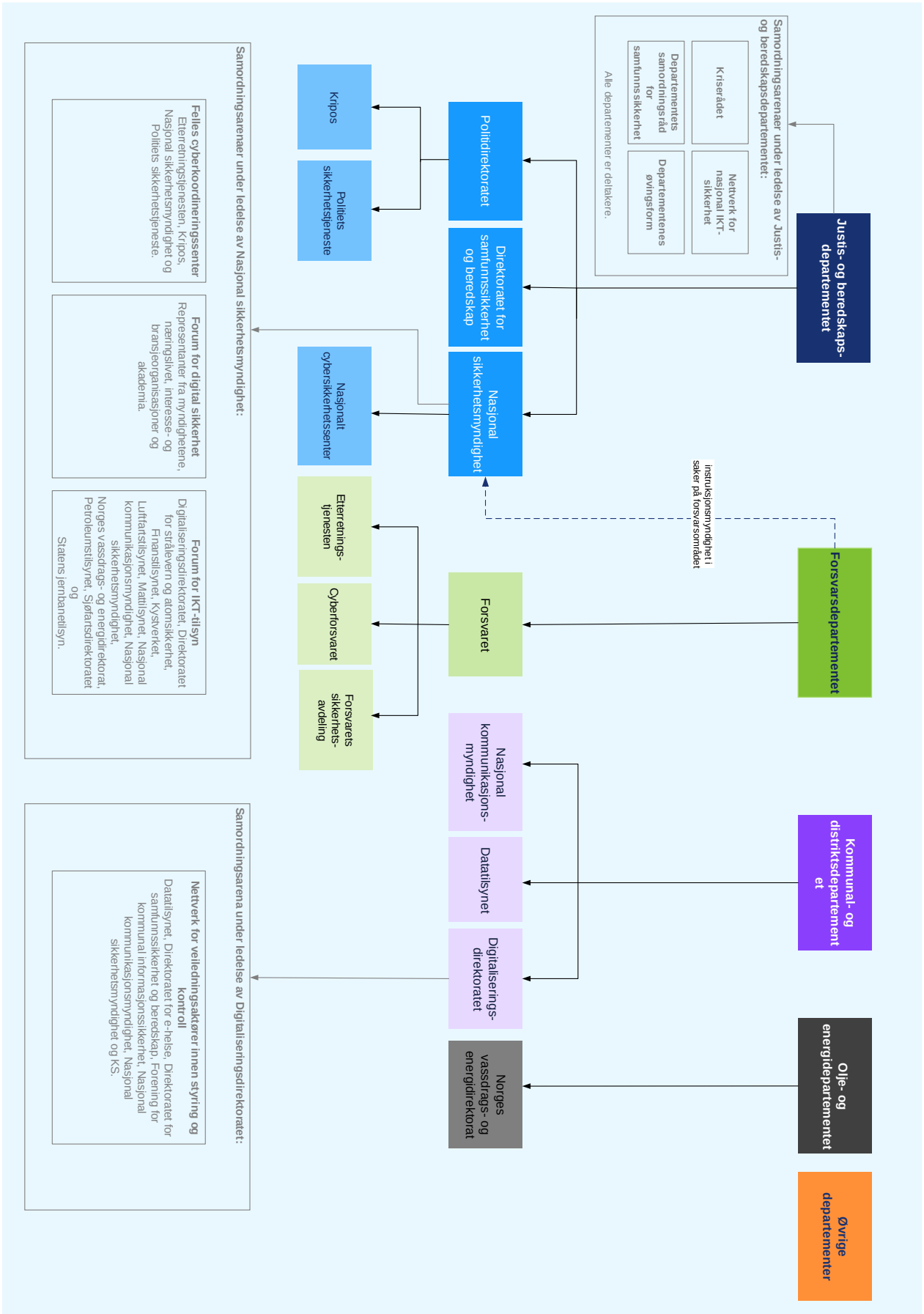
[49] Direktoratet for forvaltning og økonomistyring (2021) *Samordning* [Hentedato 10. juni 2021].
[50] Direktoratet for forvaltning og økonomistyring (2021) *Samordning* [Hentedato 10. juni 2021].

Samordningsstigen kan brukes som en modell for å indikere graden av og behovet for samordning på noen av undersøkelsens ulike områder, men ikke alle. Når det for eksempel gjelder oppfølging av tiltak og strategier hvor én part er ansvarlig, eller vurdering av regelverkskrav, vil stigen være mindre egnet som analyseverktøy. Stigen kan derfor kun brukes til å få indikasjoner på graden av samordning. Stigen har dessuten noen svakheter i form av at trinnene i stigen ikke nødvendigvis bygger på hverandre. Aktørene på et område kan for eksempel utarbeide en felles plan, uten at dette bygger på en felles problemforståelse, og uten at de har en forståelse av hverandres ansvarsområder og roller. Samordningen kan etter stigen derfor vurderes til å være på et høyere nivå enn den i realiteten er. Som følge av det ovennevnte har vi begrenset oss til å bruke stigen der det er snakk om samordning av aktører og/eller prosesser mellom flere parter.

4.1 De sentrale aktørene i arbeidet med digital sikkerhet

Arbeidet med digital sikkerhet i sivil sektor inkluderer en rekke aktører. I det følgende gir vi en nærmere beskrivelse av de ulike myndighetsaktørenes ansvarsområder knyttet til arbeidet med digital sikkerhet. Se Figur 2 for en oversikt over sentrale myndighetsaktører og samordningsarenaer.

Figur 2 Oversikt over sentrale myndighetsaktører på det digitale sikkerhetsområdet



4.1.1 Justis- og beredskapsdepartementet

Justis- og beredskapsdepartementet har en samordningsrolle for det nasjonale digitale sikkerhetsarbeidet i sivil sektor, fastsatt ved kgl.res. av 10. mars 2017 nr. 312.[51] Kgl. res. av 22. mars 2013 beskriver ansvarsoverføringen. Justis- og beredskapsdepartementet har videre et overordnet ansvar for det forebyggende sikkerhetsarbeidet i sivil sektor, jf. kgl.res. av 20. desember 2018.[52]

Justis- og beredskapsdepartementet har blant annet fullmakt til å fastsette krav til departementenes arbeid med samfunnssikkerhet, etablere nasjonale krav til digital sikkerhet og gi nærmere bestemmelser om egen samordningsrolle og tilsynsfunksjon.[53] Pådriver- og samordningsrollen til Justis- og beredskapsdepartementet innebærer blant annet å initiere og koordinere prosesser på tvers av departementer, veilede departementene i deres arbeid på området, sørge for at problemstillinger på tvers av sektorer blir håndtert, og legge fram uenighetssaker for regjeringen eller ved behov for Kongen i statsråd.[54] Samordningsansvaret innebærer også å sørge for at myndighetene har en helhetlig tilnærming til digital sikkerhet, og at kompetansebyggingen møter framtidens behov.[55]

Saker som gjelder den nasjonale sikkerheten, skal forelegges Justis- og beredskapsdepartementet, og departementene skal jevnlig rapportere til Justis- og beredskapsdepartementet om statusen i arbeidet med digital sikkerhet og om kartlagte kritiske samfunnsfunksjoner, avhengigheter, objekter og informasjonsstrukturer.[56]

Justis- og beredskapsdepartementet har i tillegg ansvar for å forvalte sikkerhetsloven og *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017). Departementet er også pådriver i arbeidet med sektorvise responsmiljøer. Nasjonal sikkerhetsmyndighet er ansvarlige for etableringen og oppfølgingen av responsmiljøene.

Ifølge Justis- og beredskapsdepartementet kan samordningsoppgaven være krevende, noe som særlig skyldes sektorprinsippet og at departementene varierer med hensyn til hvor høyt de prioriterer sikkerhetsarbeidet. Justis- og beredskapsdepartementet bemerker selv at bredden i deres samordningsansvar er omfattende, og at en sentral del av ansvaret er å være pådriver ovenfor de andre aktørene som har ansvar for digital sikkerhet.[57] Departementet viser også til at det er en varierende vilje til samarbeid departementene imellom.[58]

4.1.2 Nasjonal sikkerhetsmyndighet

I henhold til sikkerhetsloven er Nasjonal sikkerhetsmyndighet fagmyndighet for forebyggende nasjonal sikkerhet. Nasjonal sikkerhetsmyndighet er også det nasjonale fagmiljøet innenfor digital sikkerhet. Nasjonal sikkerhetsmyndighet skal, både i sivil og militær sektor, gi råd og gjennomføre tilsyn og andre kontrollaktiviteter knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. Videre skal Nasjonal sikkerhetsmyndighet vedlikeholde et helhetlig risikobilde innenfor forebyggende sikkerhet og særskilt innenfor digital sikkerhet.[59]

Administrativt er Nasjonal sikkerhetsmyndighet underlagt Justis- og beredskapsdepartementet. Forsvarsdepartementet har imidlertid instruksjonsmyndighet overfor Nasjonal sikkerhetsmyndighet i saker innenfor Forsvarsdepartementets ansvarsområde. Den faglige etatsstyringen er dermed delt mellom Forsvarsdepartementet og Justis- og beredskapsdepartementet. Nasjonal

[51] Kgl.res. av 10. mars 2017 nr. 312 *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet* punkt 2.
[52] Kgl. res. av 20. desember 2018 *Ikraftsetting av lov 1. juni 2018 nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.*
[53] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) (1. september 2017).
[54] Prop. 1 S (2020–2021) Justis- og beredskapsdepartementet.
[55] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*.
[56] Prop. 1 S (2020–2021) Justis- og beredskapsdepartementet.
[57] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[58] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[59] Forsvarsdepartementet og Justis- og beredskapsdepartementet (2019) *Hovedinstruks for Nasjonal sikkerhetsmyndighet*, 3. mars 2019.

sikkerhetsmyndighet skal bistå de to departementene med å utøve ansvaret de blant annet har for den digitale sikkerheten nasjonalt.[60]

Nasjonal sikkerhetsmyndighet har også et nasjonalt ansvar for å avdekke, varsle om og koordinere håndteringen av alvorlige digitale angrep rettet mot samfunnskritisk infrastruktur og andre viktige samfunnsfunksjoner. Høsten 2019 ble Nasjonalt cybersikkerhetssenter etablert som en del av Nasjonal sikkerhetsmyndighet for å ivareta deler av dette ansvaret. På vegne av Nasjonal sikkerhetsmyndighet drifter og organiserer senteret et nasjonalt sensornettverk, Varslingssystemet for digital infrastruktur (VDI).[61] I tillegg er Nasjonal sikkerhetsmyndighet leder for Felles cyberkoordineringssenter. Felles cyberkoordineringssenter er et permanent, samlokalisert fagmiljø med representanter fra Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos som blant annet skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep.[62]

4.1.3 Direktoratet for samfunnssikkerhet og beredskap

Direktoratet for samfunnssikkerhet og beredskap skal ha oversikt over risiko og sårbarhet i samfunnet og være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser. De skal også sørge for god beredskap og effektiv ulykkes- og krisehåndtering. Direktoratet for samfunnssikkerhet og beredskap har gjort risikoanalyser av alvorlige hendelser som kan ramme det norske samfunnet siden 2011. Direktoratet har også ansvar for nød- og beredskapskommunikasjon og statens eierskap til Nødnett.[63]

Direktoratet for samfunnssikkerhet og beredskap understøtter Justis- og beredskapsdepartementets samordningsrolle for samfunnssikkerhet på direktoratsnivå (jf. kgl. res 24. juni 2005) og er fag- og tilsynsorgan innenfor sivil samfunnssikkerhet og beredskap på vegne av Justis- og beredskapsdepartementet. Direktoratet for samfunnssikkerhet og beredskap skal veilede fylkeskommunene og kommunene om risiko- og sårbarhetsanalyser i arealplanleggingen og veilede statsforvaltere i deres samfunnssikkerhetsarbeid.

Direktoratet for samfunnssikkerhet og beredskap skal sikre systematisk oppfølging, implementering av læringspunkter og kompetanseheving etter øvelser og større hendelser.

4.1.4 Politiets sikkerhetstjeneste

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. PST er underlagt Justis- og beredskapsdepartementet og sidestilt med Politidirektoratet. PST har ansvar for å ivareta rikets sikkerhet og bekjempe terrorisme, sabotasje, spredning av masseødeleggelsesvåpen og industrispionasje og for å drive kontraetterretning. Deres primære oppgave er å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. Dette gjøre de blant annet gjennom analyser, trusselvurderinger, etterforskning og rådgivning. PST samarbeider tett med en rekke andre aktører, og er representert i Felles cyberkoordineringssenter.[64]

4.1.5 Kripos og Nasjonalt cyberkriminalitetssenter

Kripos er den nasjonale politienheten for bekjempelse av organisert kriminalitet og annen alvorlig kriminalitet, herunder digital kriminalitet.

I 2019 etablerte Kripos Nasjonalt cyberkrimsenter som en egen avdeling. Avdelingen skal fungere som et ekspertorgan og er ansvarlig for forebygging, etterretning, etterforskning og

[60] Justis- og beredskapsdepartementet og Forsvarsdepartementet (2019) *Hovedinstruks for Nasjonal sikkerhetsmyndighet,* 3. mars 2019.
[61] Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT* [Hentedato 4. februar 2022].
[62] Departementene (2019) *Nasjonal strategi for digital sikkerhet.*
[63] Justis- og beredskapsdepartementet (2021) *Tildelingsbrev til Direktoratet for samfunnssikkerhet og beredskap.*
[64] Politiets sikkerhetstjeneste (2017) *Hva gjør vi?* [Hentedato 11. november 2021].

hendelseshåndtering i det digitale rom, med særlig fokus på datakriminalitet og internettrelaterte overgrep. Avdelingen er også ansvarlig for å utvikle metoder innenfor teknisk og taktisk forebygging og operativ polititjeneste på internett. Nasjonalt cyberkrimsenter drifter det nasjonale kriminaltekniske laboratoriet for elektroniske spor. Avdelingen gir bistand til politidistrikter og særorganer og representerer Kripos i Felles cyberkoordineringssenter.[65]

4.1.6 Kommunal- og distriktsdepartementet

Kommunal- og distriktsdepartementet har ansvaret for den digitale sikkerheten knyttet til elektroniske kommunikasjonsnett og -tjenester. Kommunal- og distriktsdepartementet har også samordningsansvar for regjeringens IT-politikk og ansvar for å koordinere arbeidet med digitaliseringen av offentlig sektor. Dette omfatter arbeidet med å styrke og oppnå en mer helhetlig tilnærming til informasjonssikkerhet i forvaltningen.[66]

Kommunal- og distriktsdepartementet har ansvar for å føre tilsyn med informasjonssikkerheten i egen sektor og underliggende virksomheter, herunder Datatilsynet, Departementenes service- og sikkerhetstjeneste, Digitaliseringsdirektoratet, Nasjonal kommunikasjonsmyndighet og statsforvalterembetene. Kommunal- og distriktsdepartementet har i tillegg det overordnede ansvaret for regjeringens personvernpolitikk, ekomloven, eForvaltningsforskriften, IKT-forskriften og personopplysningsforskriften.[67]

4.1.7 Digitaliseringsdirektoratet

Ifølge virksomhetsinstruksen skal Digitaliseringsdirektoratet være samordner og pådriver i offentlig sektors arbeid med forebyggende informasjonssikkerhet. Digitaliseringsdirektoratet skal særskilt bidra til at alle statlige virksomheter har et system for internkontroll av informasjonssikkerhet. Videre skal direktoratet legge til rette for at offentlig forvaltning får gjennomført tiltak og handlingsplaner i samsvar med vedtatte strategier på området. Direktoratet arbeider også for å utvikle nye digitale tjenester rettet mot innbyggere, kommuner og næringsliv.[68]

Digitaliseringsdirektoratet har siden 2014 hatt et veiledningsansvar for hele forvaltningen, herunder kommunene, som bunner i eForvaltningsforskriften § 15 (krav til styringssystem for informasjonssikkerhet).[69]

Digitaliseringsdirektoratet har i tillegg det operative ansvaret for fellesløsningene som Kommunal- og distriktsdepartementet har etatsstyringsansvar for. Disse er Altinn, digital postkasse til innbyggerne, eFormidling, eInnsyn, elektronisk mottaksregister (ELMA), eSignering, ID-porten, Kontakt- og reservasjonsregisteret, Maskinporten og Norge.no.[70]

4.1.8 Datatilsynet

Datatilsynet er et uavhengig forvaltningsorgan som er underlagt Kommunal- og distriktsdepartementet. Datatilsynets hovedoppgave er å bidra til at personvernlovgivningen etterleves. Datatilsynet veileder og fører tilsyn med informasjonssikkerhet etter personvernforordningens artikkel 24, 25, 28, 30, 32, 33, 34 og 35. De fører også tilsyn med at reglene om informasjonssikkerhet, helseregisterloven, helseforskningsloven og politiregisterloven etterleves.

Datatilsynet er ansvarlig for å godkjenne behandlingen av personopplysninger etter personopplysningsloven. De behandler henvendelser og klager, driver veiledning, forsknings-,

[65] Kripos (2016) *Strategi 2016–2025*.
[66] Verifisert intervju med Kommunal- og distriktsdepartementet, 7. mai 2021.
[67] Kommunal- og distriktsdepartementet (u.å.) *Notat samfunnssikkerhet og beredskap*.
[68] Digitaliseringsdirektoratet (u.å.) *Kva er Digitaliseringsdirektoratet?* [Hentedato 15. november 2021].
[69] Verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021.
[70] Digitaliseringsdirektoratet (u.å.) *Kva er Digitaliseringsdirektoratet?* [Hentedato 15. november 2021].

utviklings- og utredningsarbeid og drifter den regulatoriske sandkassen for kunstig intelligens[71] og personvernombudsordningen. Datatilsynet deltar også i flere råd og utvalg.[72]

4.1.9 Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet, som er administrativt underlagt Kommunal- og distriktsdepartementet og faglig underlagt Kommunal- og distriktsdepartementet og Samferdselsdepartementet, arbeider for gode og sikre nett for elektronisk kommunikasjon (ekom). Nasjonal kommunikasjonsmyndighet skal styrke robustheten og sikkerheten i den nasjonale digitale infrastrukturen og sørge for at internett- og cybersikkerheten i ekomsektoren håndteres på en effektiv måte.[73]

Nasjonal kommunikasjonsmyndighet fører tilsyn med at kravene i ekomloven, sikkerhetsloven og klassifiseringsforskriften etterleves, og har ansvar for å utøve myndighet ved håndtering av hendelser innenfor ekomsektoren (gjennom EkomCERT, som er ekomsektorens responsmiljø) og for forvaltningen av taushetsplikten i post- og ekomsektoren.[74]

4.1.10 Norges vassdrag- og energidirektorat

Norges vassdrags- og energidirektorat (NVE) er underlagt Olje- og energidepartementet og har ansvar for å forvalte landets vann- og energiressurser og for å ivareta de statlige forvaltningsoppgavene innenfor skredforebygging. NVE skal også arbeide for å styrke den digitale sikkerheten i kraftforsyningen, herunder følge opp tiltak som følger av risiko- og sårbarhetsanalyser for kraftsektoren.[75]

Ifølge energiloven og kraftberedskapsforskriften skal NVE føre tilsyn med virksomheter som er definert som enheter i kraftforsyningens beredskapsorganisasjon. I tillegg fører NVE tilsyn med at sikkerhetsloven etterleves i kraftsektoren.[76]

4.1.11 Forsvarsdepartementet

Forsvarsdepartementet har et primært ansvar for å ivareta statssikkerheten. Forsvarsdepartementet har ansvaret for den digitale sikkerheten i forsvarssektoren. Dette omfatter arbeidet med forebyggende digital sikkerhet og oppgavene med å sikre at sikkerhetsloven etterleves. Forsvarsdepartementet har sammen med Justis- og beredskapsdepartementet et overordnet ansvar for å følge opp *Nasjonal strategi for digital sikkerhet* fra 2019 med tilhørende tiltak.[77]

Sentrale underliggende virksomheter i Forsvarsdepartementets arbeid med digital sikkerhet er Cyberforsvaret, Etterretningstjenesten og Forsvarets sikkerhetsavdeling.[78]

4.1.12 Kunnskapsdepartementet

Kunnskapsdepartementet har sammen med Justis- og beredskapsdepartementet ansvaret for utformingen og oppfølgingen av *Nasjonal strategi for digital sikkerhetskompetanse* fra 2019 med tilhørende tiltak (beskrives nærmere i kapittel 6.2).[79]

[71] Den regulatoriske sandkassen ble etablert i 2020 og skal tilby gratis veiledning til utvalgte private og offentlige virksomheter av forskjellige typer og størrelser, på tvers av ulike sektorer. Den overordnede målsettingen med den regulatoriske sandkassen er å stimulere til utvikling og bruk av etisk og ansvarlig kunstig intelligens fra et personvernperspektiv.
[72] Kommunal- og distriktsdepartementet (u.å.) *Notat samfunnssikkerhet og beredskap*; Datatilsynet (2020) *Årsrapport 2020*.
[73] Kommunal- og distriktsdepartementet (2021) *Tildelingsbrev til Nasjonal kommunikasjonsmyndighet*.
[74] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[75] Olje- og energidepartementet (2021) *Tildelingsbrev til Norges vassdrags- og energidirektorat*.
[76] Olje- og energidepartementet (2021) *Tildelingsbrev til Norges vassdrags- og energidirektorat*.
[77] Justis- og beredskapsdepartementet og Forsvarsdepartementet (2019) *Nasjonal strategi for digital sikkerhet*.
[78] Forsvaret (2020) *Forsvarets fellestjenester* [Hentedato 15. november 2021].
[79] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.

4.2 Samordning mellom aktørene

For at ulike aktører som har ansvar knyttet til den nasjonale digitale sikkerheten, skal kunne utveksle informasjon, kunnskap og erfaringer, er det etablert en rekke tverrsektorielle samordningsarenaer. Vi har undersøkt hvordan disse er organisert, og hvor nyttige de sentrale aktørene opplever at de er, basert på dokumenter (agendaer og møtereferater) og intervjuer. I det følgende presenterer vi gjennomgangen av samordningsarenaene.

Faktaboks 4 Hva er en samordningsarena?

En samordningsarena er en fysisk eller digital møteplass der autonome og gjensidig avhengige aktører møtes for å utveksle informasjon, kunnskap og erfaringer med det formål å løse spesifikke, komplekse utfordringer. Graden av formalitet i samordningsarenaene kan variere. Møtene kan for eksempel avholdes ved behov eller på forhåndsbestemte tidspunkter. En samordningsarena er ikke en selvstendig organisatorisk enhet og har derfor ikke beslutningsmyndighet.

Kilde: Basert på definisjonen av «governance network» i Klijn, Erik-Hans og Joop Koppenjan (2014) *Complexity in governance network theory.* I: *Complexity, Governance & Networks.* 1(1) og Klijn, Erik-Hans (2008) *Governance and Governance Networks in Europe.* I: Public Management Review, 10(4).

Begrepene *arena*, *forum* og *nettverk* brukes i denne sammenheng synonymt. I det følgende holder vi oss til begrepet *samordningsarena*. Vi har identifisert totalt 19 samordningsarenaer innenfor myndighetenes arbeid med digital sikkerhet i sivil sektor. De identifiserte arenaene omhandler både forebyggende sikkerhetsarbeid og håndtering av digitale hendelser.

Tabell 2 Oversikt samordningsarenaer for myndighetenes arbeid med digital sikkerhet

Samordningsarena	Deltakere	Formål
Departementenes samordningsråd for samfunnssikkerhet	Alle departementer. Ledes av Justis- og beredskapsdepartementet.	Skal legge til rette for informasjons- og erfaringsutveksling i arbeidet med samfunnssikkerhet og beredskap, redningstjeneste og sivilt-militært samarbeid.
Departementenes øvingsforum	Alle departementer. Ledes av Justis- og beredskapsdepartementet.	Skal legge til rette for koordinert øvingsaktivitet.
Ekom sikkerhetsforum	Alle store teletilbydere, Nasjonal sikkerhetsmyndighet, PST og Etterretningstjenesten. Ledes av Nasjonal kommunikasjonsmyndighet.	Skal fremme en felles, oppdatert trusselforståelse mellom sivile og militære myndigheter og ekomsektoren. Møter fasiliteres gjennom Felles cyberkoordineringssenter.
Felles cyberkoordinerings-senter	Etterretningstjenesten, Nasjonal sikkerhetsmyndighet (administrativ ledelse), Kripos og PST.	Skal gjennom koordinering av partene bidra til å øke den nasjonale evnen til å motstå alvorlig digitale angrep.
Forum for digital sikkerhet	Representanter fra myndighetene, næringslivet, interesse- og bransjeorganisasjoner og akademia. Ledes av Nasjonal sikkerhetsmyndighet.	Skal legge til rette for diskusjon av strategiske spørsmål knyttet til digital sikkerhet mellom private og offentlige aktører og myndigheter.
Forum for IKT-tilsyn	Digitaliseringsdirektoratet, Direktoratet for strålevern og atomsikkerhet, Finanstilsynet, Kystverket, Luftfartstilsynet, Mattilsynet, Nasjonal kommunikasjonsmyndighet, NVE, Petroleumstilsynet, Sjøfartsdirektoratet og Statens jernbanetilsyn. Ledes av Nasjonal sikkerhetsmyndighet.	Skal koordinere arbeidet mellom myndigheter som fører tilsyn med den digitale sikkerheten.
Fylkesberedskaps-sjefenes arbeidsutvalg	Fylkesberedskapssjefene, Nasjonal kommunikasjonsmyndighet og Telenor.	Skal bidra til å forebygge uønskede hendelser.

Kriserådet	Regjeringsrådene ved Statsministerens kontor, Utenriksråden i Utenriksdepartementet og departementsrådene i Forsvarsdepartementet, Helse- og omsorgsdepartementet, Kommunal- og distriktsdepartementet og Justis- og beredskapsdepartementet (leder).	Øverste administrative koordineringsorgan på departementsnivå. Opprettet for å styrke den sentrale koordineringen under nasjonale kriser.
Nasjonalt cybersikkerhets-senter	Avdeling i Nasjonal sikkerhetsmyndighet og et partnerskap mellom og 49 virksomheter fra offentlig og privat sektor.	Knutepunkt mellom privat og offentlig sektor i arbeidet med digital sikkerhet. Ivaretar i tillegg oppgaven som nasjonalt responsmiljø for håndtering av alvorlige digitale angrep.
Nasjonalt øvelses- og evalueringsforum	Representanter fra direktorater, etater, fylkesmenn og kommuner samt eiere og operatører av samfunnskritisk infrastruktur. Ledes av Direktoratet for samfunnssikkerhet og beredskap.	Skal understøtte arbeidet med og koordineringen av øvelses- og evalueringsaktivitet innenfor samfunnssikkerhets- og beredskapsområdet og drive med systematisert oppfølging og læring etter hendelser.
Nettverk for informasjons-sikkerhet	Åpent for alle offentlig ansatte som arbeider med eller som har interesse for informasjonssikkerhet. Ledes av Digitaliseringsdirektoratet.	Skal legge til rettefor erfaringsutveksling om arbeid med informasjonssikkerhet på tvers av offentlige virksomheter.
Nettverk for nasjonal IKT-sikkerhet	Alle departementer. Ledes av Justis- og beredskapsdepartementet.	Skal sørge for at strategiske spørsmål knyttet til internasjonalt samarbeid og digitale sikkerhetsutfordringer blir diskutert og koordinert.
Nettverk for veiledningsaktører innen styring og kontroll	Datatilsynet, Direktoratet for e-helse, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, KS og Forening for kommunal informasjonssikkerhet. Ledes av Digitaliseringsdirektoratet.	Skal legge til rette for informasjonsutveksling om pågående samordningsprosjekter samt samarbeide om ulike tema under styring og kontroll.
Samhandlingsarena for sektortilsyn etter sikkerhetsloven	Nasjonal kommunikasjonsmyndighet og NVE. Ledes av Nasjonal sikkerhetsmyndighet.	Skal legge til rette for kunnskaps- og erfaringsutveksling for å sikre kvalitet og enhetlig praksis for tilsynsvirksomhet etter sikkerhetsloven.
Sentraltotalforsvars-forumet	Alle etatslederne i totalforsvaret og Forsvaret. Ledes av Direktoratet for samfunnssikkerhet og beredskap og Forsvarsstaben.	Skal utarbeide analyser og beslutningsgrunnlag med det formål å forebygge uønskede hendelser samt for å sikre en god felles respons ved slike hendelser.
Strategisk nettverk for informasjons-sikkerhet og personvern	Ansatte med ansvar for digital sikkerhet, personvern eller digitalisering i kommunene. Ledes av KS.	Skal styrke kommunenes kompetanse på informasjonssikkerhet og personvern samt gi kommunene en felles arena for å drøfte sikkerhetsutfordringer.
Styring og koordinering av tjenester i e-forvaltning	Arkivverket, Brønnøysundregistrene, Digitaliseringsdirektoratet, Direktoratet for byggekvalitet, Direktoratet for e-helse, Kartverket, kommunene Halden og Oslo, KS, Kunnskapssektorens tjenesteleverandør NAV, Skatteetaten, Statistisk sentralbyrå. Ledes av Kommunal- og distriktsdepartementet og KS.	Skal bidra til å styrke informasjonssikkerheten i forvaltningen.
Styringsgruppen for Normen	Datatilsynet, Digitaliseringsdirektoratet og Nasjonal sikkerhetsmyndighet. Ledes av Direktoratet for e-helse.	Skal bidra til å sikre en god og sikker informasjonsbehandling og arbeide for å sikre Normen[80] som bransjenorm i sektoren.
Topplederforum for digital sikkerhet	Finanstilsynet, Nasjonal kommunikasjonsmyndighet, NVE, Petroleumstilsynet. Etablert av Nasjonal sikkerhetsmyndighet.	Skal legge til rette for informasjonsutveksling og diskusjon på strategisk nivå om regelverksutvikling, tilsynsutfordringer og behov for operative digitale sikkerhetstiltak.

[80] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.

Av samordningsarenaene i Tabell 2 er 16 rettet mot myndighetenes forebyggende arbeid med digital sikkerhet. Disse arenaene omtales nærmere i kapittel 4.2.1. Med forebyggende arbeid menes her tiltak for å redusere muligheten for en uønsket hendelse eller tiltak for å redusere konsekvensene av en mulig hendelse.[81] De tre siste er rettet mot hendelseshåndtering: Kriserådet, Felles cyberkoordineringssenter og Nasjonalt cybersikkerhetssenter. Sistnevnte arbeider også forebyggende.

4.2.1 Samordningsarenaer for forebyggende digital sikkerhet

Samordningsarenaene består av mange aktører på ulike nivåer, samtidig som flere av aktørene deltar i forskjellige arenaer. Samordningsarenaene innenfor det forebyggende sikkerhetsarbeidet består av et bredt spekter av deltakere, i hovedsak fra offentlig sektor. Tematisk er det mye overlapp mellom arenaene, og flere av samordningsarenaene favner bredt.

Nasjonal kommunikasjonsmyndighet forteller at tematikken som diskuteres i samordningsarenaene, er delvis overlappende, og at det kan være vanskelig å skille klart mellom de ulike tematikkene fordi arbeidet med digital sikkerhet er så komplekst. Arenaene har imidlertid ulike perspektiver. Nasjonal kommunikasjonsmyndighet opplever dynamikken i og mellom samordningsarenaene som nyttig. De forteller for eksempel at møtedeltakelsen varierer etter situasjonen og behovene. Tilsvarende vil nye arenaer komme til og andre forsvinne avhengig av det digitale sikkerhetsbildet. Dette anser Nasjonal kommunikasjonsmyndighet som naturlig og hensiktsmessig i arbeidet med digital sikkerhet.[82]

Ingen av aktørene vi har intervjuet i forbindelse med undersøkelsen, har uttalt at de savner samordningsarenaer som tar opp en bestemt tematikk.[83]

I intervjuer forteller aktørene at de deltar i møter i samordningsarenaene etter behov og noe avhengig av virksomhetens ressurssituasjon. Det generelle budskapet deres er at arenaene er nyttige, og at dette særlig skyldes at de gir dem en mulighet til å klargjøre hva slags roller og ansvar de ulike aktørene har. For aktørene oppleves det nyttig å utveksle erfaringer og informasjon om hva de arbeider med, og om ulike prosjekter og tiltak.[84]

Basert på vår undersøkelse av samordningsarenaene – og sett i lys av samordningsstigen til Direktoratet for forvaltning og økonomistyring – ser det ut til at samordningsgraden i de fleste arenaene ligger på trinn én (dele informasjon) og i noen tilfeller på trinn to (utvikle felles forståelse). Arenaene brukes i hovedsak til å opplyse og orientere hverandre om pågående arbeid. Det gjøres i liten grad operativt og konkret arbeid for økt samordning av det forebyggende digitale sikkerhetsarbeidet i de gjennomgåtte arenaene. Selv om det i *Nettverk for nasjonal IKT-sikkerhet* og *Forum for digital sikkerhet* er blitt arbeidet med felles planer/strategier (jf. trinn fire), ser det ikke ut til at arenaene i sin helhet er samordnet til dette nivået. Nettverkenes hovedformål er imidlertid å diskutere «saker av nasjonal betydning for digital sikkerhet»[85] og «sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid blir diskutert mellom private aktører og myndighetene».[86] Å utvikle felles planer og strategier er ikke et uttalt mål for noen av arenaene, og slik sett er det ikke å forvente at arenaene er samordnet til trinn fire i samordningsstigen.

[81] Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*
[82] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022
[83] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022; verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT; verifisert intervju med Kunnskapsdepartementet, 26. januar 2022; Svar på skriftlige spørsmål fra Digitaliseringsdirektoratet, besvart 6. mai 2022; verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021; Svar på skriftlige spørsmål fra Direktoratet for sikkerhet og beredskap, besvart 9. mai 2022; Riksrevisjonens dybdeundersøkelse, 22. april 2022; verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[84] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022; verifisert intervju med Forsvarsdepartementet, 19. januar 2022; verifisert intervju med Kunnskapsdepartementet, 26. januar 2022, Svar på skriftlige spørsmål fra Digitaliseringsdirektoratet, besvart 6. mai 2022; verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021; Svar på skriftlige spørsmål fra Direktoratet for sikkerhet og beredskap, besvart 9. mai 2022; Riksrevisjonens dybdeundersøkelse; verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[85] Departementene (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[86] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*

I undersøkelsen har vi sett nærmere på de fem samordningsarenaene for forebyggende sikkerhetsarbeid som inngår i *Nasjonal strategi for digital sikkerhet* (2019):

- *Nettverk for nasjonal IKT-sikkerhet*
- *Forum for digital sikkerhet*
- *Forum for IKT-tilsyn*
- *Nettverk for veiledningsaktører innen styring og kontroll*
- *Nasjonalt cybersikkerhetssenter*

I det følgende går vi nærmere inn på fire av disse med hensyn til arenaenes formål og det opplevde utbyttet til de utvalgte deltakerne. *Forum for IKT-tilsyn* omtales i kapittel 4.6.2 om samordningen av tilsyn med den digitale sikkerheten.

Nettverk for nasjonal IKT-sikkerhet

Det tidligere Koordineringsutvalget for informasjonssikkerhet ble opprettet i 2003, og ble overført til Justis- og beredskapsdepartementet fra Kommunal- og distriktsdepartementet i 2013. Nettverkets arbeid omfattet spørsmål knyttet til rikets sikkerhet, nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Nettverket skulle samordne videreutviklingen av IT-sikkerhetsregelverket og fremme felles standarder, normer, metoder og verktøy for digital sikkerhet. De skulle også drøfte aktuelle risiko- og sårbarhetsspørsmål og bidra til å koordinere informasjonstiltak og beredskapsplanlegging.[87] Justis- og beredskapsdepartementet forteller at det var varierende erfaringer med nettverket etter at de overtok ansvaret for det. Departementet foretok derfor en evaluering som gjorde at nettverkets sammensetning ble endret i 2015. Det ble som følge av dette etablert et nytt mandat, og nettverkets navn ble endret til *Nettverk for informasjonssikkerhet.*[88]

Det fulgte av *IKT-sikkerhetsmeldingen* (2017) at *Nettverk for informasjonssikkerhet* skulle videreutvikles for å sikre at strategiske spørsmål blir diskutert og at betydningen av offentlig-privat, sivilt-militært og internasjonalt samarbeid skulle vektlegges.[89] Det ble derfor etablert en arbeidsgruppe som bestod av Forsvarsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet og Nærings- og fiskeridepartementet. Det ble i 2017 etablert et nytt mandat, som ble forelagt alle departementene sammen med departementsforeleggelsen av *IKT-sikkerhetsmeldingen* (2017). Nettverket ble hetende *Nettverk for Nasjonal IKT-sikkerhet*, men essensen i nettverkets innhold ble ikke vesentlig endret med videreutviklingen. Det nye mandatet tydeliggjorde imidlertid den strategiske dimensjonen for arbeidet i nettverket, Utenriksdepartementets rolle, og kravet om at deltakerne i nettverket skal være sikkerhetsklarerte forsvant. Det nåværende mandatet har krav om at deltagerne skal ha ansvar for, eller en rolle knyttet til utforming av digital sikkerhetspolitikk i sin sektor.[90]

Nettverk for nasjonal IKT-sikkerhet skal diskutere saker av nasjonal betydning for den digitale sikkerheten.[91] Alle departementer deltar fast i nettverket med én eller to representanter. Siden nettverkets mandat ble oppdatert i 2017 har det vært gjennomført ti møter, i tillegg til to møter sammen med *Forum for digital sikkerhet*. Nettverket koordinerer sine saker med *Departementenes samordningsråd for samfunnssikkerhe*t, hvor alle departementene er representert. Samordningsrådet ledes av Justis- og beredskapsdepartementet og har som mål å sikre informasjons- og erfaringsutveksling mellom departementene i arbeidet med samfunnssikkerhet og beredskap, redningstjeneste og sivilt-militært samarbeid.

Ett av de årlige møtene i *Nettverk for nasjonal IKT-sikkerhet* foregår i *Forum for digital sikkerhet*, der 21 representanter fra myndighetene, næringslivet, interesse- og bransjeorganisasjoner og akademia

[87] Digi.no (2004) *Statlig utvalg skal koordinere norsk IT-sikkerhet* [Hentedato 30. august 2022].
[88] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[89] Meld. St. 38 (2016−2017) *IKT-sikkerhet. Et felles ansvar.*
[90] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[91] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*

deltar. Formålet er å sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid blir diskutert.[92] Det årlige fellesmøtet skal føre til økt samhandling, særlig med næringslivet som er representert i *Forum for digital sikkerhet*. På grunn av koronapandemien har det de siste to årene har vært lavere møtefrekvens i fagnettverket enn normalt.[93]

Justis- og beredskapsdepartementet forteller at de har brukt nettverket i utarbeidelsen og oppfølgingen av den nasjonale strategien for digital sikkerhet. Strategien var det primære diskusjonstemaet i nettverket i tiden da den ble utarbeidet.[94] Utover dette har blant annet arbeidet med et nytt EU-direktiv om digital sikkerhet (NIS-direktivet), *Øvelse Digital 2020*, *Rammeverk for håndtering av IKT-hendelser* (2017), status for oppfølgingen av *Nasjonal strategi for digital sikkerhet* (2019), informasjonsutveksling og norsk deltakelse i multilaterale diskusjoner om digital sikkerhet vært gjenstand for diskusjon i nettverket.[95]

For Justis- og beredskapsdepartementet er nettverket en arena for å samordne ansvaret for digital sikkerhet i sivil sektor, for Forsvarsdepartementet er det en arena for å ta opp sivil-militære spørsmål knyttet til digital sikkerhet, og for Utenriksdepartementet er det en arena som brukes i departementets rolle som koordinator for norske posisjoner i internasjonal cyberpolitikk.[96] Både Kunnskapsdepartementet og Forsvarsdepartementet forteller at de deltar med to personer hver i nettverket, og at det er nyttig for dem å delta. De to departementene forteller at de først og fremst har utbytte av nettverket fordi det gir deltakerne anledning til å utveksle informasjon, blant annet om hva de arbeider med. De forteller videre at det sendes ut forslag til møteagenda før møtene, og at deltakerne slik sett har mulighet til å spille inn ønsker til diskusjon i møtene.[97] Kunnskapsdepartementet viser til at de blant annet har brukt nettverket til å informere om departementets ph.d.-ordninger innenfor informasjonssikkerhet.[98] Forsvarsdepartementet trekker fram innsikt i andre departementers erfaringer fra etableringen av sektorvise responsmiljøer som eksempel på hvordan arenaen har vært nyttig.[99]

Ifølge Justis- og beredskapsdepartementet er nettverket et viktig verktøy for samordningsansvaret de har innenfor digital sikkerhet. De forteller at de ønsket å gjøre nettverket mer relevant for Utenriksdepartementet og Forsvarsdepartementet, gjennom i større grad å bringe inn det internasjonale perspektivet. Ifølge Forsvarsdepartementet er Utenriksdepartementets orientering om saker som har betydning for den digitale sikkerheten, fra ulike internasjonale arenaer nyttig.[100] Dette tyder på at man har klart å bringe inn det internasjonale perspektivet i større grad. Dette kommer også til uttrykk gjennom møtereferatene fra nettverket.[101]

I 2020 ble det på bakgrunn av tiltak 10 i *Nasjonal strategi for digital sikkerhet* (2019) gjennomført en intern evaluering av nettverket. Evalueringen viste at flere av utfordringene som gjaldt for det tidligere koordineringsutvalget, fortsatt gjaldt. Følgende utfordringer ble identifisert i evalueringen:

- Informasjonsutvekslingen er altfor ensidig. Deltakerne ønsker å holde nettverksmøtene på et strategisk nivå framfor på et operativt og problemorientert nivå.
- Deltakerne opplever at sammensetningen av nettverket ikke har relevant erfaringsgrunnlag, og bare noen få personer deltar i diskusjonene.
- Forsvars- og Utenriksdepartementets framtredende rolle i nettverket fungerer i varierende grad. Før 2017 driftet Utenriksdepartementet en cyberkoordineringsgruppe hvor et utvalg departementer

[92] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[93] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[94] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[95] Tilsendte møtereferater, Justis- og beredskapsdepartementet, 2017–2022.
[96] NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*
[97] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[98] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[99] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[100] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[101] Tilsendte møtereferater, Justis- og beredskapsdepartementet, 2017–2022.

deltok. For å unngå for mange møtefora og sikre tettere kobling mellom det nasjonale og internasjonale nivået besluttet Justis- og beredskapsdepartementet og Utenriksdepartementet i 2017 at cyberkoordineringsgruppen skulle inngå i nettverket.
- Det er varierende engasjement når det gjelder deltakelse og innmelding av saker.[102]

Justis- og beredskapsdepartementet oppgir at evalueringen førte til et internt arbeid hvor man så på muligheter for å slå nettverket sammen med *Departementenes samordningsråd for samfunnssikkerhet*. Formålet var å samle et utvalg av samordningsarenaer. Ideen om sammenslåingen dreide seg også om at digital sikkerhet (jf. samfunnssikkerhetsinstruksen) er en integrert del av samfunnssikkerhetsarbeidet. Arbeidet stoppet imidlertid opp på grunn av endrede prioriteringer som følge av pandemien, og fordi den aktuelle avdelingen i departementet fikk et utvidet ansvar for den nasjonale sikkerheten og sammensatte trusler. Justis- og beredskapsdepartementet har derfor hatt behov for å se nærmere på mandatet til et slikt nettverk. Dette betyr at evalueringen per september 2022 ikke har ført til noen endringer.[103]

Forum for digital sikkerhet

I *Forum for digital sikkerhet* sitter 21 representanter fra myndighetene, næringslivet, interesse- og bransjeorganisasjoner og akademia. Forumet, som ble etablert i 2017, ble de første årene ledet av Justis- og beredskapsdepartementet, før Nasjonal sikkerhetsmyndighet overtok ansvaret i 2021. Siden Nasjonal sikkerhetsmyndighet overtok ansvaret for forumet, har det blitt holdt tre møter (to i 2021 og ett i 2022).

Formålet til *Forum for digital sikkerhet* er å sikre at strategiske spørsmål knyttet til digitale sikkerhetsutfordringer og internasjonalt samarbeid blir diskutert mellom myndighetene og private aktører. Forumet skal bidra til åpenhet, tillit og samhandling mellom offentlige og private aktører når det gjelder å dele informasjon og diskutere problemstillinger knyttet til digital sikkerhet.[104] På samme måte som *Nettverk for nasjonal IKT-sikkerhet* skal forumet være et verktøy som Justis- og beredskapsdepartementet og Forsvarsdepartementet kan bruke når de skal ivareta samordnings- og koordineringsansvaret de har for digital sikkerhet. Forumet skal videre benyttes som referansegruppe for arbeidet med nasjonale strategier og handlingsplaner.[105]

Tema som har blitt diskutert i møtene, er offentlig-privat samarbeid og informasjonsdeling på det digitale sikkerhetsområdet, forskrifter til ny sikkerhetslov, lovreguleringen av det digitale sikkerhetsarbeidet, Nasjonalt cybersikkerhetssenter, *Nasjonal strategi for digital sikkerhet* (2019), *Nasjonal strategi for digital sikkerhetskompetanse* (2019) og tilsynsvirksomhet for arbeidet med digital sikkerhet og bruk av tjenesteutsetting og skytjenester.[106]

Forum for digital sikkerhet ble evaluert i 2019. Evalueringen var basert på svar på spørsmål fra åtte av representantene. Generelt viser evalueringen at deltakerne synes at forumet er nyttig. Utover dette er de viktigste tilbakemeldingene at diskusjonene preges av tidvis tynt erfaringsgrunnlag til å diskutere nasjonale sikkerhetsspørsmål spørsmål på strategisk nivå, og at det er for mange IT-leverandører i forumet. Det viktigste funnet i evalueringen handler om sammensetningen av deltakerne. Det er ønskelig med flere aktører som representerer kritisk infrastruktur og kritiske samfunnsfunksjoner. I tillegg er det et ønske om at Nasjonal sikkerhetsmyndighet, Kommunal- og distriktsdepartementet og Digitaliseringsdirektoratet skal delta i forumet. Nærings- og fiskeridepartementet, Utenriksdepartementet og Forsvarsdepartementet på sin side får kritikk for å vise lite engasjement for forumet. Det er også et ønske om at diskusjonene i forumet i større grad skal holdes på et strategisk

[102] Justis- og beredskapsdepartementet (2020) *Nettverk for nasjonal IKT-sikkerhet – forslag om innlemmelse i Departementenes samordningsråd for samfunnssikkerhet.*
[103] Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet, 12. september 2022.
[104] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[105] NOU (2018: 14) *IKT-sikkerhet i alle ledd*. *Organisering og regulering av nasjonal IKT-sikkerhet.*
[106] Tilsendte møtereferater fra Justis- og beredskapsdepartementet i perioden 2018–2021.

nivå og legge vekt på nasjonens behov framfor å handle om situasjonen i enkeltselskaper. I forbindelse med evalueringen ble det utarbeidet et konkret endringsforslag om forumets sammensetning.[107]

Justis- og beredskapsdepartementet oppgir at de fulgte oppfordringen om å endre forumets sammensetning. Kort sagt var det åtte virksomheter som ble takket av for å frigi plass til andre typer virksomheter. Endringen førte til at forumet fikk et større innslag av virksomheter med ansvar for kritisk digital infrastruktur og kritiske samfunnsfunksjoner. I tillegg ble Nasjonal sikkerhetsmyndighet invitert til å delta som nasjonalt fagmiljø, mens Kommunal- og distriktsdepartementet ble invitert til å delta med utgangspunkt i departementets ansvar for ekomsikkerhet. Forumets mandat ble justert som følge av endringene.[108]

Nettverk for veiledningsaktører innen styring og kontroll

Nettverk for veiledningsaktører innenfor styring og kontroll er rettet mot aktører som driver med veiledning innenfor arbeidet med digital sikkerhet. Nettverket ledes av Digitaliseringsdirektoratet og er en del av direktoratets arbeid med å styrke en helhetlig tilnærming til informasjonssikkerhet i forvaltningen.[109]

I nettverket møtes Digitaliseringsdirektoratet, Direktoratet for forvaltning og økonomistyring, Datatilsynet, Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap, Direktoratet for e-helse, Sikt − Kunnskapssektorens tjenesteleverandør, Direktoratet for høyere utdanning og kompetanse, Norsk senter for informasjonssikring, Kommunesektorens organisasjon, Foreningen kommunal informasjonssikkerhet og Nasjonal kommunikasjonsmyndighet. Nettverket skal fremme økt dialog mellom veiledningsaktørene på området og bidra til en helhetlig tilnærming innen styring og kontroll, med informasjonssikkerhet som fokusområde.[110]

I 2021 ble partene i nettverket enige om å etablere retningslinjer for samordning av veiledning, som blant annet inkluderer et sett med kjøreregler man jobber etter for å involvere hverandre på tvers. Dette inkluderer blant annet at alle medlemmer i nettverket etterstreber å involvere hverandre på følgende punkter i arbeidet:

- Ved oppstart/planlegging
- Under arbeid
- Før ferdigstillelse
- Ved publisering

Digitaliseringsdirektoratet forteller i intervju at partene har en ambisjon om å avholde to til fire møter i året. I 2021 ble det avholdt to møter. Digitaliseringsdirektoratet melder inn og innhenter ønsker og behov fra deltakerne i forkant av møtene. Nasjonal kommunikasjonsmyndighet forteller i intervju at de selv bare har deltatt i ett eller to møter i nettverket. De sier at de har kommet inn i nettverket ved en tilfeldighet.[111]

Direktoratet for samfunnssikkerhet og beredskap forteller at de opplever nettverket som en nyttig arena for informasjonsdeling, som bidrar til en avstemming av de deltakende virksomhetenes ulike aktiviteter. De viser også til at Digitaliseringsdirektoratet og Nasjonal sikkerhetsmyndighet har samarbeidet om å utvikle veiledningsmateriell gjennom nettverket. Direktoratet forsøker å stille i alle

[107] Justis- og beredskapsdepartementet (2019) *Evaluering av «Forum for nasjonal IKT-sikkerhet».*
[108] Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet, 12. september 2022.
[109] Digitaliseringsdirektoratet (u.å.) *Nettverk for veiledningsaktører − styring og kontroll.*
[110] Digitaliseringsdirektoratet (u.å.) *Nettverk for veiledningsaktører − styring og kontroll.*
[111] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.

møtene, men har måttet nedprioritere enkelte møter på grunn av koronapandemien og krigen i Ukraina.[112]

Nasjonalt cybersikkerhetssenters forebyggende sikkerhetsarbeid

Nasjonalt cybersikkerhetssenter er en del av Nasjonal sikkerhetsmyndighet og har en todelt funksjon. Senteret skal både være en arena for erfaringsutveksling og styrking av det offentlig-private samarbeidet innenfor forebyggende sikkerhetsarbeid, og et nasjonalt responsmiljø ved digitale hendelser. Det forebyggende arbeidet er organisert som et partnerskap som skal fungere som et knutepunkt mellom privat og offentlig sektor i arbeidet med digital sikkerhet. Partnerskapet hadde i november 2022 49 partnere fra både offentlig og privat sektor. Partnerne har inntil fem personer hver som har adgang til Nasjonalt cybersikkerhetssenters lokaler, og inntil ti personer som kan delta på digitale aktiviteter.

Partnerne i Nasjonalt cybersikkerhetssenter møtes annenhver uke til en operativ brief. Her utveksler de informasjon om hva som har skjedd den siste tiden, råd og anbefalinger knyttet til identifisert risiko og informasjon om aktuelle problemstillinger og utfordringer.[113]

Nasjonal sikkerhetsmyndighet forteller i intervju at de opprinnelig hadde tenkt at partnermøtene i Nasjonalt cybersikkerhetssenter skulle være fysiske, men at pandemien la begrensninger på dette. Til tross for at Nasjonal sikkerhetsmyndighet opplever at de digitale møtene har lagt noen begrensninger på informasjonsutvekslingen og muligheten til å bygge tillit mellom partene, har møtene bidratt til økt informasjonsutveksling, noe som har gjort at partene har fått et tydeligere situasjonsbilde enn det som ville vært mulig ellers.[114]

De intervjuede deltakerne er gjennomgående fornøyde med utbyttet de får av å delta i partnerskapet. En intervjuet virksomhet forteller at de har prioritert de ukentlige møtene i Nasjonalt cybersikkerhetssenter og foredragene som har blitt avholdt digitalt. Selv om det under pandemien ikke har vært anledning til å møte de andre partene og bygge relasjoner, har virksomheten hatt nytte av de digitale møtene og arrangementene.[115] En annen intervjuet virksomhet sier at det ikke er så viktig at partene i Nasjonalt cybersikkerhetssenter møtes fysisk, og forklarer det med at virksomhetene ikke nødvendigvis deler informasjon friere selv om de befinner seg i samme lokale. Ifølge virksomheten skjer informasjonsutvekslingen i etterkant av en hendelse, ikke mens den pågår.[116]

De digitale aktivitetene under pandemien gjorde ifølge Nasjonal sikkerhetsmyndighet at flere av partnerne enn normalt kunne delta. Flere av virksomhetene har også meldt til Nasjonal sikkerhetsmyndighet at de har interne møter i etterkant av møtene i Nasjonalt cybersikkerhetssenter for å diskutere hvordan de skal jobbe videre med det som har vært tema for møtet. Nasjonal sikkerhetsmyndighet ser dette som en positiv effekt av at aktivitetene i større grad er digitale. I 2021 ble det gjennomført tre fysiske og 28 digitale møter i Nasjonalt cybersikkerhetssenter. I de digitale møtene har ulike partnere hatt regi, og partene har blant annet diskutert sikkerhetsarbeid i regi av Statkraft, sikkerhet knyttet til stortingsvalget i 2021, krypto og digitale verdikjeder.[117]

Alt i alt opplever Nasjonal kommunikasjonsmyndighet, Forsvarsdepartementet, Digitaliseringsdirektoratet og virksomhetene i dybdeundersøkelsen partnerskapet i Nasjonalt cybersikkerhetssenter som nyttig. Her trekkes særlig de digitale situasjonsbildene og

[112] Svar på skriftlige spørsmål fra Direktoratet for sikkerhet og beredskap, besvart 9. mai 2022.
[113] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[114] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[115] Riksrevisjonens dybdeundersøkelse.
[116] Riksrevisjonens dybdeundersøkelse.
[117] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.

sikkerhetskonferansen fram som positive bidrag.[118] Nasjonal kommunikasjonsmyndighet forteller i intervju at de deltar i ukentlige møter i Nasjonalt cybersikkerhetssenter, og at særlig EkomCERT er tett involvert i partnerskapet.[119] Digitaliseringsdirektoratet forteller at de har benyttet møtene i Nasjonalt cybersikkerhetssenter til å tilegne seg informasjon om aktørenes behov for veiledning, som de så har tilpasset.[120] Forsvarsdepartementet mener at etableringen av Nasjonalt cybersikkerhetssenter har bidratt til å forbedre samarbeidet innenfor forebyggende digital sikkerhet og hendelseshåndtering. Ifølge departementet er det imidlertid fortsatt noen utfordringer som ikke er løst.[121] En intervjuet virksomhet forteller at de ikke prioriterer alle møtene og foredragene i Nasjonalt cybersikkerhetssenter fordi de erfarer at tematikken i møtene er gjentakende, og at man tidvis diskuterer for enkle forhold, som viktigheten av passordbytte og systemoppdateringer.[122]

4.2.2 Samordningsarenaer for hendelseshåndtering

I *Nasjonal strategi for digital sikkerhet* (2019) listes tre viktige samordningsarenaer for håndtering av digitale hendelser:

- Nasjonalt cybersikkerhetssenter
- Felles cyberkoordineringssenter
- sektorvise responsmiljøer

Nedenfor følger en gjennomgang av Nasjonalt cybersikkerhetssenter og de sektorvise responsmiljøene, mens Felles cyberkoordineringssenter behandles i et sikkerhetsgradert vedlegg. Dette skyldes at store deler av informasjonen som er knyttet til partene som deltar i samarbeidet, er sikkerhetsgradert etter sikkerhetsloven.

Nasjonalt cybersikkerhetssenters arbeid med hendelseshåndtering

Nasjonalt cybersikkerhetssenter har funksjonen som Norges nasjonale responsfunksjon for alvorlige digitale angrep. I tillegg ligger drift av det nasjonale varslingssystemet for digital infrastruktur (VDI) til Nasjonalt cybersikkerhetssenter.

Nasjonalt cybersikkerhetssenter ble etablert for å styrke Norges robusthet i det digitale rom. Senterets viktigste oppgaver er å overvåke og reagere på digitale trusler.[123] Når det oppstår alvorlige digitale hendelser, bistår Nasjonalt cybersikkerhetssenter den aktuelle virksomheten direkte eller indirekte via det sektorvise responsmiljøet. Ved alvorlige digitale hendelser varsler Nasjonalt cybersikkerhetssenter også departementer, sektorvise responsmiljøer eller andre relevante virksomheter som deltar i senterets nettverk, med informasjon om hvilke tiltak som bør iverksettes for å hindre at en liknende hendelse skal ramme andre.[124]

Nedenfor beskriver vi et eksempel på et hendelsesforløp hvor virksomheten har fått bistand fra Nasjonalt cybersikkerhetssenter.

Faktaboks 5 Eksempel på hendelsesforløp

Angriperen utnyttet en nulldagssårbarhet[125] for å få tilgang til en av virksomhetenes servere som var koblet opp mot internett. Siden det digitale angrepet skjedde etter endt arbeidstid, ble det først oppdaget da de ansatte kom på jobb dagen etter. Et par timer etter at angrepet ble

[118] Riksrevisjonens dybdeundersøkelser; Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022; Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT; Verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021.
[119] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[120] Verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021.
[121] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[122] Riksrevisjonens dybdeundersøkelse.
[123] Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT* [Hentedato 4. februar 2022].
[124] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[125] En nulldagssårbarhet er en sårbarhet som leverandører av systemet ikke har vært klar over, men som en trusselaktør utnytter.

oppdaget, varslet virksomheten Nasjonalt cybersikkerhetssenter. Gjennom sine tekniske systemer kunne Nasjonalt cybersikkerhetssenter bekrefte at angrepet hadde funnet sted, og gi råd om hva virksomheten skulle foreta seg videre. Virksomheten skulle blant annet undersøke datatrafikklogger for å se om annen trafikk kunne knyttes til angrepet.

Samme formiddag isolerte virksomheten systemet, også dette etter råd fra Nasjonalt cybersikkerhetssenter. Formålet med å isolere systemet var å skaffe full oversikt over hendelsen, både med tanke på hvilke verdier som hadde blitt rammet, og omfanget av angrepet. Sammen med Nasjonalt cybersikkerhetssenter analyserte virksomheten minne- og diskdump fra den aktuelle serveren. I denne prosessen ble både telefon og kryptert e-post benyttet. På denne måten kunne de logge seg inn i hverandres systemer og laste opp dataene som trengtes for å gjennomføre de nødvendige analysene. Det ble identifisert to bakdører som angriperen hadde laget for å utnytte på et senere tidspunkt. Det var imidlertid ikke mulig å identifisere om angrepet var målrettet. Angrepet ble ikke anmeldt til politimyndighetene.

Det tok om lag en måned før normaltilstanden for systemet var opprettet. Fordi virksomheten hadde andre systemer som kunne ta over funksjonen til den rammede serveren mens analysearbeidet pågikk, førte ikke angrepet til nedetid. Virksomheten mistet noen data som følge av angrepet, men utover dette fikk det ingen alvorlige konsekvenser. Fram til situasjonen var avklart, og i noe tid etterpå, hadde virksomheten løpende dialog med Nasjonalt cybersikkerhetssenter via telefon og e-post.

Kilde: Riksrevisjonens dybdeundersøkelse

I Riksrevisjonens dybdeundersøkelse er de intervjuede virksomhetene gjennomgående fornøyde med arbeidet som Nasjonalt cybersikkerhetssenter gjør i forbindelse med hendelseshåndtering, og de opplever at de har fått god bistand ved hendelser. Ifølge en av virksomhetene er Nasjonalt cybersikkerhetssenter den aktøren på feltet som deler mest informasjon, og som sørger for størst grad av utvikling innenfor arbeidet med digital sikkerhet. En fellesnevner for virksomhetene som deltok i dybdeundersøkelsene, er at hele eller deler av virksomheten understøtter en grunnleggende nasjonal funksjon. Virksomhetene er derfor tildelt en egen kontaktperson i Nasjonalt cybersikkerhetssenter. Virksomhetene framhever det som svært positivt at de har direkte kontakt med Nasjonalt cybersikkerhetssenter gjennom den faste kontakten. En av virksomhetene bemerker imidlertid at ikke alle norske virksomheter er tildelt en slik kontaktperson, og at bistanden fra senteret trolig oppleves noe annerledes for disse virksomhetene når det oppstår hendelser.[126] Dette bekreftes i intervju med representanter for kommunesektoren, hvor det kom fram at noen kommuner har opplevd at det er vanskelig å komme i kontakt med og få bistand fra Nasjonalt cybersikkerhetssenter, både ved digitale hendelser og når tilstanden er normal.[127]

Vår undersøkelse har avdekket utfordringer med Nasjonal sikkerhetsmyndighets tekniske systemer VDI og Allvis NOR, som blant annet brukes av Nasjonalt cybersikkerhetssenter til å overvåke uønsket aktivitet og kartlegge sårbarheter. Dette utdypes videre i kapittel 6.4.1. For at Nasjonalt cybersikkerhetssenter til enhver tid skal ha et oppdatert situasjonsbilde på det digitale området, er det derfor viktig at virksomhetene varsler om sårbarheter og hendelser. I intervju bemerker Nasjonal sikkerhetsmyndighet at Nasjonalt cybersikkerhetssenter mottar mye og relevant informasjon fra partnerne som deltar i senterets nettverk.[128] En av virksomhetene som har deltatt i dybdeundersøkelsene, uttaler midlertid til at de som følge av begrenset kapasitet må gjøre en avveiing av hvilken informasjon de skal dele med Nasjonalt cybersikkerhetssenter ved digitale hendelser, da

[126] Riksrevisjonens dybdeundersøkelser.
[127] KS *SV: Riksrevisjonens undersøkelse av samordningen av digital sikkerhet - oppfølgingsspørsmål.* E-post til Riksrevisjonen 10. november 2022.
[128] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.

informasjonsdelingen er tid- og ressurskrevende for virksomheten, som også skal håndtere hendelsen.[129]

Justis- og beredskapsdepartementet, Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet viser alle til at etableringen av Nasjonalt cybersikkerhetssenter har hatt positive effekter på den digitale sikkerheten nasjonalt.[130] Ifølge Forsvarsdepartementet har etableringen også bidratt til å forbedre samarbeidet innenfor hendelseshåndtering, til tross for at det fortsatt er noen utfordringer.[131] Også Nasjonal sikkerhetsmyndighet uttaler at etableringen av senteret har vært vellykket.[132]

Felles cyberkoordineringssenter

Felles cyberkoordineringssenter ble etablert i 2017 og er et permanent, samlokalisert fagmiljø med representanter fra Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos. Felles cyberkoordineringssenter skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep, understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde av det digitale rom. Felles cyberkoordineringssenter er ikke et selvstendig organ med egen beslutningsmyndighet, og etableringen av senteret innebar ingen endringer i partenes rettsgrunnlag, roller eller oppgaver.[133]

I *Nasjonal strategi for digital sikkerhet* fra 2019 trekkes Felles cyberkoordineringssenter fram som sentralt for å sikre et godt samarbeid mellom viktige aktører med ansvar for digital sikkerhet. Felles cyberkoordineringssenter presenteres som tiltak 43 i strategiens tiltaksoversikt. Forsvarsdepartementet og Justis- og beredskapsdepartementet har ansvar for gjennomføringen og oppfølgingen av tiltak.

Vår undersøkelse av samordningen mellom partene i Felles cyberkoordineringssenter inngår i et sikkerhetsgradert vedlegg til rapporten.

Sektorvise responsmiljøer

Gjennom Meld. St. 29 (2011−2012) *Samfunnssikkerhet*, jf. Innst. 426 S (2012−2013), ble det vedtatt at det skulle arbeides for å etablere responsmiljøer i de ulike sektorene, heretter omtalt som sektorvise responsmiljøer, for å håndtere alvorlige digitale hendelser. Som en minimumsløsning skal det i hver sektor etableres et kontaktpunkt for alvorlige digitale hendelser og prosedyrer for varsling, både internt og opp mot Nasjonalt cybersikkerhetssenter (tidligere NorCERT). Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere digitale sikkerhetshendelser, og hvordan de eventuelt skal skalere opp responsmiljøene sine.

Etableringen av sektorvise responsmiljøer nevnes også i *Nasjonal strategi for informasjonssikkerhet* fra 2012. Der ble det vist til at det skulle opprettes digitale varslingsmiljøer med en grunnleggende kapasitet til å koordinere, varsle om og håndtere uønskede digitale hendelser i alle samfunnssektorer og i de viktigste virksomhetene som understøtter kritiske samfunnsfunksjoner.[134]

I henhold til *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017) er det departementene som skal påse at det er etablert et sektorvist responsmiljø med operativt ansvar for å dekke virksomheter innenfor hele eller deler av departementets myndighetsområde.

[129] Riksrevisjonens dybdeundersøkelser.
[130] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT; verifisert intervju med Justis- og beredskapsdepartementet 28. juni 2022; verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[131] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[132] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[133] Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos (2022) *Retningslinjer for cybersamarbeid.*
[134] Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Fornyings-, administrasjons- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet,* s. 21.

Responsmiljøer for håndtering av digitale sikkerhetshendelser omtales ofte som CERT- eller CSIRT-miljøer. Se faktaboks 6 for begrepsforklaring.

Faktaboks 6 CERT/CSIRT

CERT står for *Computer Emergency Response Team*. CERT er et registrert varemerket eid av Carneige Mellon University, som tidligere sertifiserte responsmiljøer for håndtering av digitale sikkerhetshendelser over hele verden. Universitetet tilbyr imidlertid ikke lenger sertifisering utenfor USA. CERT-begrepet er derfor i stor grad blitt erstattet med EUs eget CSIRT-begrep, som står for *Computer Security Incident Response Team*. Flere av de norske responsmiljøene som er sertifisert etter den gamle ordningen, bruker imidlertid fortsatt CERT i navnet.

Enisa (2006) *CSIRT Setting up Guide in English* [Hentedato 5. april 2022].

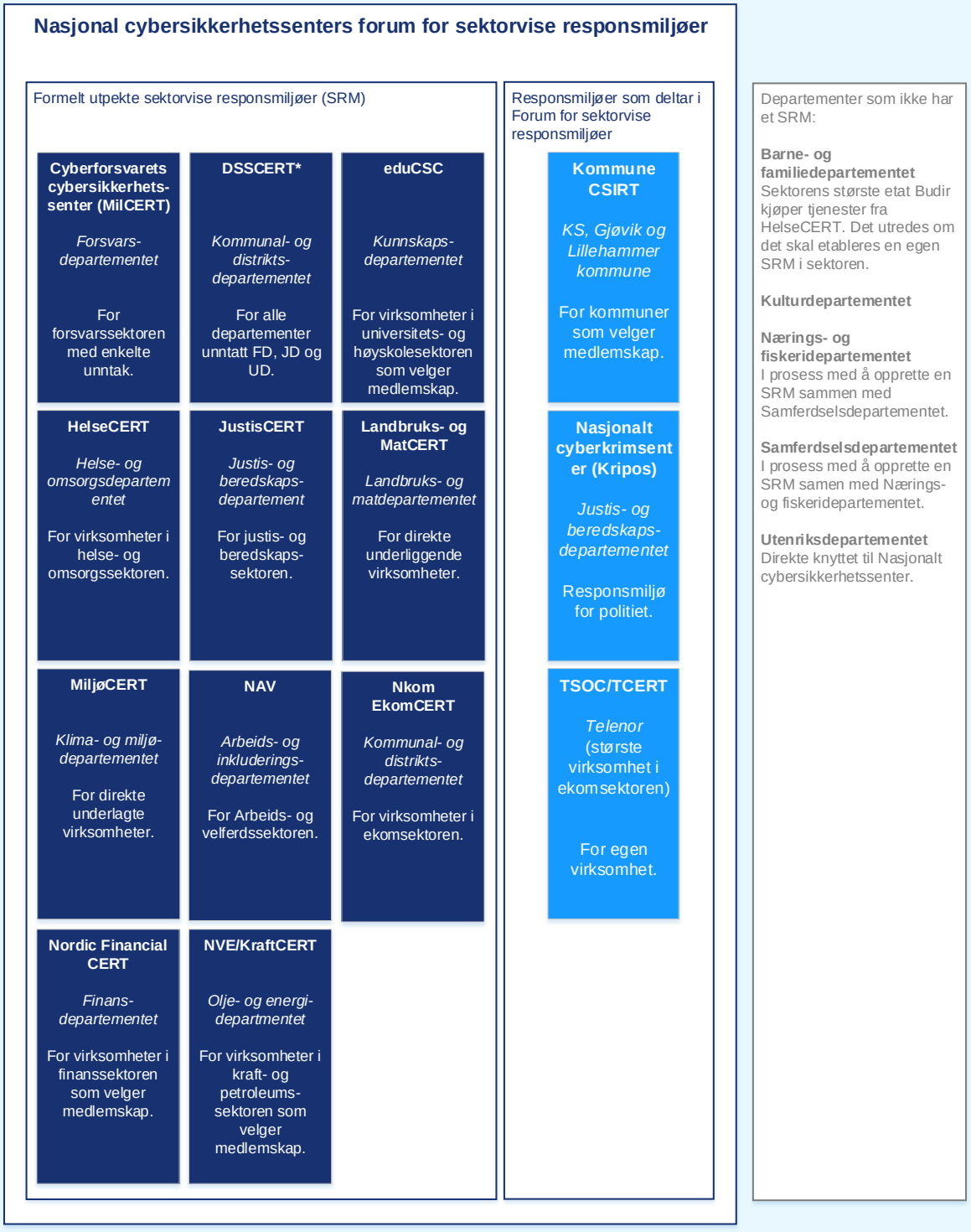
Flere av de etablerte CERT-/CSIRT-miljøene i Norge har etter 2012 fått status som sektorvise responsmiljøer. Begrepene *sektorvise responsmiljøer*, *CERT* og *CSIRT* blir derfor i stor grad brukt om hverandre. I den videre framstillingen bruker vi bare begrepene *sektorvist responsmiljø* eller *responsmiljø for håndtering av digitale sikkerhetshendelser* (forkortet *responsmiljø*), bortsett fra når CERT eller CSIRT er en del av egennavn.

De fleste departementene har opprettet et sektorvist responsmiljø for sektoren. Per september 2022 var det etablert elleve sektorvise responsmiljøer.[135] Alle de sektorvise responsmiljøene er partnere i Nasjonalt cybersikkerhetssenter. Senteret har etablert et eget forum for sektorvise responsmiljøer for å koordinere disse. Tanken er at responsmiljøene skal dele erfaringer og kompetanse seg imellom. For de sektorvise responsmiljøene er det også etablert en felles lynmeldingstjeneste for ugradert kommunikasjon, kalt IRC[136].[137] Nasjonal kommunikasjonsmyndighet forteller at det er mye kommunikasjon responsmiljøene imellom, og at det er viktig å opprettholde kontakten under normal drift, slik at aktørene kan jobbe godt sammen ved alvorlige hendelser.[138] Figur 3 gir en oversikt over den nasjonale strukturen for sektorvise responsmiljøer.

I tillegg til de sektorvise responsmiljøene er det etablert flere responsmiljøer for håndtering av digitale sikkerhetshendelser som ikke har status som sektorvise responsmiljøer. Disse responsmiljøene driftes av både private og offentlige virksomheter. Per juni 2021 var det etablert 23 slike miljøer i Norge. Tre av disse er ikke formelt utpekt av som sektorvist responsmiljø, men deltar likevel i Nasjonalt cybersikkerhetssenters forum for sektorvise responsmiljøer. Dette er KommuneCSIRT, Nasjonalt cyberkrimsenter og TelenorCERT.

[135] Justis- og beredskapsdepartementet (2022) *Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet*, E-post til Riksrevisjonen 12. september 2022.
[136] Forkortelse for *Internet Relay Chat.*
[137] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser,* s. 11–16.
[138] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 21. mai 2021.

Figur 3 Den nasjonale strukturen for sektorvise responsmiljøer



Kilde: Justis- og beredskapsdepartementet (2022) Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet, e-post til Riksrevisjonen 12. september 2022.

Enkelte sektorer mangler et sektorvist responsmiljø, mens andre sektorer fortsatt jobber med å etablere et slikt miljø. Her kan det blant annet nevnes at Samferdselsdepartementet og Nærings- og fiskeridepartementet arbeider med å etablere et felles responsmiljø. Det er også besluttet at det skal etableres et felles sektorvist responsmiljø for hele kommunesektoren.[139] Ifølge Justis- og beredskapsdepartementer vurderer Kommunal- og distriktsdepartementet blant annet en løsning der HelseCERT får funksjonen som felles responsmiljø for kommunesektoren.[140] I et gruppeintervju med representanter fra kommunesektoren kommer det fram at god hendelseshåndtering er en sentral forutsetning for å ivareta den digitale sikkerheten i kommunene. Flere av representantene mener at et felles kommunalt hendelseshåndteringsmiljø kunne ha vært et godt grep for å bedre den nasjonale digitale sikkerheten, da kommunenes evne til å håndtere hendelser varierer både med hensyn til kapasitet og modenhet.[141]

I sektorer der det ikke er identifisert et responsmiljø, er det i noen tilfeller etablert egne responsmiljøer for utvalgte deler av sektoren eller virksomheter i sektoren. I forsvarssektoren er det for eksempel ikke etablert et felles responsmiljø, men Cyberforsvarets cybersikkerhetssenter (MilCERT) fungerer som et responsmiljø for Forsvaret.[142]

Verken Barne- og likestillingsdepartementet, Kulturdepartementet eller Utenriksdepartementet har etablert et eget sektorvist responsmiljø. Barne- og familiedepartementet har imidlertid inngått et samarbeid mellom Barne-, ungdoms- og familiedirektoratet og HelseCERT.[143] Sektorer som mangler et sektorvist responsmiljø får en del av den sikkerhetsmessige overvåkingen og hendelseshåndteringen dekkes gjennom samarbeid med Nasjonalt cybersikkerhetssenter og deltakelse i VDI-sensornettverket. I intervju uttaler Nasjonal sikkerhetsmyndighet at de likevel mener at det i alle sektorer bør etableres sektorvise responsmiljøer i tråd med *Rammeverket for alvorlige IKT-sikkerhetshendelser*.[144]

Hvordan fungerer de sektorvise responsmiljøene?

De sektorvise responsmiljøene er svært forskjellige av karakter og tilbyr ulike tjenester. Enkelte av miljøene fungerer bare som koordinerende enheter ved digitale sikkerhetshendelser, mens andre miljøer bistår virksomheter med håndteringen slike hendelser. I tillegg tilbyr noen miljøer tjenester som sikkerhetsovervåking, rådgivning og veiledning.

I IKT-sikkerhetsutvalgets rapport fra 2018 pekes det på at ulikhetene mellom de sektorvise responsmiljøene bidrar til uklar ansvars- og rollefordeling ved håndtering av hendelser.[145] Også Justis- og beredskapsdepartementet poengterer at responsmiljøene har hatt ulik modenhet, og at noen har kommet lenger i arbeidet enn andre. Dette gjelder for eksempel finanssektoren, som har lagt vekt på digital sikkerhet over lengre tid. Departementene er dessuten organisert på ulike måter og har ulik grad av tilknytning til næringslivet. Disse ulikhetene gjenspeiles i de sektorvise responsmiljøene.[146]

I henhold til nærhetsprinsippet i samfunnssikkerhetsinstruksen skal digitale hendelser som hovedregel håndteres på lavest mulig nivå, det vil si i virksomheten eller i virksomhetens responsmiljø eller det sektorvise responsmiljøet. I de sektorene hvor det ikke er etablert et sektorvist responsmiljø, eller hvor det er responsmiljøer som ikke har status som sektorvist responsmiljø, forholder Nasjonalt cybersikkerhetssenter seg direkte til virksomheten som er rammet av angrepet.[147] Dersom det er

[139] Verifisert intervju med Kommunal- og distriktsdepartementet, 7. mai 2021.
[140] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[141] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[142] Justis- og beredskapsdepartementet (2022) *Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet*, E-post til Riksrevisjonen 12. september 2022.
[143] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet*, Justis- og beredskapsdepartementets innspill. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet*. Brev til Riksrevisjonen, 11. november 2022.
[144] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[145] NOU (2018:14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet,* s. 50.
[146] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[147] Verifisert intervju fra Nasjonal sikkerhetsmyndighet, 1. desember 2021.

etablert et sektorvist responsmiljø, skal dette responsmiljøet som hovedregel fungere som koordinerende enhet og håndtere kontakten mellom Nasjonalt cybersikkerhetssenter og virksomheten som er rammet. Det vurderes imidlertid i hvert enkelt tilfelle hva som er mest hensiktsmessig. Justis- og beredskapsdepartementet opplyser om at medlemmer av VDI-nettverket som oftest har direkte kontakt med Nasjonal sikkerhetsmyndighet.[148]

En av virksomhetene som deltok i dybdeundersøkelsene, uttaler at det er forstyrrende at kontakten med Nasjonal sikkerhetsmyndighet og Nasjonalt cybersikkerhetssenter må gå via det sektorvise responsmiljøet, og at de hadde foretrukket å ha direkte kontakt.[149] Kommunene må på sin side forholde seg til flere ulike sektorvise responsmiljøer, og dette kan tidvis være et hinder for god hendelseshåndtering, da koordineringen mellom de ulike responsmiljøene oppleves som svak.[150] Dersom responsmiljøet mangler kapasitet eller kompetanse til å håndtere hendelsen på en god nok måte, hender det at Nasjonalt cybersikkerhetssenter må håndtere hendelsen selv.[151]

Våren 2022 igangsatte Justis- og beredskapsdepartementet en evaluering av ordningen med sektorvise responsmiljøer. Formålet var blant annet å vurdere hvordan ordningen kan forbedres for å ivareta virksomhetenes og sektorenes behov og nasjonale behov. [152] Evalueringen ble gjennomført av KPMG, som leverte sin rapport 1. juli 2022.[153]

Evalueringen viser at samarbeidet mellom de involverte aktørene ser ut til å fungere godt, og at ordningen med sektorvise responsmiljøer har bidratt til et mer samlet digitalt sikkerhetsmiljø i Norge. Det går imidlertid fram at det er uklarheter knyttet til rolle- og ansvarsfordelingen ved håndteringen av hendelser. Videre skaper ulikhetene i organisering og virkemåte i noen tilfeller uklare ansvarsforhold for det sektorvise responsmiljøet. Den uklare ansvarsdelingen kan også skape risiko for at enkelte sektorer og/eller virksomheter ikke dekkes av et sektorvist responsmiljø. Evalueringen viser dessuten at det er ulike tolkninger av hvorvidt føringer som er gitt i *Rammeverk for håndtering av IKT-hendelser* fra 2017, er krav eller ment som veiledning. Evalueringen viser til at sektorprinsippet i forvaltningen skaper utfordringer for arbeidet med digital sikkerhet, som er sektorovergripende av natur. Det er også utfordrende at det i rammeverket ikke går fram hvilken rolle private leverandører av IKT-infrastruktur og andre kritiske samfunnstjenester skal ha i den overordnede modellen. Endelig er et utfordrende rekrutteringsmarked og begrenset tilgang på relevant kompetanse trukket fram som utfordringer.[154]

Basert på disse funnene anbefaler KPMG at et oppdatert rammeverk for digitale sikkerhetshendelser i større grad bør inkludere forebyggende arbeid med digital sikkerhet. Den nasjonale innsatsen bør samles for å sikre de grunnleggende nasjonale funksjonene. Dessuten bør det være sektorens behov som ligger til grunn for etableringen av et sektorvist responsmiljø. KPMG anbefaler videre at det fastsettes formelle minimumskrav for et utpekt sektorvist responsmiljø, og at de ulike aktørenes rolle i hendelseshåndteringen bør nyanseres og tydeliggjøres. Ifølge KPMG bør man tillate ulike løsninger etter hvor kritiske de tilhørende virksomhetene er for den nasjonale sikkerheten, og etter hvor omfattende konsekvenser en digital sikkerhetshendelse i disse virksomhetene vil ha. Videre bør arbeidet med å utforme sektorvise responsmiljøer knyttes til det pågående arbeidet med å identifisere grunnleggende nasjonale funksjoner og virksomheter som har vesentlig eller avgjørende betydning for disse. Det foreslås en tre-nivå-modell der samhandlingsnivået og minimumskravene øker med virksomhetenes betydning for de grunnleggende nasjonale funksjonene.[155]

[148] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet*, Justis- og beredskapsdepartementets innspill. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet*. Brev til Riksrevisjonen, 11. november 2022.
[149] Riksrevisjonens dybdeundersøkelser.
[150] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[151] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[152] *Referat Nettverk for nasjonal IKT-sikkerhet,* 9. mars 2022.
[153] KPMG (2022) *Evaluering av sektorvise responsmiljøer.*
[154] KPMG (2022) *Rapport: Evaluering av sektorvise responsmiljøer*, s. 2–3.
[155] KPMG (2022) *Rapport: Evaluering av sektorvise responsmiljøer*, s. 2–3.

4.2.3 Øvrig samarbeid på det digitale sikkerhetsområdet

Nasjonal kommunikasjonsmyndighet, Datatilsynet og Nasjonal sikkerhetsmyndighet understreker at det i tillegg til samordningsarenaene er et utstrakt samarbeid og løpende kontakt mellom etatene.[156] Nasjonal kommunikasjonsmyndighet mener at samordningsarenaer ikke alltid er den mest hensiktsmessige samarbeidsformen, da det digitale sikkerhetsarbeidet i flere tilfeller krever en rask reaksjon. I slike tilfeller kreves det mer spontan kontakt virksomhetene imellom.[157]

I denne sammenheng kan det vises til (se punktene i listen nedenfor) at det foregår mye bi- og trilateralt samarbeid mellom aktørene som har en rolle i arbeidet med digital sikkerhet i sivil sektor.

- Datatilsynet, Nasjonal sikkerhetsmyndighet og Digitaliseringsdirektoratet har faste møter hvor de utveksler kunnskap og erfaringer knyttet til veiledning innenfor informasjonssikkerhet i forvaltningen.[158]
- Nasjonal sikkerhetsmyndighet og Digitaliseringsdirektoratet har regelmessige møter for å koordinere aktiviteter og initiativ.
- Nasjonal sikkerhetsmyndighet samarbeider med flere FoU-miljøer.[159]
- Kunnskapsdepartementet har jevnlige temamøter med Universitetet i Oslo om informasjonssikkerhet.[160]
- Nasjonal kommunikasjonsmyndighet og Datatilsynet har jevnlige fagmøter,[161]
- og Forsvarsdepartementet og Justis- og beredskapsdepartementet har tett dialog om spørsmål knyttet til det digitale sikkerhetsarbeidet.[162]
- Det arrangeres en rekke konferanser, samlinger og lignende knyttet til digital sikkerhet, hvor offentlige og private virksomheter både er arrangører og deltakere. Direktoratet for samfunnssikkerhet og beredskap inviterer for eksempel direktorater, etater og statsforvaltere til samvirkekonferanser der formålet er å utveksle informasjon, slik at partene skal oppnå en felles situasjonsforståelse.
- Direktoratet for samfunnssikkerhet og beredskap arrangerer også beredskapsmøter med statsforvalterembetene ved hendelser av nasjonal betydning.[163]
- Nasjonal sikkerhetsmyndighet arrangerer en årlig sikkerhetskonferanse der formålet er nettverksbygging og tilby faglige oppdateringer om beste praksis.[164]
- Direktoratet for samfunnssikkerhet og beredskap og Nasjonal kommunikasjonsmyndighet har de siste årene jobbet med en konseptvalgutredning for framtidens nød- og beredskapskommunikasjon.[165]

Digitaliseringsdirektoratet opplyser i intervju at Datatilsynet og Nasjonal sikkerhetsmyndighet er blant deres primære samarbeidspartnere og kontaktpunkter. De tre etatene har faste møter og samarbeider også gjennom *Nettverk for veiledningsaktører* og egne dialogmøter. I tillegg samarbeider de med konkret utvikling av veiledninger innenfor digital sikkerhet.[166] Nasjonal sikkerhetsmyndighet og Datatilsynet oppgir i intervju at de i hovedsak finner samarbeidet godt og nyttig.[167] Datatilsynet har imidlertid opplevd at samarbeidet og koordineringen mellom etatene og eierdepartementene ikke alltid har vært god nok.[168] Datatilsynet har erfart at Kommunal- og distriktsdepartementet og Justis- og beredskapsdepartementet ikke alltid klarer å involvere de rette etatene og få til den nødvendige koordineringen. Datatilsynet mener dette er uheldig, men at det ikke får store konsekvenser for dem.

[156] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022; verifisert intervju med Datatilsynet, 17. februar 2022; verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2022.
[157] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[158] Verifisert intervju med Datatilsynet, 17. februar 2022.
[159] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[160] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[161] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[162] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[163] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[164] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[165] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[166] Verifisert intervjureferat Digitaliseringsdirektoratet, 3. desember 2021.
[167] Verifisert intervjureferat Nasjonal sikkerhetsmyndighet 1. desember 2021, UGRADERT; Verifisert intervju med Datatilsynet, 17. februar 2022.
[168] Verifisert intervju med Datatilsynet, 17. februar 2022.

Det kan imidlertid gjøre det vanskelig for virksomheter som må forholde seg til alle de ulike etatene som arbeider med digital sikkerhet.

4.3 Regelverk som er sentrale i arbeidet med digital sikkerhet

Justis- og beredskapsdepartementet forvalter både sikkerhetsloven og samfunnssikkerhetsinstruksen. Disse legger grunnlaget for arbeidet med nasjonal sikkerhet og samfunnssikkerhet, der digital sikkerhet er en integrert del. I det følgende presenterer vi regelverkenes formål og virkeområde. Se faktaboks 7 for en kort forklaring av de ulike sikkerhetsbegrepene. Vi omtaler flere andre relevante regelverk som angår digital sikkerhet, i kapittel 4.4, men sikkerhetsloven og samfunnssikkerhetsinstruksen inneholder de mest sentrale kravene for arbeidet med digital sikkerhet.

Faktaboks 7 Samfunnssikkerhet, statssikkerhet og nasjonal sikkerhet

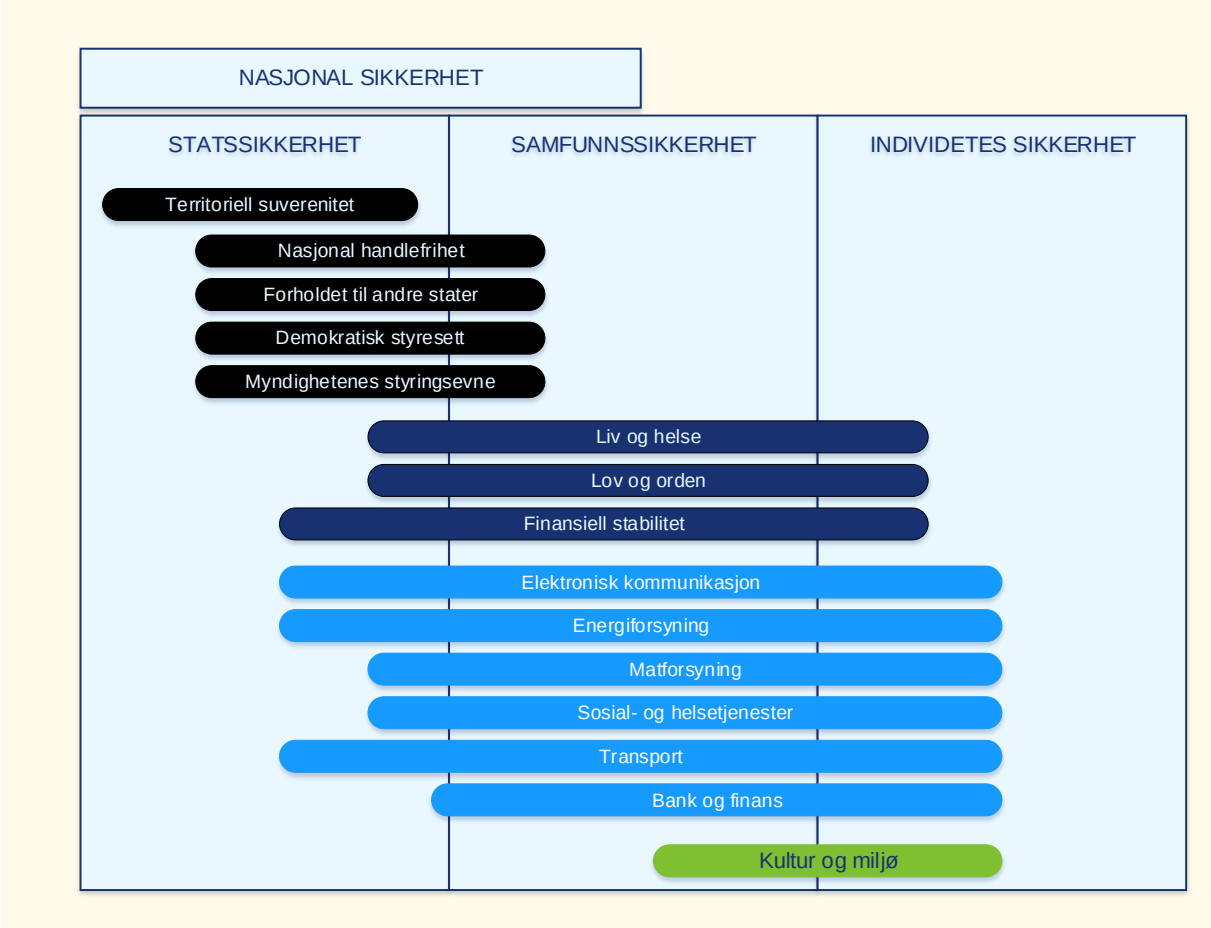
Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier som setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger. Myndighetens samfunnssikkerhetsarbeid reguleres gjennom samfunnssikkerhetsinstruksen.

Statssikkerhetens formål er å ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet. Statssikkerhet har tradisjonelt vært knyttet til forsvaret av territoriet mot væpnede angrep, men den kan også utfordres gjennom påvirkning med ulike andre former for pressmidler mot norske myndigheter og samfunnsaktører.

Samfunnssikkerheten og statssikkerheten er gjensidig avhengig av hverandre. Fremveksten av nye sikkerhetsutfordringer, herunder anslag fra ikke-statlige aktører, kan utfordre både samfunnssikkerheten og statssikkerheten. Aldri før har teknologi som kan true staters sikkerhet vært tilgjengelig for så mange. Dette gjør at skillet mellom samfunnssikkerheten og statssikkerhet blir mer utydelig, og det kan bli mer utfordrende å se hvem som egentlig treffes av en bestemt trussel.

Begrepet **nasjonal sikkerhet** defineres som statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser. De nasjonale sikkerhetsinteressene er angitt i sikkerhetslovens § 1-5.

Illustrasjonen på neste side viser forholdet mellom nasjonal sikkerhet, statssikkerhet, samfunnssikkerhet og individets sikkerhet.



Kilde: Prop. 153 L (2016−2017) Lov om nasjonal sikkerhet (sikkerhetsloven).

4.3.1 Sikkerhetsloven

Den nye sikkerhetsloven trådte i kraft i januar 2019. Den erstattet med dette den tidligere sikkerhetsloven, som ble kunngjort i 1998. Formålet med sikkerhetsloven er å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Videre skal den forebygge, avdekke og motvirke sikkerhetstruende virksomhet og bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.[169]

Sikkerhetsloven gjelder for alle statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. Loven kan også gjøres gjeldende for private rettssubjekter etter vedtak med hjemmel i § 1-3. Nasjonal sikkerhetsmyndighet er fag- og tilsynsmyndighet etter sikkerhetsloven. Nasjonal sikkerhetsmyndighet skal i henhold til loven koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden hos alle virksomheter underlagt sikkerhetsloven. Nasjonal sikkerhetsmyndighet har også det sektorovergripende ansvaret for at det forebyggende sikkerhetsarbeidet i virksomhetene utføres i samsvar med loven.[170]

I forarbeidene til den nye sikkerhetsloven vises det til at samfunnet har gjennomgått store endringer innenfor sikkerhetsområdet siden 2001. Risiko- og trusselbildet er mer sammensatt enn tidligere, med store teknologiske, demografiske og sikkerhetsmessige endringer. Den tiltakende digitaliseringen av samfunnet har også ført til behov for å gjøre enkelte endringer i reglene om informasjonssikkerhet.[171]

[169] *Prop. 153 L (2016−2017) Lov om nasjonal sikkerhet* (sikkerhetsloven).
[170] Forsvarsdepartementet og Justis- og beredskapsdepartementet (2019) *Hovedinstruks for Nasjonal sikkerhetsmyndighet*, 3. mars 2019.
[171] Innst. 103 L (2017–2018), s. 3.

Blant annet er begrepet *sikkerhetstruende virksomhet* bredere definert i den nye loven. Tidligere var begrepet definert som «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet», mens det nå er definert som «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser» (jf. sikkerhetsloven § 3-2).

Videre er begrepet *skjermingsverdig informasjon* utvidet i den nye loven. I den tidligere loven var begrepet knyttet til sikkerhetsgradert informasjon, og det var da utelukkende konfidensialitetsbehov som skulle vurderes. I den nye loven omfatter skjermingsverdig informasjon både informasjon som er sikkerhetsgradert, og som må beskyttes av konfidensialitetsbehov, og informasjon som må beskyttes av integritets- og tilgjengelighetsbehov.[172] I § 6-1 i den nye sikkerhetsloven heter det at et «informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner». Dette er en utvidelse av den tidligere loven som bare krevde at informasjonssystemer som behandlet sikkerhetsgradert informasjon, skulle beskyttes.[173]

Sikkerhetsloven stiller krav til departementenes forebyggende sikkerhetsarbeid. Av § 2-1 følger det at departementene skal identifisere og holde oversikt over *grunnleggende nasjonale funksjoner* − herunder tverrsektorielle grunnleggende nasjonale funksjoner – identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, og melde inn oversikt over disse til Nasjonal sikkerhetsmyndighet. Departementene skal i tillegg fatte vedtak om hvilke virksomheter loven skal gjelde for innenfor deres virkeområde. Dette gjelder virksomheter som behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller virksomheter som driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner (jf. § 1-3).

Faktaboks 8 Hva er en grunnleggende nasjonal funksjon?

Grunnleggende nasjonale funksjoner er definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser». Eksempler på grunnleggende nasjonale funksjoner er departementenes virksomhet, handlefrihet og beslutningsmyndighet, helseberedskap (Helse- og omsorgsdepartementet), lov og orden (Justis- og beredskapsdepartementet) og norsk utenrikstjeneste (Utenriksdepartementet).

Tverrsektorielle grunnleggende nasjonale funksjoner er funksjoner som inngår i flere departementers ansvarsområder, og der det ikke er ett departement som har hovedansvaret for området som funksjonen inngår i. Eksempler på innmeldte tverrsektorielle grunnleggende nasjonale funksjoner er satellittbasert kommunikasjon, romværvarslingstjenesten og matvareforsyning.

Kilde: Sikkerhetsloven § 1-5 nr. 2; Nasjonal sikkerhetsmyndighet (2021) *Oversikt over innmeldte grunnleggende nasjonale funksjoner* [Hentedato 8. mars 2022].

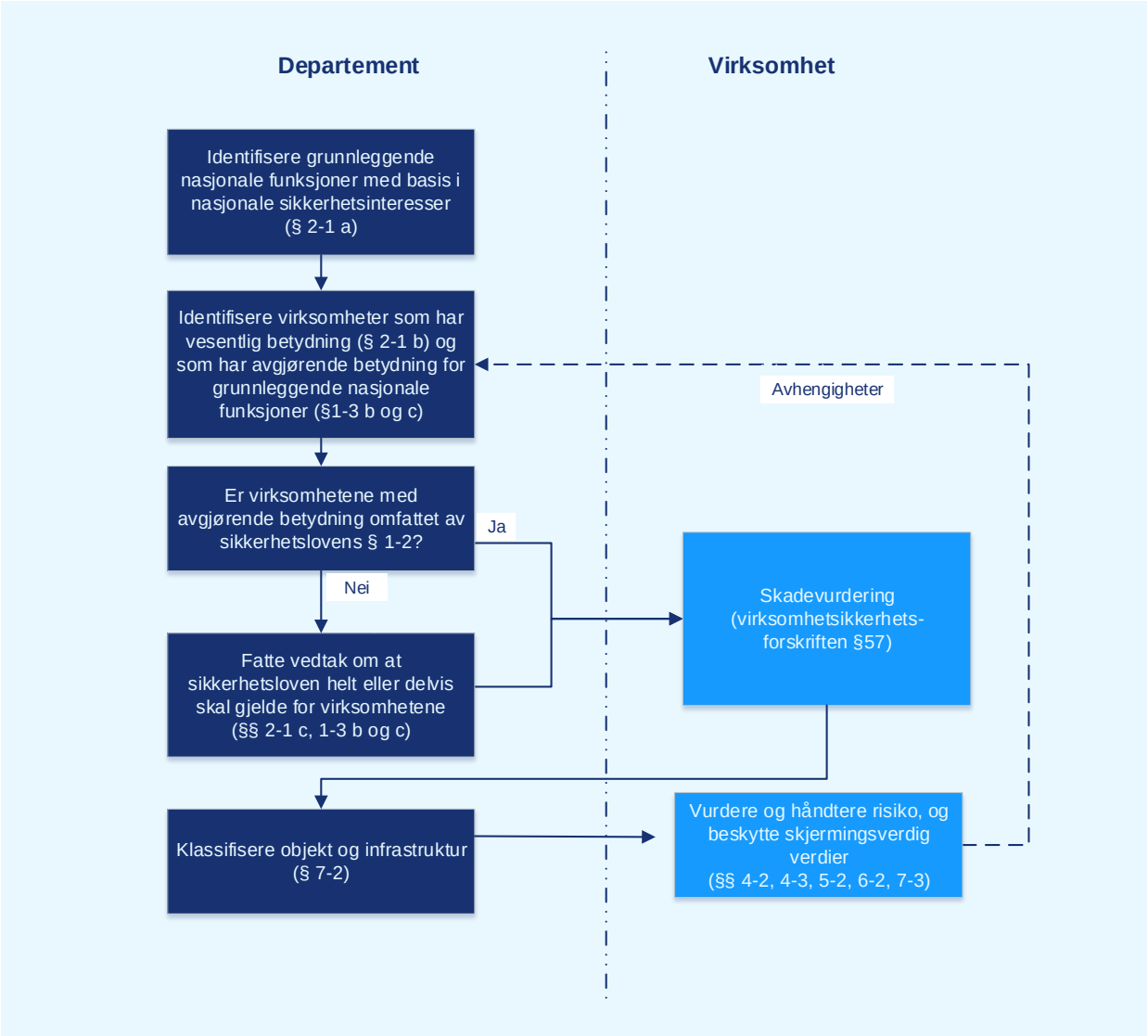
Som en del av virksomhetens risikovurdering skal virksomheten regelmessig kartlegge hvilke andre virksomheter den er avhengig av for å fungere som den skal (jf. sikkerhetsloven § 4-2). Virksomhetssikkerhetsforskriften gjelder dermed for virksomheter som omfattes av sikkerhetsloven. Forskriften angir at en virksomhet som vurderer risiko, skal ta hensyn til hvilken betydning virksomhetens skjermingsverdige verdier har for grunnleggende nasjonale funksjoner (jf.

[172] Med *konfidensialitet* menes at det har en verdi at informasjonen ikke blir kjent for uvedkommende. Med *integritet* menes at det har en verdi at informasjonen er korrekt. Med *tilgjengelighet* menes at det har en verdi at informasjonen er tilgjengelig ved behov. Prop. 153 L (2016–2017), s. 88.
[173] Prop. 153 L (2016–2017) s. 8 og 178.

virksomhetssikkerhetsforskriften § 12). Dersom virksomheten er avhengig av andre virksomheter for å fungere slik den skal, skal en oversikt sendes til Nasjonal sikkerhetsmyndighet og det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren (jf. virksomhetssikkerhetsforskriften § 13 siste ledd).

Basert på en risikovurdering skal virksomheter som er underlagt sikkerhetsloven, i neste omgang beskytte informasjonssystemene, objektene og infrastrukturen de har pekt ut, mot redusert funksjonalitet, skadeverk, ødeleggelse eller rettsstridig overtakelse. De skal også ta hensyn til utpekte avhengigheter. På dette grunnlaget skal virksomhetene iverksette sikkerhetstiltak for å oppnå et forsvarlig sikkerhetsnivå (jf. sikkerhetsloven kapittel 5.2). Se Figur 4 for en illustrasjon av prosess for arbeid med forebyggende nasjonal sikkerhet, og hvordan ansvaret for de ulike delene av prosessen fordeler seg mellom departements- og virksomhetsnivå.

Figur 4 Prosess for arbeid med forebyggende nasjonal sikkerhet



Kilde: Nasjonal sikkerhetsmyndighet (u.å.) *Virksomheter av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner.*

Ifølge sikkerhetsloven § 2-4 skal Nasjonal sikkerhetsmyndighet drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur. Virksomheter som er underlagt sikkerhetsloven, plikter å varsle Nasjonal sikkerhetsmyndighet dersom virksomheten er rammet av eller har begrunnet mistanke om sikkerhetstruende virksomhet, og ved alvorlige brudd på sikkerhetskravene (jf. sikkerhetslovens § 4-5).

Implementeringen av sikkerhetsloven er forsinket i henhold til Justis- og beredskapsdepartementets framdriftsplan. I kapittel 5.2 utdyper vi dette, og konsekvensene av forsinkelsen, nærmere.

4.3.2 Samfunnssikkerhetsinstruksen

Samfunnssikkerhetsinstruksen trådte i kraft i 2017 og setter krav til departementenes arbeid med samfunnssikkerhet. Formålet med instruksen er å styrke samfunnets evne til å forebygge kriser og til å håndtere alvorlige hendelser gjennom et helhetlig og koordinert arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen, kapittel I).

Instruksen består av én del som er rettet mot alle departementer, og én del som er rettet mot departementer med hovedansvar for samfunnets kritiske funksjoner. Instruksen regulerer videre Justis- og beredskapsdepartementets samordningsrolle når det gjelder forebygging og beredskap på samfunnssikkerhetsområdet og departementets ansvar for å føre tilsyn.

Justis- og beredskapsdepartementet har et generelt samordningsansvar for samfunnssikkerhet og beredskap i sivil sektor. Dette omfatter blant annet å definere hvilke samfunnsfunksjoner som i et tverrsektorielt perspektiv er å anse som kritiske.

Faktaboks 9 Hva er samfunnets kritiske funksjoner?

En samfunnsfunksjon er definert som kritisk hvis bortfall av den får konsekvenser som truer befolkningens og samfunnets grunnleggende behov. Befolkningens og samfunnets grunnleggende behov kan defineres som ivaretakelse av grunnleggende samfunnsverdier som liv og helse, natur og miljø, økonomi, samfunnsstabilitet, styringsevne og kontroll.

Samfunnsfunksjonene står i stor grad i et avhengighetsforhold til hverandre. Svikt i en funksjon vil i mange tilfeller forplante seg til andre funksjoner.

Kilde: Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner*.

Det følger av samfunnssikkerhetsinstruksen at departementenes arbeid med samfunnssikkerhet skal være basert på systematisk risikostyring. Et departementet skal kunne dokumentere at det avklarer og beskriver sentrale roller og ansvarsområder innenfor samfunnssikkerhet i sektoren, gjør systematiske risiko- og sårbarhetsanalyser av hendelser som kan true sektorens funksjonsevne, iverksetter nødvendige kompenserende tiltak og utarbeider mål for samfunnssikkerhetsarbeidet i sektoren.

Departementet skal ivareta ansvaret for krisehåndtering i sektoren, som blant annet innebærer å ha et planverk for håndtering av uønskede hendelser og sørge for at det øves målrettet i egen sektor og tverrdepartementalt. Som ansvarlig for kritisk infrastruktur skal departementet også sørge for at det utarbeides risiko- og sårbarhetsanalyser for sektoren, og ha oversikt over tilstanden knyttet til sårbarheter.[174]

I kapittel 5.5 ser vi nærmere på status- og tilstandsvurderingene og departementenes arbeid med risiko- og sårbarhetsanalyser etter kravene i samfunnssikkerhetsinstruksen.

4.3.3 Rammeverk for grunnleggende nasjonale funksjoner og samfunnets kritiske funksjoner

Myndighetene har ulike rammeverk for å identifisere grunnleggende nasjonale funksjoner og tilhørende avhengigheter og for å identifisere samfunnets kritiske funksjoner og understøttende

[174] Samfunnssikkerhetsinstruksen, del 4 og 5; Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*.

virksomheter. Direktoratet for samfunnssikkerhet og beredskap utgav *Veileder for samfunnets kritiske funksjoner* i 2016, mens Nasjonal sikkerhetsmyndighet utgav *Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner* i 2020. Veilederne redegjør for sentrale begreper og metoder i prosessen med å identifisere og vurdere de nevnte funksjonene og tilhørende avhengigheter / understøttende virksomheter.

Grunnen til at det er etablert to rammeverk, er at rammeverket for samfunnets kritiske funksjoner gjelder samfunnssikkerhet, mens rammeverket for grunnleggende nasjonale funksjoner gjelder nasjonal sikkerhet. *Nasjonal sikkerhet* er definert som statssikkerhet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.[175] Se faktaboks 7 for en nærmere beskrivelse av begrepene. Som følge av at disse områdene overlapper, er det også deler av samfunnets kritiske funksjoner som overlapper med grunnleggende nasjonale funksjoner.[176] Nasjonal sikkerhetsmyndighet oppfordrer derfor departementene om å benytte Direktoratet for samfunnssikkerhet og beredskaps rammeverk for samfunnets kritiske funksjoner i arbeidet med å identifisere og vurdere grunnleggende nasjonale funksjoner.[177]

Direktoratet for samfunnssikkerhet og beredskap viser også til at rammeverkene har ulike formål, og at det er ulik grad av forpliktelse knyttet til rammeverkene. Sikkerhetsloven har et mer begrenset virkeområde. Et kriterium for identifisering av en samfunnsfunksjon som kritisk er at et avbrudd i syv døgn eller mindre vil true befolkningens grunnleggende behov. For grunnleggende nasjonale funksjoner gjelder ikke dette tidskriteriet. Dermed kan sikkerhetsloven ha et virkeområde som omfatter flere og mer av funksjonene enn rammeverket for samfunnets kritiske funksjoner.[178] Det kreves derfor mer av virksomheter som understøtter en grunnleggende nasjonal funksjon enn samfunnets kritiske funksjoner. Dette skyldes også sikkerhetshetslovens krav til sikkerhet og tilsynsvirksomheten.

Hovedformålet med rammeverket for samfunnets kritiske funksjoner er å få oversikt over og informere om hvilke funksjoner det er viktig for samfunnet å opprettholde, og hvordan disse funksjonene henger sammen på tvers av virksomheter og sektorer. Videre bemerker Direktoratet for samfunnssikkerhet og beredskap at det ikke finnes et tverrsektorielt regelverk som stiller særskilte krav til virksomheter som understøtter samfunnets kritiske funksjoner. Sikkerheten i disse funksjonene reguleres hovedsakelig gjennom ulike sektorregelverk.[179]

Direktoratet for samfunnssikkerhet og beredskap er i ferd med å revidere rammeverket for samfunnets kritiske funksjoner. Dette gjøres i samspill med Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet. Alle departementene har levert innspill til revisjonen. Innspillene omhandler blant annet oppdatering av eksisterende og etablering av nye kritiske samfunnsfunksjoner.[180]

Ifølge Direktoratet for samfunnssikkerhet og beredskap har det skapt en del forvirring i departementene at myndighetene opererer med to ulike rammeverk. For å løse dette har Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet også samarbeidet om å utarbeide en beskrivelse av forholdet mellom de to rammeverkene. Samtidig vurderes om det skal utarbeides et felles rammeverk for samfunnets kritiske funksjoner og grunnleggende nasjonale funksjoner. Ifølge direktoratet må dette også ses i sammenheng med NATOs syv krav til nasjonal beredskap og implementeringen av EUs *Direktivet om tiltak for et høyt felles sikkerhetsnivå i nettverk og informasjonssystemer i hele Unionen* (NIS-direktivet)[181] Formålet med EU-direktivet er å etablere et

[175] Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden*, s. 11.
[176] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[177] Nasjonal sikkerhetsmyndighet (2020) *Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner.*
[178] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[179] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[180] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[181] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.

tverrsektorielt regelverk med særskilte krav til virksomheter som understøtter kritiske samfunnsfunksjoner i EU, inkludert samarbeidsland som Norge. IKT-sikkerhetsutvalget (2018) støttet et slikt forslag.[182] Se faktaboks 10 og 11 for mer om NATOs syv krav og NIS-direktivet.

Faktaboks 10 NATOs syv krav til nasjonal beredskap («7 baselines»)

NATOs syv krav har som formål å sikre sivil beredskap og at NATOs forsvar samsvarer med dagens sikkerhetstrusler. Ifølge NATO-kravene skal den nasjonale beredskapen:

- sikre kontinuiteten i regjeringen og kritiske offentlige tjenester
- sikre robuste energiforsyninger
- ha evne til å håndtere ukontrollert bevegelse av mennesker effektivt
- sørge for motstandsdyktige mat- og vannressurser
- ha evne til å håndtere masseskader
- sørge for robuste sivile kommunikasjonssystemer
- sørge for robuste sivile transportsystemer

Kilde: NATO (2019) *Resilience: the first line of defence* [Hentedato 22. mars 2022].

Faktaboks 11 EUs NIS-direktiv om tiltak for nettverks- og informasjonssikkerhet

Bakgrunnen for NIS-direktivet er et behov for mer tilstrekkelige og helhetlige beskyttelsestiltak i EU på tvers av sektorer og ulike typer infrastruktur. Direktivet pålegger medlemsstatene å sørge for et visst digitalt sikkerhetsnivå gjennom blant annet å utarbeide en nasjonal strategi for digitalt sikkerhetsarbeid, etablere en digital sikkerhetsberedskapsenhet og pålegge operatører og leverandører av samfunnskritiske tjenester digitale sikkerhetskrav og varslingsplikt ved alvorlige digitale sikkerhetshendelser. I 2020 la kommisjonen fram et forslag til et nytt direktiv, NIS2, som skal erstatte det tidligere direktivet. Med NIS2 innlemmes flere sektorer, og EU ønsker blant annet å stille strengere krav til prosessen for digital hendelseshåndtering. Det er også foreslått å innføre krav om grunnleggende sikkerhetselementer som skal ligge til grunn for sikkerhetsarbeidet.

Regjeringen besluttet i 2016 å implementere NIS-direktivet og et utkast til lov som gjennomfører direktivet i norsk rett var på høring i 2018. Høringsuttalelsene ga tydelig uttrykk for et ønske om en felles digital sikkerhetslov. Per mars 2022 var den nasjonale proposisjonen som omhandler direktivet i norsk rett, ennå ikke fremmet. Ifølge Justis- og beredskapsdepartementet er framdriften redusert som følge av annet lovarbeid som må prioriteres, og det er usikkert når proposisjonen vil bli fremmet.

Kilde: EØS-notatbasen (2016) *NIS-direktivet* [Hentedato 22. mars 2022]; Meld. St. 5 2020–2021 *Samfunnssikkerhet i en usikker verden*; Møtereferat Nettverk for nasjonal IKT-sikkerhet, 9. mars 2022.

[182] NOU (2018:14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*

4.4 Samordning av regelverket for digital sikkerhet

Som nevnt finnes det en rekke regelverk som direkte omhandler eller som berører virksomheters arbeid med digital sikkerhet. Overordnet kan regelverkene deles inn i generelle lover, for eksempel sikkerhetsloven og personopplysningsloven, og sektorspesifikke lover, for eksempel energiloven og helseregisterloven.[183] Vi har identifisert og gjennomgått seks generelle og 15 sektorspesifikke lover med tilhørende forskrifter. Gjennomgangen med tilhørende analyse presenteres i det følgende.

Vi har gått gjennom regelverkene for å undersøke graden av samordning mellom dem. Med samordning av regelverk menes at ulike regelverk skal utfylle og supplere hverandre framfor å overlappe hverandre eller være motstridende med hensyn til innholdet. Samordningen skal forenkle rettsanvendelsen. Vi har i intervjuer også innhentet erfaringer med etterlevelsen av regelverkskravene.

I *samfunnssikkerhetsmeldingen* (2020) går det fram at det er en målsetting at etatene som har ansvar for oppfølgingen av den digitale sikkerheten, opptrer koordinert, og at Justis- og beredskapsdepartementet skal bidra til at rådgivnings- og veiledningsaktiviteter innenfor digital sikkerhet koordineres på en bedre måte. All veiledning springer ut av regelverkskravene, og dermed er det viktig at regelverkskravene framstår samordnet fra et brukerperspektiv.[184]

Regelverkene for digital sikkerhet har i flere sammenhenger blitt kritisert for å være omfattende og uoversiktlige fra et brukerperspektiv. Vår undersøkelse viser også dette. Regelverkskravene er ikke motstridende, men de overlapper. Brukerne opplever dessuten at det er kompetanse- og ressurskrevende å etterleve de funksjonsbaserte bestemmelsene. Dette er noe myndighetene i varierende grad tar hensyn til.

4.4.1 Tidligere påpekte utfordringer med samordning av regelverket

Det har gjennom årene vært nedsatt en rekke utvalg som har undersøkt lovgivningen på informasjonssikkerhetsområdet, herunder Seip-utvalget[185], styrings- og arbeidsgruppene for samordning av regelverk for beskyttelse av informasjon[186] og Willoch-utvalget.[187] Overlapp i regelverket for digital sikkerhet / informasjonssikkerhet har vært tematisert i en årrekke. I 2005 ble det satt ned en arbeidsgruppe for regelverk og informasjonssikkerhet, som på oppdrag fra Koordineringsutvalget for informasjonssikkerhet skulle utarbeide en oversikt over regelverket for informasjonssikkerhet og identifisere begrensninger i regelverket. Arbeidsgruppen ble også bedt om å komme med anbefalinger til forbedringer.

Arbeidsgruppen for regelverk og informasjonssikkerhet pekte på at det er mange og til dels omfattende overlapp mellom og manglede koordinering av regelverkene, og at lovgivningen er fragmentert. Arbeidsgruppen konkluderte med at det er utfordrende for brukere av regelverket å tyde hva som ligger i skjønnsmessige begreper som *tilstrekkelig sikret*, *tilfredsstillende* eller *forholdsmessig sikkerhet*. Arbeidsgruppen hevdet også at brukere av regelverket opplever det vanskelig å finne fram til regelverkskravene som angår dem, fordi de er spredt i ulike lover, forskrifter, instrukser og andre rettskilder. En annen type kritikk handlet om at rettsreglene har økt i volum og omfang og slik sett bidratt til unødvendig byråkrati og juridiske barrierer. Arbeidsgruppen trakk fram eksempler som uklare roller, omfattende krav som er krevende å etterleve, og mange tilsynsorganer på området.[188] I 2005

[183] Se vedlegg 1 for fullstendig oversikt over regelverk vi har identifisert og gjennomgått.
[184] Meld. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden.*
[185] NOU (1986: 12) *Datateknikk og samfunnets sårbarhet*.
[186] Rapport fra en arbeidsgruppe nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet, desember 1991: *Samordning av regelverk for beskyttelse av informasjon*.
[187] NOU (2000: 24) *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.*
[188] Arbeidsgruppen regelverk og informasjonssikkerhet; oversikt og forslag til KIS AE/MHa 21.09.2005.

var det utfordrende for brukerne å se sammenhengen mellom regelverkene. Dette gjaldt særlig kommunene, som også da måtte forholde seg til en rekke ulike regelverk for informasjonssikkerhet.[189]

Riksrevisjonens undersøkelse fra 2006 om myndighetenes arbeid med å sikre IT-infrastruktur viste at det kan være krevende for brukerne å forstå samspillet mellom regelverkene. Flere etater og bransjeorganisasjoner som inngikk i undersøkelsen, pekte på forhold ved regelverket som vanskeliggjør samordning. Informantene mente at mange av de administrative problemene som gjelder ansvarsforhold, bunner i et til dels sprikende regelverk.[190]

Grupper underlagt Koordineringsutvalget for informasjonssikkerhet har i årene etter at arbeidsgruppen ble nedsatt, arbeidet med tiltak for å få bukt med inkonsekvent begrepsbruk i regelverk og rammeverk for klassifisering og beskyttelse av informasjon. I *Dokument 1 (2014–2015)* vurderte Riksrevisjonen imidlertid at departementets ambisjon om å forenkle og harmonisere regelverket ikke var realisert.[191]

I *Nasjonal strategi for informasjonssikkerhet* fra 2012 ble det pekt på overlapp mellom flere regelverk for digital sikkerhet, og strategien la vekt på at regelverket skulle samordnes bedre. Strategien problematiserte også at det ikke finnes ett sett med minimumskrav for sikkerhetsprosedyrer eller tekniske sikkerhetstiltak for statlig sektor.[192] IKT-sikkerhetsutvalget viser også i NOU (2018: 14) *IKT-sikkerhet i alle ledd* til at få regelverk stiller direkte krav til digital sikkerhet. Ifølge utvalget var det i mange tilfeller uklart om lovene og forskriftene faktisk stiller krav om forsvarlig digital sikkerhet, for eksempel når loven viser til krav om *forsvarlig sikkerhet*. Utvalget antok at det var krevende for brukerne å vurdere hvorvidt kravene omfatter digital sikkerhet. IKT-sikkerhetsutvalget antok også at det var krevende for brukerne å vurdere hvilke tekniske og organisatoriske tiltak som må gjennomføres for å oppnå forsvarlig sikkerhet etter regelverkene. Utvalget pekte på at disse forholdene forutsetter at både underlagte virksomheter og tilsynsmyndigheter har høy digital sikkerhetskompetanse.[193]

Også i høringssvarene til forslaget om å gjennomføre NIS-direktivet i norsk lov i 2018 pekte flere av høringsinstansene på hvor viktig det er med god samordning mellom regelverkene, og at de per 2018 opplevde at det var mye overlapp. Særlig næringslivet pekte på viktigheten av stabile rammebetingelser og klare forventninger i lovverket for det digitale sikkerhetsarbeidet.[194]

4.4.2 Regelverket inneholder ikke motstridende bestemmelser

Vi har som nevnt gått gjennom regelverkene etter det juridiske kriteriet om samordning. For at regelverkene skal virke etter hensikten, er det viktig at de som er underlagt regelverket forstår det materielle innholdet i bestemmelsene. De fleste virksomheter er underlagt flere regelverk for digital sikkerhet. Derfor er det avgjørende at regelverkene utfyller og supplerer hverandre framfor at de er motstridende med hensyn til innholdet.

Vi har ikke identifisert motstridende bestemmelser i regelverksgjennomgangen. Bestemmelsene i sektorregelverket er i stor grad de samme som bestemmelsene i det overordnede regelverket, bortsett fra at formuleringene i sektorregelverket om mulig er mer konkrete. På dette området tilsvarer graden av samordning trinn tre i samordningsstigen til Direktoratet for økonomistyring – å unngå å svekke andres måloppnåelse.

Nasjonal sikkerhetsmyndighet forteller i intervju at de på tross av overlapp mellom sikkerhetsloven og sektorregelverket ikke opplever at det er motstrid mellom regelverkskravene. På grunn av overlappet

[189] Arbeidsgruppen regelverk og informasjonssikkerhet; oversikt og forslag til KIS AE/MHa 21.09.2005.
[190] Dokument nr. 3:4 (2005–2006) *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur.*
[191] Dokument 1 (2010–2011) *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2009.*
[192] Fornyings- administrasjons- og kirkedepartementet, Forsvarsdepartementet, Justis- og beredskapsdepartementet og Samferdselsdepartementet (2012) *Nasjonal strategi for informasjonssikkerhet*.
[193] NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*
[194] Justis- og beredskapsdepartementet (2018) Høring – NOU 2018: 14 *IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*.

vil antakelig en virksomhet som oppfyller kravene i sektorregelverket, også oppfylle kravene i sikkerhetsloven.[195]

4.4.3 Det er mye tematisk overlapp i regelverket

Regelverksbestemmelsene om digital sikkerhet er ikke i motstrid. Gjennomgangen vår viser imidlertid at det er mye tematisk overlapp mellom regelverkene. Dette bemerkes også av Nasjonal sikkerhetsmyndighet.[196] For eksempel inneholder både sikkerhetsloven, samfunnssikkerhetsinstruksen, personopplysningsloven, sivilbeskyttelsesloven og eForvaltningsforskriften krav om risiko-/sikkerhetsstyring og IKT-sikkerhetstiltak.

Av det sektorspesifikke regelverket inneholder 10 av 15 lover krav om digitale sikkerhetstiltak. Sektorregelverkene er naturligvis tilpasset ulike virksomheter og er ment å treffe smalere enn de generelle lovene, men det er mange virksomheter, særlig kommuner, som omfattes både av generelt og sektorspesifikt regelverk for digital sikkerhet. Det kan være krevende for brukerne å forholde seg til flere regelverk som helt eller delvis berører de samme forholdene, tidvis med ulike vinklinger. Det kan også være krevende fra et brukerperspektiv, å manøvrere i et landskap med ulike regelverksforvaltere.

Faktaboks 12 Hvordan utspiller overlappet seg i praksis?

Et eksempel på en virksomhet som omfattes både av generelt og sektorspesifikt regelverk, er politiet. Politiet må for eksempel forholde seg til at kravene i politiregisterloven overlapper med innholdet i eForvaltningsforskriftens krav om sikkerhetsstrategi (styring) for informasjonssikkerhet. Samtidig reguleres informasjonssikkerheten gjennom politiregisterforskriftens kapittel 39 om internkontroll og kapittel 40 om informasjonssikkerhet.

Det samme gjelder for virksomheter i helse- og omsorgssektoren, som må forholde seg til krav om informasjonssikkerhet i pasientjournalloven, helseregisterloven, personopplysningsloven og eForvaltningsforskriften. Dersom disse virksomhetene i tillegg er underlagt sikkerhetsloven, vil ne nevnte kravene også overlappe med kapittel 4 om forebyggende sikkerhetsarbeid (herunder sikkerhetsstyring og vurdering av risiko) og kapittel 5 om informasjonssikkerhet.

Kilde: Politiregisterloven, eForvaltningsforskriften, pasientjournalloven, helseregisterloven og sikkerhetsloven

I intervju med representanter fra kommunesektoren, kom det fram at de synes regelverket for digital sikkerhet er omfattende, og at det er krevende å få oversikt over gjeldende bestemmelser. De synes også at det er utfordrende å se lovverket som er knyttet til de ulike sektorene i sammenheng, for eksempel å se bestemmelser om internkontroll i sammenheng med bestemmelser om risikostyring og sikkerhetstiltak.[197]

Et konkret eksempel på slike utfordringer, som i dette tilfellet handler om hvilke deler av kommunen som er underlagt sikkerhetsloven, og hvordan sikkerhetsloven og et sektorspesifikt lovverk fungerer sammen, gjelder områdene helse og vann og avløp i en kommune. Helse- og omsorgsdepartementet har utpekt helsetjenester til befolkningen som en grunnleggende nasjonal funksjon. Samtidig har kommunen fått beskjed fra Kommunal- og distriktsdepartementet om at vann- og avløpssystemet i kommunen ikke er stort nok til å defineres som en grunnleggende nasjonal funksjon, mens helse- og omsorgstjenestene understreker at vann- og avløpssystemet i kommunen er avgjørende for driften av helsetjenestene. Generelt etterlyser representantene for kommunesektoren en mer sentral beslutning

[195] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[196] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[197] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.

om hvordan kommunene skal forholde seg til sikkerhetsloven, og hvordan avhengigheter mellom sektorer skal defineres.[198]

Ifølge Schartum (2005)[199] kan det virke skjerpende at krav gjentas på tvers av lovverk. Det kan på sett og vis fremme samordning fordi like regler kan skape en felles aksept og forventning om lik rettsanvendelse. Like regelverk er også positivt fra et styringsperspektiv. En fordel med større grad av likhet mellom regelverk kan være at de ulike aktørene og sektorene anser reglene som «sine», samtidig som det foregår en form for samordning. Samordningseffekten kan imidlertid avta etter hvert som de ulike aktørene setter sitt preg på forståelsen av bestemmelsene.[200] I høringssvarene til forslaget om å gjennomføre NIS-direktivet i norsk lov er det flere som framhever at en slik lov må være tilpasset de ulike sektorene, samtididig som det er viktig at man oppnår en enhetlig forståelse og rettsanvendelse på tvers av sektorene.[201] Det kommer også fram at overlappet mellom regelverkene i dag ikke har direkte negative konsekvenser for høringsinstansene. Når NIS-direktivet blir en del av norsk lov, vil det imidlertid være viktig at man etterstreber en helhetlig koordinering og får klarhet i hvordan en slik lov skal ses opp mot det eksisterende regelverket for digital sikkerhet.[202]

4.4.4 Det er krevende å etterleve de funksjonsbaserte regelverkskravene

Regelverksgjennomgangen viser at kravene både i generelt og sektorspesifikt regelverk i hovedsak er funksjonsbaserte. Dette innebærer at regelverket i stor grad gir virksomheten ansvar for å bedømme sin egen risiko og iverksette nødvendige sikkerhetstiltak for å håndtere denne risikoen. Funksjonsbaserte regelverk egner seg godt for områder i rask utvikling, som digital sikkerhet. Med slike regelverk trenger man nemlig ikke å endre kravene i regelverket hver gang det skjer endringer i teknologien. Ifølge Nasjonal kommunikasjonsmyndighet er det viktig og nødvendig med funksjonelle bestemmelser ettersom utviklingen på det digitale sikkerhetsområdet går raskt. Dersom regelverket er for detaljert, vil det fort bli utdatert, mener Nasjonal kommunikasjonsmyndighet.[203]

Faktaboks 13 Hva er et funksjonsbasert regelverk?

Et funksjonsbasert regelverk fastslår hva slags sikkerhetsnivå som skal oppnås, men ikke hvordan. Det er opp til virksomheten selv å innfri kravene på den måten de anser som den beste. Hensikten bak et funksjonsbasert regelverk er blant annet å unngå detaljstyrende bestemmelser og synliggjøre aktørenes ansvar for å finne løsningene. Dette skal tilrettelegge for fleksibilitet i valg av metoder, framgangsmåter og teknologiutvikling, slik at løsningene best kan tilpasses den enkelte virksomheten.

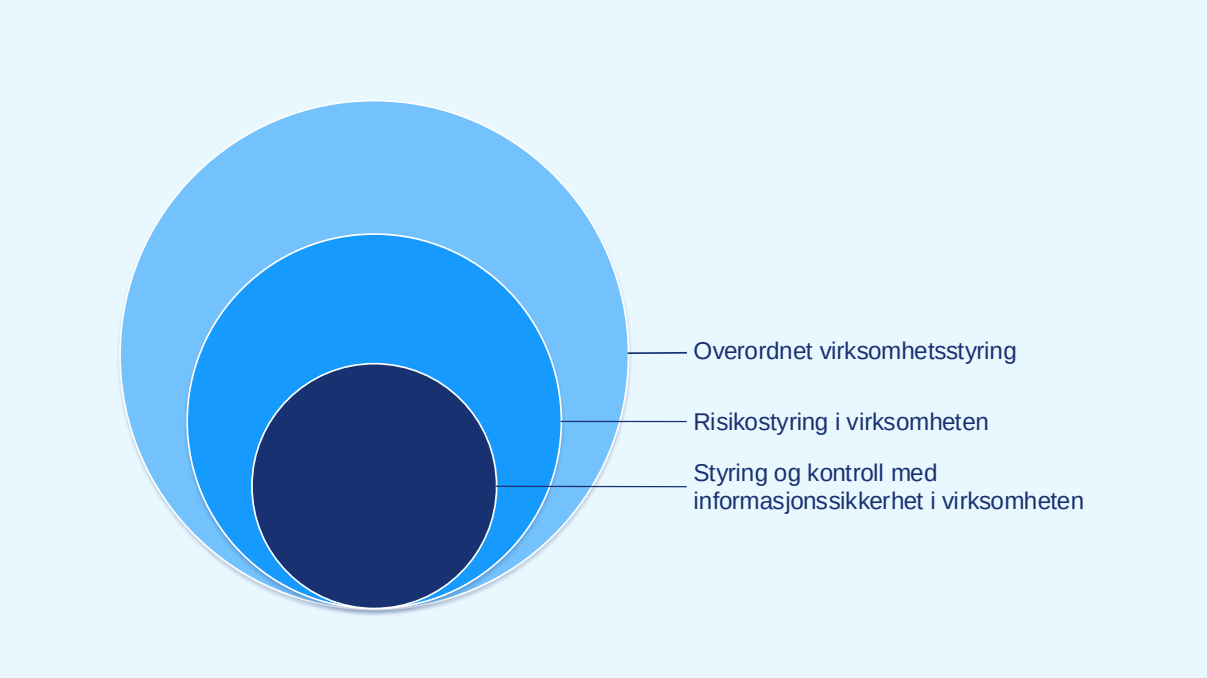
Motsatt vil et kravsbasert regelverk uttrykke eksplisitt hva virksomheten må gjøre for å oppnå et bestemt mål, for eksempel om forsvarlig sikkerhet. Et kravsbasert regelverk legger ikke opp til at den berørte virksomheten skal bruke skjønn i rettsanvendelsen.

Kilde: Petroleumstilsynet (2019) Hvilket regelverk gjelder? [Hentedato 2. juni 2022].

Et av formålene med for eksempel den nye sikkerhetsloven er at det digitale sikkerhetsarbeidet i større grad skal tilpasses forholdene i den enkelte virksomhet, og at digital sikkerhet skal anses som en del av virksomhetens risikostyring og den helhetlige virksomhetsstyringen, slik Figur 5 illustrerer.

[198] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[199] Schartum, Dag Wiese (2005) *Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning*, Nordisk Årbok i rettsinformatikk, Norstedts forlag, s. 11–13.
[200] Schartum, Dag Wiese (2005) *Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning*, Nordisk Årbok i rettsinformatikk, Norstedts forlag, s. 11–13.
[201] Justis- og beredskapsdepartementet (2018) Høring – NOU 2018: 14 *IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*.
[202] Justis- og beredskapsdepartementet (2018) Høring – NOU 2018: 14 *IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*.
[203] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.

Figur 5 Hva vil det si å jobbe helhetlig?



Kilde*:* Digitaliseringsdirektoratet (u.å.) *Hva vil det si å jobbe helhetlig?* [Hentedato 2. juni 2022].

I intervju viser Nasjonal sikkerhetsmyndighet til at dagens funksjonsbaserte regelverk stiller større krav til kompetanse hos virksomhetene, og at manglende kompetanse hos virksomhetene er en barriere for implementering av sikkerhetsloven.[204] Også Justis- og beredskapsdepartementet bemerker at dagens funksjonsbaserte regelverk krever mer kompetanse og ressurser enn tidligere. Ifølge departementet er det krevende for virksomhetene å vurdere hva som for eksempel skal anses som et akseptabelt sikkerhetsnivå.[205] Nasjonal sikkerhetsmyndighet påpeker at forskjellene i utformingen av regelverkene (graden av funksjons- eller kravsbasert regelverk) kan føre til at noen virksomheter får mindre erfaring i å foreta egne verdi-, trussel- og sårbarhetsvurderinger.[206]

En av konsekvensene av utfordringene knyttet til kompetanse og kapasitet er ifølge Justis- og beredskapsdepartementet at arbeidet med å implementere regelverket tar lengre tid. En annen konsekvens av det funksjonsbaserte regelverket kan være at virksomhetene legger listen for sikkerhetsnivået for lavt, fordi det blir for krevende å tolke og implementere kravene. Justis- og beredskapsdepartementet erfarte at mange syntes det var krevende da de tidligere konkrete lovkravene ble erstattet av funksjonelle bestemmelser i den nye sikkerhetsloven.[207]

I likhet med sikkerhetsloven ble samfunnssikkerhetsinstruksen i 2017 endret i en mer funksjonsbasert retning. Tidligere hadde for eksempel instruksen krav til øvelsesfrekvens, mens den nå fikk et funksjonskrav om å utføre et *tilstrekkelig* antall øvelser. Typisk heter det at virksomheten skal ha oversikt over relevant risiko, at det skal iverksettes tiltak etter identifisert risiko, eller at sensitiv informasjon skal skjermes eller beskyttes. Datatilsynet viser også til personvernforordningen som eksempel på et regelverk med en funksjonsbasert tilnærming til sikkerhetskrav.[208] Virksomhetene skal selv vurdere risikoen og behovet for tiltak på grunnlag av identifisert risiko. Ifølge Datatilsynet ville mange brukere av regelverket ha foretrukket tydeligere og helt konkrete krav, for eksempel om hvilken to-faktorløsning som er god nok for å oppnå tilstrekkelig sikkerhet.[209] Se Faktaboks 14 for eksempler på funksjonsbaserte formuleringer fra ulike regelverk.

[204] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[205] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[206] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[207] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[208] Verifisert intervju med Datatilsynet, 17. februar 2022.
[209] Verifisert intervju med Datatilsynet, 17. februar 2022.

Faktaboks 14 Eksempler på funksjonsbaserte krav

«Departementenes arbeid med samfunnssikkerhet skal være basert på systematisk risikostyring».

«Den dataansvarlige og databehandler skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen».

«Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak».

«Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon».

«Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene. Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten».

Kilde: Samfunnssikkerhetsinstruksen kapittel IV; forskrift om behandling av personopplysninger § 4-4 (plikt til å sørge for informasjonssikkerhet og internkontroll); sikkerhetsloven § 4-2 (vurdering av risiko); kraftberedskapsforskriften § 6-3 (beskyttelse, avskjerming og tilgangskontroll); forskrift om IKT-systemer i banker mv. § 3 (risikoanalyse).

Det er stor variasjon mellom regelverkene med hensyn til om de stiller konkrete krav til og omtaler digital sikkerhet / IKT-sikkerhet eksplisitt. Regelverkene innenfor luftfart, havnevirksomhet og helse og velferd omtaler for eksempel tematikken mindre eksplisitt. Regelverket for helse- og omsorgssektoren stiller i hovedsak krav om forsvarlig sikring av informasjon. Dette er imidlertid bestemmelser som regulerer den digitale sikkerheten indirekte. Andre lovverk, for eksempel innenfor finans, ekom og kraft, stiller mer eksplisitte krav til digital sikkerhet / IKT-sikkerhet. For eksempel har energiloven krav til grunnsikring for digitale informasjonssystemer (jf. § 6-5).

Digital sikkerhet / informasjonssikkerhet omtales verken i sivilbeskyttelsesloven eller i den tilhørende veilederen. Derimot omtales *uønskede hendelser* i stort (jf. §§ 1 og 14). Heller ikke helseberedskapsloven omtaler tematikken eksplisitt. Her står det at formålet med loven blant annet er å sørge for at det kan tilbys nødvendige helse- og omsorgstjenester og sosiale tjenester *under krig og ved kriser og katastrofer i fredstid* (jf. § 1-1).

I intervju med representanter fra kommunesektoren går det fram at kommunene opplever en perspektivforskjell avhengig av om man snakker om digital sikkerhet eller om samfunnssikkerhet og beredskap i stort, hvor sistnevnte tradisjonelt har hatt mer oppmerksomhet i kommunene. Digital sikkerhet har imidlertid fått noe større oppmerksomhet i kommunesektoren den siste tiden. Men representantene fra kommunesektoren mener det fortsatt er behov for i større grad å sette digital sikkerhet inn i et helhetlig kommunalt sikkerhetsperspektiv.[210]

I intervjuet kommer det også fram at det er krevende for kommunene å etterleve regelverket for det digitale sikkerhetsarbeidet, og at de ønsker seg konkretiseringer av regelverksbestemmelsene, for eksempel en minimumsstandard til utforming av risiko- og sårbarhetsanalyser og større klarhet i begrepsbruken, slik at det er kjent hva som ligger i begreper som *forsvarlig sikkerhet*?[211]

[210] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[211] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.

Kommunene forteller i intervju at de tror utfordringene med å etterleve regelverket dreier seg om manglende kapasitet, og at arbeidet med digital sikkerhet i for liten grad prioriteres i kommunene.[212] I KS' kartlegging av digital modenhet i kommunesektoren fra 2018 oppgav 61 prosent *ressursmangel* som det største hinderet i arbeidet med informasjonssikkerhet.[213] Digitaliseringsdirektoratet fant i 2020 at manglende kompetanse og forståelse hos medarbeidere og ledere, samt manglende sikkerhetskultur, utgjorde de største hindringene for arbeidet med informasjonssikkerhet i norske kommuner.[214]

Som en del av undersøkelsen har vi gått gjennom fire kommunale tilsynsrapporter, tre interne kommunerevisjoner relatert til sikkerhet og beredskap og ni kommunale beredskapsplaner / risiko- og sårbarhetsanalyser. I de kommunale planene vies digital sikkerhet lite oppmerksomhet. For eksempel har den ene kommunen utarbeidet 10 scenarioer for uønskede hendelser. Ingen av disse scenarioene omhandler digitale angrep.[215] I beredskapsplanene vektlegges først og fremst risiko- og sårbarhetsanalyser, øvelser og beredskapsplanlegging i stort. I noen tilfeller omtales digitale sikkerhetshendelser gjennom scenarioer i risiko- og sårbarhetsanalyser. I én plan blir alvorlig tilsiktede og utilsiktede digitale hendelser og langvarig svikt i ekomtjenester vurdert som tre av 25 mulige uønskede hendelser.[216] Tilsvarende viser gjennomgangen av interne kommunerevisjoner at digital sikkerhet / informasjonssikkerhet i liten grad er omtalt. Kommunerevisjonene omhandler øvelser, risiko- og sårbarhetsanalyser og beredskapsplanlegging.[217] Dette kan være en gjenspeiling av innholdet i sivilbeskyttelsesloven med tilhørende veileder, hvor digital sikkerhet ikke er eksplisitt omtalt.

Justis- og beredskapsdepartementet er i ferd med å utvikle et støtteverktøy og en felles myndighetsportal for å bistå virksomheter med å implementere regelverkskravene innenfor digital sikkerhet. Departementet håper at deres kommende støtteverktøy og den felles myndighetsportalen som er under utvikling, kan bøte på utfordringene med å implementere det funksjonsbaserte regelverket. Departementet legger videre til at Nasjonal sikkerhetsmyndighet vier utfordringene knyttet til det funksjonsbaserte regelverket stor oppmerksomhet i direktoratets veiledningsmateriell og i kommunikasjonen utad.[218]

4.5 Veiledningen på det digitale sikkerhetsområdet er lite samordnet

Veiledning er en gjenspeiling av regelverket det tilhører, og skal bistå brukerne med å etterleve regelverket. De gjennomgåtte utfordringene med regelverket − tematisk overlapp og at det er krevende å etterleve de funksjonsbaserte bestemmelsene – kan løses, eller minimeres, gjennom god veiledning.

Aktørene som forvalter og fører tilsyn med det aktuelle regelverket, skal veilede innenfor sitt område. Datatilsynet skal veilede på personvernområdet, Digitaliseringsdirektoratet skal veilede om styring og kontroll på informasjonssikkerhetsområdet, og Nasjonal sikkerhetsmyndighet skal veilede om sikkerhetstiltak som følger av sikkerhetsloven og deres *Grunnprinsipper for IKT-sikkerhet (2020)*. Direktoratet for samfunnssikkerhet og beredskap er ansvarlig for å tilby kommunesektoren veiledning på samfunnssikkerhetsområdet, mens de øvrige tilsynsmyndighetene skal tilby veiledning på sine områder. Digitaliseringsdirektoratet har også fått en veiledningsrolle overfor kommunene (se kapittel 4.5.4). Vi har gått gjennom 36 veiledere tilknyttet det generelle lovverket og 16 veiledere tilknyttet det

[212] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[213] KS (2018) *Kartlegging av digital modenhet i kommunesektoren*, s. 13.
[214] Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner*, s. 21.
[215] Meløy kommune (2020) *Plan for oppfølging av samfunnssikkerhet og beredskap 2020-2023.*
[216] Sarpsborg kommune (2019) *Helhetlig risiko- og sårbarhetsanalyse.*
[217] Agder kommunerevisjon IKS (2019) *Samfunnssikkerhet og beredskap i Songdalen kommune*; Viken kommunerevisjon IKS (2020) *Samfunnssikkerhet og beredskap – 2020*; Østre Viken kommunerevisjon (2020) *Samfunnssikkerhet og beredskap.*
[218] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

sektorspesifikke lovverket. I det følgende presenterer vi funnene fra gjennomgangen med tilhørende analyse.

I *samfunnssikkerhetsmeldingen* (2020) går det fram at samordningen av den digitale sikkerheten på etatsnivå skal bli tydeligere. Justis- og beredskapsdepartementet skal bidra til bedre koordinering av rådgivnings- og veiledningsaktiviteter innenfor digital sikkerhet. Målet er at all rådgivning og veiledning som myndighetene tilbyr brukerne, skal være samordnet. Vår undersøkelse viser at veiledningen som tilbys av myndighetene, oppleves som lite samordnet og tilgjengelig fra et brukerperspektiv. Vi vurderer samordningen av veiledningsmateriell å være på trinn én etter Direktoratet for forvaltning og økonomistyrings samordningsstige − utveksling av informasjon, erfaringer og kunnskap. Aktørene på veiledningsområdet har i liten grad samarbeidet om å utvikle en felles problem- og løsningsforslag (trinn to).

4.5.1 Tidligere påpekte utfordringer med å samordne veiledningen

I NOU (2018: 14) *IKT-sikkerhet i alle ledd* pekte IKT-sikkerhetsutvalget på at det er overlapp mellom veilederne fra de ulike aktørene innenfor arbeidet med digital sikkerhet, særlig i veilederne rettet mot stat og kommune. Utvalget viste for eksempel til Datatilsynet og tidligere Direktoratet for forvaltning og IKT, som begge veileder i internkontroll og informasjonssikkerhet. Begge tar utgangspunkt i ISO 27001-standarden[219], men med noe ulik innretning. Utvalget viste også til at både Direktoratet for forvaltning og IKT og Nasjonal sikkerhetsmyndighet gir veiledning til statsforvaltningen om tilgrensende områder. Direktoratet for forvaltning og IKT gav på dette tidspunktet veiledning om informasjonssikkerhet knyttet til styring og kontroll og spesifikt til eForvaltningsforskriften § 15. Nasjonal sikkerhetsmyndighet veileder om spesifikke sikkerhetstiltak knyttet til sikkerhetsloven og med utgangspunkt i *Grunnprinsippene for IKT-sikkerhet*. Også her tar begge virksomhetene utgangspunkt i ISO 27001. I informasjonen utvalget hentet inn, kom det fram at brukerne er usikre på hvor de skal henvende seg for å få råd og veiledning om IKT-sikkerhet. I referat fra *Forum for digital sikkerhet* 26. april 2018 kommer det fram at deltakerne på dette tidspunktet ønsket større grad av felles veiledning.

Digitaliseringsdirektoratet gjennomførte på oppdrag fra det daværende Kommunal- og moderniseringsdepartementet en undersøkelse på informasjonssikkerhetsområdet, *Arbeidet med informasjonssikkerhet i statsforvaltningen* (2018). Undersøkelsen viste at det er behov for fortsatt styrking av arbeidet med styring og kontroll med informasjonssikkerhet i virksomhetene. Videre kom det fram at alle departementene i etatsstyringen bør bli bedre på å følge opp sikkerhetsarbeidet i underliggende etater, at det bør øves mer på informasjonssikkerhet, og at virksomhetene bør kartlegge egen kompetanse og sikkerhetskultur.[220]

4.5.2 Veilederne er i hovedsak prosessorienterte

Som følge av det funksjonsbaserte regelverket er veilederne i hovedsak orientert om prosesser framfor om konkrete tiltak som viser hvordan virksomhetene kan etterleve regelverket. Nasjonal sikkerhetsmyndighet understreker at de gjennom veiledningen skal bidra til *effektiv selvhjelp*, og at det er virksomhetene selv som er ansvarlig for å implementere tiltakene.[221] Også Datatilsynet forteller i intervju at de på grunn av regelverkets utforming er tydelige på at de kun rådfører virksomhetene, og at de ikke kan komme med klare føringer om hva virksomhetene skal gjøre.[222] Flere virksomheter, herunder kommunene, kunne imidlertid ønske seg tydeligere råd og anbefalinger om hva som er et akseptabelt risikonivå, og hva slags sikkerhetstiltak som vil være nødvendige for å bøte på den identifiserte risikoen.[223] Representantene fra kommunesektoren forteller at de savner veiledning fra de statlige aktørene om hvordan de skal jobbe med å implementere regelverket for digital sikkerhet. De

[219] ISO 27001 er den ledende internasjonale standarden for informasjonssikkerhet. Den viser hvordan organisasjoner kan beskytte informasjon på en systematisk og kostnadseffektiv måte ved å ta i bruk et styringssystem for informasjonssikkerhet.
[220] Digitaliseringsdirektoratet (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen.* Difi-rapport 2018:4.
[221] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2022.
[222] Verifisert intervju med Datatilsynet, 17. februar 2022.
[223] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.

opplever at det er krevende å få svar på konkrete problemstillinger, for eksempel knyttet til gjennomføring av risiko- og sårbarhetsanalyser. Representantene forteller at de heller ikke får veiledning fra statsforvalteren om digital sikkerhet. Unntaket er representantene fra en kommune som har vært i kontakt med statsforvalteren i forbindelse med planleggingen av en tabletop-øvelse[224] innenfor digital sikkerhet.[225]

Næringslivets sikkerhetsråd, som har om lag 300 medlemmer fra både offentlig og privat sektor, forteller at de fungerer som en arena hvor medlemmene kan diskutere og få råd om hvordan de kan håndtere sikkerhetsutfordringene de står overfor. Næringslivets sikkerhetsråd hjelper virksomhetene med å forstå og tilpasse rådene fra for eksempel Nasjonal sikkerhetsmyndighet. Næringslivets sikkerhetsråd bistår også medlemmene med veiledning dersom de rammes av digitale angrep. Næringslivets sikkerhetsråd opplever at næringslivet mangler ressurser og kompetanse til å tolke og omsette informasjonen fra myndighetenes overordnede trussel- og risikovurderinger til tiltak som virksomhetene kan iverksette for å øke egen sikkerhet.[226] Næringslivets sikkerhetsråds rolle i å veilede virksomhetene kan tyde på at det finnes et udekket behov for veiledning fra de statlige aktørene.

Faktaboks 15 Næringslivets sikkerhetsråd

Næringslivets sikkerhetsråd er en medlemsorganisasjon som skal legge til rette for effektivt og tillitsfullt samarbeid på tvers av sektorer og bransjer, med mål om å kartlegge, forebygge og bekjempe hele bredden av sikkerhetstrusler som næringslivet står overfor. De tilbyr direkte rådgivning til virksomheter etter behov og har utover dette et etablert samarbeid med politiets næringslivskontakter. Næringslivets sikkerhetsråd er også medlem i Nasjonalt cybersikkerhetssenter og Nasjonalt cyberkrimsenter, og samarbeider med blant andre Norsk senter for informasjonssikring om å utvikle faglige råd til virksomheter. Videre arbeider Næringslivets sikkerhetsråd med å påvirke myndighetenes sikkerhetsarbeid i tråd med eiernes og næringslivets uttalte behov.

Kilde: Næringslivets sikkerhetsråd (u.å.) Om NSR; intervju med Næringslivets sikkerhetsråd, 13. desember 2021.

Selv om de fleste veilederne innenfor det digitale sikkerhetsområdet har overordnede nedslagsfelt og formuleringer, er noen mer konkrete i innholdet. Eksempler på slike er Nasjonal sikkerhetsmyndighets veiledere om verdivurdering av informasjon og godkjenning av informasjonssystemer[227] og Nasjonal sikkerhetsmyndighets *Grunnprinsipper for personellsikkerhet*.[228] Tilsvarende er enkelte veiledere rettet mot spesifikke aktører og nivåer. Eksempler er Direktoratet for samfunnssikkerhet og beredskaps *Veileder til samfunnssikkerhetsinstruksen*[229] som er rettet mot departementene, Direktoratet for samfunnssikkerhet og beredskaps veiledere som er rettet mot kommunene, og Digitaliseringsdirektoratets veiledningsmateriell om internkontroll av informasjonssikkerhet som er tilpasset toppledere. Noen veiledere går mer konkret til verks og inneholder blant annet sjekklister og maler, for eksempel for å utarbeide scenarioer i risikovurderingen eller for å kategorisere en uønsket hendelse. Nasjonal sikkerhetsmyndighets veiledere inneholder også råd om anerkjente standarder som kan benyttes i arbeidet med risikovurderinger.

Veilederne varierer også med hensyn til hvor tydelig de er tilknyttet det aktuelle lovverket, og om de tar for seg hele lovverket (for eksempel sikkerhetsloven i sin helhet) eller spesifikke paragrafer i en lov eller en spesifikk forskrift. Direktoratet for samfunnssikkerhet og beredskaps *Veileder til forskrift om*

[224] En tabletop-øvelse (bordøvelse) er en diskusjonsbasert øvelse hvor man arbeider med ulike problemstillinger og oppgaver man kan møte på under uønskede hendelser.
[225] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[226] Intervju med Næringslivets sikkerhetsråd, 13. desember 2021.
[227] Nasjonal sikkerhetsmyndighet (2020) *Håndbok i verdivurdering av informasjon og veileder for godkjenning av informasjonssystemer.*
[228] Nasjonal sikkerhetsmyndighet (u.å.) *Grunnprinsipper for personellsikkerhet.*
[229] Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*.

kommunal beredskapsplikt[230] er et eksempel på det sistnevnte. Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet (2020)*[231] og *Grunnprinsipper for sikkerhetsstyring*[232] henviser til sikkerhetsloven i stort. Det samme gjelder for Direktoratet for samfunnssikkerhet og beredskaps *Veileder til samfunnssikkerhetsinstruksen*.[233]

Veilederne varierer også med hensyn til hvor eksplisitt digital sikkerhet / IKT-sikkerhet er tematisert. Flere veiledere dreier seg for eksempel om risikostyring og internkontroll i stort. Eksempler på veiledere hvor temaet omtales konkret er NVEs *Veileder for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen*[234] og Direktoratet for e-helses *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*.[235]

I og med at det foreligger en del overlapp mellom generelt og sektorspesifikt regelverk, for eksempel mellom energiloven og sikkerhetsloven, henvises det i de sektorspesifikke veiledningene i flere tilfeller til veiledningene for det generelle regelverket.

4.5.3 Samordning av det skriftlige veiledningsmateriellet

Akkurat som for regelverket er det viktig at veilederne er samordnet, slik at brukerne ikke må forholde seg til ulike krav og anbefalinger. Basert på vår gjennomgang av veiledningsmateriell finner vi ikke at veilederne inneholder motstridende krav og anbefalinger. Det er imidlertid flere veiledere som omhandler den samme tematikken. Kun syv av de gjennomgåtte veilederne tilknyttet generelle regelverk tar for seg bare én tematikk. 24 veiledere tar for seg sikkerhetstiltak for håndtering av risiko, 22 veiledere omhandler risikoanalyse/risikovurdering, og 20 veiledere omhandler sikkerhetsstyring/internkontroll.

Det finnes også eksempler på varierende begrepsbruk og på at det henvises til ulike modeller og standarder, for eksempel for internkontroll og risikostyring. Ett eksempel finner vi innenfor tematikken sikkerhetsstyring/internkontroll, hvor følgende begreper (med samme meningsinnhold) brukes om hverandre:

- internkontroll
- sikkerhetsstyring
- styringssystem for sikkerhet
- kvalitetssystem
- sikkerhetsstrategi
- risikostyring

Videre tillegges begrepene *tekniske sikkerhetstiltak* og *sikkerhetstiltak* ulike betydninger og brukes om hverandre. Når det er snakk om prosessuelle tiltak/styringstiltak (etter Digitaliseringsdirektoratets definisjon), for eksempel om viktigheten av å oppdatere programvaren, omtales disse i noen tilfeller som tekniske sikkerhetstiltak. Å utforme prosedyrer for god ansvars- og rollefordeling omtales i noen tilfeller som sikkerhetstiltak, selv om dette i og for seg dreier seg om sikkerhetsstyring. Varierende begrepsbruk og ulikt meningsinnhold kan gjøre det krevende for brukerne å vite hvilke råd og anbefalinger de skal følge. Det kan også gjøre det krevende å vite hva rådene og anbefalingene egentlig innebærer.

Veiledningsmateriellet som omhandler tilsyn med den kommunale beredskapsplikten, vurderes som delvis overlappende innholdsmessig. Kommunene selv forteller at de opplever at veiledningsmateriellet er omfattende og tidvis uoversiktlig og overlappende, at begrepsbruken varierer,

[230] Direktoratet for sikkerhet og beredskap (2021) *Veileder til forskrift om kommunal beredskapsplikt*.
[231] Nasjonal sikkerhetsmyndighet (2020) *Grunnprinsipper for IKT-sikkerhet.*
[232] Nasjonal sikkerhetsmyndighet (u.å.) *Grunnprinsipper for sikkerhetsstyring.*
[233] Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*.
[234] Norges vassdrag- og energidirektorat (2020) *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen.*
[235] Direktoratet for e-helse (2020) *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger.*

og at innfallsvinklene er ulike. Det er mange ulike aktører å forholde seg til, og det kan være krevende å avgjøre hvilke råd som skal være førende. Kommunene ønsker seg et mer komprimert veiledningsmateriell som er tilpasset de ulike sektorene. De trekker fram veilederne på helseområdet som et godt eksempel og uttrykker særlig behov for mer veiledning om digital sikkerhet innenfor oppvekst og skole.[236]

4.5.4 Veiledning om sikker digitalisering i offentlig sektor

Det er iverksatt flere tiltak for å styrke samordningen i veiledningsmateriellet innenfor digital sikkerhet i offentlig forvaltning. Arbeidet med tiltakene ble etablert som et samarbeid mellom Digitaliseringsdirektoratet, Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap, Datatilsynet og Norsk senter for informasjonssikring.[237] Samarbeidet omtales som tiltak 5 − sikker digitalisering i offentlig sektor − i *Nasjonal strategi for digital sikkerhet* fra 2019. Målet med tiltak 5 er å samordne og utvikle veiledningsmateriell og verktøy innenfor områdene informasjonssikkerhet i styringsdialogen, øvelser, sikkerhetskultur, kompetanse og styring og kontroll.[238]

Som en del av tiltaket har Digitaliseringsdirektoratet fått en utvidet veiledningsrolle ovenfor kommunene, Digitaliseringsdirektoratet og Direktoratet for forvaltning og økonomistyring har utarbeidet en veileder for å følge opp den digitale sikkerheten i etatsstyringen, og Direktoratet for samfunnssikkerhet og beredskap har utarbeidet en digital øvelsesportal for offentlig virksomheter. Videre har Digitaliseringsdirektoratet laget en samleside for veiledning innenfor digital sikkerhet for offentlig virksomheter.

Digitaliseringsdirektoratet planlegger å evaluere sine veiledere for å vurdere behov, endringer og eventuell videreutvikling av veiledningsmateriellet. Så langt er ikke veilederne og verktøyene som følge av tiltak 5 evaluert, men de virksomhetene som samarbeider om tiltaket, skal dele bruksstatistikk for veiledningsmateriellet. Bruksstatistikken gir imidlertid bare informasjon om hvor mange som har besøkt veiledernes nettsider. Statistikken gir ikke informasjon om hvorvidt veiledere og verktøy faktisk er tatt i bruk av virksomhetene, eller hvilke erfaringer virksomhetene har hatt.

I samarbeid med en rekke sentrale veiledningsaktører har Digitaliseringsdirektoratet utarbeidet en oversikt over relevante veiledningsaktører på informasjonssikkerhetsområdet. Oversikten, som ligger på Digitaliseringsdirektoratets hjemmesider, beskriver ansvarsområdene til de aktørene som har et ansvar for å tilby veiledning om digital sikkerhet. Formålet med dette arbeidet har vært å sikre god styring og kontroll og bidra til at man ser informasjonssikkerhet som en del av virksomhetsstyringen og opp mot sikkerhetsloven. Veiledningsaktørene som er involvert i arbeidet, er blant annet Nasjonal sikkerhetsmyndighet, Datatilsynet, Direktoratet for forvaltning og økonomistyring, Direktoratet for e-helse (eier av Normen), Norsk senter for informasjonssikring, KS, Foreningen kommunal informasjonssikkerhet og Direktoratet for samfunnssikkerhet og beredskap. Disse utgjør Digitaliseringsdirektoratets mest sentrale samarbeidspartnere blant veiledningsaktørene.

Kommunal- og distriktsdepartementet uttaler i intervju at det fortsatt er behov for å se nærmere på hvordan forvaltningen skal veiledes i arbeidet med digital sikkerhet, blant annet med tanke på felles begrepsbruk.[239]

Justis- og beredskapsdepartementet er i ferd med å utvikle et støtteverktøy for å bistå virksomheter med å implementere regelverkskravene innenfor digital sikkerhet. Departementet har erfart at for få virksomheter kjenner til myndighetenes råd og anbefalinger, men at de som kjenner til dem, i stor grad

[236] Verifisert intervju med representanter fra kommunesektoren, 2. juni. 2022.
[237] Verifisert intervju med Nasjonal sikkerhetsmyndighet (BEGRENSET), 1. desember 2021, utdraget det henvises til, er UGRADERT.
[238] Verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021; verifisert intervju med Kommunal- og distriktsdepartementet, 7. mai 2021.
[239] Verifisert intervju med Kommunal- og distriktsdepartementet, 7. mai 2021.

bruker dem i arbeidet, uavhengig av virksomhetens størrelse eller sektortilhørighet. Departementets vurdering er derfor at det er hensiktsmessig å utforme generisk anvendbare råd, men at det er behov for i større grad å nå ut med disse, spesielt til små og mellomstore virksomheter i privat sektor.[240]

Støtteverktøyet er inspirert av svenske myndigheter, som har utviklet og lansert et støtteverktøy for digital sikkerhet som tilbys alle virksomheter i offentlig sektor, inkludert kommunene. Justis- og beredskapsdepartementet vurderer at løsningen også er relevant for norske virksomheter. Departementet tror verktøyet vil bidra til at virksomhetene selv kan undersøke sin egen sikkerhetstilstand og vurdere hvordan de kan videreutvikle arbeidet med digital sikkerhet. Det vil i sin tur bidra til et mer systematisk arbeid med digital sikkerhet hos virksomhetene. Verktøyet vil også være viktig i departementets arbeid med tilpasning av råd og veiledning. Justis- og beredskapsdepartementet uttaler at det vil være naturlig å se støtteverktøyet i sammenheng med Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* (2020) og muligens også Digitaliseringsdirektoratets veiledere og støtteverktøy.[241]

Oppfølging av den digitale sikkerheten i etatsstyringen

Som en del av tiltak 5 om sikker digitalisering i offentlig sektor skal Digitaliseringsdirektoratet (tidligere Direktoratet for forvaltning og IKT[242]) i samarbeid med Direktoratet for forvaltning og økonomistyring tilby veiledning til etatsstyrer for å kunne følge opp området digital sikkerhet på en god måte. Tiltaket er basert på funnene i gjennomgangen Direktoratet for forvaltning og IKT gjorde i 2018, hvor de fant at *alle departementer i sin etatsstyring bør bli bedre på oppfølging av sikkerhetsarbeidet i underliggende virksomheter*.[243] Digitaliseringsdirektoratet har på bakgrunn av dette utviklet en veileder i samarbeid med Direktoratet for forvaltning og økonomistyring som ble publisert på sistnevntes nettsider februar 2020.[244] I Digitaliseringsdirektoratets veileder til veilederen heter det at *dialogen om informasjonssikkerhet bør inngå i den ordinære styringsdialogen*. Det vil si at den bør inkluderes i instruksen, tildelingsbrevet, årsrapporten og etatsstyringsmøtene.[245]

En gjennomgang Riksrevisjonen har gjort i forbindelse med undersøkelsen, av hovedinstrukser, tildelingsbrev og årsrapporter for utvalgte virksomheter, viser at det er en del variasjon mellom departementene med hensyn til hvilke krav som stilles til arbeidet med digital sikkerhet i etatsstyringen. De utvalgte virksomhetene er virksomheter som understøtter grunnleggende nasjonale funksjoner eller kritiske samfunnsfunksjoner, eller som har sentrale oppgaver med å følge opp den digitale sikkerheten. Enkelte departementer[246] stiller spesifikke krav til at virksomhetene skal sertifiseres etter ISO 27001-standarden[247] eller legge standarden til grunn for arbeidet med informasjonssikkerhet. Andre departementer[248] henviser til Nasjonal sikkerhetsmyndighets grunnprinsipper for digital sikkerhet som standard for arbeidet med digital sikkerhet. Noen departementer krever bare at arbeidet skal utføres etter anerkjente standarder, eller refererer til anbefalinger om digital sikkerhet utgitt av Justis- og beredskapsdepartementet i forbindelse med *Nasjonal strategi for digital sikkerhet* (2019).[249]

Kunnskapsdepartementet, Samferdselsdepartementet, Nærings- og fiskeridepartementet og Helse- og omsorgsdepartementet har utarbeidet egne strategier og policyer for digital sikkerhet i sektorene de har ansvar for.

[240] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[241] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[242] I 2018 ble Direktoratet for forvaltning og IKT sammen med Altinn og deler av Brønnøysundregisteret samlet i Digitaliseringsdirektoratet.
[243] Digitaliseringsdirektoratet (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen.* Difi-rapport 2018:4.
[244] Direktoratet for forvaltning og økonomistyring (2021) *Støtte til styringsdialogen om informasjonssikkerhet.* Veileder publisert på direktoratets nettsider. [Hentedato 23. november 2021]
[245] Digitaliseringsdirektoratet (u.å) *Veiledning om etatsstyring og oppfølging av virksomheter.* Veileder publisert på direktoratets nettsider. [Hentedato 23. november 2021].
[246] Klima- og miljødepartementet; Kommunal- og distriktsdepartementet; Landbruks- og matdepartementet.
[247] ISO 27001-standarden er en internasjonal standard for informasjonssikkerhetsstyring.
[248] Finansdepartementet; Justis- og beredskapsdepartementet; Samferdselsdepartementet.
[249] Arbeids- og sosialdepartementet; Nærings- og fiskeridepartementet.

Justis- og beredskapsdepartementet innhentet i 2021 en statusrapportering fra de andre departementene om arbeidet med tiltak tilhørende på *Nasjonal strategi for digital sikkerhet* (2019). Basert på departementenes innrapportering fant Justis- og beredskapsdepartementet at styringsdialogen brukes til å følge opp den digitale sikkerheten. Departementet slo imidlertid fast at det i begrenset grad rapporteres om hvordan arbeidet med digital sikkerhet følges opp i virksomhetene, og om det gir resultater innad i sektoren.[250]

Digitaliseringsdirektoratets veiledning om styring og kontroll skal omfatte kommunene

Gjennom *Nasjonal strategi for digital sikkerhet* fra 2019 og tiltak om veiledning innenfor styring og kontroll (tiltak 5) fikk Digitaliseringsdirektoratet også et veiledningsansvar overfor kommunene når det gjelder eForvaltningsforskriften § 15 om informasjonssikkerhet. Som følge av dette har Digitaliseringsdirektoratet utarbeidet et kunnskapsgrunnlag som beskriver informasjonssikkerhetstilstanden i kommunene, med anbefalte tiltak. Digitaliseringsdirektoratet fant at fylkeskommuner og kommuner, og spesielt små og mellomstore kommuner, ikke har god nok styring og kontroll på informasjonssikkerhetsområdet. Videre fant de svakheter i kommunenes arbeid med å etablere og opprettholde systematisk internkontroll på informasjonssikkerhetsområdet. Også dette gjaldt spesielt små og mellomstore kommuner. Funnene indikerer at kommunestørrelse kan ha betydning for hvordan det arbeides med informasjonssikkerhet. Det viste seg også at under halvparten av de små og mellomstore kommunene gjennomfører kompetansehevende aktiviteter minst én gang i året, og at store kommuner gjør dette i større grad enn små og mellomstore kommuner.[251]

Utfordringene i kommunene er i stor grad identiske med utfordringene som ble avdekket i statsforvaltningen i 2018. Veilederen som ble utviklet som en del av tiltak 5, treffer derfor også kommunenes behov for verktøy og veiledning for å styrke arbeidet på disse områdene. Digitaliseringsdirektoratet opplyser at de har styrket samarbeidet med KS og *Kommunenes nettverk for informasjonssikkerhet* etter at de fikk et veiledningsansvar overfor kommunene. KS og *Kommunenes nettverk for informasjonssikkerhet* er invitert med i *Nettverk for veiledningsaktører innen styring og kontroll* og har i den anledning mulighet til å bli orientert om og orientere andre om pågående og planlagte aktiviteter. Videre har de invitert til samarbeid i konkrete prosjekter, blant annet har de invitert kommuner til å delta på kurs i verktøy for styring av informasjonssikkerhet. Som en del av kurset hadde Digitaliseringsdirektoratet både en direkte oppfølging med kommunene som deltok, om hva de syntes om kurset, og de planlegger å kontakte deltakerne på nytt etter seks måneder for å finne ut om de faktisk har fått bruk for materiellet som ble gjennomgått, i det praktiske arbeidet. Utover dette er også KS invitert til å gi bidrag til veiledningen *Helhetlig styring og kontroll av informasjonssikkerhet*.[252]

Kommunene vi har intervjuet, har ikke forholdt seg til Digitaliseringsdirektoratet etter at direktoratet fikk veiledningsansvar overfor kommunene i 2020. De har ikke benyttet seg av direktoratets veiledning for internkontroll, og de opplever at det er urealistisk for dem å benytte seg av Digitaliseringsdirektoratets skriftlige veiledningsmateriell.[253]

4.6 Samordning av tilsyn med arbeidet med digital sikkerhet

I denne delen gjennomgår og analyserer vi graden av samordning mellom tilsynsmyndighetene som fører tilsyn med det digitale sikkerhetsarbeidet.

[250] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet.*
[251] Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner*.
[252] Verifisert intervju med Digitaliseringsdirektoratet, 3. desember 2021.
[253] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.

Tilsyn er et sentralt virkemiddel når Justis- og beredskapsdepartementet og øvrige myndigheter skal kontrollere at regelverk implementeres og overholdes. Nasjonal sikkerhetsmyndighet har fått i oppdrag av Justis- og beredskapsdepartementet å koordinere arbeidet mellom myndigheter som fører tilsyn med den digitale sikkerheten, og skal legge til rette for hensiktsmessig samhandling mellom disse.

4.6.1 Tidligere påpekte utfordringer med samordningen av tilsyn

I 2005 gjennomførte en arbeidsgruppe nedsatt av Koordineringsutvalget for informasjonssikkerhet en foranalyse for å få en oversikt over regelverket, påpeke mulige problemområder og ut fra det komme med anbefalinger.[254] I forprosjektrapporten skriver de følgende:

> «Det er påvist et omfattende tilsynsregime som i større eller mindre grad har likeartede oppgaver som omhandler informasjonssikkerhet. Både private og offentlige virksomheter må forholde seg til flere tilsyn, direktorater og departementer samtidig. Fordi de enkelte lovene og forskriftene så å si har sine egne tilsyn, vil det være slik at jo flere lover og forskrifter en virksomhet må forholde seg til, jo flere tilsynsregimer og andre myndigheter skal ha et ord med i laget».

Kilde: Koordineringsutvalget for informasjonssikkerhet (2005) *Forprosjektrapport fra arbeidsgruppen Regelverk og informasjonssikkerhet til Koordineringsutvalget for informasjonssikkerhet (KIS)*, s. 28 og 59.

Gruppen anbefalte blant annet at det ble satt i gang konkrete samarbeid mellom tilsynene, herunder utvikling av rutiner for samordning av tilsyn og (videre)utvikling av tilsynsmetodikk.

IKT-sikkerhetsutvalget identifiserte i 2018 tre forhold knyttet til tilsyn med IKT-sikkerhet som kunne forbedres; Tilsynsmyndighetene framstår som lite koordinert i tid, begrepsbruk og metodikk. Det er mangler og hull i tilsynsvirksomheten, og tilsynsmyndighetene har ikke nok kompetanse til å foreta tekniske IKT-tilsyn. På grunn av manglende oversikt over den digitale verdikjeden er det også utfordringer knyttet til hjemmelsgrunnlag for tilsyn med underleverandører av varer og tjenester.[255]

I *samfunnssikkerhetsmeldingen* (2020) går det fram at Justis- og beredskapsdepartementet skal bidra til bedre koordinering av tilsyn. Et sentralt virkemiddel i dette arbeidet er Nasjonal sikkerhetsmyndighets *Samhandlingsarena for sektortilsyn med sikkerhetsloven*.[256] Formålet med arenaen er blant annet å bidra til enhetlige tilsyn med mest mulig felles tilsynsmetodikk, kompetanseheving og kunnskapsoverføring mellom tilsynsmyndighetene. Arenaen omfatter i første omgang de sektortilsynene som blir utpekt av departementene til å føre tilsyn etter sikkerhetsloven.

4.6.2 Det er lite samordning av tilsyn og tilsynsmetodikk

Som vist ovenfor treffes flere virksomheter, og spesielt kommunene, av flere krav fra generelt og sektorspesifikt regelverk samtidig. Det innebærer at de også er underlagt tilsyn fra flere tilsynsmyndigheter som alle kan føre tilsyn med den digitale sikkerheten i virksomheten. For eksempel kan en kommune bli underlagt tilsyn fra Datatilsynet om sikring av personopplysninger, fra statsforvalteren om samfunnssikkerheten i kommunen, og fra Helsetilsynet om digital sikring av helseregistre. Det finnes også regelverk med krav til digital sikkerhet som ikke følges opp gjennom tilsyn, blant annet forvaltningsloven (herunder eForvaltningsforskriften), arkivloven og beskyttelsesinstruksen. I denne undersøkelsen kommer det fram at samordningen av tilsyn tilsvarer trinn én – som innebærer å dele informasjon – i samordningsstigen til Direktoratet for forvaltning og økonomistyring.

[254] Koordineringsutvalget for informasjonssikkerhet (2005) *Forprosjektrapport fra arbeidsgruppen Regelverk og informasjonssikkerhet til Koordineringsutvalget for informasjonssikkerhet (KIS)*, s. 28 og 59.
[255] NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet,* s. 51.
[256] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden,* s. 83.

Vår gjennomgang av tilsynspraksisen hos utvalgte tilsynsmyndigheter viser at de fleste tilsyn gjennomføres som systemtilsyn (dette omtales nærmere i kapittel 5.6). Flere av tilsynsmyndighetene er i ferd med å utvikle metodikken for tilsyn med den digitale sikkerheten, uten at det ser ut til å være lagt opp til koordinering mellom tilsynsmyndighetene.

Datatilsynet samordner sine tilsyn med statsforvalterne ved hjelp av tilsynskalendre. Datatilsynet har imidlertid hatt få tilsyn de siste årene og har dermed benyttet kalenderne i liten grad. Hendelsesbaserte tilsyn skrives ikke inn i kalenderne, da disse ikke kan planlegges på forhånd. Datatilsynet deltar i tillegg på minst ett møte med hver statsforvalter i løpet av året. Datatilsynet opplyser at Kommunal- og distriktsdepartementet har en møteserie knyttet til koordinering og samordning av tilsyn der Datatilsynet er en aktiv deltaker. I disse møtene informerer deltakerne hverandre om innholdet i planlagte tilsyn og erfaringer knyttet til tilsyn. Datatilsynet opplyser at mange tilsynsmyndigheter deltar i disse møtene, blant annet Helsetilsynet, Veivesenet, Kystverket og Jernbanetilsynet. Datatilsynet har vært observatør under tilsyn fra NVE og revisjoner fra Riksrevisjonen fordi det var noen grensedragninger mot personvern. Datatilsynet har også involvert Nasjonal sikkerhetsmyndighet, Arbeidstilsynet, Helsetilsynet og Nasjonal kommunikasjonsmyndighet med flere under tilsyn når området for tilsyn har vært delt eller sammenfallende. Datatilsynet opplever at dette er nyttig med tanke på å samordne tilsynene, og mener at det vil være uheldig hvis Datatilsynet har gjennomført tilsyn og for eksempel Nasjonal sikkerhetsmyndighet gjennomfører tilsyn i etterkant og finner andre avvik.[257]

Direktoratet for samfunnssikkerhet og beredskap opplyser at direktoratet ikke samarbeider med andre tilsynsmyndigheter for å koordinere tilsyn med den digitale sikkerheten, men at de utveksler tilsynskalendre med Nasjonal sikkerhetsmyndighet. Direktoratet har tidligere gjennomført ett tilsyn i samarbeid med Nasjonal sikkerhetsmyndighet. Begge parter erfarte da at tilsynspraksisen deres var så ulik at det var mest hensiktsmessig å gjennomføre separate tilsyn. Direktoratet for samfunnssikkerhet og beredskap deler heller ikke observasjoner om brudd på andre regelverk enn samfunnssikkerhetsinstruksen med respektive tilsynsmyndigheter. Det er Justis- og beredskapsdepartementet som eier tilsynsrapportene, og dersom Justis- og beredskapsdepartementet vurderer at det er relevant å dele tilsynsfunn med andre, er det de som må følge opp dette.[258]

Justis- og beredskapsdepartementet har ikke evaluert innretningen av tilsyn med den digitale sikkerheten på tvers av tilsynsmyndighetene.[259] Justis- og beredskapsdepartementet opplever at samordningen av tilsyn ivaretas gjennom samordningsarenaen *Forum for IKT-tilsyn*. Arenaen har som formål å samordne tilsynene på tvers av tilsynsmyndighetene. I tillegg er det etablert en samhandlingsarena for sektortilsyn etter sikkerhetsloven.

Samhandlingsarena for sektortilsyn etter sikkerhetsloven

I *samfunnssikkerhetsmeldingen* (2020) omtales Nasjonal sikkerhetsmyndighets *Samhandlingsarena for sektortilsyn etter sikkerhetsloven* som et sentralt virkemiddel for å oppnå bedre koordinering av tilsyn.[260] Arenaen består av Nasjonal sikkerhetsmyndighet, NVE og Nasjonal kommunikasjonsmyndighet. Sikkerhetsloven stiller krav om at gjennomføringen av tilsyn skal samordnes med andre tilsynsmyndigheter så langt det er mulig.[261] Selv om tilsyn med forebyggende sikkerhetsarbeid gjennomføres av forskjellige tilsynsmyndigheter; Nasjonal sikkerhetsmyndighet og sektormyndigheter med tilsynsansvar, skal tilsynet være enhetlig på tvers av sektorer.[262]

[257] Verifisert intervju med Datatilsynet 17. februar 2022.
[258] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[259] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[260] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*.
[261] Sikkerhetsloven § 3-2.
[262] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2, s. 6.

Samhandlingsarenaen for sektortilsyn skal bidra til erfaringsutveksling, enhetlige tilsyn med mest mulig felles tilsynsmetodikk og kunnskapsoverføring mellom Nasjonal sikkerhetsmyndighet og sektortilsynene. Nasjonal sikkerhetsmyndighet opplyser at det har vært avholdt flere møter i samhandlingsarenaen hvor ulike problemstillinger knyttet til sikkerhetsloven har blitt diskutert. Formålet med møtene er å sikre en enhetlig kontroll med at sikkerhetslovens bestemmelser etterleves. Møtene har opplevdes nyttige og vært en arena for gjensidig erfaringsutveksling. På grunn av koronapandemien har møtene primært vært gjennomført digitalt på en ugradert plattform.[263] Øvrig samordning av tilsyn med sikkerhetsloven omtales i kapittel 5.6.

Nasjonal kommunikasjonsmyndighet og NVE samarbeider om gjensidige avhengigheter i kraft- og ekomsektoren fordi begge er sektortilsyn for sikkerhetsloven, og de har jevnlig møter om sikkerhet og beredskap i kraft- og ekomsektoren.[264] Nasjonal kommunikasjonsmyndighet opplyser at de samarbeider med NVE om tilsyn etter sikkerhetsloven, blant annet gjennom Nasjonal sikkerhetsmyndighets *Samhandlingsarena for sektortilsyn etter sikkerhetsloven*, men at de ikke har samarbeidet om konkrete tilsyn.

Nasjonal kommunikasjonsmyndighet forteller at de har en god dialog med Nasjonal sikkerhetsmyndighet om tilsynsarbeidet, men at de har hatt behov for mange avklaringer før de har inngått avtaler om at Nasjonal kommunikasjonsmyndighet skal gjøre tilsyn etter sikkerhetsloven.[265] Nasjonal kommunikasjonsmyndighet opplever at Nasjonal sikkerhetsmyndighet nok har ønsket å ha mer styring over etatens tilsynsvirksomhet. Nasjonal kommunikasjonsmyndighet forteller at de har samarbeidet med Nasjonal sikkerhetsmyndighet om tilsyn siden 2014. De har vært observatør på Nasjonal sikkerhetsmyndighets tilsyn, og de to aktørene har gjennomført felles tilsyn på ulike områder.[266] Nasjonal kommunikasjonsmyndighet deler tilsynsplaner med Nasjonal sikkerhetsmyndighet, men det har foreløpig ikke vært noen tilsynsresultater å dele. Tilsynsplanene er «til orientering» og skal ikke godkjennes, men Nasjonal sikkerhetsmyndighet kan komme med innspill og eventuelt føre tilsyn med Nasjonal kommunikasjonsmyndighet siden direktoratet har det overordnede tilsynsansvaret.

Nasjonal sikkerhetsmyndighet opplyser at det ikke gjøres noen formell avsjekk, for eksempel av tidspunktet eller tema for tilsynet med de øvrige tilsynsmyndighetene i forkant av et tilsyn. De øvrige sektortilsynene som fører tilsyn etter sikkerhetsloven, er imidlertid bedt om å sende en årlig oversikt til Nasjonal sikkerhetsmyndighet over planlagte tilsyn.[267]

Justis- og beredskapsdepartementet opplyser at de ikke har gjennomført eller initiert noen evaluering av samordningsarenaen. De legger imidlertid til at Nasjonal sikkerhetsmyndighet melder om positive erfaringer med arenaen så langt. [268]

Forum for IKT-tilsyn

Nasjonal sikkerhetsmyndighet har fått i oppdrag å koordinere arbeidet mellom myndigheter som har en rolle innenfor forebyggende digital sikkerhet, og skal legge til rette for hensiktsmessig samhandling mellom disse. På bakgrunn av dette opprettet Nasjonal sikkerhetsmyndighet et samarbeidsforum, *Forum for IKT-tilsyn*, for tilsynsmyndigheter som fører tilsyn med IKT-sikkerhet i egen sektor. Det ble avholdt oppstartsmøte i forumet 9. mars 2021. Mattilsynet, Petroleumstilsynet, Nasjonal kommunikasjonsmyndighet, NVE, Finanstilsynet, Luftfartstilsynet, Kystverket, Digitaliseringsdirektoratet, Direktoratet for strålevern og atomsikkerhet og Nasjonal

[263] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[264] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[265] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[266] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[267] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[268] Verifisert intervju med Justis- og beredskapsdepartementet 28. juni 2022.

sikkerhetsmyndighet deltok.[269] NVE opplyser at de deltar i forumet og har spilt en aktiv rolle i de få møtene som har vært.[270] Nasjonal kommunikasjonsmyndighet opplever at det foreløpig er litt uklart hvem som skal delta i forumet, og hva forumet egentlig skal være, men at de to siste møtene har ført deltakerne inn i et godt spor. Nasjonal kommunikasjonsmyndighet tror forumet kan bli en velfungerende samarbeidsarena.[271]

Nasjonal sikkerhetsmyndighet uttaler i intervju at det ikke er gjort noen systematisk gjennomgang av hvem som skal delta i *Forum for IKT-tilsyn*, og at det heller ikke er gjort noen systematisk kartlegging av hvilke sektortilsyn som fører tilsyn med den digitale sikkerheten. Invitasjonene til å delta ble basert på hvem Nasjonal sikkerhetsmyndighet anså det som naturlig å ha med, da forumet ble etablert. Det er ikke gjort noen ny vurdering av deltakerne.[272] Datatilsynet, som fører tilsyn med personvernreglementet, er ikke representert i *Forum for IKT-tilsyn*. Justis- og beredskapsdepartementet opplyser imidlertid om at *Forum for IKT-tilsyn* ble etablert etter en systematisk identifisering av tilsynsorgan med ansvar for etterlevelse av regelverksbestemmelser om digital sikkerhet. Gjennomgangen resulterte i en invitasjon fra Nasjonal sikkerhetsmyndighet til 14 tilsynsorgan, deriblant Datatilsynet som valgte å ikke bli med i forumet.[273]

Nasjonal sikkerhetsmyndighet vurderer dagens sammensetning i forumet som hensiktsmessig og velfungerende. Deltakerne veksler på å være vertskap for møtene, og det er tilsynsmyndigheten som er vertskap, som setter agendaen.[274]

Nasjonal sikkerhetsmyndighet opplyser videre at tema for møtene i forumet varierer etter hva de ulike tilsynene ønsker å ta opp. Direktoratet oppfatter at forumet er nyttig for å utveksle informasjon om tilsyn generelt og om tilsyn innenfor digital sikkerhet spesielt. De påpeker at informasjonen flyter begge veier mellom partene i forumet, og viser for eksempel til at Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* (2020) har blitt diskutert. Da det er et viktig mål at grunnprinsippene skal være tverrsektorielle, er forumet en viktig arena som bidrar til at Nasjonal sikkerhetsmyndighet får tilbakemeldinger på grunnprinsippene fra de ulike sektorene. Ifølge Nasjonal sikkerhetsmyndighet er det stor variasjon i kompetansen og bevisstheten knyttet til digital sikkerhet blant medlemmene i forumet. Direktoratet antar at dette følger av hvor mye de ulike myndighetene arbeider med digital sikkerhet i sitt daglige virke.[275] På oppstartsmøtet ble de deltakende tilsynsmyndighetene bedt om å gi innspill om aktuelle tema for kommende møter i forumet.[276] Referatet fra møtet viser at det var bred enighet om å dele erfaringer og drive kunnskapsoverføring i forumet, og deltakerne ble oppfordret til å ta kontakt med hverandre ved behov utenom de formelle samlingene. Felles tilsynsmetodikk eller koordinering av tilsynsplaner synes ikke å ha vært diskutert.

[269] Nasjonal sikkerhetsmyndighet - *Referat SIG Digital Brief 2021-03-09.*
[270] Norges vassdrags- og energidirektorat (2022) *SV: Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet*. E-poster til Riksrevisjonen, 23. mai 2022.
[271] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[272] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[273] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[274] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[275] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[276] Nasjonal sikkerhetsmyndighet - *Referat SIG Digital Brief 2021-03-09.*

5 Justis- og beredskapsdepartementets oversikt over den nasjonale digitale sikkerhetstilstanden

Den siste *samfunnssikkerhetsmeldingen* (2020) viser til at økende kompleksitet i digitale systemer og verdikjeder medfører økt sårbarhet.[277] Flere og flere digitale løsninger kobles sammen. Dette skaper uoversiktlige avhengigheter og gjør det krevende å holde oversikt over den digitale sikkerhetstilstanden. Aktører bak digitale angrep utnytter sårbarheter i en verdikjede. Samfunnets avhengighet av digitale systemer tilsier at digital sikkerhet er helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale sikkerhetsinteresser.[278] Justis- og beredskapsdepartementet skal som en del av sitt samordningsansvar ha oversikt over tilstanden på samfunnssikkerhetsområdet, herunder den nasjonale digitale sikkerhetstilstanden (jf. samfunnssikkerhetsinstruksen kapittel VI punkt 1 a). God oversikt over den nasjonale digitale sikkerhetstilstanden er en forutsetning for å oppnå god samordning av aktører og tiltak.

I dette kapitlet svarer vi på den andre problemstillingen: *Har Justis- og beredskapsdepartementet en helhetlig oversikt over den nasjonale digitale sikkerhetstilstanden?* Først presenterer vi kildene som departementet bruker til å holde oversikt over den nasjonale digitale sikkerhetstilstanden. Så går vi gjennom prosessen rundt implementeringen den nye sikkerhetsloven, da dette er et sentralt premiss for å kunne ha oversikt over verdiene som skal sikres. Videre går vi gjennom rammeverk som brukes i arbeidet med å kartlegge digitale verdikjeder, og departementenes arbeid med status- og tilstandsvurderinger etter samfunnssikkerhetsinstruksen. Deretter går vi gjennom prosessen med å utarbeide risiko- og sårbarhetsanalyser for kritiske samfunnsfunksjoner i departementene. Så presenterer vi tilsyn med det digitale sikkerhetsarbeidet, da oppsummert informasjon om og eksempler fra tilsyn er viktig grunnlagsinformasjon i arbeidet med å holde oversikt over sikkerhetstilstanden.

5.1 Kilder til departementets oversikt over den digitale sikkerhetstilstanden

Justis- og beredskapsdepartementet har identifisert en rekke kilder som sentrale for departementets oversikt over den nasjonale digitale sikkerhetstilstanden:

- sikkerhets- og tilsynsrapporter fra Nasjonal sikkerhetsmyndighet
- trussel- og sikkerhetsvurderingene fra etterretnings- og sikkerhetstjenestene
- sikkerhets- og tilsynsrapporter fra Direktoratet for samfunnssikkerhet og beredskap
- departementenes rapportering på implementeringen av sikkerhetsloven
- departementenes rapportering på arbeidet som følger av samfunnssikkerhetsinstruksen
- departementenes tilstands- og statusvurderinger
- departementenes rapportering på gjennomføring og oppfølging av tiltak i *Nasjonal strategi for digital sikkerhet* fra 2019
- nasjonale utredninger, forskningsrapporter og øvrige undersøkelser
- innspill fra internasjonale samarbeidspartnere
- rapportering fra samordningsarenaene på det digitale området
- rapportering fra deltakere i digitale øvelser
- rapportering fra virksomheter som er involvert ved alvorlig digitale hendelser
- rapportering til NATO på Cyber Defence Pledge[279]

[277] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden,* s. 27–28.
[278] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden,* s. 79.
[279] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021 og 28. juni 2022.

Justis- og beredskapsdepartementet mener at de, basert på de overnevnte kildene, har god nok oversikt over den nasjonale digitale sikkerhetstilstanden til å kunne treffe nødvendige beslutninger og tiltak. Samtidig poengterer departementet at det digitale sikkerhetsområdet er komplekst og i konstant utvikling, og at oversikten over den digitale sikkerhetstilstanden kun er et øyeblikksbilde. Justis- og beredskapsdepartementet understreker også at departementene selv har ansvaret for å ha tilstrekkelig oversikt over den digitale sikkerhetstilstanden i egne sektorer.[280]

Vår undersøkelse har likevel avdekket en del svakheter ved de kildene som departementet oppgir som grunnlag for å holde oversikt over den digitale sikkerhetstilstanden:

- treg implementering av sikkerhetsloven (omtales i kapittel 5.2)
- departementenes status- og tilstandsvurderinger av samfunnets kritiske funksjoner (omtales i kapittel 5.4)
- rapportering på arbeidet med tiltak i *Nasjonal strategi for digital sikkerhet* (2019) (omtales i kapittel 6.1.2)
- oppsummering av informasjon om resultatene fra tilsyn med digital sikkerhet (omtales i kapittel 5.6)
- tekniske systemer for avdekking av trusler og sårbarheter (omtales i kapittel 6.4.1 og 6.4.2)

5.2 Forsinket implementering av sikkerhetsloven gir mangelfull oversikt over verdier og avhengigheter

Justis- og beredskapsdepartementet beskriver sikkerhetsloven som det mest sentrale tiltaket for å øke den nasjonale digitale sikkerheten. Departementet viser videre til at rapportering på bakgrunn av sikkerhetsloven er en viktig kilde til informasjon for å holde oversikt over den digitale sikkerhetstilstanden.[281] Nasjonal sikkerhetsmyndighet ble i 2019 styrket med 38 millioner kroner for å implementere nye og utvidede oppgaver som sikkerhetsmyndighet i henhold til den nye sikkerhetsloven. Implementeringen av den nye sikkerhetsloven er utformet som et av tiltakene i *Nasjonal strategi for digital sikkerhet* (2019) (jf. tiltak 29).

Justis- og beredskapsdepartementets framdriftsplan for implementering av sikkerhetsloven viser at den konkrete gjennomføringen skulle være ferdig innen november 2021. Planen består av følgende seks milepæler (frist for milepælene vises i Tabell 3):

1. Departementene har identifisert grunnleggende nasjonale funksjoner i sine sektorer.
2. Virksomhetene som råder over skjermingsverdige objekter og infrastruktur, har utarbeidet skadevurderinger for disse med utgangspunkt i identifisert grunnleggende nasjonal funksjon og virksomhetens funksjon.
3. Departementene har vurdert skadevurderinger fra virksomhetene og fattet vedtak om klassifisering av skjermingsverdige objekter og infrastruktur.
4. Departementene har fattet vedtak om at loven gjelder for virksomheter med skjermingsverdige objekter og infrastruktur.
5. Andre virksomheter som virksomheter med skjermingsverdige objekter og infrastruktur er avhengige av, er innrapportert til departement og Nasjonal sikkerhetsmyndighet.
6. Sikkerhetsmyndigheten har oversikt og legger til rette for informasjonsdeling.

[280] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[281] Verifisert intervju med Justis- og beredskapsdepartementet, 21. mai 2021.

Tabell 3 Framdriftsplan for implementering av sikkerhetsloven

	Milepæl 1	Milepæl 2	Milepæl 3	Milepæl 4	Milepæl 5	Milepæl 6
Grunnleggende nasjonale funksjoner	21.08.20	30.09.20	15.11.20	31.12.20	31.01.21	Kun NSM: 30.06.21
Tverrsektorielle grunnleggende nasjonale funksjoner	30.09.20	15.11.20	31.12.20	31.06.21	31.07.21	Kun NSM: 31.11.21

Kilde: Justis- og beredskapsdepartementet (2020) *Framdriftsplan for implementering av sikkerhetsloven*, s. 7.

Justis- og beredskapsdepartementet bemerker at framdriftsplanen ikke må betraktes som en plan for å sluttføre arbeidet med implementeringen. Framdriftsplanen må betraktes som et verktøy som skal hjelpe departementene å identifisere grunnleggende nasjonale funksjoner, vesentlige virksomheter samt skjermingsverdige objekter og infrastruktur som enten allerede er klassifisert etter den gamle loven, eller som er åpenbare ut fra den nye sikkerhetsloven. Deretter skal departementene kartlegge avhengigheter til de grunnleggende nasjonale funksjonene i sin sektor og på tvers av sektorene. Justis- og beredskapsdepartementet understreker at det er det enkelte departement som er ansvarlig for at framdriftsplanen overholdes i hver enkelt sektor, og at arbeidet med grunnleggende nasjonale funksjoner er en kontinuerlig prosess.[282]

Justis- og beredskapsdepartementet rapporterer at Nasjonal sikkerhetsmyndighet per 29. august 2022 besitter en samlet oversikt over identifiserte grunnleggende nasjonale funksjoner, skjermingsverdige objekter og infrastrukturer og innmeldte vedtak om virksomheter som er underlagt sikkerhetsloven med bakgrunn i sikkerhetslovens § 1-3. Dette tilsvarer milepæl fire i milepælsplanen (Tabell 3). Justis- og beredskapsdepartementet mottar en sikkerhetsgradert oversikt over objekter og infrastrukturer i sivil sektor fra Nasjonal sikkerhetsmyndighet årlig og ved endringer av betydning.[283]

Justis- og beredskapsdepartementet erfarer at arbeidet med å kartlegge avhengighetene til de grunnleggende nasjonale funksjonene har vært mer komplisert enn opprinnelig antatt. Arbeidet med å få oversikt over avhengighetene er derfor ikke kommet like langt som identifiseringen av grunnleggende nasjonale funksjoner og skadevurderingen av objekter og infrastrukturer.[284] Et eksempel på slike avhengigheter er at alle departementene er avhengige av Politiets sikkerhetstjeneste for å kunne tilby statsrådene sine livvakttjeneste, og at de derfor melder denne avhengigheten til Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet. De er også avhengige av for eksempel strøm for å kunne opprettholde sin funksjon. Denne avhengigheten skal de melde til Olje- og energidepartementet og Nasjonal sikkerhetsmyndighet.[285]

5.2.1 Nasjonal sikkerhetsmyndighet mener den nasjonale forståelsen av sikkerhetsloven er svak

I Nasjonal sikkerhetsmyndighets nasjonale risikovurdering for 2022 peker sikkerhetsmyndigheten på at arbeidet med å implementere sikkerhetsloven går for sakte, og at implementering av loven er en forutsetning for at utsatte virksomheter skal kunne beskytte seg tilstrekkelig mot digitale trusler.[286] I Justis- og beredskapsdepartementets statusvurdering for *Nasjonal strategi for digital sikkerhet* (2019) våren 2021 vises det også til at arbeidet med implementeringen går for sakte. Ifølge Nasjonal

[282] Justis- og beredskapsdepartementet (2022) *Innspill til møtereferat og supplerende informasjon*, s. 1–3.
[283] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[284] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[285] Svar på skriftlige spørsmål fra Justis- og beredskapsdepartementet, 12. september 2022.
[286] Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022*, s. 11.

sikkerhetsmyndighets nasjonale risikovurdering for 2021 gjenstår det mye arbeid før sikkerhetsloven er fullt ut implementert.[287]

Vår gjennomgang av tildelingsbrev fra departementene, med unntak av Forsvarsdepartementet[288], til underliggende virksomheter for 2022 viser at kun tre departementer, Arbeids- og inkluderingsdepartementet, Olje- og energidepartementet og Samferdselsdepartementet, eksplisitt gir underliggende virksomheter i oppdrag å følge opp arbeidet med implementering av sikkerhetsloven. Forsvarsdepartementet oppgir i intervju at de stiller krav til arbeidet med sikkerhetsloven i tildelingsbrevene til underliggende virksomheter.[289]

Nasjonal sikkerhetsmyndighet gir i intervju uttrykk for at de vurderer den nasjonale forståelsen av sikkerhetsloven som for svak. Det er stor variasjon i hvor langt departementene har kommet med implementeringen av kravene i den nye loven. Nasjonal sikkerhetsmyndighet mener at dette blant annet skyldes manglende kompetanse i de underliggende virksomhetene. De viser som nevnt til at det er kompetansekrevende å implementere den nye sikkerhetsloven, da den i større grad er funksjonelt utformet enn den forrige sikkerhetsloven. I Nasjonal sikkerhetsmyndighets spørreundersøkelse om sikkerhetstilstanden til departementene trekker flere departementer fram manglende sikkerhetsfaglig kompetanse innenfor sikkerhetsstyring og manglende kunnskap om risikovurdering og sikkerhetstiltak som en utfordring.[290] Ifølge Nasjonal sikkerhetsmyndighets nasjonale risikovurdering for 2021 fører den nye sikkerhetsloven til at det er et større behov for å sette virksomhetene som er underlagt loven i stand til å gjennomføre sikkerhetsstyring generelt og risikovurdering spesielt. Dersom virksomhetene mangler relevant kompetanse om forebyggende sikkerhet, utgjør det en sårbarhet. Hvilke fagområder innenfor forebyggende sikkerhet den enkelte virksomhet faktisk trenger kompetanse på, avhenger av virksomhetens natur og hvilke verdier den forvalter.[291]

5.2.2 Kartleggingen av avhengigheter er kompleks og krevende

Også Justis- og beredskapsdepartementet beskriver den nye sikkerhetsloven som mer kompetansekrevende å implementere og etterleve enn den forrige.[292] Vår dybdeundersøkelse bekrefter at det oppleves krevende å implementere sikkerhetsloven. En av de offentlige virksomhetene som deltok i undersøkelsen, opplyser at de ennå ikke har mottatt en beskrivelse fra ansvarlig departement om hvilke deler av virksomheten som er underlagt sikkerhetsloven, og en begrunnelse om hvorfor det er slik.[293] I gruppeintervju med representanter fra kommunesektoren kommer det fram at det er usikkerhet om hvilke deler av kommunen som er underlagt sikkerhetsloven, og at dette gjør det digitale sikkerhetsarbeidet krevende.[294] Næringslivets sikkerhetsråds beredskapsundersøkelse i 2021 viser at kun 32 prosent av virksomhetene som deltok i undersøkelsen, visste om de var underlagt sikkerhetsloven eller ikke.[295]

Forsvarsdepartementet forteller i intervju at det pågår et omfattende arbeid med å få oversikt over verdikjeder knyttet til grunnleggende nasjonale funksjoner i forsvarssektoren. Departementet beskriver kartleggingen av avhengigheter som komplekst og krevende fordi digitale verdikjeder i stadig større grad er tverrsektorielle. Som eksempel på kompleksiteten viser departementet til at flere av Forsvarets grunnleggende nasjonale funksjoner er knyttet til muligheten til å kommunisere. Disse funksjonene er i stor grad avhengig av for eksempel sivil kommunikasjonsinfrastruktur og satellittbasert kommunikasjon, hvor ansvaret ligger utenfor forsvarssektoren.[296]

[287] Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021*, s. 15–16.
[288] Tildelingsbrevene fra Forsvarsdepartementet er sikkerhetsgraderte og derfor ikke inkludert i sammenstillingen.
[289] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[290] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[291] Nasjonal sikkerhetsmyndighet (2021*) Risiko 2021*, s. 17.
[292] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[293] Riksrevisjonens dybdeundersøkelser.
[294] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[295] Næringslivets sikkerhetsråd (2021) *Beredskapsundersøkelsen 2021*, s. 12.
[296] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.

En av utfordringene med å kartlegge skjermingsverdige informasjonssystemer og infrastruktur innad i forsvarssektoren er ifølge Forsvarsdepartementet at sektoren har svært mange og gamle IKT-systemer. Videre opplever Forsvarsdepartementet at det er en utfordring at ikke alle sektorer har kommet like langt med å implementere sikkerhetsloven. Dette medfører en risiko for at forsvarssektoren har avhengigheter til andre sektorer som ikke er tilstrekkelig beskyttet.[297] Også Nasjonal kommunikasjonsmyndighet poengterer at den trege prosessen med å identifisere grunnleggende nasjonale funksjoner har fått konsekvenser for arbeidet med å identifisere avhengigheter til ekom.[298]

Justis- og beredskapsdepartementet forteller at de har flere samarbeidsprosesser gående, og at målet med disse er å kartlegge tverrsektorielle verdikjeder på bakgrunn av identifiserte grunnleggende nasjonale funksjoner. Olje- og energidepartementet representerer ifølge departementet en kritisk sektor å få kartlagt verdikjedene i. Det har tatt lang tid å komme i gang med arbeidet, men Olje- og energidepartementet har omsider begynt å vurdere hvilke virksomheter i sektoren som skal underlegges sikkerhetsloven. Justis- og beredskapsdepartementet mener at tregheten i arbeidet kan svekke den nasjonale sikkerheten ved at verdier som skal beskyttes, ennå ikke er identifisert og beskyttet godt nok.[299]

5.2.3 Kartleggingen og identifiseringen av verdier og avhengigheter er et løpende arbeid

Justis- og beredskapsdepartementet bemerker at de selv bruker uttrykket *implementering av sikkerhetsloven*, men at dette kan gi et feilaktig inntrykk fordi arbeidet med sikkerhetsloven er en kontinuerlig prosess. Verdiene som identifiseres, må følge av det identifiserte risikobildet, og sikkerhetstiltak må iverksettes som følge av den identifiserte risikoen. Departementet understreker at det er viktig å skape en forståelse for at arbeidet med sikkerhetsloven er en kontinuerlig prosess, blant annet fordi stadig nye samfunnsområder blir en del av det digitale sikkerhetsbildet. Romvirksomhet er for eksempel et nytt område hvor det må identifiseres grunnleggende nasjonale funksjoner og avhengigheter. Departementet skal gjøre dette arbeidet sammen med tre andre departementer.[300]

Også Nasjonal sikkerhetsmyndighet påpeker at arbeidet med å kartlegge avhengighetene til grunnleggende nasjonale funksjoner er en kontinuerlig og dynamisk prosess som påvirkes av den teknologiske utviklingen, endringer i trusselbildet og den generelle samfunnsutviklingen. Sikkerhetsmyndigheten forventer flere innmeldinger av avhengigheter i tiden framover, samtidig som de innmeldte avhengighetene hos virksomhetene vil kunne endre seg over tid.[301]

Ifølge Justis- og beredskapsdepartementet har krigen i Ukraina bidratt til å illustrere den økte kompleksiteten i sikkerhetsarbeidet og til å øke forståelsen av hvor viktig det er å implementere sikkerhetsloven. Departementet benytter denne situasjonen til å jobbe for å øke bevisstheten om digital sikkerhet i de andre departementene, og de har fått god bistand fra Statsministerens kontor i dette arbeidet. Justis- og beredskapsdepartementet synes at prosessen rundt arbeidet med å implementere sikkerhetsloven er god. De understreker samtidig at hvert departement har ansvar for arbeidet med å implementere loven i egne sektorer.[302]

[297] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[298] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[299] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[300] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[301] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[302] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

5.3 Arbeidet med kartlegging av digitale verdikjeder

Justis- og beredskapsdepartementet forteller i intervju at de er særlig opptatt av å identifisere risikoen knyttet til digitale verdikjeder som understøtter samfunnets kritiske funksjoner.[303] Justis- og beredskapsdepartementet er sammen med Direktoratet for samfunnssikkerhet og beredskap ansvarlige for å utvikle et nasjonalt rammeverk for en helhetsvurdering av verdikjeder (jf. tiltak 35 i *Nasjonal strategi for digital sikkerhet* (2019)). Høsten 2018 gav Justis- og beredskapsdepartementet Direktoratet for samfunnssikkerhet og beredskap i oppdrag å sette ned en arbeidsgruppe som skulle utarbeide et nasjonalt rammeverk for å kartlegge digitale verdikjeder. Et av formålene var at rammeverket skal kunne benyttes i prosessen med å identifisere funksjoner som understøtter samfunnets kritiske funksjoner. Et annet var å gi myndighetene en samlet oversikt over digitale verdikjeder. Oppdraget er en oppfølging av NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*.

Høsten 2019 leverte Direktoratet for samfunnssikkerhet og beredskap rapporten *Risikostyring i digitale verdikjeder* til Justis- og beredskapsdepartementet. Rapporten ble utgitt i januar 2020. Et sentralt funn i rapporten er at myndighetene i begrenset grad kan styre sikkerheten i de digitale verdikjedene direkte. De fleste digitale verdikjedene strekker seg utenfor Norges grenser og opereres i stor grad av private leverandører og underleverandører.

Direktoratet for samfunnssikkerhet og beredskap forteller at de ikke har mottatt noen konkret oppfølging av rapporten fra Justis- og beredskapsdepartementet, men at de ba om å få legge den ut på nettsidene sine. Utover dette har ikke Direktoratet for samfunnssikkerhet og beredskap fått flere oppdrag knyttet til rapporten. Det er heller ikke planlagt noen konkret oppfølging eller implementering av rammeverket.[304]

Justis- og beredskapsdepartementet forteller at de ikke bruker rammeverket som presenteres i rapporten *Risikostyring i digitale verdikjeder*, direkte i arbeidet med å kartlegge digitale verdikjeder i samfunnet. Departementet bemerker at rammeverket var et viktig første steg for å ta anbefalingene fra Lysneutvalget videre, og at det har gitt en bedre forståelse for kompleksiteten knyttet til verdikjeder. Departementet er imidlertid i dialog med Kommunal- og distriktsdepartementet om å sette ut et oppdrag for å kartlegge risikoen i digitale verdikjeder og innhente anbefalinger om hvordan man kan tilegne seg en mer risikobasert styring av verdikjedene. Her skal *Rammeverk for kartlegging av digitale verdikjeder* danne et kunnskapsgrunnlag og slik sett bidra til å ta arbeidet med digitale verdikjeder et steg videre. Justis- og beredskapsdepartementet ser dette arbeidet opp mot *Nasjonal strategi for digital sikkerhet* (2019) og hovedmålet om å styrke den digitale grunnmuren i samfunnet. Justis- og beredskapsdepartementet legger til at arbeidet med å kartlegge og styrke digitale verdikjeder er komplekst, og at det derfor har tatt mye tid.[305] Justis- og beredskapsdepartementet bemerker også at dette er et område som det jobbes mye med internasjonalt og som blir sett på som krevende. Departementet har oversatt *Rammeverk for kartlegging av digitale verdikjeder* til engelsk for å kunne dele det med internasjonale samarbeidspartnere og bidra med et kunnskapsgrunnlag i det videre arbeidet på feltet. Videre kommenterer departementet at det har skjedd en utvikling internasjonalt siden rammeverket ble utarbeidet som Nasjonal sikkerhetsmyndighet har arbeidet videre med, kombinert med rammeverket. Departementet mener dette, sammen med oppdraget som skal settes ut i samarbeid med Kommunal- og distriktsdepartementet, vil bidra til en større modenhet og utvikling på området fremover.[306]

[303] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[304] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[305] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[306] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

5.4 Det er stor variasjon i kvaliteten på status- og tilstandsvurderinger av kritiske samfunnsfunksjoner

Departementer med hovedansvar for kritiske samfunnsfunksjoner skal etter samfunnssikkerhetsinstruksens kapittel V punkt 2 *ha oversikt over tilstanden knyttet til sårbarheter for de områder som departementet har et hovedansvar for, og utarbeide status- og tilstandsvurderinger for disse som fremlegges for Stortinget i de årlige budsjettproposisjonene*. Status- og tilstandsvurderingene skal gi Justis- og beredskapsdepartementet en oversikt over samfunnssikkerhetsområdet (jf. kapittel VI punkt 1 a).

I perioden 2017–2021 ble det gjennomført status- og tilstandsvurderinger for alle kritiske samfunnsfunksjoner. Kvaliteten på vurderingene er imidlertid veldig varierende. Det er hovedansvarlig departement[307] som er ansvarlig for å gjennomføre status- og tilstandsvurderinger. Vurderingene tar utgangspunkt i Direktoratet for samfunnssikkerhet og beredskaps rapport *Samfunnets kritiske funksjoner* fra 2016. Rapporten angir hvilke funksjoner som er samfunnskritiske, hvem som er ansvarlige for dem, og hvilke funksjonsevner (kapabiliteter) som skal ivaretas. Digitale angrep som rammer nødvendig styrings- og kommunikasjonsinfrastruktur, står oppført som en sårbarhet som skal vurderes for alle de samfunnskritiske funksjonene.

Departementene har utarbeidet status- og tilstandsvurderingene med ulik framgangsmåte og det varierer med hensyn til hvor omfattende de er. Forsvarets forskningsinstitutt gikk i 2020 gjennom de åtte vurderingene som hadde blitt rapportert til Stortinget, og uttrykker at de fleste vurderingene gir gode beskrivelser av regelverk og systemer. Forsvarets forskningsinstitutt påpeker at i vurderingene framheves de som anses å fungere bra, og at det er gitt lite oppmerksomhet til sårbarhetene i systemene som er vurdert. En annen utfordring som trekkes frem av Forsvarets forskningsinstitutt er at vurderingene er overordnede og i liten grad gir konkrete forslag til forbedringer og tiltak. Et krav i samfunnssikkerhetsinstruksen er at status- og tilstandsvurderingene skal gi en oversikt over tilstanden knyttet til sårbarheter. Forsvarets forskningsinstitutt mener at det i mange av vurderingene er krevende å få oversikt, og at en mer ensartet presentasjon av vurderingene kunne ha gjort det enklere å få en helhetlig oversikt over tilstanden.[308]

Et viktig formål med status- og tilstandsvurderingene er at regjeringen skal rapportere til Stortinget om det brede samfunnssikkerhetsarbeidet, hva tilstanden er, hvilke risikoer og sårbarheter som er gjeldende innenfor de ulike kritiske samfunnsfunksjonene, hvilke tiltak som er igangsatt, og hvilke tiltak som bør prioriteres framover. Ifølge Forsvarets forskningsinstitutt er det krevende at vurderingene presenteres for Stortinget som en del av budsjettproposisjonene for de respektive departementene. Det kan være utfordrende å holde oversikt over hvor de de ulike status- og tilstandsvurderingen finnes. I og med at de forekommer i ulike budsjettproposisjoner over en fireårsperiode, kan det være vanskelig å få en samlet oversikt over hvilke status- og tilstandsvurderinger som faktisk er utført.[309] Videre framstår vurderingene mer som en beskrivelse av alle tiltak som er i prosess, enn en framstilling av risiko og sårbarheter og behovene for forbedring. I tillegg er informasjon om sårbarheter ofte sensitiv informasjon som myndighetene ikke ønsker å offentliggjøre, noe som kan føre til at viktig informasjon om sårbarheter utelates.[310]

I *Veileder til samfunnssikkehetsinstruksen* fra 2019 går det fram at status- og tilstandsvurderingene bør utarbeides etter en så lik ramme som mulig og gi et mest mulig realistisk bilde av hvilke utfordringer samfunnet står overfor på området, tiltakenes betydning og hvilke ytterligere tiltak som kan være nødvendige. Videre søker Justis- og beredskapsdepartementet å utarbeide et felles rammeverk for slike status- og tilstandsvurderinger. Justis- og beredskapsdepartementet forteller at

[307] Departementet som er hovedansvarlig for hver funksjon, står i Prop. 1 S for Justis- og beredskapsdepartementet.
[308] Forsvarets forskningsinstitutt (2020) *Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger*, s. 67–68.
[309] Forsvarets forskningsinstitutt (2020) *Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger*, s. 68.
[310] Forsvarets forskningsinstitutt (2020) *Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger*, s. 68.

det ved oppstart av arbeidet med hver enkelt status- og tilstandsvurdering har hatt møte med det hovedansvarlige departementet. I møtet har Justis- og beredskapsdepartementet lagt fram et forslag til hvordan en slik vurdering kan gjennomføres. Samtidig har det blitt understreket at det er opp til hvert ansvarlig departement å bestemme hvordan vurderingene skal gjennomføres. Dette gjenspeiles ifølge Justis- og beredskapsdepartementet i noe ulik innretning på og detaljeringsgrad i vurderingene av status og tilstand. [311]

I intervju oppgir Justis- og beredskapsdepartementet at det per juni 2022 ikke er utarbeidet et felles rammeverk for gjennomføringen av status- og tilstandsvurderinger. Ifølge instruksen skal status- og tilstandsvurderinger inngå i departementenes budsjettproposisjoner. Departementet har dette til vurdering og opplyser at arbeidet med å etablere et rammeverk for gjennomføring og rapportering omfattes av en varslet revisjon av samfunnssikkerhetsinstruksen som skal pågå høsten 2022.[312]

5.5 Departementenes risiko- og sårbarhetsanalyser benyttes ikke som kilde

I henhold til samfunnssikkerhetsinstruksen skal departementene som et ledd i arbeidet med samfunnssikkerhet utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser. Disse skal utarbeides på grunnlag av vurderinger av tilsiktede og utilsiktede hendelser som kan true departementets og sektorens funksjonsevne og sette liv, helse og materielle verdier i fare (jf. samfunnssikkerhetsinstruksen kapittel IV punkt 2). Tilsvarende skal departementene med hovedansvar for kritiske samfunnsfunksjoner utarbeide og vedlikeholde risiko- og sårbarhetsanalyser for disse funksjonene (jf. samfunnssikkerhetsinstruksen kapittel V punkt 1).

Vi har som en del av undersøkelsen sendt ut skriftlige spørsmål til departementene om hvordan de gjennomfører sine risiko- og sårbarhetsanalyser. Svarene fra departementene viser at det varierer hvordan arbeidet med risiko- og sårbarhetsanalysene er organisert, hvor mye og hvordan digital sikkerhet er tematisert i analysene, hvordan underliggende virksomheter har blitt involvert i analysene, hvilke faglige standarder, rammeverk, veiledere og kilder som har blitt benyttet i arbeidet, og hvorvidt departementene har fått veiledning fra Justis- og beredskapsdepartementet eller Direktoratet for samfunnssikkerhet og beredskap. Vi presenterer funnene fra gjennomgangen i det følgende.

Det er gjennomgående små forskjeller i svarene på de skriftlige spørsmålene knyttet til risiko- og sårbarhetsanalysene av departementets og sektorens funksjonsevne og svarene knyttet til risiko- og sårbarhetsanalysene av de kritiske samfunnsfunksjonene. Svarene er derfor slått sammen i den følgende oppsummeringen.

Samfunnssikkerhetsinstruksen stiller krav til systematikk og dokumentasjon i arbeidet med risiko- og sårbarhetsanalysen for sektoren. Analysen må derfor nedfelles skriftlig, gjennomgås jevnlig og oppdateres ved behov. Oppdateringsfrekvensen kan blant annet vurderes på grunnlag av utviklingen i risikoforholdene og/eller kunnskapsgrunnlaget innenfor departementets ansvarsområde.

Det digitale sikkerhetsområdet er et område i rask utvikling, og risikoen for digitale angrep er i stadig vekst, slik det poengteres i risikovurderingene fra etterretnings- og sikkerhetstjenestene. Det er slik sett viktig at risiko- og sårbarhetsanalysene av uønskede digitale hendelser oppdateres jevnlig. Tre departementer (Justis- og beredskapsdepartementet, Helse- og omsorgsdepartementet og Klima- og miljødepartementet) ferdigstilte eller oppdaterte risiko- og sårbarhetsanalysen av departementets og sektorens funksjonsevne siste gang i 2019. To departementer (Utenriksdepartementet og Kunnskapsdepartementet) oppdaterte sine analyser i 2020. Barne- og familiedepartementet og Nærings- og fiskeridepartementet oppdaterte sine analyser i 2021 og Olje- og energidepartementet og

[311] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[312] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

Kultur- og likestillingsdepartementet i 2022. Landbruks- og matdepartementet oppdaterte risiko- og sårbarhetsanalysen i 2016, og bemerker at trussel- og risikovurderinger knyttet til digital sikkerhet kommer fram i andre dokumenter. Finansdepartementet oppdaterte sin analyse i 2017, og bemerker at de er i ferd med å oppdatere den departementsinterne risiko- og sårbarhetsanalysen. Arbeids- og inkluderingsdepartementet oppdaterte sin analyse i 2018, men har planlagt å ferdigstille en ny analyse ved årsskiftet 2022/2023.

Utover risiko- og sårbarhetsanalysen for sektoren trekker flere av departementene fram interne risiko- og sårbarhetsanalyser for departementet, departementets interne styringssystem og risiko- og sårbarhetsanalyser gjennomført i underliggende virksomheter, hvor digitale uønskede hendelser har blitt inkludert som tematikk/scenario.

5.5.1 Behandlingen av digitale hendelser i risiko- og sårbarhetsanalysene

Alle departementene svarer at digitale angrep er behandlet i den siste overordnede risiko- og sårbarhetsanalysen for sektoren. Departementene varierer med hensyn til hvor mange av scenarioene i risiko- og sårbarhetsanalysen som omhandler uønskede digitale hendelser, og om dette oppgis. For eksempel viser Kunnskapsdepartementet til at fire av de tjue skisserte scenarioene i risiko- og sårbarhetsanalysen for sektoren omhandler digitale, tilsiktede handlinger. Samferdselsdepartementet viser til at digitalt angrep ble tematisert i risiko- og sårbarhetsanalysen, og at risiko og sårbarhet knyttet til digital avhengighet i transportsektoren ble viet spesiell oppmerksomhet, uten å utdype dette ytterligere. I Arbeids- og inkluderingsdepartementets siste risiko- og sårbarhetsanalyse vurderte de seks ulike scenarioer under den samfunnskritiske funksjonen «IKT-sikkerhet i sivil sektor».

Nedenfor følger noen eksempler på scenarioer som var inkludert i risiko- og sårbarhetsanalysene knyttet til uønskede digitale hendelser.

Faktaboks 16 Eksempel på scenarioer

«Cyberangrep fra annen stat mot ekom-infrastruktur» (Justis- og beredskapsdepartementet, sektor-ROS)

«Svikt i IKT-systemer» (Nærings- og fiskeridepartementet, sektor-ROS)

«Cyberangrep mot banknæringene» (Finansdepartementet, sektor-ROS)

«Alvorlig svikt i IKT-infrastrukturen i Folketrygdfondet» (Finansdepartementet, sektor-ROS)

«Digitalt angrep mot ekom-infrastruktur som rammer Meteorologisk institutt» (Klima- og miljødepartementet, sektor-ROS)

«Sensitiv informasjon på avveie» (Klima- og miljødepartementet, sektor-ROS)

Scenarioer relatert til sikring av registre og arkiver (Arbeids- og inkluderingsdepartementet, ROS-analyse knyttet til den kritiske samfunnsfunksjonen «IKT-sikkerhet i sivil sektor»)

Scenarioer knyttet til hendelser i informasjons- og kommunikasjonssystemer (Arbeids- og inkluderingsdepartementet, ROS-analyse knyttet til den kritiske samfunnsfunksjonen «IKT sikkerhet i sivil sektor»)

Kilde: Svar på Riksrevisjonens spørsmål til departementene om risiko- og sårbarhetsanalyser, april 2022.

Noen av scenarioene er bredt beskrevet, for eksempel «svikt i IKT-systemer» og «sensitiv informasjon på avveie», mens andre er mer konkrete, for eksempel «digitalt angrep mot ekom-infrastruktur som rammer Meteorologisk institutt». Departementene ser imidlertid ut til å ha en noenlunde lik oppfatning av hva som menes med en uønsket digital hendelse.

5.5.2 Organiseringen av arbeidet med risiko- og sårbarhetsanalyser

Føringene for risiko- og sårbarhetsanalysene gis i tildelingsbrevet og/eller i virksomhetsinstruksen. Overordnet sett organiserer som nevnt departementene arbeidet med risiko- og sårbarhetsanalyser tilknyttet digitale angrep på ulike måter. Tre av departementene, Justis- og beredskapsdepartementet, Nærings- og fiskeridepartementet og Finansdepartementet, har satt ut arbeidet med risiko- og sårbarhetsanalyser til eksterne, herunder Direktoratet for samfunnssikkerhet og beredskap, Forsvarets forskningsinstitutt og PwC. Resten av departementene kan grovt sett skilles fra hverandre basert på om ansvaret for å gjennomføre risiko- og sårbarhetsanalysene ligger hos administrasjons- og/eller organisasjonsavdelingen eller hos sikkerhets- og/eller beredskapsavdelingen.

I *Veileder til samfunnssikkerhetsinstruksen* fra 2019 anbefales departementet å involvere underliggende/tilknyttede virksomheter og innhente og vurdere analyser fra de virksomhetene som er relevante for departementets risikobilde. Videre heter det at departementet kan komme med bestillinger om hva disse analysene skal inneholde.

Ifølge veilederen er den vanligste videre prosedyren at analysene forelegges fagavdelingene, administrasjons- og/eller organisasjonsavdelingen eller sikkerhets- og/eller beredskapsavdelingen i departementene. Alle departementene svarer at underliggende/tilknyttede virksomheter ble involvert i arbeidet med departementets siste risiko- og sårbarhetsanalyse. Hvordan innspillene ble innhentet, og hvordan de ble benyttet, varierer imidlertid. Åtte av departementene svarer at de har benyttet virksomhetenes egne risiko- og sårbarhetsanalyser som underlag for sine analyser, og at disse i hovedsak ble benyttet for å identifisere spesielt utsatte områder i sektoren. Resten av departementene oppgir at de kun benyttet innspill fra underliggende/tilknyttede virksomheter i sine analyser. Syv departementer gav spesifikke bestillinger til underliggende virksomheter om at risiko- og sårbarhetsanalysene skulle omfatte risikoen for digitale angrep. Det varierer hvor konkrete disse bestillingene var vedrørende analysenes innhold.

Ifølge samfunnssikkerhetsinstruksen skal det enkelte departement kunne dokumentere at det koordinerer sitt eget arbeid med forebygging, beredskap og krisehåndtering med andre berørte departementer (jf. kapittel IV punkt 6). Seks av departementene svarer at de ikke har samarbeidet med andre departementer om risiko- og sårbarhetsanalysen av departementets og sektorens funksjonsevne, som omfatter digitale angrep. Flere av disse trekker imidlertid fram at de har latt seg inspirere av andre departementers risiko- og sårbarhetsanalyser. Flere trekker også fram samhandlingsarenaen *Nettverk for nasjonal IKT-sikkerhet* og *Samordningsrådet for samfunnssikkerhet*, hvor arbeidet med risiko- og sårbarhetsanalyser har vært diskutert. Samarbeidet mellom departementene synes å være tettere når det gjelder risiko- og sårbarhetsanalysene knyttet til de kritiske samfunnsfunksjonene hvor ansvaret er delt mellom ulike departementer. Dette skyldes at analysene i slike tilfeller utvikles i samarbeid mellom de ansvarlige departementene. Det varierer imidlertid hvor tette og formaliserte disse samarbeidene er.

Risiko- og sårbarhetsanalysene som departementene utarbeider, bør ifølge *Veileder til samfunnssikkerhetsinstruksen* forankres i egen organisasjon og ledelse. Prosessen for å forankre og følge opp risiko- og sårbarhetsanalysene i departementene beskrives relativt likt. Samtlige departementer oppgir at prosessen for risiko- og sårbarhetsanalysene følger den ordinære linjen for beslutninger i departementet. Dette gjelder imidlertid risiko- og sårbarhetsanalysen i sin helhet. Vi har ikke informasjon om hvor stor oppmerksomhet den delen av analysen som omfatter digitale uønskede hendelser, får hos ledelsen, og hvilken betydning forankringen har.

5.5.3 Informasjonsunderlag og veiledning i arbeidet med risiko- og sårbarhetsanalyser

Samfunnssikkerhetsinstruksen stiller krav til at departementenes risiko- og sårbarhetsanalyser skal bygge på blant annet nasjonale trussel- og risikovurderinger. Det varierer som nevnt hvilke faglige standarder, rammeverk, veiledere og kilder som har blitt benyttet i arbeidet med risiko- og sårbarhetsanalysene, og hvorvidt departementene har bedt om og fått veiledning i arbeidet. Svarene på Riksrevisjonens skriftlige spørsmål viser at departementene til sammen legger 23 ulike veiledere, faglige standarder og rammeverk til grunn for arbeidet med risiko- og sårbarhetsanalysene. Flest ganger nevnes *Veileder for fylkesmannens arbeid med risiko- og sårbarhetsanalyser* (2020) (utarbeidet av Direktoratet for samfunnssikkerhet og beredskap). Klima- og miljødepartementet har utviklet sin egen *Veileder for sektor-ROS*, blant annet inspirert av *Veileder for fylkesmannens arbeid med risiko- og sårbarhetsanalyser* (2020), i mangel av en veileder for helhetlig risiko- og sårbarhetsanalyse på departements- og sektornivå.

Utover *Veileder for fylkesmannens arbeid med risiko- og sårbarhetsanalyser* (2020) nevner de fleste departementene at de benyttet standard for risikostyring ISO-31000[313] og NS5814[314] samt Direktoratet for samfunnssikkerhet og beredskaps arbeid knyttet til analyse av krisescenarioer. Utover rammeverk, veiledere og faglige standarder nevner departementene en rekke ulike kilder (totalt 29) som de benyttet i arbeidet med risiko- og sårbarhetsanalysene. Samtlige har brukt en kombinasjon av flere kilder. Flere oppgir trusselvurderingene fra sikkerhets- og etterretningstjenestene og Direktoratet for samfunnssikkerhet og beredskaps *Analyse av krisescenarioer fra 2019* som kilder.

Åtte av tretten departementer svarer at de ikke har bedt om eller fått veiledning fra Justis- og beredskapsdepartementet eller Direktoratet for samfunnssikkerhet og beredskap i forbindelse med utarbeidelsen av risiko- og sårbarhetsanalysene knyttet til digitale angrep. Fem oppgir at de har bedt om og fått veiledning, alle fra Direktoratet for samfunnssikkerhet og beredskap. Ett departement har fått bistand både fra Justis- og beredskapsdepartementet og Direktoratet for samfunnssikkerhet og beredskap.

Justis- og beredskapsdepartementet forteller i intervju at de ikke bruker departementenes risiko- og sårbarhetsanalyser som kilde for å holde oversikt over den digitale sikkerhetstilstanden. Selv om departementene vurderer sårbarheter i egne sektorer i disse analysene, er Justis- og beredskapsdepartementet usikker på om de dekker den digitale sikkerheten godt nok til å gi innsikt i den digitale sikkerhetstilstanden. Siden departementene utfører risiko- og sårbarhetsanalysene på ulike måter, antar Justis- og beredskapsdepartementet at arbeidet med å sammenstille analysene ville ha vært for ressurskrevende og utfordrende sammenlignet med det utbyttet de hadde fått igjen for det.[315]

5.6 Tilsyn med den digitale sikkerheten

I dette delkapitlet presenterer vi tilsynsvirksomheten på det digitale sikkerhetsområdet. For myndighetene er tilsyn et sentralt virkemiddel som skal sikre at regelverkene som regulerer arbeidet med digital sikkerhet, overholdes. Resultatene fra tilsynsvirksomheten kan gi myndighetene viktig informasjon om statusen for det pågående sikkerhetsarbeidet og sikkerhetsnivået i de ulike sektorene. Justis- og beredskapsdepartementet omtaler tilsynsrapporter som en viktig kilde til departementets oversikt over den nasjonale digitale sikkerhetstilstanden.[316]

[313] ISO 31000 er et verktøy som organisasjoner kan bruke til å utvikle en strategi for risikostyring for å identifisere og begrense risikoer og på den måten øke sannsynligheten for å nå mål og forbedre beskyttelsen av anlegg og verdier. Det overordnede målet er å utvikle en risikostyringskultur der ansatte og interessenter er klar over hvor viktig det er å overvåke og håndtere risiko.
[314] NS 5814 *Krav til risikovurderinger* handler om krav til risikovurderinger og er et hjelpemiddel som bedrifter kan bruke når de skal ta beslutninger om tiltak eller velge løsninger for å forebygge risiko. Standarden stiller krav til elementene som kan inngå i en slik prosess.
[315] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[316] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

Departementene har ansvar for å følge opp at virksomhetene i egen sektor gjennomfører aktiviteter i tråd med aktuelt regelverk, og at samfunnssikkerheten i sektoren ivaretas. Direktoratet for samfunnssikkerhet og beredskap skal, på vegne av Justis- og beredskapsdepartementet, føre tilsyn med departementenes arbeid med å følge opp egen sektor etter samfunnssikkerhetsinstruksen. Tilsvarende gjennomfører statsforvalteren tilsyn med kommunenes samfunnssikkerhetsarbeid etter sivilbeskyttelsesloven.

Nasjonal sikkerhetsmyndighet og Datatilsynet er de mest sentrale tilsynsvirksomhetene når det gjelder det generelle regelverket. I tillegg er det en rekke tilsynsmyndigheter som gjennomfører tilsyn etter de ulike sektorspesifikke regelverkene. I det følgende redegjør vi for framgangsmåten og omfanget av tilsynene etter samfunnssikkerhetsinstruksen, sivilbeskyttelsesloven og sikkerhetsloven. Vi omtaler også tilsynsvirksomheten til Datatilsynet, Nasjonal kommunikasjonsyndighet og NVE.

5.6.1 Tilsyn med samfunnssikkerhet

Digital sikkerhet, som er en integrert del av samfunnssikkerhetsarbeidet, inngår i samfunnssikkerhetsinstruksens og sivilbeskyttelseslovens virkeområde og kan være en del av tilsynene med samfunnssikkerhet.[317]

Justis- og beredskapsdepartementet er pålagt å føre tilsyn med departementenes arbeid med samfunnssikkerhet og beredskap gjennom kgl.res. av 10. mars 2017 nr. 312 (gjelder ikke Forsvarsdepartementet). Direktoratet for samfunnssikkerhet og beredskap gjennomfører tilsynene på vegne av Justis- og beredskapsdepartementet, mens Helse- og omsorgsdepartementet fører tilsyn med hvordan Justis- og beredskapsdepartementet ivaretar samordningsrollen på samfunnssikkerhetsområdet, eventuelt med bistand fra Direktoratet for samfunnssikkerhet og beredskap. Gjennomføringen av slike tilsyn er regulert i kapittel VII i samfunnssikkerhetsinstruksen og tjener to formål – å fremme god kvalitet på samfunnssikkerhetsarbeidet som de enkelte departementene har ansvar for, og å fremme et samordnet og helhetlig arbeid med samfunnssikkerhet på tvers av departementer og sektorer.

Tilsyn med Justis- og beredskapsdepartementets samordningsrolle

Det siste tilsynet med Justis- og beredskapsdepartementets samordningsrolle ble gjennomført av Helse- og omsorgsdepartementet i 2013, og da ble det påpekt noen brudd på krav.[318] Direktoratet for samfunnssikkerhet og beredskap hadde tidligere gjennomført tilsyn med Justis- og beredskapsdepartementet i 2002 og 2007/2008.[319] Bruddene og andre forbedringspunkter omfatter Justis- og beredskapsdepartementets oppgaver både i egen sektor og i samordningsrollen. Når det gjelder tilsyn med departementenes samfunnssikkerhetsarbeid, har det ifølge rapporten fra Helse- og omsorgsdepartementets tilsyn i 2013 vært en betydelig utvikling i tilsynsarbeidet. Tilsynene har gått fra å være utredninger med relativt forsiktige råd, til å bli mer tradisjonelle tilsyn ut fra instruksverk der det forventes at departementet som har vært underlagt tilsyn retter opp eventuelle påpekte forhold. Det går også fram at tilsynene i større grad framstår som brede gjennomganger enn som tilsyn som er spisset mot risiko og vesentlighet, og at Direktoratet for samfunnssikkerhet og beredskap bør involveres sterkere i oppfølgingen.

Justis- og beredskapsdepartementet har arbeidet systematisk for å lukke bruddene som er påpekt i rapporten, og avvik ble utbedret i det påfølgende året. Etter Helse- og omsorgsdepartementets tilsyn endret Justis- og beredskapsdepartementet tilsynsmetodikken, og den ble tatt inn i samfunnssikkerhetsinstruksen i 2017. Det er ikke gjennomført tilsyn eller andre evalueringer av Justis-

[317] Justis- og beredskapsdepartementet (2019) *Veileder til samfunnssikkerhetsinstruksen*, s. 7.
[318] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[319] Helsetilsynet (2014) *Rapport fra tilsyn med samfunnssikkerhets- og beredskapsarbeidet i Justis- og beredskapsdepartementet. Inkludert undersøkelser i Direktoratet for samfunnssikkerhet og beredskap, Politidirektoratet og to politidistrikter*.

og beredskapsdepartementets samordningsrolle eller arbeid med samfunnssikkerhet i egen sektor etter at instruksen ble endret.

Tilsyn med departementenes arbeid med samfunnssikkerhet

Fra 2002 til 2017 gjennomførte Direktoratet for samfunnssikkerhet og beredskap, på vegne av Justis- og beredskapsdepartementet, tre tilsynsrunder med alle departementene og deres arbeid med samfunnssikkerhet og beredskap. Tilsynsrundene ble gjennomført etter en plan over fem år, og hvert tilsyn strakk seg over en periode på vel to år.

Den tredje tilsynsrunden ble i 2017 evaluert av Forsvarets forskningsinstitutt og Direktoratet for forvaltning og IKT.[320] I evalueringsrapporten trekkes det fram flere svakheter, blant annet at tilsynene burde vært basert på risiko og vesentlighet, slik at de i større grad konsentreres om de mest kritiske samfunnsfunksjonene. Det gikk også fram at tverrsektorielle utfordringer burde vektlegges mer, slik at Justis- og beredskapsdepartementet framstår som en tydelig premissleverandør for samfunnssikkerhetsarbeidet, og at kravene i instruksen burde tydeliggjøres bedre. Evalueringen ble lagt til grunn for Direktoratet for samfunnssikkerhet og beredskaps arbeid med å utvikle en ny samfunnssikkerhetsinstruks og en ny veileder. I den nye instruksen blir det stilt krav om hvordan Justis- og beredskapsdepartementet skal ivareta samordningsansvaret. Det blir også stilt krav om at tilsyn skal baseres på risiko, og det blir stilt mer spesifikke krav til departementer med hovedansvar for kritiske samfunnsfunksjoner. Ifølge Direktoratet for samfunnssikkerhet og beredskap var det en oppfatning at tilsynsrundene tidvis kunne bli slaviske, og at tilsynene ikke traff så godt som ønskelig. Direktoratet opplever at den nye instruksen har tydeliggjort kravene til departementene.[321]

Da Helsetilsynet i 2013–2014 førte tilsyn med Justis- og beredskapsdepartementets arbeid med samfunnssikkerhet, omfattet tilsynet vurderinger av om det forelå brudd på kravene samfunnssikkerhetsinstruksen stiller. Denne praksisen ble videreført i de påfølgende tilsynene i tilsynsrunde tre, og da samfunnssikkerhetsinstruksen ble revidert i 2017, ble det presisert at tilsyn skulle omtale eventuelle brudd på instruksens krav. Justis- og beredskapsdepartementet besluttet at det skulle gjennomføres tilsyn med nye krav i de tre departementene som ikke hadde vært gjenstand for tilsyn med «brudd på krav»-tilnærmingen i tilsynsrunde tre. Siden 2017 har det derfor vært ført tilsyn med Klima- og miljødepartementet, Nærings- og fiskeridepartementet og Olje- og energidepartementet. Disse tilsynene avslutter tredje tilsynsrunde.[322]

Det er Justis- og beredskapsdepartementet som avgjør hvilke departementer det skal føres tilsyn med, og de angir dette i tildelingsbrev til Direktoratet for samfunnssikkerhet og beredskap.[323] Et tilsyn dreier seg hovedsakelig om arbeidet til det departementet som har ansvar for en samfunnskritisk funksjon, men det kan også gjelde andre departementer fordi en funksjon kan eies av flere. Tilsynet skal omfatte etterlevelsen av samfunnssikkerhetsinstruksens kapittel IV, V og VI, men ikke områder som andre myndigheter fører tilsyn med etter eget lov- og forskriftsverk. Justis- og beredskapsdepartementet opplyser at Direktoratet for samfunnssikkerhet og beredskap innhenter informasjon og utarbeider forslag til hvordan tilsynet skal innrettes, basert på risiko og vesentlighet. Justis- og beredskapsdepartementet gir Direktoratet for samfunnssikkerhet og beredskap innspill til innretningen dersom departementet er kjent med særskilte forhold som bør omfattes av tilsynet.[324]

For at tilsynet skal kunne verifisere at departementet etterlever instruksens krav, og at kritiske samfunnsfunksjoner er tilstrekkelig ivaretatt, kan det ifølge instruksen omfatte målrettede og avgrensede undersøkelser i departementet og underlagte virksomheter. I tilsynet med Olje- og energidepartementets samfunnssikkerhetsarbeid ble det for eksempel gjennomført intervjuer/samtaler

[320] Forsvarets forskningsinstitutt og Direktoratet for forvaltning og IKT (2017) *Evaluering av tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid - tredje tilsynsrunde.* Difi-rapport 2017:4.
[321] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[322] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[323] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[324] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.

med NVE siden direktoratet blant annet bidrar til departementets risiko- og sårbarhetsanalyser. Ifølge veilederen bør tilsynene være systemrettede, samtidig som det er viktig å kontrollere at styringssystemene på samfunnssikkerhetsområdet faktisk fungerer og har reell betydning for styringen av departementet og sektoren.

I tillegg til kravene i samfunnssikkerhetsinstruksen undersøker Direktoratet for samfunnssikkerhet og beredskap om relevante områder i *Nasjonal strategien for digital sikkerhet* fra 2019 med tilhørende tiltaksplan følges opp, for eksempel områder knyttet til risiko- og sårbarhetsanalyser og arbeidet med responsmiljøer for håndtering av digitale sikkerhetshendelser. Direktoratet for samfunnssikkerhet og beredskap erfarer at departementene tar arbeidet med risiko- og sårbarhetsanalyser på stort alvor. Tilsynet kan også omfatte departementenes arbeid med øvelser og hvordan de inkluderer digital sikkerhet i disse. Det omfatter derimot ikke detaljer i IKT-løsninger, men tilsynet kan for eksempel undersøke hvordan arbeidet med digital sikkerhet følges opp i etatsstyringen og i departementenes dialog med underliggende virksomheter samt internt i departementet. Direktoratet for samfunnssikkerhet og beredskap undersøker om pålagt dokumentasjon er på plass, og om innholdet i dokumentasjonen virker fornuftig.[325] I den ovennevnte evalueringsrapporten fra 2017 står det at hvis formålet med tilsynsordningen er å identifisere og avdekke reelle sårbarheter i sektoren, så var tilsyn den gang ikke det riktige virkemiddelet. Dette ble begrunnet med at tilsynene er systemtilsyn, at departementene er målgruppen for tilsynene, og at formålet med tilsynet er å kontrollere departementets samfunnssikkerhet- og beredskapsarbeid, ikke identifisere sårbarheter i sektoren.[326] Innretningen av tilsynene etter den nye samfunnssikkerhetsinstruksen er ikke vesentlig endret på dette området.

Direktoratet for samfunnssikkerhet og beredskap har utarbeidet vurderingskriterier for tilsyn og en mal for gjennomgang av dokumentasjon til hjelp i gjennomføringen av tilsyn. Hensikten med kriteriegrunnlaget er å skape forutsigbare og enhetlige tilsyn ved at de ulike departementene blir vurdert opp mot de samme vurderingskriteriene.[327] Direktoratet for samfunnssikkerhet og beredskap fører dokumenttilsyn på systemnivå og understreker at det ikke foretas tekniske undersøkelser som en del av tilsynene.[328] Basert på en dokumentgjennomgang og intervjuer utarbeider direktoratet en rapport som beskriver forbedringsområder og/eller brudd på krav. Ved brudd på krav kan departementet pålegges å gjennomføre tiltak.[329] Justis- og beredskapsdepartementet sender rapporten til det aktuelle departementet og rapporterer til regjeringen dersom det er avdekket brudd på krav.[330]

Av de tre tilsynsrapportene fra perioden 2020–2022 går det fram at departementenes oppfølging av den digitale sikkerheten skal være integrert i arbeidet med samfunnssikkerhet.[331] Ifølge Justis- og beredskapsdepartementet er disse tilsynene i mye større grad enn tidligere basert på risiko og vesentlighet når det gjelder valg av tema. Videre opplyser departementet at det vil bli interessant å vurdere om ordningen med risikobaserte tilsyn har fungert etter intensjonen når tilsynene med Klima- og Miljødepartementet og Nærings- og fiskeridepartementet er avsluttet.[332] Tilsynene ble avsluttet henholdsvis august 2021 og mars 2022. Justis- og beredskapsdepartementet hadde per november 2022 ikke vurdert hvordan ordningen med risikobaserte tilsyn fungerer.[333]

[325] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[326] Forsvarets forskningsinstitutt og Direktoratet for forvaltning og IKT (2017) *Evaluering av tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid - tredje tilsynsrunde.* Difi-rapport 2017:4.
[327] Direktoratet for samfunnssikkerhet og beredskap − *Samfunnssikkerhetsinstruksen for departementene − Vurderingskriterier for tilsyn av 6. mars 2020*.
[328] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[329] Justis- og beredskapsdepartementet (u.å.) *Prosesstrinn tilsyn v 5(1).* Veileder publisert på departementets nettsider. [Hentedato 2. mars 2022].
[330] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[331] Direktoratet for samfunnssikkerhet og beredskap (2021) *Rapport: Tilsyn med Nærings- og fiskeridepartementets arbeid med samfunnssikkerhet*, 23. mars 2022; Direktoratet for samfunnssikkerhet og beredskap (2020) *Rapport fra tilsyn med Olje- og energidepartementets samfunnssikkerhetsarbeid*, 2. juni 2020; Direktoratet for samfunnssikkerhet og beredskap (2021) *Rapport: Tilsyn med Klima- og miljødepartementets arbeid med samfunnssikkerhet*, 31. august 2021.
[332] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[333] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

Direktoratet for samfunnssikkerhet og beredskap har på bakgrunn av innsendt dokumentasjon gjennomført en vesentlighets- og risikovurdering av de ulike temaene i instruksen. Vurderingen ligger til grunn for hvilke temaer som velges ut for nærmere undersøkelse gjennom tilsyn, og hvilke som vurderes som tilfredsstillende ivaretatt, og som dermed ikke omfattes av tilsynet. Tilsynene omfatter departementenes generelle arbeid med samfunnssikkerhet og ikke departementenes oppfølging av den digitale sikkerheten eller andre områder spesielt.[334] Justis- og beredskapsdepartementet antar at dette skyldes at digital sikkerhet ikke har bemerket seg i Direktoratet for samfunnssikkerhet og beredskaps risikovurderinger og dermed ikke har vært gjenstand for tilsyn.[335] I tilsynsrapportene beskriver Direktoratet for samfunnssikkerhet og beredskap statusen for arbeidet på de områdene som er plukket ut til tilsyn, direktoratets vurdering av statusen sett opp mot kravene i instruksen og en konklusjon. I konklusjonen presenteres eventuelle brudd på krav og forbedringsområder. I alle de tre tilsynene har direktoratet påpekt avvik eller forbedringsområder for risiko- og sårbarhetsanalyser, beskrivelse av tiltak, øvelser og evaluering av øvelser og hendelser. Alle funnene er beskrevet generelt, og statusen for departementenes oppfølging av den digitale sikkerheten framgår ikke.

Direktoratet for samfunnssikkerhet og beredskap har ikke avdekket manglende digital sikkerhetskompetanse i departementene gjennom tilsyn. Direktoratet forholder seg i først og fremst til dokumentasjon og følger ved behov opp dokumentasjonen med samtaler med ansatte i departementet. I disse samtalene er det ikke blitt avdekket mangel på kompetanse.[336] Direktoratet for samfunnssikkerhet og beredskap opplever at departementene tar oppgaven med digital sikkerhet på stort alvor, og at det jobbes systematisk med å følge opp kravene på området. Direktoratet legger til at pandemien har gjort at disse tilsynene har tatt lengre tid enn planlagt.[337]

Direktoratet for samfunnssikkerhet og beredskap opplever videre at arbeidet med digital sikkerhet handler om modning og bevisstgjøring i departementene. For eksempel er forvaltningen mest oppmerksom på konsekvensene av bortfall av sentral infrastruktur, og hvordan det kan håndteres. Generelt sett ser direktoratet en større modenhet i departementene nå enn tidligere når det gjelder forståelsen av bredden i arbeidet med digital sikkerhet. Direktorat mener at forståelsen i departementene er viktig for arbeidet i de underliggende virksomhetene. Alle hendelsene som har funnet sted den siste tiden, får tydelig fram de konkrete konsekvensene av et digitalt angrep og fører dermed til at arbeidet med digital sikkerhet får økt oppmerksomhet. Her er angrepet på Østre Toten et godt eksempel.[338]

Tilsyn med samfunnssikkerhet i kommunesektoren

Kommunenes samfunnssikkerhetsarbeid reguleres av sivilbeskyttelsesloven og helseberedskapsloven. Direktoratet for samfunnssikkerhet og beredskap har som forvalter av sivilbeskyttelsesloven et særlig tilsynsansvar overfor kommunene. Selve tilsynet etter denne loven gjennomføres av statsforvalteren, mens Direktoratet for samfunnssikkerhet og beredskap gir veiledning. Statsforvalteren avgjør selv hvilke kommuner det skal føres tilsyn med.[339]

Det er et lovbestemt krav at det hvert år skal føres risikobaserte tilsyn etter sivilbeskyttelsesloven og helseberedskapsloven med én fjerdedel av kommunene. Tilsynene etter helseberedskapsloven gjennomføres som felles tilsyn med kommunal beredskapsplikt basert på en felles veileder som er utarbeidet av Direktoratet for samfunnssikkerhet og beredskap og Helsetilsynet.[340]

[334] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[335] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[336] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[337] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[338] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[339] Direktoratet for forvaltning og økonomistyring (2020) *Statlig tilsyn med kommunene, Kartlegging av omfang, samordning og nytte*. DFØ-rapport 2020:9.
[340] Direktoratet for forvaltning og økonomistyring (2020) *Statlig tilsyn med kommunene, Kartlegging av omfang, samordning og nytte*. DFØ-rapport 2020:9.

Tilsynsrapportene vi har gått gjennom, beskriver ikke digital sikkerhet eller informasjonssikkerhet direkte. Tilsynene omhandler beredskapsplaner, risiko- og sårbarhetsanalyser og gjennomføring av øvelser etter forskrift om kommunal beredskapsplikt § 7 første ledd, men dette gjelder samfunnssikkerhet generelt og ikke digital sikkerhet spesielt.[341]

Den generelle tilsynspraksisen i kommunene har gått i retning av mindre omfattende tilsyn (volumkrav og antall landsomfattende tilsyn er redusert) og mer frihet til statsforvalteren, både når det gjelder valg av tilsynsobjekt, metode og tema for tilsynet. Direktoratet for forvaltning og økonomistyring gikk i 2020 gjennom statlige tilsyn med kommunene og fant at andelen tilsyn etter sivilbeskyttelsesloven og helseberedskapsloven har vært synkende. Dette kan ha påvirket mengden tilsyn med den digitale sikkerheten, da digitale hendelser kan inngå i uønskede hendelser etter forskrift om kommunal beredskap. Det gjennomføres flere hendelsesbaserte tilsyn, særlig på helseområdet, som følge av et økende antall klager på kommunene.[342]

Ingen av representantene vi har intervjuet fra kommunesektoren, kjenner til at det har vært gjennomført tilsyn med den digitale sikkerheten i kommunene. Statsforvalterne har ikke lagt vekt på digital sikkerhet i tilsynene med den kommunale beredskapsplikten.[343] Det vises imidlertid til to kartleggingssamtaler som er gjennomført av Norsk helsenett. Samtalene tok form av noen timers intervjuer, og kommunene fikk grønt lys basert på det som kom fram i samtalene. Kartleggingssamtalene førte ikke til at det ble gjort ytterligere undersøkelser med informasjonssikkerheten i kommunene.

Justis- og beredskapsdepartementet viser til at Kommunal- og distriktsdepartementet er ansvarlige for arbeidet med digital sikkerhet i kommunesektoren. Kommunal- og distriktsdepartementet har som nevnt ansvar for den overordnede IKT- og digitaliseringspolitikken, og departementet har det administrative ansvaret for statsforvalterne, som fører tilsyn etter sivilbeskyttelsesloven i kommunene. Departementets ansvar og statsforvalternes tilsyn med kommunene omfatter ikke arbeidet med digital sikkerhet spesielt. Digitaliseringsdirektoratet, som er underlagt Kommunal- og distriktsdepartementet, har imidlertid fått utvidet veiledningsansvaret for digital sikkerhet til å gjelde kommunesektoren. I den forbindelse uttaler Justis- og beredskapsdepartementet at de ikke har hatt særlig oppmerksomhet på kommunesektoren. Dette skyldes at deres samordningsansvar gjelder nasjonalt og dermed berører kommunene indirekte. Departementet har imidlertid hatt mye dialog med Kommunal- og distriktsdepartementet og KS om den digitale sikkerheten i kommunene, men de har ikke diskutert tilsyn med den digitale sikkerheten og hvem som skal ha særskilt ansvar for dette.[344]

5.6.2 Tilsyn med den digitale sikkerheten etter sikkerhetsloven

Sikkerhetsloven stiller krav om at det skal gjennomføres tilsyn for å kontrollere at bestemmelser i sikkerhetsloven med forskrifter etterleves. De overordnede formålene med tilsynet er å skape tillit til det forebyggende sikkerhetsarbeidet og bidra til å redusere sårbarheter i en virksomhet, en sektor og i nasjonen som helhet. Tilsyn skal bidra til forbedring av virksomhetenes arbeid med forebyggende sikkerhet.[345]

Det skal føres tilsyn med alle virksomheter som omfattes av sikkerhetsloven.[346] Nasjonal sikkerhetsmyndighet har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller sine plikter etter loven.[347] Myndigheter med

[341] Fylkesmannen i Oppland (2012) *Rapport fra tilsyn med samfunnssikkerhet og beredskap i Lillehammer kommune*; Helsetilsynet (2012) *Rapport fra tilsyn med samfunnssikkerhets- og beredskapsarbeidet i Lardal kommune 2012*; Helsetilsynet (2021) *Tilsyn med kommunal beredskapsplikt og helseberedskap Åfjord kommune 2021*; Bindal kommune (2021) *Tilsyn.*
[342] Direktoratet for forvaltning og økonomistyring (2020) *Statlig tilsyn med kommunene.*
[343] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[344] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[345] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[346] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[347] *Samarbeidsavtale om tilsyn inngått mellom Nasjonal sikkerhetsmyndighet og Nasjonal kommunikasjonsmyndighet*, signert 19. desember 2019.

sektoransvar kan føre tilsyn med virksomheter som er omfattet av sikkerhetsloven i egen sektor. Dette gjøres blant annet for å øke antall tilsyn etter sikkerhetsloven, og for at tilsynene skal være tilpasset sektoren.[348] Nasjonal sikkerhetsmyndighet har inngått samarbeidsavtaler om tilsyn etter sikkerhetsloven med NVE og Nasjonal kommunikasjonsmyndighet. For øvrige sektorer og for departementene ivaretar Nasjonal sikkerhetsmyndighet tilsynsansvaret. Selv om både Nasjonal sikkerhetsmyndighet, NVE og Nasjonal kommunikasjonsmyndighet skal gjennomføre tilsyn med forebyggende sikkerhetsarbeid, skal tilsynene være enhetlige på tvers av sektorene.[349]

Tilsyn skal planlegges på grunnlag av risiko og vesentlighet for å sikre at de blir gjennomført ofte nok, i stort nok omfang og med tilstrekkelige ressurser. Nasjonal kommunikasjonsmyndighet og NVE skal orientere Nasjonal sikkerhetsmyndighet om planlagte tilsyn, redegjøre for gjennomførte tilsyn og informere om eventuelle avvik og pålegg. Nasjonal sikkerhetsmyndighet kan gi Nasjonal kommunikasjonsmyndighet og NVE pålegg om å gjennomføre tilsyn. Slike pålegg kan være aktuelle når tilsyn ikke planlegges, gjennomføres eller følges opp i henhold til kravene i sikkerhetsloven med forskrifter.[350]

Nasjonal sikkerhetsmyndighets tilsyn etter sikkerhetsloven

Nasjonal sikkerhetsmyndighet utarbeider en årlig tilsynsplan. Valg av tema og virksomheter det skal føres tilsyn med, er basert på sikkerhetsmyndighetens vurdering av hvor det er høyest risiko. I tillegg brukes tilsyn som virkemiddel dersom Nasjonal sikkerhetsmyndighet får melding om sikkerhetsbrudd. Slike ad hoc-tilsyn kommer i tillegg til de planlagte tilsynene. Enkelte sektorregelverk har svært konkrete krav til blant annet sikkerhet, mens sikkerhetsloven som nevnt er funksjonelt innrettet og overlater ansvaret for å dimensjonere sikkerhetstiltak til virksomhetene som er omfattet av loven.[351]

Nasjonal sikkerhetsmyndighet opplyser at de har egne rutiner for gjennomføring av tilsyn, og at disse innebærer at virksomhetene som omfattes av tilsynet, får varsel om dette i forkant. Nasjonal sikkerhetsmyndighet innhenter informasjon gjennom dokumentanalyser, intervjuer og inspeksjoner i virksomhetene. Etter at informasjonen er analysert, har sikkerhetsmyndigheten møte med virksomheten om funn i tilsynet, og virksomheten får en tilsynsrapport til uttalelse. Ved eventuelle avvik kan Nasjonal sikkerhetsmyndighet gi pålegg om at disse skal utbedres, og virksomheten skal melde fra til direktoratet når avvikene er utbedret. Nasjonal sikkerhetsmyndighet gjennomfører tidvis verifikasjonstilsyn for å kontrollere at avvikene faktisk er utbedret. De opplyser at antall verifikasjonstilsyn varierer fra år til år, men at det i snitt gjennomføres to til tre slike tilsyn årlig, basert på risiko og vesentlighet. Nasjonal sikkerhetsmyndighet finner at virksomhetene i stor grad utbedrer avvikene som påpekes i tilsynet, men at de har større utfordringer med å identifisere og utbedre den bakenforliggende årsaken til avvikene.[352]

Nasjonal sikkerhetsmyndighet gir hvert år ut en ugradert kontrollmelding med oversikt over de tilsynene som er gjennomført. I tillegg utarbeider direktoratet sikkerhetsgraderte kontrollmeldinger for hver enkelt sektor med oversikt over tilsyn og avvik.[353] Nasjonal sikkerhetsmyndighet skriver i *Kontrollmeldingen 2020* at forebyggende sikkerhetsarbeid skiller seg fra øvrig sikkerhetsarbeid, blant annet med hensyn til særegne formål, virkemidler og risiko, og at sikkerhetstilstanden for skjermingsverdige verdier ikke uten videre kan antas å sammenfalle med virksomhetens sikkerhetstilstand for øvrig.[354]

[348] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[349] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[350] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[351] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[352] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021
[353] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021
[354] Nasjonal sikkerhetsmyndighet (2020) *Kontroll av nasjonal sikkerhet - Kontrollmeldingen 2020.*

Tilsynsmetodikk med hovedvekt på styringssystemene

Tilsyn etter sikkerhetsloven kan gjennomføres som systemrevisjon eller IKT-revisjon.[355]

Faktaboks 17 Tilsynsmetoder

Systemrevisjon er en systematisk undersøkelse av et styringssystem for å avgjøre om det oppfyller fastlagte kriterier og fungerer etter hensikten. Systemrevisjon gjennomføres for å identifisere eventuelle mangler ved styringssystemet som grunnlag for korrigering og forbedring.

IKT-revisjon er en systematisk undersøkelse av sikkerheten i informasjonssystemer og sikkerheten ved bruk av slike systemer. IKT-revisjon gjennomføres for å identifisere eventuelle mangler ved informasjonssikkerheten og informasjonssystemsikkerheten.

Kilde: Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.

Av virksomhetssikkerhetsforskriften går det fram at tilsyn som hovedregel skal gjennomføres som systemrevisjon.[356] Siden sikkerhetstiltakene skal dimensjoneres i forhold til risiko, omfatter dette også undersøkelser av risikostyringen. Nasjonal sikkerhetsmyndighet har utarbeidet *Veileder for tilsyn med forebyggende sikkerhetsarbeid* med vedlegg som angir kriterier for tilsyn. I veilederen anbefales det å gjennomføre tilsyn i henhold til *NS-EN ISO 19011 Retningslinjer for revisjon av ledelsessystemer.*[357]

Sikkerhetsloven har bestemmelser om beskyttelse av informasjon og informasjonssystemer i kapittel 5 og 6, og tilsyn må ifølge *Veileder for tilsyn med forebyggende sikkerhetsarbeid* også omfatte disse bestemmelsene. Virksomhetssikkerhetsforskriften angir metoden for kontroll av sikkerhetstilstanden i informasjonssystemer. Slike tilsyn kan gjennomføres som IKT-revisjon.[358] Ifølge veilederen er aktuelle revisjonskriterier for IKT-revisjon Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* (2020) og *NS-EN ISO 27001/27002*, og kan omfatte automatiserte metoder[359] for innsamling av teknisk informasjon.

Nasjonal kommunikasjonsmyndighet er kjent med *Veileder for tilsyn med forebyggende sikkerhetsarbeid*, men har ikke så stor nytte av den fordi den etter deres oppfatning er mer tilpasset mindre erfarne tilsynsaktører.[360] Veilederen inneholder en del metodikk som etaten som erfaren tilsynsmyndighet oppfatter som ganske selvsagt.

Av Nasjonal sikkerhetsmyndighets kontrollmelding for 2020 går det fram at de gjennomfører tilsyn som systemrevisjoner understøttet av fagspesifikke undersøkelser.[361] I tilsynene undersøker de sikkerheten i styringssystemet samtidig som de gjennomfører undersøkelser innenfor forskjellige sikkerhetsfag, som informasjonssikkerhet, informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet og personellsikkerhet. Tilsynene gjennomføres vanligvis som stedlige tilsyn, men også andre tilsynsformer kan benyttes, for eksempel dokumentundersøkelser, tematilsyn eller tilsynssaker i forbindelse med uønskede hendelser.

Nasjonal sikkerhetsmyndighet definerer funn fra egne kontrollaktiviteter som sårbarheter i kontrollmeldingen for 2020. Det er departementene og virksomhetene selv som skal identifisere og implementere egne konkrete forbedringer.

[355] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[356] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[357] Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid,* versjon 2.
[358] Virksomhetssikkerhetsforskriften § 89 fjerde ledd.
[359] Automatiserte metoder kan eksempelvis være dataprogrammer eller applikasjoner som på selvstendig grunnlag samler inn info.
[360] Intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[361] Nasjonal sikkerhetsmyndighet (2020) *Kontroll av nasjonal sikkerhet − Kontrollmeldingen 2020.*

Oppsummert viser resultatene fra Nasjonal sikkerhetsmyndighets kontrollaktiviteter i 2020 følgende:[362]

1. Manglende implementering av sikkerhetsloven: Både departementer og virksomheter mangler oversikt over nasjonale verdikjeder. Verdier som egentlig er skjermingsverdige, er derfor ikke alltid forsvarlig sikret og kontrollert siden de ikke er korrekt utpekt.
2. Lav bevissthet om sikring av nasjonale verdier: Mange virksomheter sikrer seg først og fremst mot hendelser som kan forstyrre driften. Slike sikringstiltak beskytter ikke nødvendigvis verdier som virksomheten forvalter på vegne av nasjonen, mot alle relevante uønskede hendelser, for eksempel avlytting, innsidere eller strategiske oppkjøp.
3. Alvorlige sårbarheter i grensesnittet mellom virksomheter: Det oppstår sårbarheter der det er samarbeid mellom offentlige virksomheter, eller i sikkerhetsgraderte anskaffelser. Virksomheter belager seg på eller antar at den andre parten ivaretar sikkerhetsarbeidet på et felles ansvarsområde.
4. Risiko vurderes ikke jevnlig eller helhetlig: Risikovurderingsarbeidet gjennomføres sporadisk eller begrenses til visse verdier, fagområder eller trusler. Vurderingene skal gi føringer for alt videre sikkerhetsarbeid og prioritering av ressurser.

Sårbarheter som er avdekket gjennom Nasjonal sikkerhetsmyndighets kontrollaktiviteter i 2021, viser følgende:[363]

1. Mangelfull rapportering av uønskede hendelser: Hendelser blir ofte håndtert fortløpende uten at de blir registrert og rapportert til virksomhetens egen sikkerhetsorganisasjon eller til Nasjonal sikkerhetsmyndighet eksternt.
2. Mangelfull verdikartlegging: Identifiseringen, avklaringen og operasjonaliseringen av grunnleggende nasjonale funksjoner har vært mangelfull. Dette skaper uklare rammer når virksomheten skal identifisere og peke ut skjermingsverdige verdier og fører til at Norge i flere sektorer ikke har forutsetninger for å ha kontroll med den nasjonale sikkerheten fordi det ikke finnes oversikt over slike verdier.
3. Mangelfull kommunikasjon mellom departementer og underliggende virksomheter når det gjelder hvilke objekter og infrastruktur departementene hadde utpekt, og hvilke klassifiseringsnivå de var gitt.
4. Økonomiske hensyn blir prioritert høyere enn nasjonal sikkerhet i anskaffelser. Private leverandører ønsker at anskaffelser i hovedsak skal være ugradert, og oppdragsgiver nedgraderer anskaffelser for å få flere og billigere tilbud.

Kompetansen til og veiledningen av sektortilsynene

Sektortilsynene har ansvaret for å kartlegge eget kompetansebehov og tilegne seg kompetansen de trenger for å gjennomføre tilsyn. Nasjonal sikkerhetsmyndighet skal bistå sektortilsynene med å tilegne seg den nødvendige kompetansen ved å tilby opplæring i forebyggende sikkerhetsarbeid og tilsyn ved direktoratets kurssenter. Dersom Nasjonal sikkerhetsmyndighet gir en virksomhet konkrete råd om hvordan den kan etterleve bestemmelser i sikkerhetsloven, skal dette skje i dialog med sektortilsynet for å sikre enhetlig rådgivning.[364]

Både NVE og Nasjonal kommunikasjonsmyndighet har ifølge Nasjonal sikkerhetsmyndighet god kompetanse og lang erfaring med å gjennomføre tilsyn. Begge etatene har ansvar for å gjennomføre tilsyn med beskyttelse av informasjon, objekter og infrastrukturer etter sine respektive regelverk.[365] Nasjonal sikkerhetsmyndighet skal legge til rette for felles opplæring av tilsynspersonell.[366] Sektortilsynene har etter Nasjonal sikkerhetsmyndighets vurdering god tilsynsmetodikk og en planmessig tilnærming til kontrollarbeidet. Ifølge direktoratet vil det være områder i sikkerhetsloven

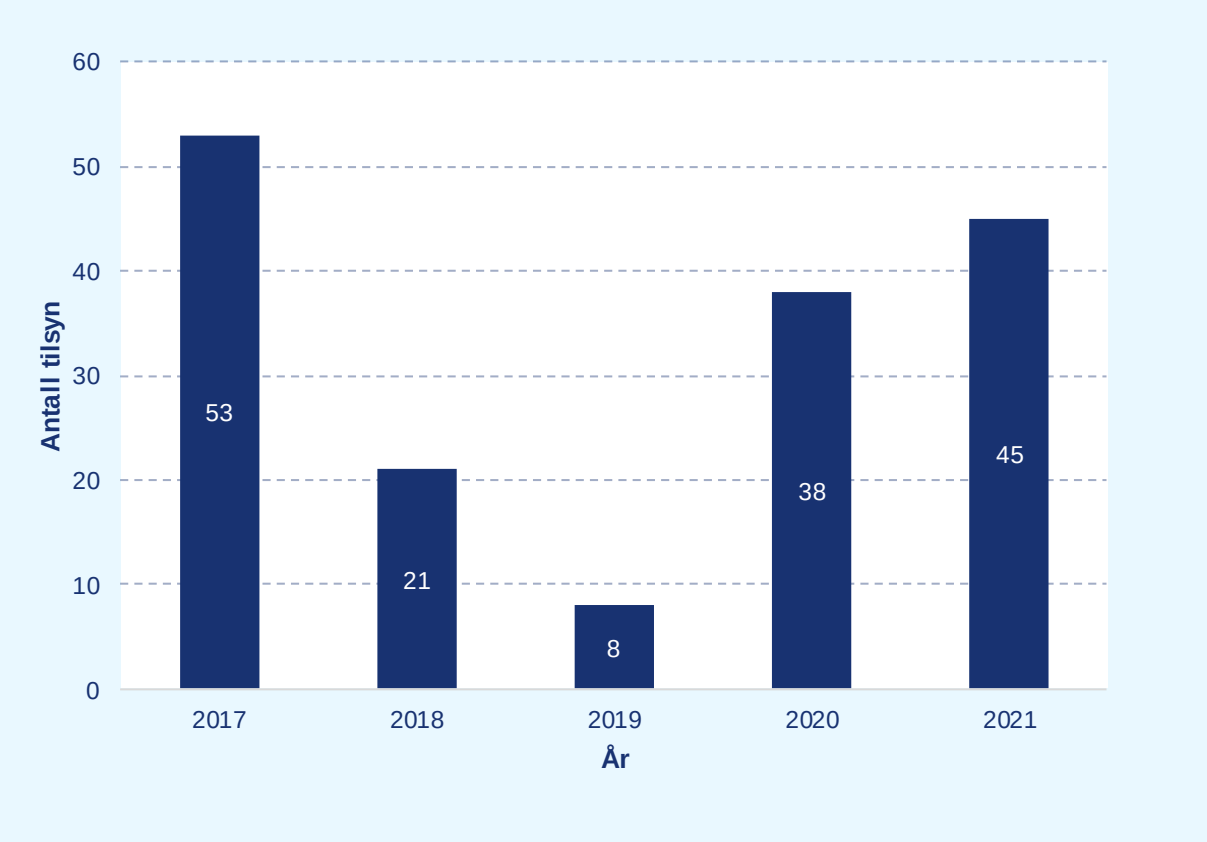
[362] Nasjonal sikkerhetsmyndighet (2020) *Kontroll av nasjonal sikkerhet − Kontrollmeldingen 2020.*
[363] Nasjonal sikkerhetsmyndighet (2020) *Kontroll av nasjonal sikkerhet − Kontrollmeldingen 2022.*
[364] *Samarbeidsavtale om tilsyn inngått mellom Nasjonal sikkerhetsmyndighet* og Nasjonal kommunikasjonsmyndighet, signert 19. desember 2019.
[365] Verifisert intervju med Nasjonal sikkerhetsmyndighet (BEGRENSET). Utdraget det henvises til er UGRADERT. 1. desember 2021.
[366] *Samarbeidsavtale om tilsyn inngått mellom Nasjonal sikkerhetsmyndighet og Nasjonal kommunikasjonsmyndighet,* signert 19. desember 2019.

hvor sektortilsynene ikke har vesentlig erfaring, men i slike tilfeller kan de få bistand fra og delta på kurs i regi av Nasjonal sikkerhetsmyndighet. Etter at Nasjonal kommunikasjonsmyndighet ble utpekt som tilsynsmyndighet for sikkerhetsloven, har etaten opplevd Nasjonal sikkerhetsmyndighets veiledning som særlig viktig.[367] Nasjonal sikkerhetsmyndighet har også etablert *Samhandlingsarena for sektortilsyn etter sikkerhetsloven* hvor digital sikkerhet er et viktig tema.[368]

Antall tilsyn etter sikkerhetsloven er lavt sammenlignet med antall tilsynsobjekter

Nasjonal sikkerhetsmyndighet, Nasjonal kommunikasjonsmyndighet og NVE kan føre tilsyn etter sikkerhetsloven. I *Kontrollmeldingen 2020* viser Nasjonal sikkerhetsmyndighet til at det føres et begrenset antall tilsyn per år sammenlignet med det totale antallet virksomheter som er underlagt sikkerhetsloven. Begrenset antall tilsyn i 2019 og 2020 følger av beslutning om å være tilbakeholdne med undersøkelser av et nylig etablert sikkerhetsregelverk.[369] Videre viser vår undersøkelse at Nasjonal kommunikasjonsmyndighet og NVE ikke har gjennomført tilsyn etter sikkerhetsloven i egen sektor i første halvdel av 2022. Det er heller ikke planlagt for slike tilsyn i siste halvdel av 2022. I *Kontrollmelding 2022* skriver Nasjonal sikkerhetsmyndighet at antall tilsyn har økt jevnt siden 2019, og at de antar at antall tilsyn vil fortsette å øke framover. Antatt tilsynsomfang i 2022 vil ifølge Nasjonal sikkerhetsmyndighet være omlag 50, noe som fortsatt representerer en jevn stigning.[370]

Figur 6 Nasjonal sikkerhetsmyndighets tilsyn med virksomheter underlagt sikkerhetsloven i 2017–2021



Kilde: Nasjonal sikkerhetsmyndighet (2022) *Kontroll av nasjonal sikkerhet − Kontrollmeldingen 2022*.

[367] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[368] Verifisert intervju med Nasjonal sikkerhetsmyndighet (BEGRENSET), 1. desember 2021, utdraget det henvises til, er UGRADERT.
[369] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[370] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

I 2020 har Nasjonal sikkerhetsmyndighets avdeling for kontroll hatt kontrollaktiviteter i flere sektorer. Over tid skal Nasjonal sikkerhetsmyndighet kontrollere nasjonal sikkerhet i alle sektorer. [371]

Nasjonal kommunikasjonsmyndighet opplyser at tilbydere av ekomtjenester som var underlagt den tidligere sikkerhetsloven, er grundig gjennomgått. Dette var ifølge etaten til god hjelp da de skulle identifisere objekter som skulle underlegges den nye sikkerhetsloven og gjøres til gjenstand for tilsyn. Kommunal- og distriktsdepartementet har valgt å legge vekt på de fire største aktørene i ekomsektoren[372], da disse bærer den tyngste infrastrukturen.

Nasjonal kommunikasjonsmyndighet har nylig meldt inn nye skadevurderinger som viser at det er mange nye objekter som nå bør omfattes av sikkerhetsloven. Dette trenger imidlertid ikke å være en utfordring for ekomtilbyderne, da de ifølge Nasjonal kommunikasjonsmyndighet allerede er spesialister på sikkerhet. Siden skadevurderingene har tatt lengre tid enn planlagt, har Nasjonal kommunikasjonsmyndighet foreløpig ikke gjennomført sektortilsyn etter sikkerhetsloven.[373] Etaten forteller at prosessen med skadevurderingene er omfattende og må følge strenge krav, og at dette bidrar til å øke bevisstheten hos tilbyderne. Gjennom arbeidet har Nasjonal kommunikasjonsmyndighet fått detaljinformasjon om alle informasjonssystemene i sektorene, og de har kartlagt hvilken rolle disse systemene spiller for den nasjonale digitale infrastrukturen. Skadevurderingene omhandler i stor grad digital sikkerhet, og digitale angrep anses å være den trusselen som har størst skadepotensial i ekomsektoren. Ifølge Nasjonal kommunikasjonsmyndighet har de kommet lengre med skadevurderinger i ekomsektoren enn i andre sektorer. Halvparten av de utpekte objektene, informasjonssystemene og infrastrukturen som understøtter grunnleggende nasjonale funksjoner så langt, er i ekomsektoren. Nasjonal kommunikasjonsmyndighet forteller at tilbyderne som har vært underlagt sikkerhetsloven en stund, er varslet om tilsyn, og at to nyere tilbydere blir gitt veiledning i første runde.

NVE opplyser at de ikke har planlagt noen tilsyn etter sikkerhetsloven i 2022, da direktoratets arbeid med sikkerhetsloven er forsinket på grunn av pandemien. Det er kun Statnett som er underlagt sikkerhetsloven i energisektoren, og NVE mener at dette i praksis er en begrenset del av sektoren.[374]

5.6.3 Andre tilsyn med den digitale sikkerheten

Datatilsynet

Datatilsynet gjennomfører tilsyn etter personopplysningsloven i både privat og offentlig sektor. Datatilsynet fører også tilsyn etter reglene om informasjonssikkerhet i helseregisterloven, helseforskningsloven og politiregisterloven, men i det følgende retter vi oppmerksomheten mot tilsynene etter personopplysningsloven.

Tilsyn etter personopplysningsloven går ut på å undersøke om tilsynsobjektene oppfyller personvernprinsippene og etterlever bestemmelsene som gjelder innebygd personvern, behandlingsansvar og ivaretakelse av de registrertes rettigheter. Videre kan et slik tilsyn omfatte om det er opprettet personvernombud og ombudets plass i organisasjonen, og kontrollere tilsynsobjektenes styringssystem for personvern og informasjonssikkerhet. Målet med tilsynene er å avdekke sårbarheter som kan føre til kompromittering, endringer eller tap av innbyggernes personopplysninger, og sikre at tilsynsobjektene har eller får på plass tiltak, rutiner og/eller retningslinjer som bidrar til robuste systemer for behandling av personopplysninger.[375]

[371] Nasjonal sikkerhetsmyndighet (2020) Kontroll *av nasjonal sikkerhet – Kontrollmeldingen 2020.*
[372] Telenor, Telia, ICE og Global Connect.
[373] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[374] Norges vassdrags- og energidirektorat (2022) *SV: Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet*. E-poster til Riksrevisjonen, 19. og 23. mai 2022.
[375] Datatilsynet (2022) *Tilsynsvirksomheten vår i 2022* [Hentedato 16. juni 2022].

Da den nye personvernforordningen trådte i kraft, hadde Datatilsynet behov for å oppdatere tilsynsmetodikken. De satte i gang et eget prosjekt som skulle arbeide med dette, og har siden 2021 arbeidet med å etablere ny tilsynsmetodikk. For å få et innblikk i hvordan andre myndigheter gjennomfører tilsyn, tok prosjektet kontakt med blant annet Riksrevisjonen, Lotteritilsynet, Konkurransetilsynet, Nasjonal sikkerhetsmyndighet og det britiske datatilsynet, ICO. Datatilsynet opplyser at de gjennomfører hendelsesbaserte tilsyn og egeninitierte tilsyn hvor tilsynsobjektene velges ut fra en risikotilnærming. Fra og med 2021 har de valgt ut virksomheter til risikobaserte tilsyn med utgangspunkt i innkommende tips, klager og innmeldte avvik. Egeninitierte tilsyn kan være innrettet på ulike måter. Når Datatilsynet gjennomfører et bredt tilsyn, sjekker de for eksempel virksomhetenes dokumentasjon på internkontroll mot personvern og om virksomhetene har oversikter og rutiner på området.

Datatilsynet kan også gjennomføre spissede tilsyn, der en konkret løsning eller algoritme blir kontrollert, eller såkalte brevlige tilsyn, der de ber virksomheter redegjøre for hvordan de etterlever ulike tilsynskriterier. Datatilsynet opplyser at hendelsesbaserte tilsyn ofte omfatter informasjonssikkerhet. I 2021 gjennomførte Datatilsynet få egeninitierte tilsyn. Av 14 planlagte egeninitierte tilsyn ble fem startet opp og tre fullført. Datatilsynet opplyser at antall tilsyn er et spørsmål om kapasitet og ressurser.[376]

I intervjuet med representanter fra kommunesektoren forteller informantene at Datatilsynet ikke har gjennomført tilsyn hos dem. Det gjøres i hovedsak saksbehandlingstilsyn knyttet til konkrete hendelser.[377] Datatilsynets tilsyn med personvernbestemmelsene i kommunene samordnes med statsforvalternes tilsyn.[378]

Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet fører tilsyn etter ekomloven, lov om elektroniske tillitstjenester og sikkerhetsloven. Ifølge Nasjonal kommunikasjonsmyndighet er sikkerhetsloven overordnet ekomloven, men det er ekomloven ekomtilbyderne i hovedsak forholder seg til i det daglige arbeidet. Lovene overlapper hverandre noe når det gjelder krav til sikkerhet. Nasjonal kommunikasjonsmyndighet opplyser at tilbydere som er underlagt sikkerhetsloven, skal tilfredsstille kravene både i ekomloven og sikkerhetsloven. Nasjonal kommunikasjonsmyndighet følger opp kravene i begge lovene i egen sektor.[379]

Nasjonal kommunikasjonsmyndighet gjennomfører planlagte og hendelsesbaserte tilsyn etter ekomloven. Begge former for tilsyn kan gjennomføres som stedlige tilsyn eller dokumenttilsyn. Hendelsesbaserte tilsyn skjer som følge av en logisk hendelse (IKT) eller en tradisjonell hendelse som for eksempel graveskade. Hendelser som får landsdekkende konsekvenser, er som regel logiske, mens fysiske hendelser ofte har lokale konsekvenser. De fleste hendelsene er forårsaket av strøm- og fiberbrudd, vær, vind og graveskader.[380]

Nasjonal kommunikasjonsmyndighet har et styringssystem som skal sikre at de fører tilsyn der risikoen og vesentligheten er størst. Etaten har over en lengre periode hatt mest oppfølging av de største og mest sentrale tilbyderne i sektoren og har hatt mindre kontakt med de mindre selskapene. Under koronapandemien planla og gjennomførte Nasjonal kommunikasjonsmyndighet mange dokumenttilsyn både etter ekomloven, lov om elektroniske tillitstjenester og sikkerhetsloven. Ved å bruke dokumenttilsyn kunne de nå ut til mange aktører for å få et oversiktsbilde og identifisere behov

[376] Verifisert referat fra møte med Datatilsynet, 17. februar 2022.
[377] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[378] Verifisert referat fra møte med Datatilsynet, 17. februar 2022.
[379] Verifisert referat fra møte med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[380] Verifisert referat fra møte med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.

for videre tilsyn. Nasjonal kommunikasjonsmyndighet pleier å varsle om tilsyn på forhånd.[381] De opplever at dette virker skjerpende og bidrar til å øke aktiviteten i virksomhetene. [382]

Våren 2021 gjennomførte Nasjonal kommunikasjonsmyndighet 20 kartleggingstilsyn av mindre tilbydere. Et av formålene med kartleggingstilsynene var å få informasjon om hvilke virksomheter som burde følges opp med ytterligere tilsyn. Nasjonal kommunikasjonsmyndighet opplever metodikken som funksjonell fordi det er mulig å plukke ut tilsynsobjekter for ytterligere tilsyn basert på svakheter som ble avdekket i den brede kartleggingen. Nasjonal kommunikasjonsmyndighet forteller at litt over halvparten av virksomhetene de gjorde tilsyn med hadde etablert et styringssystem for IKT-sikkerhet. Etaten har utarbeidet en tilsynsrapport til hver av virksomhetene. I den påpekes eventuelle avvik, og virksomhetene som fikk pålegg, har fått en frist for å lage tiltaksplaner før tilsynene kan lukkes.[383]

Norges vassdrags- og energidirektorat

NVE fører tilsyn etter energiloven og kraftberedskapsforskriften. Tilsynsobjektene er virksomheter som er definert som enheter i kraftforsyningens beredskapsorganisasjon. NVEs tilsyn med IKT-sikkerhet består i hovedsak av tilsyn med driftskontrollsystemer (systemer som brukes til å styre strømforsyningen) og tilsyn med informasjonssikkerhet. I tillegg omfatter generelle beredskapstilsyn enkelte krav som også er relevante for IKT-sikkerheten, som risikovurderinger, beredskapsplanlegging, internkontrollsystem og beskyttelse av kraftsensitiv informasjon. NVE gjennomførte tilsyn med informasjonssikkerhet etter kraftberedskapsforskriften for første gang i 2019.[384]

NVE utarbeider en årlig tilsynsplan for hele tilsynsvirksomheten for å kunne styre på en helhetlig måte og synliggjøre hva som skal være tema for årets tilsyn. I tillegg utarbeider direktoratet en årlig revisjonsplan med informasjon om alle planlagte tilsyn for kommende år.[385] *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*, Dokument nr. 3:7 (2020–2021), viste at det er svakheter ved NVEs tilsyn med IKT-sikkerhet. NVE hadde på dette tidspunktet gjennomført få IKT-sikkerhetstilsyn, tilsynsmetodikken avdekket i liten grad den faktiske IKT-sikkerhetstilstanden, og det var svakheter ved NVEs risikovurderinger ved valg av tema og selskaper til IKT-sikkerhetstilsyn. NVE har fulgt opp rapporten blant annet ved å gi et konsulentselskap i oppdrag å kartlegge sårbarheter i leverandørkjeden og anbefale tiltak som NVE kan iverksette.[386] Et av de anbefalte tiltakene går ut på å gjennomføre en tilsynsserie rettet mot oppfølgingen av leverandører. NVE arbeider også med å utvikle tilsynsmetodikken. I første omgang skal de stille mer detaljerte spørsmål i tilsynene, og dernest skal de arbeide med en opptrappingsplan for den videre utviklingen av tilsyn på IKT-sikkerhetsområdet.

[381] Verifisert referat fra møte med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[382] Verifisert referat fra møte med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[383] Verifisert referat fra møte med Nasjonal kommunikasjonsmyndighet, 30. mars 2022.
[384] Dokument 3:7 (2020–2021) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.*
[385] Dokument 3:7 (2020–2021) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.*
[386] Norges vassdrag- og energidirektorat (2022) *NVE følger opp Riksrevisjonens rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen* [Hentedato 16. juni 2022].

6 Justis- og beredskapsdepartementets arbeid med strategier og tiltak for den nasjonale digitale sikkerheten

I dette kapitlet svarer vi på problemstilling tre: *Ivaretar Justis- og beredskapsdepartementet samordningsrollen for den digitale sikkerheten på samfunnssikkerhetsområdet på en god nok måte?* Justis- og beredskapsdepartementet skal som en del av samordningsansvaret utarbeide og følge opp nasjonale strategier og planlegge, gjennomføre og følge opp nasjonale øvelser. Vi innleder derfor kapitlet med å presentere *Nasjonal strategi for digital sikkerhet* fra 2019 og den tilhørende strategien *Nasjonal strategi for digital sikkerhetskompetanse* fra samme år. Deretter presenterer vi arbeidet som er gjort knyttet til evaluering av uønskede digitale hendelser og øvelser. Vi avslutter kapitlet med å presentere status for sentrale tiltak til *Nasjonal strategi for digital sikkerhet* (2019) som har blitt iverksatt for å forbedre evnen til å oppdage og stanse digitale angrep, herunder nasjonal digital hendelseshåndtering.

6.1 Nasjonal strategi for digital sikkerhet

I *samfunnssikkerhetsmeldingen* (2020) framheves *Nasjonal strategi for digital sikkerhet* (2019) som et sentralt virkemiddel i regjeringens arbeid med digital sikkerhet. Strategien ble utgitt i januar 2019 og er et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet. Strategien er den fjerde nasjonale strategien for digital sikkerhet. De tidligere strategiene ble utgitt i 2003, 2007 og 2012.[387]

Justis- og beredskapsdepartementet viser til at departementet har hatt en systematisk og kunnskapsbasert tilnærming til utarbeidelsen av *Nasjonal strategi for digital sikkerhet* (2019). Etter at Justis- og beredskapsdepartementet overtok samordningsansvaret for digital sikkerhet fra det tidligere Fornyings- og administrasjonsdepartementet i 2013, har det vært utarbeidet flere utredninger og styrende dokumentet på dette området. Arbeidet ligger til grunn for utarbeidelsen av strategien i 2019. Se faktaboks 18 for en oversikt over disse. Blant annet har det vært nedsatt to nasjonale utvalg for å utrede særskilte forhold knyttet til nasjonal digital sikkerhet. [388] Lysneutvalget, nedsatt i 2014, skulle kartlegge samfunnets digitale sårbarhet, og foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten. Utvalget overleverte sin utredning i november 2015.[389] Som en del av oppfølgingen til Lysneutvalgets utredning nedsatte Regjeringen i 2017 et nytt utvalg som skulle utrede rettslig regulering på det digitale sikkerhetsområdet og organisering av tverrsektorielt ansvar. IKT-sikkerhetsutvalget leverte sin utredning i desember 2018.[390] I 2017 kom også den første stortingsmeldingen som utelukkende omhandler digital sikkerhet.[391] Justis- og beredskapsdepartementet bemerker at det i denne meldingen ble lansert at det ville komme en ny strategi på det digitale sikkerhetsområdet, og at det ble lagt inn flere prioriteringer og satt en strategisk kurs for det videre arbeidet.[392]

[387] Nærings- og handelsdepartementet, Forsvarsdepartementet og Justis- og politidepartementet (2003) *Nasjonal strategi for informasjonssikkerhet*; Fornyings-, administrasjons- og kirkedepartementet, Samferdselsdepartementet, Forsvarsdepartementet og Justis- og beredskapsdepartementet (2007) *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010*; Fornyings-, administrasjons- og kirkedepartementet, Samferdselsdepartementet, Forsvarsdepartementet og Justis- og beredskapsdepartementet (2012) *Nasjonal strategi for informasjonssikkerhet*.

[388] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

[389] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*.

[390] NOU (2018: 14) *Sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*.

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

[392] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

Faktaboks 18 Utredninger og styrende dokumenter innenfor digital sikkerhet

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.

Meld. St. 38 (2016–2017) IKT-sikkerhet – et felles ansvar (IKT-sikkerhetsmeldingen). Første stortingsmelding som utelukkende omhandler digital sikkerhet.

Internasjonal cyberstrategi for Norge (2017) gjør rede for styrende prinsipper og strategiske prioriteringer for den internasjonale innsatsen for å fremme et åpent, sikkert, robust og fritt digitalt rom.

Nasjonal strategi for digital sikkerhet (2019) angir mål og strategiske prioriteringer som skal ligge til grunn for myndighetenes arbeid. Strategien retter seg mot alle norske virksomheter og privatpersoner.

Nasjonal strategi for digital sikkerhetskompetanse (2019) utdyper kompetansemålene i den nasjonale strategien for digital sikkerhet og skal legge til rette for en langsiktig oppbygning av kompetanse.

NOU (2018: 14) IKT-sikkerhet i alle ledd (IKT-sikkerhetsutvalget). Utvalget vurderer behovet for rettslige og organisatoriske endringer innenfor digital sikkerhet.

Risikostyring i digitale verdikjeder (2019) beskriver hvordan offentlige og private virksomheter kan arbeide med digitale verdikjeder.

Evaluering av hendelseshåndteringen av IKT-sikkerhetshendelsene hos Helse Sør-Øst Regionalt helseforetak og fylkesmannsembetene 2018. Levert av Forsvarets forskningsinstitutt i juni 2020.

Prop. 62 S (2019–2020) Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren, jf. Innst. 334 S (2019–2020), og Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren. Gjennom langtidsplanen for forsvarssektoren ble regjeringens arbeid med kryptopolitikk lagt fram høsten 2020.

Helhetlig digitalt risikobilde. Rapporten utgis årlig av Nasjonal sikkerhetsmyndighet med en rekke bidragsytere.

Kilde: Meldt. St. 5 (2020−2021) *Samfunnssikkerhet i en usikker verden*, s. 89.

Justis- og beredskapsdepartementet viser også til at forut for utgivelsen av *Nasjonal strategi for digital sikkerhet* i 2019 ble alle relevante aktører på det digitale sikkerhetsområdet i Norge invitert inn i strategiprosessen. Det ble blant annet invitert til en konferanse i starten av arbeidet, arbeidsmøter underveis og lansering av strategien ved arbeidets slutt. I tillegg ble det avholdt en rekke møter med både nasjonale og internasjonale aktører for å få innspill til strategien og mulige tiltak. Dette ble gjort fordi Justis- og beredskapsdepartementet ønsket innspill fra et så bredt utvalg av aktører som mulig, og for å kvalitetssikre de valg som ble gjort i løpet av strategiprosessen. Det var også viktig for departementet at strategien opplevdes relevant for flere og at flere kunne bidra til oppfølgingen.[393]

6.1.1 Videreføring fra tidligere nasjonale strategier og erfaringer fra oppfølgingsarbeidet

Nasjonal strategi for informasjonssikkerhet, utgitt i 2012, var et samarbeid mellom Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Fornyings- og

[393] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

administrasjonsdepartementet. I strategien pekte de ut fire overordnede mål for arbeidet med digital sikkerhet i samfunnet med en tilhørende handlingsplan.[394] De fire målene var som følger:

1. Styrket samordning og felles situasjonsforståelse
2. Robust og sikker IKT-infrastruktur i hele samfunnet
3. Sterkere evne til å håndtere uønskede IKT-hendelser
4. Høy kompetanse og sikkerhetsbevissthet

Justis- og beredskapsdepartementet målte ikke effekten av tiltakene i 2012-strategien, men oppgir at de i 2014 evaluerte strategien basert på rapportering fra de andre departementene. [395] Justis- og beredskapsdepartementets interne notat om evalueringen viser at rapporteringen var av svært varierende kvalitet med hensyn til nivå og detaljeringsgrad. De fleste departementene rapporterte på aktiviteter, tiltak og prosesser i departementet og underlagte virksomheter, men i mye mindre grad om den faktiske tilstanden i departementet eller sektoren.[396] I intervju viser Justis- og beredskapsdepartementet til at de benyttet resultatene fra evalueringen i 2014 da de utarbeidet 2019-strategien. Departementet viser til at tiltak som hadde vist seg å fungere godt, ble videreført, for eksempel etableringen av sektorvise responsmiljøer.[397] *Nasjonal strategi for digital sikkerhet* i 2019 bygger således videre på strategien fra 2012.

Nasjonal strategi for digital sikkerhet fra 2019 legger vekt på styrket samarbeid mellom offentlig og privat sektor og mellom sivil og militær sektor. I tillegg legger den vekt på å løfte grunnsikringen i *alle* virksomheter for å styrke nasjonal sikkerhet. Strategien peker ut fem strategiske prioriteringer basert på strategiens mål for digital sikkerhet:

1. Norske virksomheter digitaliserer på en tillitsvekkende og måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.
2. Kritiske samfunnsfunksjoner understøttet av en robust og pålitelig datastruktur.
3. Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.
4. Samfunnet har en bedret evne til å avdekke og håndtere digitale angrep.
5. Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.

Vår undersøkelse omfatter ikke den siste prioriteringen om bekjempelse av data- og IKT-relatert kriminalitet, da dette ble undersøkt i *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT* fra 2021.[398]

Justis- og beredskapsdepartementet bemerker at digital sikkerhet er et område i stor utvikling.[399] Dette har medført at mange av utfordringene fra 2012 fortsatt består, for eksempel utfordringene tilknyttet digital sikkerhetskompetanse og digital hendelseshåndtering. Etter hvert som kompetansebehovene og angrepsmetodene endrer seg, må det også være tiltak for å møte disse endringene. Videre framhever departementet tiltaket om å utvikle sektorvise responsmiljøer. Dette kom i 2012 som en helt ny føring og er ifølge departementet viktig å følge opp videre i 2019-strategien. I en sammenligning av strategiene fra 2012 og 2019 blir det klart at det er flere fellestrekk ved strategiene:

- Det underliggende risikobildet er ganske likt. Begge strategiene nevner følgende utfordringer: økende kompleksitet og integrering av informasjonssystemer, utenlandsk etterretningsvirksomhet i form av spionasje og sabotasje med digitale virkemidler, økt risiko for digital kriminalitet, økt sårbarhet for driftsavbrudd i digital infrastruktur samt at økt bruk av utenlandske tjenesteleverandører gir dårligere oversikt og kontroll over verdikjedene.

[394] Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Fornyings-, administrasjons- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet*.
[395] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[396] Justis- og beredskapsdepartementet (2014) *Rapportering fra departementene om informasjonssikkerhet, sikkerhetstilstanden i departementet og underlagte virksomheter og øvelser.* UNNTATT OFFENTLIGHET.
[397] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[398] Dokument nr. 3:5 (2020–2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT.*
[399] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

- De overordnede målene for strategiene og de strategiske prioriteringene er like over tid. Begge strategiene legger vekt på følgende: mer samordning av forebyggende arbeid, forbedre samfunnets evne til å oppdage og håndtere digitale angrep, øke kvaliteten og kapasiteten når det gjelder nasjonal kompetanse på digital sikkerhet, og bekjempe digital kriminalitet. I 2019-strategien legges det imidlertid mer vekt på samarbeid i ulike dimensjoner, det vil si sivilt-militært og offentlig-privat samarbeid, og virksomheters egenbeskyttelse mot digital trusler og angrep.
- Flere av tiltakene i 2019-strategien er en videreføring av tiltakene fra 2012-strategien, blant annet: å etablere bedre informasjonsgrunnlag for å oppnå et felles risiko- og situasjonsbilde, å kartlegge verdier som skal beskyttes, at Direktoratet for forvaltning og IKT / Digitaliseringsdirektoratet skal bidra til å bedre styringen av digital sikkerhet i offentlig sektor, robust digital-infrastruktur og sikkerhetsgraderte kommunikasjonsløsninger.

6.1.2 Tiltaksoversikten til *Nasjonal strategi for digital sikkerhet* er ikke oppdatert eller evaluert

Det er Justis- og beredskapsdepartementet og Forsvarsdepartementet som har det overordnede ansvaret for å følge opp *Nasjonal strategi for digital sikkerhet* (2019). Strategien understøttes av en oversikt over tiltak som er iverksatt for å bedre den digitale sikkerheten. Tiltaksoversikten er todelt, og del én omfatter sentrale tiltak som støtter oppunder målene for strategien. Det enkelte departement er ansvarlig for at strategiens prioriteringer og tiltaksoversikten blir fulgt opp i egen sektor. Del to lister opp ti grunnleggende sikkerhetstiltak som private og offentlige virksomheter anbefales å gjennomføre for å øke sin egen evne til å beskytte seg mot og håndtere digitale angrep.

De fleste av tiltakene og aktivitetene som beskrives i tiltaksoversikten var allerede planlagt og finansiert da strategien ble utformet. Det innebærer at tiltaksoversikten ikke følger av strategiens overordnede mål og strategiske prioriteringer, men at den i stor grad er en oppsummering av myndighetenes pågående arbeid på det digitale sikkerhetsområdet. Justis- og beredskapsdepartementet viser til at dette følger av at det i norsk forvaltning ikke er mulig å lage tiltaksplaner som krever framtidige investeringer som det ikke er vedtatt midler til. Tiltaksplanen beskrives slik sett av departementet som et øyeblikksbilde av hva som var besluttet på tidspunktet da strategien ble utgitt.[400] Justis- og beredskapsdepartementet bemerker at enkelte av tiltakene som beskrives i tiltaksoversikten ble planlagt og finansiert parallelt med at 2019-strategien ble utarbeidet. Beslutningen om å gjennomføre *Øvelse Digital 2020* trekkes fram som eksempel på et slikt tiltak. Videre bemerkes at tiltakene også må ses i sammenheng med *IKT-sikkerhetsmeldingen* (2017), der det ble lagt inn flere prioriteringen og satt en strategisk kurs som det bygges videre på og som forsterkes i strategien fra 2019.[401]

Det er utpekt ansvarlige departementer og etater for hvert av tiltakene i tiltaksoversikten, og det er satt et gjennomføringstidspunkt og en plan for oppfølgingen av disse. Hvorvidt det er fastsatt om, og i tilfellet når tiltakene skal evalueres, varierer fra tiltak til tiltak. Tiltaksoversikten inneholder til sammen 63 tiltak som understøtter strategien.[402] Vi har omtalt et utvalg av disse tiltakene i de foregående kapitlene i denne rapporten. Utvalget er basert på risikoen for at tiltakene ikke er gjennomført som planlagt, og hvilke konsekvenser dette kan ha for det helhetlige arbeidet med digital sikkerhet. Risikoen har framkommet fra informasjon vi har hentet inn både i planleggingen og gjennomføringen av denne undersøkelsen. Utvalget omfatter følgende tiltak:

- Forebyggende digital sikkerhet:
  - tiltak for oppfølging av stortingsmeldinger og utredninger på området, herunder Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*, NOU (2015: 13) *Digital sårbarhet* –

[400] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[401] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[402] Justis- og beredskapsdepartementet (2019*) Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*

sikkert samfunn, (Lysneutvalget), NOU (2018: 14) *Sikkerhet i alle ledd.* (IKT-sikkerhetsutvalget)
    - nasjonale anbefalinger og rådgivning/veiledning (se kapittel 4.5)
    - samarbeidsfora- og arenaer for sentrale aktører, blant annet tilsynsmyndigheter og Nasjonalt cybersikkerhetssenter (se kapittel 4.2 og 4.6)
    - sikkerhetsgradert datakommunikasjon mellom departementene (se kapittel 6.4.5 og sikkerhetsgradert vedlegg til denne rapporten)

- Digital sikkerhet i kritiske samfunnsfunksjoner:
    - innføring av ny sikkerhetslov som trådte i kraft i 2019 (se kapittel 5.2)
    - EUs NIS-direktiv og konsekvenser for norsk regelverk (se kapittel 4.3.3)
    - Utarbeidelse av et nasjonalt rammeverk for helhetsvurdering av verdikjeder (se kapittel 5.3)

- Digital sikkerhetskompetanse (se kapittel 6.2):
    - langsiktig forskning av god kvalitet
    - tilstrekkelig nasjonal spesialistkompetanse
    - digital sikkerhet i IKT-utdanning i videre- og etterutdanning

- Avdekke og håndtere digitale angrep:
    - etablering og evaluering av sektorvise responsmiljøer (se kapittel 4.2.2)
    - bruk og utvikling av *Rammeverk for håndtering av IKT-sikkerhetshendelser* (se kapittel 6.4.4)
    - gjennomføring av en nasjonal IKT-sikkerhetsøvelse – Øvelse Digital 2020 (se kapittel 6.3)
    - Nasjonalt cybersikkerhetssenter (se kapittel 4.2.2)
    - Felles cyberkoordineringssenter − behandles i sikkerhetsgradert vedlegg til rapporten
    - utredning av behov for en tverssektoriell cyberreserve (se kapittel 6.4.3)

Tiltaksoversikten ble ikke oppdatert etter statusgjennomgang i 2021

Status for tiltakene i *Nasjonal strategi for digital sikkerhet* (2019) skulle følges opp av Justis- og beredskapsdepartementet i løpet av de to første årene.[403] Våren 2021 innhentet derfor Justis- og beredskapsdepartementet informasjon om status for tiltakene fra de øvrige departementene. Departementene ble også bedt om å komme med innspill til nye tiltak som kunne inngå i en mulig revidert tiltaksoversikt. Formålet med statusgjennomgangen var å få et bilde av hvor departementene og sektorene står i det digitale sikkerhetsarbeidet. Det skulle også innhentes kunnskap om utfordringer som krever særlig oppmerksomhet framover, og positive utviklingstrekk som det kan bygges videre på. Justis- og beredskapsdepartementet trekker fram statusoppdateringene fra de ansvarlige departementene som en viktig kilde til oversikt over den digitale sikkerhetstilstanden i sektorene.[404]

Justis- og beredskapsdepartementet oppsummerer statusgjennomgangen med at tiltaksoversikten i all vesentlighet fortsatt er gjeldende, men at enkelte av tiltakene er forsinket. Forsinkelsene skyldes hovedsakelig pandemihåndtering og anses av departementet ikke å være kritiske. I tilknytning til statusgjennomgangen vurderte Justis- og beredskapsdepartementet risikoen i det digitale rom, og konkluderer med at risikoen har endret seg i negativ retning siden strategien ble lansert i 2019. Dette understøttes av etterretnings- og sikkerhetstjenestenes trusselvurderinger. Justis- og beredskapsdepartementet mener det er en risiko for at digitale hendelser av nasjonal betydning ikke oppdages og skadebegrenses.[405]

Justis- og beredskapsdepartementet oppsummerer statusgjennomgangen i fem sentrale funn:[406]

[403] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*
[404] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[405] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet*, 11. mai 2021.
[406] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet*, 11. mai 2021.

- Ifølge rapporteringen bruker departementene styringsdialogen aktivt. Det rapporteres imidlertid i liten grad på hvordan arbeidet følges opp, og om arbeidet gir resultater innad i sektorene. Flere departementer har utarbeidet eller jobber med sektorstrategier, langtidsplaner og lignende for å systematisere sektorenes arbeid med digital sikkerhet.
- Virksomheters egenrapportering om sikkerhetstilstanden viser at det er behov for tettere oppfølging fra departementene og fra Justis- og beredskapsdepartementet i kraft av sistnevntes samordningsrolle. I denne sammenheng vurderer departementet tydeligere fellesføringer om rapportering på sikkerhetstilstanden.
- Det er etablert fagnettverk og møtearenaer for deling av informasjon og kompetansebygging i de fleste sektorer. Det rapporteres om økt bruk av tekniske sikkerhetsundersøkelser, sikkerhetsrevisjon og tredjepartsvalidering for å kartlegge avvik og forbedre sikkerheten.
- Departementene har god oversikt over sektorenes grunnleggende nasjonale funksjoner, men oversikten over kritisk infrastruktur og digitale avhengigheter som understøtter de grunnleggende nasjonale funksjonene og samfunnets kritiske funksjoner, er ikke like god. Justis- og beredskapsdepartementet peker på at det viktigste tiltaket for å bøte på dette er å opprettholde innsatsen for å implementere sikkerhetsloven, blant annet å arbeide med skadevurderinger og peke ut skjermingsverdige objekter og infrastruktur. Det vises til *samfunnssikkerhetsmeldingen* (2020), hvor det går fram at departementet vil oppdatere den eksisterende kartleggingen av digitale sårbarheter i samfunnet.
- Departementet mener tiden er moden for å evaluere hvordan ordningen med sektorvise responsmiljøer kan forbedres og styrkes for å ivareta virksomhetenes og sektorenes behov samt nasjonale behov. Det er etablert sektorvise responsmiljøer i de fleste sektorer, men disse miljøene varierer betydelig når det gjelder modenhet, omfang, kompetanse og innretning.

Det vises i *Tiltaksoversikt til nasjonal strategi for digital sikkerhet* (2019) at tiltaksoversikten skal revideres ved behov. Ved statusgjennomgangen våren 2021 var det ingen departementer som meldte inn nye tiltak de ønsket å inkludere i tiltaksoversikten. Heller ikke Justis- og beredskapsdepartementet meldte inn tiltak de ønsket å inkludere i denne. Justis- og beredskapsdepartementet peker på at en mulig årsak til at departementene ikke meldte inn ønsker kan være at alle tiltak må være finansiert før de tas inn i oversikten.[407] På bakgrunn av departementenes rapportering konkluderte Justis- og beredskapsdepartementet med at det ikke er behov for å oppdatere tiltaksoversikten tilhørende strategien. Dette til tross for at sikkerhetsrisikoen vurderes som økt siden strategien ble utarbeidet i 2019. Begrunnelse var at de fleste tiltakene fortsatt er aktuelle, og at det er få nye tiltak å supplere med. Det vises imidlertid til at departementet vil be Nasjonal sikkerhetsmyndighet vurdere om det er grunnlag for å oppdatere de ti rådene i del to av tiltaksoversikten.[408] Justis- og beredskapsdepartementet viser også til at det på grunnlag av statusgjennomgangen ble besluttet å iverksette evaluering av ordningen for de sektorvise responsmiljøene, og at undersøkelsene som ble gjort av tiltakene knyttet til del to av tiltaksoversikten ble særlig vektlagt og danner utgangspunkt for flere av tiltakene som det ble bevilger midler til i 2022.[409]

Nye tiltak for å bedre den nasjonale digitale sikkerheten

Gjennom Prop. 78 S (2021–2022) *Endringer i statsbudsjettet 2022 (økonomiske tiltak som følge av krigen i Ukraina)*, jf. Innst. 270 S (2021–2022), er det bevilget midler til flere tiltak for å styrke arbeidet med digital sikkerhet. Tiltakene kunne ha vært inkludert i en revidert tiltaksoversikt til *Nasjonal strategi*

[407] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet*, 11. mai 2021.
[408] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet*, 11. mai 2021.
[409] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

for digital sikkerhet (2019), men Justis- og beredskapsdepartementet har ikke gjort det. Tiltakene er som følger:

- Antall stillinger i Nasjonalt cybersikkerhetssenter skal økes. Tiltaket skal bidra til å forbedre senterets koordineringsevne og hendelseshåndtering, inkludert analysekapasiteten og evnen til å tilby virksomheter som er utsatt for digitale angrep, praktisk bistand. Bevilgningene til Nasjonal sikkerhetsmyndighet økes med om lag 28 millioner i 2022 for å finansiere dette tiltaket.
- Antall virksomhet som deltar i Nasjonal sikkerhetsmyndighets nettverk knyttet til Varslingssystem for digital infrastruktur (VDI) skal økes, og analysekapasiteten i Nasjonalt cybersikkerhetssenter for å håndtere økt informasjonsmengde skal økes. Dette skal oppnås ved å fjerne deltakeravgiften for private virksomheter og la staten overta finansieringen av ordningen (dette reduserer Nasjonal sikkerhetsmyndighets inntekter med 10 millioner kroner). Midlene til å øke dekningen av virksomheter i VDI-nettverket ble ikke videreført for 2023, og private virksomheter må betale medlemsavgift fra årsskiftet.[410] Det ble i tillegg bevilget 17 millioner kroner til anskaffelser av teknisk utstyr for å legge til rette for bruk av sikkerhetsgraderte systemer i VDI.
- Det skal utvikles en felles digital myndighetsportal der alle – for eksempel den enkelte innbygger, små og mellomstore virksomheter, kommuner, eiere av kritisk infrastruktur og myndigheter – kan få ensartede råd om digital sikkerhet. Rådene skal være tilpasset hver enkelt målgruppe, uten at det forutsetter kunnskap om roller og ansvar.
- Det skal utvikles et støtteverktøy for digital sikkerhet som skal tilbys alle norske virksomheter. Verktøyet skal bidra til et systematisk arbeid med digital sikkerhet hos virksomhetene og blant annet gjøre det lettere for dem å evaluere hvor langt arbeidet med digital sikkerhet i egne systemer er kommet. Det bevilges 7 millioner kroner til utvikling av myndighetsportalen og støtteverktøyet for digital sikkerhet i 2022.

Videre har det kommet forslag til to tiltak som skal styrke den digitale sikkerheten i kommunene. Disse skal finansieres av Kommunal- og distriktsdepartementet.[411] Tiltakene er som følger:

- Det skal legges til rette for at kommunene kan knytte seg til et digitalt sikkerhetssamarbeid (responsmiljø eller tilsvarende). Målet med tiltaket er å øke kommunenes evne til å oppdage, forebygge og håndtere digitale angrep. Innretningen må avklares nærmere med de berørte aktørene. Flere alternativer kan være aktuelle, herunder å utvide kapasiteten i et eksisterende responsmiljø eller å etablere en ny kapasitet. Det er bevilget 40 millioner kroner til dette tiltaket i 2022.
- Det skal opprettes en ordning for å styrke kommunenes kompetanse og kapasitet til å oppdage, forebygge og håndtere digitale hendelser. Målet er også å bidra til at kommunene raskere kan tilegne seg denne kompetansen. Det er bevilget 10 millioner kroner til dette tiltaket.

6.2 Nasjonal strategi for digital sikkerhetskompetanse

Kompetanse er en av fem strategiske prioriteringer i *Nasjonal strategi for digital sikkerhet* fra 2019. Kompetansemålene utdypes i en egen strategi − *Nasjonal strategi for digital sikkerhetskompetanse* – fra samme år. Kompetansestrategien ble utarbeidet av Justis- og beredskapsdepartementet i nært samarbeid med Kunnskapsdepartementet. Dette er første gang det er utarbeidet en egen delstrategi

[410] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.

[411] Prop. 78 S (2021–2022) *Endringer i statsbudsjettet 2022 under Kunnskapsdepartementet, Kultur- og likestillingsdepartementet, Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet, Arbeids- og inkluderingsdepartementet, Helse- og omsorgsdepartementet, Barne- og familiedepartementet, Nærings- og fiskeridepartementet, Finansdepartementet og Forsvarsdepartementet (økonomiske tiltak som følge av krigen i Ukraina)*, s. 20.

for digital sikkerhetskompetanse. Justis- og beredskapsdepartementet bemerker at dette ble gjort for å løfte fram et særlig behov og vie kompetanseområdet ekstra oppmerksomhet.[412]

Kompetansestrategien har som overordnet mål å styrke den digitale sikkerhetskompetansen i tråd med samfunnets behov. Strategien skal legge til rette for en langsiktig oppbygging av kompetanse, herunder den nasjonale kapasiteten innenfor forskning og utvikling, utdanning og bevisstgjørende tiltak rettet mot befolkningen.[413]

I tiltaksoversikten til *Nasjonal strategi for digital sikkerhet* (2019) vises det til prioriteringer innenfor kompetanseområdet på over 800 millioner kroner. I tillegg kommer studieplasser innenfor IKT og digital sikkerhet som har blitt tildelt de tre siste årene, og budsjettmessige satsinger som følger av den reviderte langtidsplanen for forskning og høyere utdanning.[414] Også i *samfunnssikkerhetsmeldingen* (2020) vises det til at 800 millioner kroner er adressert til å styrke den digitale sikkerhetskompetansen.[415] Vår undersøkelse viser imidlertid at dette omfatter tiltak for å øke den digitale kompetansen i samfunnet generelt og ikke den digitale sikkerhetskompetansen spesielt. Satsingen på digital sikkerhetskompetanse er følgelig mindre målrettet enn det som opprinnelig ble beskrevet i strategidokumentet.

6.2.1 Behov for kompetanse

Behovet for økt nasjonal digital sikkerhetskompetanse understrekes i flere nasjonale undersøkelser og utredninger. I IKT-sikkerhetsutvalgets rapport trekkes tilgang på IKT-sikkerhetskompetanse fram som en av de største utfordringene på IKT-sikkerhetsområdet. Videre vises til at mangel på kompetanse på digital sikkerhet ikke bare er en utfordring for enkeltindividet, men også for virksomheter og samfunnet.[416]

Faktaboks 19 Utdrag fra IKT-sikkerhetsutvalgets rapport

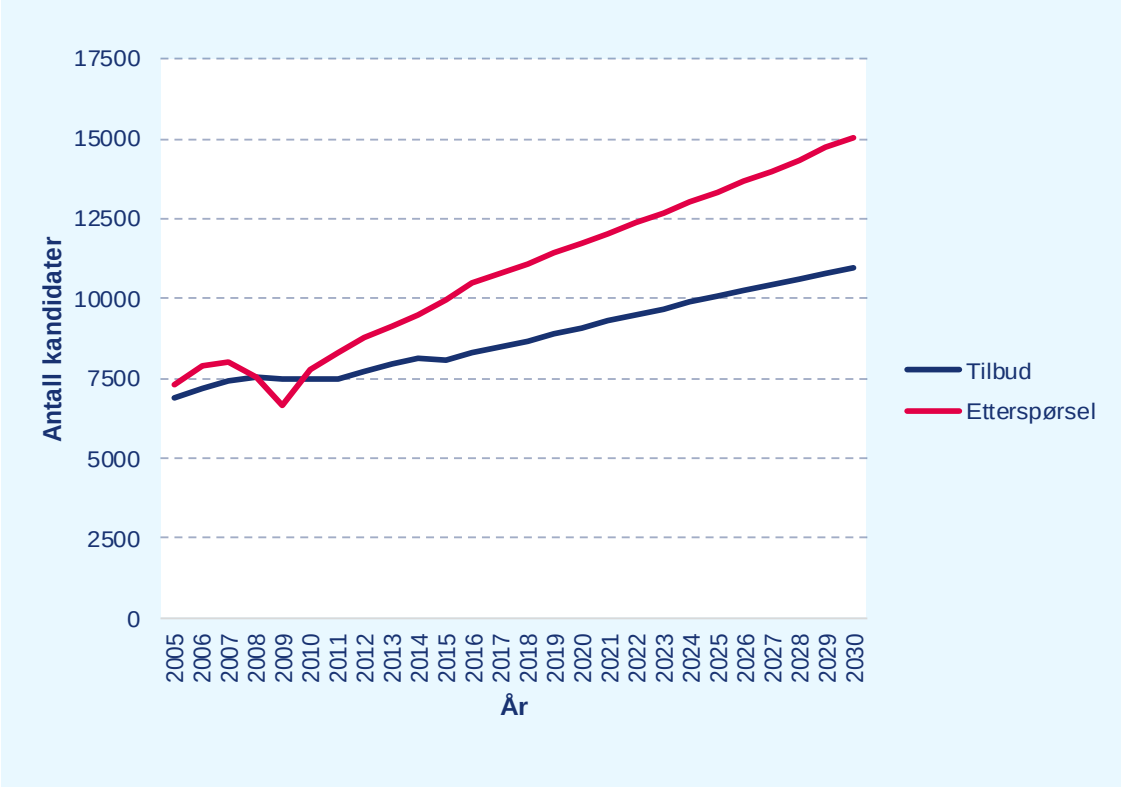
> Kompetansesituasjonen påvirker utviklingen av IKT-systemer og programvare, driften av systemene og hvordan lover og forskrifter, råd, veiledere, rutiner og styringssystemer er uformet og fulgt opp. IKT-personell må ha kompetanse til å implementere tilstrekkelig sikkerhet, og det er behov for spesialisert sikkerhetskompetanse, for eksempel innenfor kryptografi. God evne til å avdekke og håndtere uønskede digitale hendelser krever også spesialistkompetanse på flere områder.

Kilde: NOU (2018: 14) *Sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*, s. 21.

På oppdrag fra Justis- og beredskapsdepartementet gjennomførte Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) i 2017 en studie av samfunnets framtidige tilbud og etterspørsel etter digital sikkerhetskompetanse. Studien viser at til tross for en forventet stabil økning av personer med digital sikkerhetskompetanse er gapet mellom tilbud og etterspørsel økende. Det skyldes en enda kraftigere økning i etterspørselen. Ifølge studien vil det i år 2030 være et kompetansegap på om lag 4100 personer med digital sikkerhetskompetanse. Figur 7 illustrerer framskrivningen. Studien inngår som en del av kompetansestrategiens kunnskapsgrunnlag.[417]

[412] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022
[413] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*, s. 11.
[414] Justis- og beredskapsdepartementet (2019*) Tiltaksoversikt til nasjonal strategi for digital sikkerhet*, s. 10.
[415] Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*, s. 82.
[416] NOU (2018: 14) *Sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*, s. 20.
[417] Mark, Michael Spjelkavik, Cathrine Tømte, Terje Næss og Trude Røsdal (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud*. NIFU-rapport 2017: 32.

Figur 7 Framskrivning av tilbud og etterspørsel etter personell med digital sikkerhetskompetanse



Kilde: Mark m.fl. (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud*. NIFU-rapport 2017: 32.

Også Nasjonal sikkerhetsmyndighet har gjennom sine nasjonale risikovurderinger i flere år pekt på behovene for økt digital sikkerhetskompetanse og større bevissthet om risikoen digitale angrep medfører i tiden framover. [418]

6.2.2 Satsingsområder og tiltak

I kompetansestrategien vises det til at utfordringsbildet tilsier at man må ha et bredt perspektiv på læring og kompetanse for å nå strategiens overordnende mål. Tiltakene må omfatte både teknisk kompetanse og kompetanse knyttet til organisering, ledelse og trygg bruk av digitale systemer. Videre må strategien dekke bredden – fra forskning og ekspertkompetanse til bygging av god sikkerhetskultur i befolkningen. På bakgrunn av dette er strategiens satsingsområder:

- langsiktig forskning av god kvalitet
- tilstrekkelig nasjonal spesialistkompetanse
- digital sikkerhet som en del av IKT-relaterte utdanninger og tilgrensende fag
- etter- og videreutdanning innenfor IKT og digital sikkerhet
- digital sikkerhet i yrkes- og profesjonsutdanninger
- god grunnkompetanse
- bevisstgjørende tiltak og bedret digital sikkerhetskultur[419]

Som i *Nasjonal strategi for digital sikkerhet* (2019) gir kompetansestrategien hovedsakelig en oversikt over tiltak og aktiviteter på området som allerede var planlagt og finansiert da kompetansestrategien

[418] Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018*; Nasjonal sikkerhetsmyndighet (2019) *Risiko 2019*; Nasjonal sikkerhetsmyndighet (2020) *Risiko 2020*; Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021*; Nasjonal sikkerhetsmyndighet (2021) *Digitalt risikobilde 2021*.
[419] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*, s. 11.

ble utarbeidet. Justis- og beredskapsdepartementet bemerker at enkelte tiltak ble utarbeidet parallelt med strategiprosessen.[420]

Det presenteres totalt 25 tiltak som er vurdert å understøtte kompetansestrategiens syv satsingsområder. Det er imidlertid ikke alle tiltakene som er direkte rettet mot å øke den digitale sikkerhetskompetansen. Flere av tiltakene skal bidra til å øke den digitale kompetansen og samfunnssikkerheten i stort, og økt digital sikkerhetskompetanse inkluderes i ulik grad som et av flere delmål.

6.2.3 Styring og oppfølging av tiltakene

De fleste tiltakene i kompetansestrategien er rettet mot utdannings- og forskningsinstitusjoner. Kunnskapsdepartementet har ansvar for å styre og følge opp tiltaksarbeidet i disse institusjonene og andre underliggende virksomheter i utdannings- og forskningssektoren. Styring og oppfølging av tiltakene i kompetansestrategien må skje innenfor de rammer som er satt av Stortinget, blant annet gjennom langtidsplanen for forskning og høyere utdanning. Lov om universiteter og høyskoler har også bestemmelser til vern av akademisk frihet og ansvar for å sikre akademiske verdier og institusjonenes og den enkelte vitenskapelige ansattes faglige uavhengighet.[421]

I intervju viser Kunnskapsdepartement til at de benytter en rekke ulike virkemidler for å sørge for at tiltakene i kompetansestrategien gjennomføres. De nevner blant annet øremerking av midler og bevilgninger som viktige tiltak. De viser også til at Kunnskapsdepartementet samarbeider tett med både Utdanningsdirektoratet, Forskningsrådet og de ulike forskningsinstitusjonene om gjennomføringen av tiltakene. Kunnskapsdepartementet bemerker imidlertid at de i større grad kan styre innholdet i læreplanene på grunnskolenivå og videregående nivå enn innenfor høyere utdanning og forskning. Når det gjelder høyere utdanning og forskning, er det utdannings- og forskningsinstitusjonene som selv definerer og dimensjonerer innholdet i studier og prosjekter. Kunnskapsdepartementet understreker at autonomien til lærestedene er svært viktig.[422]

Justis- og beredskapsdepartementet har ansvar for å følge opp tiltak som er rettet mot aktører utenfor kunnskapssektoren. Sammen med Kunnskapsdepartementet har Justis- og beredskapsdepartementet også ansvar for å sørge for at det foreligger oppdatert statistikk og analyser som gjør det mulig å følge med på kompetansegapet på området.[423]

6.2.4 Status for tiltakene

Som en del av oppfølgingen av *Nasjonal strategi for digital sikkerhet* (2019) innhentet Justis- og beredskapsdepartementet våren 2021 rapportering fra Kunnskapsdepartementet om status for implementeringen av tiltakene i kompetansestrategien. I det følgende presenterer vi en gjennomgang av de mest sentrale tiltakene under satsingsområdene *langsiktig forskning av god kvalitet, tilstrekkelig nasjonal spesialistkompetanse*, *digital sikkerhet som en del av IKT-relaterte utdanninger* og *digital sikkerhet* og *etter- og videreutdanning*. Disse satsingsområdene har størst relevans for myndighetenes arbeid med digital sikkerhet på kort sikt. Gjennomgangen er basert på den ovennevnte rapporteringen og intervju med de to ansvarlige departementene.

[420] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[421] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*, s. 11. *Lov om universiteter og høyskoler* (universitets- og høyskoleloven).
[422] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[423] Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*, s. 11 og 21.

Styrking av midler til forskning på IKT og digital sikkerhet

Justis- og beredskapsdepartementet viser til at en viktig del av arbeidet med kompetansestrategien har vært å legge føringer på prosesser og reformer i utdannings- og forskningssektoren. Som eksempel vises det til at «Samfunnssikkerhet og samhørighet i en globalisert verden» er en ny prioritering i den reviderte langtidsplanen for forskning og høyere utdanning for 2019−2028, hvor digital sikkerhet inngår som et viktig tema.[424] Prioriteringen av digital sikkerhet utdypes i Kunnskapsdepartementets rapportering hvor det vises til at regjeringen gjennom den reviderte langtidsplanen har lansert en opptrappingsplan på 800 millioner kroner over fire år til utdanning og forskning innenfor teknologi, herunder IKT og digital sikkerhet. I perioden 2019−2021 har det blitt bevilget om lag 82 millioner kroner årlig til forskning på digital sikkerhet, inkludert styrket forskning på kryptologi, gjennom oppfølgingen av planen.[425]

Justis- og beredskapsdepartementet viser også til at det satses på forskning og forskningsmiljøer. Forskningsrådets programmer IKTPLUSS og SAMRISK trekkes fram som særlig viktige.[426] Også Kunnskapsdepartementet understreker at de to forskningsprogrammene er viktige for å øke den digitale sikkerhetskompetansen.[427]

Faktaboks 20 Forskningsrådets program IKTPLUSS

IKTPLUSS er Forskningsrådets IKT-satsing. Målet med programmet er å styrke kvaliteten, dristigheten og relevansen til norsk IKT-forskning og innovasjon og bygge et slagkraftig miljø i Norge som byr på innovative løsninger og skaper verdier for samfunnet. Programmet har tre prioriterte områder: *data og tjenester overalt*, *et trygt informasjonssamfunn* og *grensesprengende prosjekter*. Under satsingen *et trygt informasjonssamfunn* skal innsatsen styres mot konkrete samfunnsområder og sektorer som har infrastrukturer med sårbarhet og stor samfunnsmessig betydning. IKTPLUSS er løpende og uten sluttdato.

Kilde: Forskningsrådet (2018) *Programplan for IKTPLUSS.*

Faktaboks 21 Forskningsrådets program SAMRISK

SAMRISK er en videreføring av to tidligere samfunnssikkerhetsprogrammer. Målet med SAMRISK er å gi et bedre kunnskapsgrunnlag for samfunnssikkerhetsarbeidet. Programmet skal belyse sårbarheter og dilemmaer, bidra til å forebygge uønskede hendelser, opprettholde viktige samfunnsfunksjoner og ivareta befolkningens liv, helse og grunnleggende verdier før, under og etter store påkjenninger. *Teknologi og samfunnssikkerhet* er et av tre prioriterte områder. Under denne prioriteringen understrekes «behovet for kunnskapsrespons på samfunnssikkerhetssiden for å forstå og respondere på risikoer i kjølvannet av den teknologiske transformasjonen». Planperioden for SAMRISK er fra 2018–2027.

Kilde: Forskningsrådet (2018) *Programplan for SAMRISK 2018-2027*, s. 4.

De to forskningsprogrammene er omfattende og favner en rekke ulike tema. Det er Forskningsrådets porteføljestyre som forvalter midlene som er bevilget av departementene. En gjennomgang av bevilgningene til IKTPLUSS og SAMRISK i perioden 2018–2021 viser at en relativ lav andel av de totale bevilgningene er tildelt prosjekter under temaet digital sikkerhet. For IKTPLUSS utgjør

[424] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet,* 11. mai 2021.
[425] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet, mars 2021.*
[426] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet,* 11. mai 2021.
[427] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.

tildelingene til prosjekter under temaet digital sikkerhet om lag 12,5 prosent (149,7 millioner delt på 49 prosjekter), mens for SAMRISK utgjør tildelingene om lag 3 prosent (5,5 millioner kroner fordelt på 4 prosjekter).[428]

Videre viser Justis- og beredskapsdepartementet til at forskningsmiljøer som Center for Cyber and Information Security ved Norges teknisk-naturvitenskapelige universitet (NTNU) og Simula ved Universitetet i Bergen er styrket gjennom årlige grunnbevilgninger fra flere departementer. I rapporteringen fra Kunnskapsdepartementet vises det til at grunnbevilgningen fra Justis- og beredskapsdepartementet til Center for Cyber and Information Security ved NTNU fra 2016 har vært på 5 millioner kroner årlig til områder som personvern, digital etterforskning og biometri. Helse- og omsorgsdepartementet bidrar til grunnbevilgningene med 2 millioner kroner årlig (redusert til 1 million årlig i 2022). I tillegg kommer bidrag fra partnere og inntekter fra andre kilder. Fra og med 2018 tildeler også Justis- og beredskapsdepartementet, som en del av regjeringens kryptologisatsing, 5 millioner kroner til Simula ved Universitet i Bergen for å styrke forskningen innenfor kryptologi.[429]

Faktaboks 22 Beskrivelse av Center for Cyber and Information Security ved NTNU

Center for Cyber and Information Security er et nasjonalt senter for forskning, utdanning, testing, opplæring og kompetanseutvikling innenfor cyber- og informasjonssikkerhet ved NTNU Gjøvik og NTNU Trondheim. Senteret har som mål å:

- øke Norges cybersikkerhetskapasitet for å møte våre langsiktige sikkerhetsutfordringer
- utvikle cybersikkerhetskompetanse i norske etater, bedrifter og akademia
- være en profesjonell støtte til regjeringen i internasjonale diskusjoner og forpliktelser

Kilde: NTNU (2022) *Center for Cyber and Information Security.* Nettkilde. [Hentedato: 11.11.22].

Faktaboks 23 Bekrivelse av Simula ved Universitetet i Bergen

Simula er et frittstående forskningssenter innenfor informasjons- og kommunikasjonssikkerhet. Senteret ble opprettet gjennom et samarbeid mellom Institutt for informatikk ved Universitetet i Bergen og Simula Research Laboratory i Oslo. Forskningssenteret er spesielt orientert mot kryptografi, datasikkerhet og informasjonsteori.

Kilde: Universitetet i Bergen (2022) *Simula@UiB*. Nettkilde. [Hentedato: 11.11.2022].

Flere rekrutteringsstillinger innenfor digital sikkerhet og kryptologi

Kunnskapsdepartementet viser til at Universitetet i Oslo, Universitet i Bergen, NTNU og Simula i 2017 og 2018 ble tildelt midler til totalt 62 rekrutteringsstillinger innenfor IKT med vekt på digital sikkerhet og kryptologi. For 24 av stillingene ved NTNU og Simula ble det stilt krav om at institusjonen måtte samarbeide med Nasjonal sikkerhetsmyndighet og andre relevante aktører for å legge til rette for at flere med kompetanse innenfor kryptologi kunne sikkerhetsklareres. Dette samarbeidet har tatt noe tid og medførte at flere stillinger stod ubesatt da Kunnskapsdepartementet innhentet en statusoppdatering for stillingene i august 2019. Kunnskapsdepartementet har ikke innhentet ny statusoppdatering i ettertid, men uttaler at de ikke har grunn til å tro at stillingene stod ubesatt lenge etter at samarbeidet kom på plass.[430]

[428] Statistikken er hentet fra Forskningsrådets egen prosjektbank med «digital sikkerhet» som søkeord. Prosjektbanken er tilgjengelig på https://prosjektbanken.forskningsradet.no/ [Hentedato 3. august 2022].
[429] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet, mars 2021.*
[430] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet mars 2021;* verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.

Det er også bevilget midler til stillinger i Forskningsrådets ordninger Offentlig sektor-ph.d. og Nærings-ph.d. Dette er ordninger der offentlige og private virksomheter får støtte til at ansatte kan gjennomføre en doktorgrad. I 2020 ble 18 stillinger i disse ordningene øremerket digital sikkerhet og kryptologi. For disse 18 stillingene stilles krav om at kandidatene kan sikkerhetsklares.[431] Ifølge Kunnskapsdepartementet har det vært utfordrende å rekruttere kandidater som kan sikkerhetsklareres, til programmene. Det har vært få søkere, og ikke alle stillingene har blitt besatt. Per februar 2022 har Forskningsrådet kun besatt åtte av de 18 stillingene (tre innenfor ordningen Nærings-ph.d. og fem innenfor ordningen Offentlig sektor-ph.d.). Selv om midlene tildeles i et forholdvis rolig tempo, viser Kunnskapsdepartementet til at Forskningsrådet antar at de vil motta søknader også det kommende året. De lyser derfor ut midlene via ordningene Nærings-ph.d. og Offentlig sektor-ph.d. også i 2022. Dersom Forskningsrådet opplever at søkningen stopper helt opp, vil Kunnskapsdepartementet diskutere mulige alternativer med Forskningsrådet. Sammen med Justis- og beredskapsdepartementet og Forsvarsdepartementet arbeider Kunnskapsdepartementet for å gjøre tilbudet bedre kjent.[432]

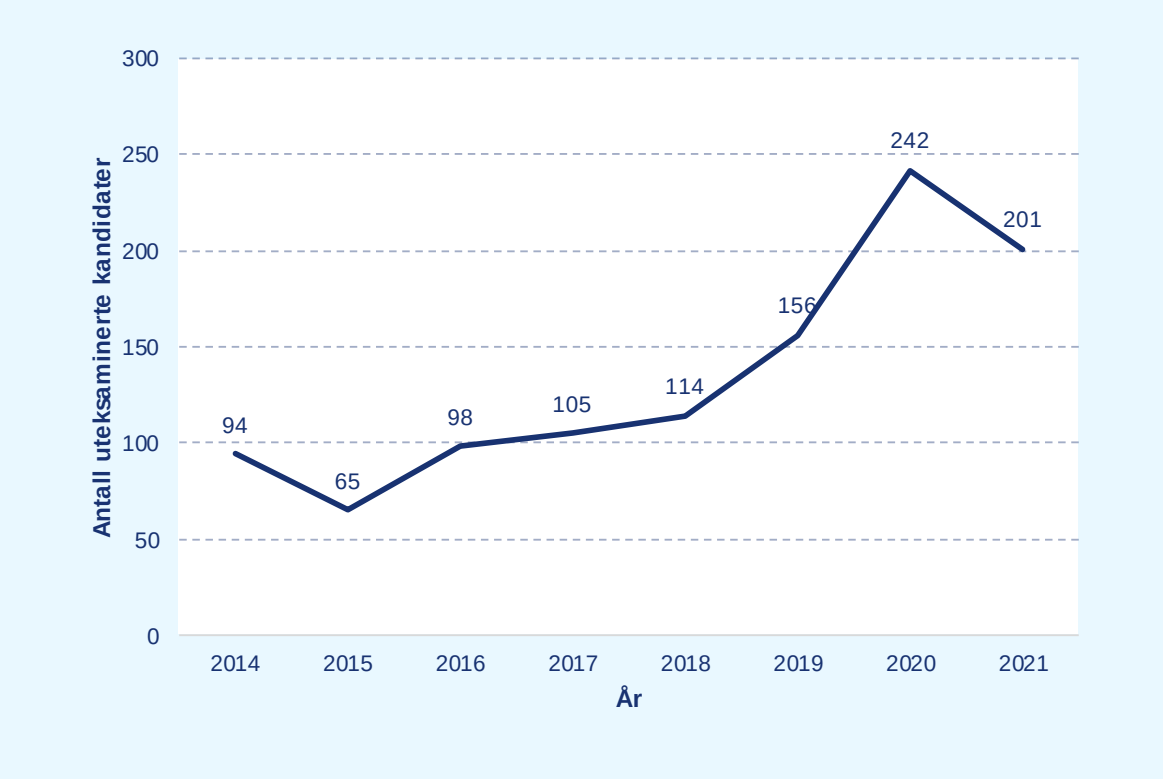
Økning i antall studenter innenfor IKT og digital sikkerhet

Justis- og beredskapsdepartementet viser til at myndighetene siden 2016 har gitt føringer og øremerket studieplasser og rekrutteringsstillinger for digital sikkerhet. I 2016 øremerket Kunnskapsdepartementet 65 stillinger til digital sikkerhet, som skulle bygges videre ut til 4-årige plasser. Fra 2015 til 2019 tildelte regjeringen midler til nesten 1600 nye studieplasser i IKT-relaterte fag ved universiteter og høyskoler, inkludert IKT-sikkerhet. Gjennom Utdanningsløftet 2020, et midlertidig tiltak iverksatt som følge av pandemien, ble det i tillegg gitt midler til 1400 studieplasser i realfag og teknologi med vekt på informatikk og IKT.[433]

Kunnskapsdepartementet viser i intervju til at det har vært en betydelig økning i antall studenter som tas opp og uteksamineres i IKT-relaterte utdanninger.[434] I statusoppdateringen vises det til at antall kandidater som ble uteksaminert fra IKT-relaterte utdanninger, økte med 72 prosent fra 2014 til 2020 (3102 kandidater i 2020).[435] Statistikk fra Direktoratet for høyere utdanning og kompetanse viser at antall uteksaminerte kandidater innenfor digital sikkerhet økte med 114 prosent i perioden 2014–2021 (201 kandidater i 2021). Figur 8 viser utviklingen i antall uteksaminerte kandidater i perioden. Både Kunnskapsdepartementet og Justis- og beredskapsdepartementet bemerker at vi ennå ikke har sett den fulle effekten av nye studieplasser, og at veksten forventes å fortsette de kommende årene.[436]

[431] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet mars 2021.*
[432] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[433] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet mars 2021.*
[434] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[435] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet,* 11. mai 2021.
[436] Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet,* 11. mai 2021.

Figur 8 Utviklingen i antall uteksaminerte kandidater innenfor IKT / digital sikkerhet (årstudier, 2-årige høyskolestudier og bachelor- og masterstudier)



Kilde: Figuren er basert på uttrekk fra Database for statistikk om høyere utdanning, Direktoratet for høyere utdanning og kompetanse. Uttrekket ble gjort av Kunnskapsdepartementet i november 2021 og sendt til Riksrevisjonen per e-post 26. januar 2022.

Midler til flere etter- og videreutdanningstilbud innenfor IKT og digital sikkerhet

Når det gjelder tiltak knyttet til kompetansestrategiens satsningsområdet etter- og videreutdanning, viser Kunnskapsdepartementet i rapporteringen til at regjeringen i 2020 kom med St. Meld. 14 (2019−2020) *Kompetansereformen − lære hele livet*. Kompetanseprogrammet, som inngår i reformen, trekkes i statusoppdateringen fram som et viktig tiltak som skal bidra til å tette kompetansegapet i samfunnet. Kompetanseprogrammet skal blant annet inneholde utlysninger av tilskudd til utvikling av fleksible utdanningstilbud, slik at virksomheter og enkeltpersoner får bedre tilgang til fleksibel og arbeidsrelevant videreutdanning.[437]

Faktaboks 24 Kompetanseprogrammet

Kompetanseprogrammet skal bidra til å lukke noe av kompetansegapet i arbeidslivet. Programmet skal skape flere nye fleksible tilbud som arbeidslivet etterspør. I tillegg vil programmet prøve ut tiltak som kan øke etterspørselen etter kompetanseutvikling. Kompetanseprogrammet skal forvaltes av Kompetanse Norge og vil i 2020 være delt inn i tre programområder:

- Programområde 1 – tilskudd til fleksible videreutdanningstilbud
- Programområde 2 – treparts bransjeprogram for kompetanseutvikling
- Programområde 3 – utprøving av insentivordninger for livslang læring

Kilde: Meld. St. 14 (2019–2020) *Kompetansereformen – Lære hele livet.*

[437] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet mars 2021.*

Ifølge Kunnskapsdepartementet ble det gjennom Kompetanseprogrammet i 2020 tildelt 20 millioner kroner til videreutdanningstilbud innenfor digital kompetanse, inkludert digital sikkerhet. Og i 2021 ble det lyst ut 40 millioner kroner til utvikling og utprøving av fleksible videreutdanningstilbud som gir kompetanse som er nødvendig for digitaliseringen. I denne utlysningen prioriterer man særlig videreutdanningstilbud for å styrke digital kompetanse, digital sikkerhet og kompetanse med tanke på det grønne skiftet. I rapporteringen bemerker Kunnskapsdepartementet at tiltakene i kompetansereformen antakelig vil bidra til at målet om bedre digital sikkerhetskompetanse nås, selv om reformen ikke er rettet direkte mot digital sikkerhetskompetanse.[438] Statusoversikten sier ingenting om resultatet av tildelingene for 2020 og 2021.

6.2.5 Foreløpig effekt av tiltakene

Ifølge Justis- og beredskapsdepartementet og Kunnskapsdepartementet er det for tidlig å stadfeste den fulle effekten av tiltakene i kompetansestrategien. Dette følger av at tiltakene i strategien er av langsiktig karakter. Per august 2022 har kompetansestrategien derfor ikke blitt evaluert i sin helhet. Det er heller ikke innhentet oppdaterte data og analyser om forholdet mellom samfunnets tilgang til og behov for digital sikkerhetskompetanse.[439] Kunnskapsdepartementet viser imidlertid til at deler av tiltakene i kompetansestrategien inngår i andre evalueringer. Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) arbeider for eksempel med en større evaluering av etter- og videreutdanningstilbudet, der digital sikkerhetskompetanse inngår. I tillegg vil deler av tiltakene i kompetansestrategien inngå i evalueringen av Kunnskapsløftet.[440]

I en foreløpig vurdering av tiltaksområdene i kompetansestrategien viser imidlertid Kunnskapsdepartementet til at det er en positiv utvikling i antall studenter som tas opp og uteksamineres i studier innenfor IKT og digital sikkerhet. Den positive utviklingen er forventet å øke i årene som kommer. Etter departementets vurdering har også tiltaket som går ut på å tildele midler til flere ph.d.-stillinger innenfor digital sikkerhet og kryptologi, truffet målgruppen, men de erkjenner at rekrutteringen har tatt tid. Når det gjelder Forskningsrådets ordning Offentlig sektor-ph.d., skyldes dette delvis at informasjonsflyten ut til relevante virksomheter har vært for liten, men også at det tar tid å utvikle forskningsprosjekter og finne samarbeidsmiljøer ved universitetene og høyskolene. Ifølge Kunnskapsdepartementet er det for tidlig å vurdere effekten av forskningsprosjekter som er igangsatt som følge av kompetansestrategien. Dette følger av at prosjektene fortsatt pågår. Departementet har ikke tall på hvor mange prosjekter som har blitt igangsatt under temaet digital sikkerhet siden 2019, men viser til at de kan innhente tall fra Forskningsrådet ved behov.[441] Justis- og beredskapsdepartementet legger til at et viktig mål med kompetansestrategien har vært å legge føringer for utdannings- og forskningsinstitusjonene i retning av økt oppmerksomhet mot digital sikkerhet. På dette området mener Justis- og beredskapsdepartementet at kompetansestrategien har hatt effekt.[442]

Kunnskapsdepartementet viser også til at en del av Direktoratet for høyere utdanning og kompetanses faste oppdrag er å følge med på samfunnets kompetansebehov. Dette inkluderer samfunnets behov for digital sikkerhetskompetanse. Under ledelse av direktøren i direktoratet har det også blitt nedsatt et ekspertutvalg, Kompetansebehovutvalget, som ser på større utviklingstrekk i Norges framtidige kompetansebehov. [443] Kompetansebehovutvalget gav ut rapporter i 2018, 2019, 2020 og 2021.[444] En

[438] Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse Kunnskapsdepartementet, mars 2021.*
[439] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022; Justis- og beredskapsdepartementet (2022) *Innspill til møtereferat 28. juni 2022 og supplerende informasjon*. Sendt til Riksrevisjonen 24. august 2022; Kunnskapsdepartementet (2022) *Svar på oppfølgingsspørsmål om Nasjonal strategi for digital sikkerhetskompetanse*. Sendt til Riksrevisjonen per e-post 26. august 2022.
[440] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[441] Kunnskapsdepartementet (2022) *Svar på oppfølgingsspørsmål om Nasjonal strategi for digital sikkerhetskompetanse*. Sendt til Riksrevisjonen per e-post 26. august 2022.
[442] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[443] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[444] NOU (2018: 2) *Fremtidige kompetansebehov 1. Kunnskapsgrunnlaget*; NOU (2019:2) *Fremtidige kompetansebehov II. Utfordringer for kompetansepolitikken*; NOU (2020: 2) *Fremtidige kompetansebehov III. Læring og kompetanse i alle ledd*; Kompetansebehovutvalget (2022) *Fremtidige kompetansebehov: Høyere yrkesfaglig utdanning for et arbeidsliv i endring*.

gjennomgang vi har gjort av disse rapportene, viser at kunnskapsgrunnlaget som utvalget har brukt for å beskrive behovene for digital sikkerhetskompetanse, i hovedsak er det samme som ble brukt til å utarbeide kompetansestrategien.

På oppdrag fra Kunnskapsdepartementet har Direktoratet for høyere utdanning og kompetanse i 2021 utarbeidet to rapporter om behovet for IKT-kompetanse i Norge − én vurdering av kunnskapsgrunnlaget og én vurdering av tiltak.[445] Rapportene skal blant annet inngå som en del av kunnskapsgrunnlaget for en ny rapport fra Kompetansebehovutvalget. I rapportene vises det til at det fortsatt er mangel på IKT-spesialister, og mangelen på sikkerhetsanalytikere trekkes fram spesielt.[446] Også direktoratet konkluderer med at det er for tidlig å vurdere effekten av tiltakene som er iverksatt på kompetanseområdet, men at det med høy grad av sikkerhet kan sies at behovet for spesialisert IKT-kompetanse ikke kommer til å bli mindre i tiden framover. Det er derimot usikkerhet knyttet til hvor mye behovet vil øke, og om arbeidslivets behov vil bli dekket. Videre viser direktoratet til at de på bakgrunn av det tilgjengelige kunnskapsgrunnlaget ikke kan si at opptrappingen av antall studieplasser de siste årene, vil være nok til å dekke arbeidslivets behov for IKT-kompetanse. Det er flere grunner til dette. Behovet øker hele tiden på grunn av digitaliseringen av samfunnet, mangelen på IKT-kompetansen er stor, og etterslepet er stort fordi mangelen på IKT-kompetanse har eksistert og økt over lang tid.[447]

I tillegg viser Kunnskapsdepartementet i intervju til at det i dialog med Justis- og beredskapsdepartementet har blitt pekt på et behov for personell med kompetanse på kvanteteknologi. Dette er en type teknologi som vil kunne ha stor påvirkning på utviklingen innenfor kryptologi.[448] Til tross for de overnevnte behovene opplyser både Kunnskapsdepartementet og Justis- og beredskapsdepartementet at det ikke foreligger planer om å revidere eller oppdatere kompetansestrategien. Kompetanseutfordringene på det digitale området vil bli håndtert på annen måte.[449]

Forsvarsdepartementet er delansvarlig for kompetansestrategien tilhørende *Nasjonal strategi for digital sikkerhet* (2019). I intervju bemerker Forsvarsdepartementet at det vil kunne ha en positiv effekt at det utdannes flere innenfor digital sikkerhet, men de vurderer likevel ikke satsingen som beskrives i kompetansestrategien, som tilstrekkelig for å dekke kompetansebehovet, verken i forsvarssektoren eller nasjonalt. Forsvarsdepartementet mener også at behovsanalysen som ligger til grunn for strategien, er noe utdatert, og viser til at de gav sine innspill til strategien tilbake i 2017. Det har skjedd store endringer på området siden den gang.[450]

6.3 Gjennomføring og evaluering av øvelser innenfor digital sikkerhet

I det følgende presenterer vi Justis- og beredskapsdepartementets og underliggende etaters arbeid med gjennomføring og evaluering av øvelser innenfor digital sikkerhet. Avslutningsvis presenterer vi også kort myndighetens arbeid med evaluering av større, uønskede digitale hendelser.

Både sikkerhetsloven og samfunnssikkerhetsinstruksen stiller krav om gjennomføring av øvelser og evalueringer i etterkant av større digitale, uønskede hendelser og etter øvelser. Se faktaboks 25 for en nærmere beskrivelse av lovkravene.

[445] Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av kunnskapsgrunnlaget.* Rapport nr. 01/2021 (utgitt september 2022); Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av tiltak.* Rapport nr. 03/2021 (utgitt november 2021).
[446] Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av kunnskapsgrunnlaget.* Rapport nr. 01/2021, s. 17.
[447] Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av tiltak.* Rapport nr. 03/2021, s. 29.
[448] Verifisert intervju med Kunnskapsdepartementet, 26. januar 2022.
[449] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[450] Verifisert intervju med Forsvarsdepartementet 19. januar 2022.

Faktaboks 25 Krav til evaluering i sikkerhetsloven og samfunnssikkerhetsinstruksen

Sikkerhetsloven § 4-3 har krav om gjennomføring av sikkerhetstiltak og øvelser. Det er nedfelt i sikkerhetsloven at virksomhetene regelmessig skal gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak.

I henhold til kapittel 4 i samfunnssikkerhetsinstruksen skal det enkelte departement øve målrettet i egen sektor og tverrdepartementalt. Departementet skal ha en øvelsesplan bestående av formål, tid og øvingsform. Departementets ledelse og andre i departementet som har definerte oppgaver ved krisehåndtering, skal øve på sine roller. Departementet skal også evaluere hendelser og øvelser og sørge for at funn og læringspunkter følges opp gjennom en ledelsesforankret vurdering og tiltaksplan. Oppfølgingen etter øvelser og hendelser skal ikke anses som avsluttet før alle punktene i tiltaksplanen er fulgt opp tilfredsstillende (jf. kapittel IV punkt 7 b og 8).

Kilde: Lov om nasjonal sikkerhet; Instruks for departementenes arbeid med samfunnssikkerhet.

6.3.1 Nasjonale øvelser og evalueringer av disse

Justis- og beredskapsdepartementet er etter samfunnssikkerhetsinstruksen ansvarlige for å planlegge, gjennomføre og evaluere nasjonale øvelser i sivil sektor (jf. kapittel VI punkt 2 b). Direktoratet for samfunnssikkerhet og beredskap er tildelt ansvaret med å sikre og utvikle systematisk oppfølging, implementering av læringspunkter og kompetanseheving etter øvelser og større hendelser. Dette ansvaret gjelder på tvers av sektorer og forvaltningsnivåer.[451] Direktoratet for samfunnssikkerhet og beredskap skal også tilrettelegge for og gjennomføre kurs i planlegging og gjennomføring av øvelser for offentlige virksomheter. Digitaliseringsdirektoratet bidrar i arbeidet med å utvikle øvelser innenfor digital sikkerhet.

Det har vært gjennomført to nasjonale øvelser innenfor digital sikkerhet de siste seks årene. Disse er IKT16 og Øvelse Digital 2020. Norge har i tillegg deltatt i en rekke internasjonale øvelser, blant annet i regi av NATO og EU. Disse omtales under punkt 6.3.2.

Planlegging og gjennomføring av Øvelse Digital 2020

Ifølge tiltak 41 i *Nasjonal strategi for digital sikkerhet* (2019) skulle det i løpet av 2020 gjennomføres en IKT-sikkerhetsøvelse med det formål å styrke sivilt-militært, offentlig-privat og internasjonalt samarbeid om hendelseshåndtering.[452] Videre var intensjonen med øvelsen å øve på håndtering, med vekt på effektiv informasjonsdeling, ulike kommunikasjonsbehov, kartlegging av relevante aktører og håndtering i henhold til gjeldende roller og ansvar. Øvelsen skulle redusere samfunnets sårbarhet for tilsiktede, uønskede digitale hendelser gjennom å 1) forbedre evnen til å håndtere tilsiktede digitale hendelser og 2) øke den digitale sikkerhetskompetansen og evnen til å forebygge og detektere digitale hendelser.

Justis- og beredskapsdepartementet, Forsvarsdepartementet og Samferdselsdepartementet var oppdragsansvarlige for øvelsen. Direktoratet for samfunnssikkerhet og beredskap hadde hovedansvar for å planlegge og utarbeide øvelsen, og har i etterkant av øvelsen ledet evaluerings- og oppfølgingsarbeidet.[453]

[451] Justis- og beredskapsdepartementet (2021) *Tildelingsbrev til Direktoratet for samfunnssikkerhet og beredskap.*
[452] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[453] Departementene (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet;* Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar, 2022.

Øvelse Digital 2020 var planlagt som et tredelt konsept som opprinnelig bestod av følgende elementer:

- Gjennomføring av kompetansehevingsløp for relevante virksomheter
- Planlegging, gjennomføring og evaluering av en todagers spilløvelse
- Utarbeidelse av diskusjonsøvelser (øvingspakker)

Grunnet koronapandemien ble imidlertid Øvelse Digital 2020 kraftig nedskalert. Justis- og beredskapsdepartementet viser til at nedstengningen av samfunnet i perioden rundt øvelsestidspunket er grunnen til at den nasjonale øvelsen ikke kunne gjennomføres som planlagt. Blant annet var mange av de ansatte i virksomhetene som opprinnelig skulle delta fysisk pålagt å sitte på hjemmekontor.[454]

Blant virksomhetene som opprinnelig skulle delta i øvelsen var Justis- og beredskapsdepartementet, Finansdepartementet, Forsvarsdepartementet, Norges Bank, Finanstilsynet, DNB, Nordic Financial CERT, Forsvarets operative hovedkvarter, Cyberforsvaret, Nasjonal sikkerhetsmyndighet, Kripos, Politidirektoratet og Direktoratet for samfunnssikkerhet og beredskap. I tillegg ble også andre direktorater og private virksomheter som ønsket å delta, invitert med.[455]

Kompetansehevingsløpet skulle bidra til å styrke den digitale sikkerhetskompetansen hos deltakende virksomheter, og ruste dem for spilløvelsen, men ble nedskalert til et mindre omfang enn hva som var planlagt. Følgende arrangementer ble gjennomført:

- Håndtering av digitale hendelser og samordning av kommunikasjon i regi av Direktoratet for samfunnssikkerhet og beredskap og Nasjonalt cybersikkerhetssenter (10. januar 2020)
- Seminar om blant annet verdivurdering og etterretningstrussel mot deg og din virksomhet, i forbindelse med planleggingskonferanse II (22.–23. januar 2020)
- Seminar om bl.a. øvingspakkene i regi av Direktoratet for samfunnssikkerhet og beredskap og Digitaliseringsdirektoratet (9. september 2020)
- Seminar om digital sikkerhet i regi av Direktoratet for samfunnssikkerhet og beredskap (14. oktober 2020)[456]

Spilløvelsen skulle etter den opprinnelige planen foregå over to dager, men ble redusert til en to timers digital diskusjonsøvelse mellom de gjenværende aktørene, og ble avgrenset mot finanssektoren, med noe kommunikasjon med andre sektorer. Diskusjonsøvelsen involverte 15 virksomheter fra offentlig sektor, private aktører og Forsvaret.

I forbindelse med del tre av Øvelse Digital 2020 − utarbeidelse av diskusjonsøvelser (øvingspakker) − har Digitaliseringsdirektoratet lagt til rette for og gjennomført kurs i planlegging og gjennomføring av øvelser for offentlige virksomheter. Etter øvelsen har Digitaliseringsdirektoratet, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal sikkerhetsmyndighet, Norsk senter for informasjonssikring og NTNU jobbet videre med å utarbeide øvelsesscenarioer basert på konseptet som ble utviklet under Øvelse Digital 2020. Dette samarbeidet presenteres som et tiltak − sikker digitalisering i offentlig sektor − i *Nasjonal strategi for digital sikkerhet* (2019). I forbindelse med nasjonal sikkerhetsmåned i november 2020 ble øvelsesscenarioene samlet gjort tilgjengelig for alle norske virksomheter gjennom lanseringen av nettsiden *ovelse.no* Formålet med nettsiden er å gjøre virksomheter bedre rustet til å håndtere digitale hendelser gjennom å tilby dem verktøy for å øve på hendelseshåndtering.[457] Direktoratet for samfunnssikkerhet og beredskap opplyste i januar 2022 om at 650 virksomheter hadde logget seg inn i nettløsningen, men at de ikke har informasjon om hvor mange som faktisk har

[454] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[455] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.
[456] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.
[457] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.

gjennomført øvelser, eller hvilken nytte virksomhetene har hatt av øvingsportalen.[458] Som en del av Øvelse Digital 2020 ble det også satt av midler til å evaluere *ovelse.no*. Evalueringen gjennomføres av NTNU. I en e-post til Riksrevisjonen 9. juni 2022 opplyser Direktoratet for samfunnssikkerhet og beredskap om at NTNU er i rute med evalueringsrapporten. Rapporten skal etter planen sendes til Direktoratet for samfunnssikkerhet og beredskap 1. februar 2023.

Erfaringer med og oppfølging av Øvelse Digital 2020

Direktoratet for samfunnssikkerhet og beredskap konkluderer i sin evaluering av Øvelse Digital 2020 med at øvelsens formål som helhet er oppnådd.[459] Også Justis- og beredskapsdepartementet vurderer øvelsen som en fullskala øvelse, ressurssituasjonen og behovene tatt i betraktning.[460]

Direktoratet for samfunnssikkerhet og beredskap finner at Øvelse Digital 2020 har bidratt til å øke den tverrsektorielle vektleggingen av digital sikkerhet. De viser særlig til det gode samarbeidet mellom Direktoratet for samfunnssikkerhet og beredskap, Nasjonal sikkerhetsmyndighet og Norsk senter for informasjonssikring i planleggingsfasen.[461]

Justis- og beredskapsdepartementet uttrykker at planleggingsarbeidet knyttet til Øvelse Digital 2020 var omfattende, og at det har gjort det mulig å identifisere forbedringsområder innenfor myndighetenes arbeid med digital sikkerhet. Departementet opplever at dette har bidratt til å øke kompetansen hos de deltakende virksomhetene.[462] Et intervall på fire år mellom hver nasjonale øvelse innenfor digital sikkerhet kan ifølge Justis- og beredskapsdepartementet være hensiktsmessig. Kvaliteten på øvelsene anses av departementet å være viktigere enn antallet, og det største læringsutbyttet og kompetansehevingen knyttet til en slik øvelse ligger ifølge departementet i planleggingen.[463] I tillegg bemerker departementet at planlegging og gjennomføring av øvelser medfører stor ressursbruk for de involverte partene, og at det ikke vil være hensiktsmessig om sentrale ressurser i for stor grad er opptatt med planlegging og gjennomføring av øvelser. Øvelser er bare et av flere virkemidler som må balanseres opp mot annet bruk av ressurser og tiltak.[464]

Selv om øvelsen måtte nedskaleres, rapporterer Direktoratet for samfunnssikkerhet og beredskap at planleggingsprosessen, kompetansehevingsløpet og arbeidet med øvingspakkene gav et stort læringsutbytte. Direktoratet erkjenner likevel at viktige elementer ble utelatt fra øvelsen som følge av nedskaleringen, og viser til at diskusjonsøvelsen ikke innfridde alle øvingsmålene. Selv om evalueringen viser gode tilbakemeldinger fra flere av deltakerne, gjorde nedskaleringen at deltakerne ikke fikk anledning til å gå i dybden på problemstillingene på samme måte som de hadde gjort ved en todagers spilløvelse. Enkelte virksomheter argumenterte derfor med at målet for Øvelse Digital 2020 ikke ble nådd.[465] Forsvarsdepartementet forteller i intervju at de vurderer utbyttet av øvelsen som begrenset. De opplevde det imidlertid som nyttig å sette digitale verdikjeder og avhengigheter i fokus, og mener øvelsen bidro til økt kjennskap til de andre aktørene på området.[466]

Evalueringen viser at det er behov for å jobbe videre med å skaffe oversikt over det komplekse aktørbildet innenfor digital sikkerhet, med samhandlingen på tvers av sektorer og med koordinert kommunikasjonshåndtering. Eksisterende planverk ble vurdert som tilstrekkelig for å håndtere denne typen hendelser, men Direktoratet for samfunnssikkerhet og beredskap finner at det er behov for å ha et bredere blikk på avhengigheter og sårbarheter på tvers av sektorer enn man har i dag. Direktoratet

[458] Verifisert intervju med Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[459] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.
[460] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[461] Verifisert intervju Direktoratet for samfunnssikkerhet og beredskap, 14. januar 2022.
[462] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[463] Verifisert intervju med Justis- og beredskapsdepartementet, 22. april 2021.
[464] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[465] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.
[466] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.

for samfunnssikkerhet og beredskap ser behov for flere og hyppigere nasjonale øvelser innenfor digital sikkerhet og utvikling av et helhetlig aktørkart. Videre kom det fram at utveksling av sikkerhetsgradert informasjon (selv om dette ikke var tematisert i øvelsen), særlig mellom offentlige og private virksomheter, vil være utfordrende dersom det skulle bli behov for å kommunisere sikkerhetsgradert i en reell hendelse.[467] Etablering av sikkerhetsgraderte kommunikasjonssystemer omtales i eget sikkerhetsgradert vedlegg til denne rapporten.

Evalueringen anbefaler videre at styringsgruppen, som en del av oppfølgingen, diskuterer hvem som skal være ansvarlige for tiltakene som er løftet i evalueringen, og forslag til eventuelle nye tiltak. Den endelige prosessen for å følge opp evalueringen er ennå ikke besluttet. Dette skal diskuteres i *Nasjonalt øvelses- og evalueringsforum* høsten 2022. Justis- og beredskapsdepartementet skal følge opp øvelsen etter dette.[468]

6.3.2 Øvrige øvelser innenfor digital sikkerhet

I statusgjennomgangen av tiltak til *Nasjonal strategi for digital sikkerhet* (2019) beskriver Justis- og beredskapsdepartementet øvelser som et velbrukt verktøy, særlig på virksomhetsnivå, men også på sektornivå.[469] Som grunnlag for denne slutningen viser Justis- og beredskapsdepartementet til at de årlig gjennomfører en kartlegging av øvelser på departementsnivå. Kartleggingen omfatter antall øvelser og hvordan øvelsen er fulgt opp. Dersom Justis- og beredskapsdepartementet ser at det er gjennomført lite øvelser kan de gi virksomhetens råd og veiledning etter ønske fra virksomheten.[470] Fra Justis- og beredskapsdepartementet etterspurte vi en oversikt over gjennomførte øvelser i perioden 2018−2020 med relevans for digital sikkerhet. Justis- og beredskapsdepartementet opplyser imidlertid om at kartleggingen ikke omfatter hva slags type øvelse som gjennomføres og at de dermed ikke har en fullstendig oversikt over øvelser av relevans for digital sikkerhet. Justis- og beredskapsdepartementet har imidlertid oversikt over større nasjonale og internasjonale øvelser knyttet til digital sikkerhet i denne perioden.[471] Oversikten gjengis i Tabell 4.

Tabell 4 Større nasjonale og internasjonale øvelser med relevans for digital sikkerhet 2018 − 2020.

Øvelse	Beskrivelse	Gjennomført
Locked Shields	Årlig teknisk øvelse i regi av NATO med formål om å øve forsvaret av nasjonale digitale informasjonssystemer og kritisk infrastruktur.	2022
Øvelse Resilience	Funksjonsøvelse for alle departementene hvor formålet var å teste sikkerhetsgraderte kommunikasjonssystem for å sikre kjennskap til alternative kommunikasjonsmidler ved forstyrrelser/bortfall.	2022
Diskusjonsøvelse i Felles cyberkoordineringssenter	Øvelse for lederne av partene i Felles cyberkoordineringssenter, herunder Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos.	2022
Polaris Gram	Forsvarsøvelse.	2021
Øvelse Digital 2020	Nasjonal tverrsektoriell sivil-militær diskusjonsøvelse som hadde som formål å redusere samfunnets samlede sårbarhet for digitale hendelser.	2020

[467] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.
[468] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET: Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[469] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[470] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[471] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

NATOs Crisis Management Exercise	Årlig NATO-øvelse med formål om å øve politiske og militære beslutningstakere på strategisk nivå i kriseledelse. Øvelsen ble imidlertid sist gjennomført i 2019, da øvelsene for 2021 og 2022 har blitt utsatt.	2019
Trident Juncture	NATO-øvelse med formålet om å øve på forsvar av Norge. I tillegg fikk Norge trent på alliert mottak og det norske totalforsvaret ble øvet.	2018
EU Hybrid Exercise Multilayer 18	Øvelse i regi av EU med formål om å øve på krisehåndtering ved sammensatte eller hybride trusler.	2018

Kilde: Justis- og beredskapsdepartementet, Oversikt over øvelser relevant for nasjonal digital sikkerhet for perioden 2018-2022. Sendt til Riksrevisjonen 31. august 2022.

I tillegg opplyser Justis- og beredskapsdepartementet at det i perioden har avholdt flere sektorinterne øvelser der digitale hendelser var hovedscenario. Som eksempel viser departementet til at Nasjonal sikkerhetsmyndighet i 2021 har deltatt i øvelser i både finans- og kraftsektoren. Videre bemerker departementet at det generiske systemet for sentral krisehåndtering øves ofte, selv om disse øvelsene ikke alltid er knyttet spesifikt til digital sikkerhet. [472]

Forsvarsdepartementet opplyser om at etatene i forsvarssektoren, inkludert Nasjonalt sikkerhetsmyndighet, i tillegg til flere av øvelsene i Tabell 4, har deltatt i internasjonale øvelser og aktiviteter som blant annet NATO-øvelsen Cyber Coalition, EU-øvelsen Cyber Europe, Nordisk CERT-øvelse, Cyber Flag og Cybernet.[473] Justis- og beredskapsdepartementet bemerker at i øvelsen Cyber Europe har Nasjonal sikkerhetsmyndighet også invitert med relevant sektormyndighet og relevante infrastruktureiere, for eksempel Luftfartstilsynet og Avinor.[474]

Også Nasjonal kommunikasjonsmyndighet forteller at de som en del av totalforsvaret deltar i flere av de nasjonale forsvars- og totalforsvarsøvelsene. For eksempel deltok Nasjonal kommunikasjonsmyndighet i Trident Juncture i 2018 og Polaris gram i 2021. Nasjonal kommunikasjonsmyndighet skal også delta i NATO-øvelsen Cold response 2022. Ifølge Nasjonal kommunikasjonsmyndighet har de nasjonale øvelsene blitt mer rettet mot det relevante trusselbildet, som i større grad har blitt digitalt. Dette betyr at ekom stadig spiller en viktigere rolle i øvelsene. Erfaringene til Nasjonal kommunikasjonsmyndighet er at myndighetene over tid har blitt bedre til å finne hverandre i kriser, og at det har vært rettet oppmerksomhet mot samordning i flere øvelser.[475]

Øvelser er også et tema i flere av de tidligere omtalte samhandlingsarenaene. I *Norsk øvelses- og evalueringsforum* har det for eksempel siden 2014 blitt gjennomført årlige møter der formålet har vært å tilrettelegge for øvelser i offentlige virksomheter.[476] Telenor, som er en annen sentral aktør i ekomsektoren, etterlyser imidlertid flere offentlig-private øvelser for digital hendelseshåndtering.[477] Som nevnt viser også evalueringen av Øvelse Digital 2020 til at det er behov for flere og hyppigere nasjonale øvelser innenfor digital sikkerhet.[478]

I intervju viser Justis- og beredskapsdepartementet til at de er opptatt av å fremme viktigheten av øvelser, og at de derfor promoterer øvingsportalen *ovelse.no* så ofte de kan. Departementet antar

[472] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[473] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[474] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[475] Verifisert intervju med Nasjonal kommunikasjonsmyndighet, 19. mai 2021.
[476] Verifisert intervju med Kommunal- og distriktsdepartementet, 7. mai 2021.
[477] Furberg, Petter-Børre (administrerende direktør Telenor), *Beredskap og sikkerhet må planlegges for selv de verste dager*. Innlegg på Nasjonal sikkerhetsmyndighets sikkerhetskonferanse i 2022. Nettkilde. [Hentedato: 19. november 2022].
[478] Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport*. UNNTATT OFFENTLIGHET.

også at den nye, felles myndighetsportalen vil bidra til å gjøre ovelse.no bedre kjent. Justis- og beredskapsdepartementet har imidlertid ikke vurdert å presisere krav til øvelser innenfor digital sikkerhet, og bemerker at det ikke må bli for mange øvelser. Dette skyldes blant annet at øvelser er svært ressurskrevende for virksomhetene som deltar.[479]

Øvelser i kommunene

Forskrift om kommunal beredskapsplikt § 7 stiller krav om øvelser og opplæring i kommunen. Kommunens beredskapsplan skal øves hvert annet år. Scenarioene for øvelsene bør etter forskriften hentes fra kommunens helhetlige risiko- og sårbarhetsanalyse. Kommunen skal øve sammen med andre kommuner og relevante aktører der valgt scenario og øvingsform gjør dette hensiktsmessig. Det stilles også krav om evaluering etter øvelser og uønskede hendelser (jf. § 8).

Vår gjennomgang av kommunale tilsynsrapporter, kommunerevisjoner og interne kommunale dokumenter viser at samtlige av disse dokumentene undersøker og omtaler kommunenes øvelsesvirksomhet. Dette gjelder imidlertid øvelser innenfor samfunnssikkerhet og beredskap i stort. Ingen av de gjennomgåtte dokumentene omhandler øvelser innenfor digital sikkerhet.

I Digitaliseringsdirektoratets undersøkelse av kommunenes arbeid med informasjonssikkerhet fra 2020 fant de at det er få kommuner som gjennomfører årlige øvelser knyttet til informasjonssikkerhet. Kun 13 prosent av de små kommunene gjennomfører slike øvelser. Tilsvarende tall er 9,2 prosent for mellomstore og 21 prosent for store kommuner.[480] I intervju forteller representanter for kommunesektoren at de opplever at det er behov for å prioritere øvelser innenfor digital sikkerhet høyere.[481]

6.3.3 Evaluering og læring knyttet til større uønskede hendelser

Tiltak 45 tilhørende *Nasjonal strategi for digital sikkerhet* (2019) omhandler åpenhet og evaluering av uønskede hendelser. Under dette tiltaket vises det blant annet til at Nasjonal sikkerhetsmyndighet på oppdrag fra Justis- og beredskapsdepartementet tidligere har utarbeidet anbefalinger om hvordan virksomheter bør vurdere åpenhet om uønskede hendelser. Både offentlige og private virksomheter er oppfordret til å følge disse.

Justis- og beredskapsdepartementet uttaler i intervju at de opplever å være pådrivere for åpenhet ved ønskede digitale hendelser, og at de sørger for at viktigheten av åpenhet omtales på politiske konferanser og i andre relevante arenaer. Departementet viser også til at de er opptatt av å fremme viktigheten av evaluering etter digitale hendelser. Som eksempel trekkes evalueringene som er gjort i etterkant av de digitale angrepene mot fylkesmannsembetene og Helse Sør-Øst i 2018 fram. Evalueringen ble gjennomført av Forsvarets forskningsinstitutt på oppdrag fra Justis- og beredskapsdepartementet.[482]

Justis- og beredskapsdepartementet viser til at også stadig flere virksomheter deler erfaringer etter uønskede digitale hendelser. Nasjonalt cybersikkerhetssenter har bidratt til denne utviklingen ved at partene som deltar i nettverket aktivt har drevet med informasjons- og erfaringsutveksling etter pandemien. Informasjons- og erfaringsutvekslingen har for øvrig blitt ytterligere styrket som følge av krigen i Ukraina.[483]

[479] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[480] Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner*, s. 19.
[481] Verifisert intervju med representanter fra kommunesektoren, 2. juni 2022.
[482] Forsvarets forskningsinstitutt (2020) *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene.*
[483] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

6.4 Sentrale tverrsektorielle tiltak for avdekking og håndtering av digitale angrep

I det følgende går vi gjennom status for sentrale tiltak for bedre hendelseshåndtering i det digitale rom. Tiltakene, som tilhører *Nasjonal strategi for digital sikkerhet* (2019), omfatter blant annet:

- Oppgradering og videreutvikling av tekniske systemer for å avdekke trusler og sårbarheter
- Utredning av mulighetene for å etablere en reservekapasitet for håndtering av spesielt store og kompliserte digitale angrep
- Revisjon av *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017)
- Etablering av systemer for sikkerhetsgradert kommunikasjon mellom beredskapsaktører.

Tiltakene anses som svært viktige fordi de skal bidra til å forbedre den nasjonale evnen til å forebygge, avdekke og håndtere store digitale angrep.

6.4.1 Varslingssystemet for digital infrastruktur

Utvikling og oppgradering av varslingssystemet for digital infrastruktur (VDI) beskrives som sentrale tiltak i *Nasjonal strategi for digital sikkerhet* fra 2019. Det overordnende målet med tiltakene er å øke den nasjonale evnen til å avdekke målrettede digitale angrep. En utdypning av utfordringer knyttet til VDI beskrives i et sikkerhetsgradert vedlegg fordi deler av informasjonen om sensornettverket er sikkerhetsgradert i henhold til sikkerhetsloven.

Eksisterende VDI-løsning

Det er Nasjonal cybersikkerhetssenter som på vegne av Nasjonal sikkerhetsmyndighet drifter og organiserer VDI.[484] VDI består av nettverkssensorer som er utplassert hos virksomheter som anses som en del av den kritiske infrastrukturen i Norge. For oppdage uønsket aktivitet overvåker sensorene internettrafikken som går til og fra virksomhetene. Kriteriene for medlemskap i VDI-nettverket er at virksomhetene er underlagt sikkerhetsloven, pekt ut som en grunnleggende nasjonal funksjon, tilhører en prioritert sektor eller av andre årsaker kan sees på som samfunnsviktige.[485]

Informasjonen fra VDI-sensorene samles og analyseres av Nasjonalt cybersikkerhetssenter. Nasjonalt cybersikkerhetssenter har dermed oversikten over alle trusler og sårbarheter som fanges opp av sensorene. Når en trussel eller sårbarhet fanges opp sender Nasjonalt cybersikkerhetssenter informasjon til VDI-nettverkets medlemmer og anbefaler tiltak, slik at de skal kunne ruste seg mot potensielle angrep. Informasjonen kan også i enkelte tilfeller sendes ut til virksomheter som ikke er medlemmer i VDI-nettverket.

Nasjonalt cybersikkerhetssenter har i tillegg til VDI-nettverket en varslingstjeneste som alle norske virksomheter kan benytte seg av. Virksomhetene kan også be om å få særskilte varsler fra Nasjonalt cybersikkerhetssenter etter en godkjenning fra Nasjonal sikkerhetsmyndighet.[486]

Nasjonal sikkerhetsmyndighet påpeker at det kan være informasjon som ikke kan deles med alle virksomheter. Noe av informasjonen er sikkerhetsgradert og er dermed kun forbeholdt enkelte virksomheter.[487] Dersom deler av informasjonen eller kilden må beskyttes, bearbeider Nasjonalt cybersikkerhetssenter informasjonen slik at tiltakene som følger av den, ikke avslører kilden. For eksempel bearbeides sikkerhetsgradert informasjon for å kunne utforme tiltak som også kan anbefales

[484] Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT* [Hentedato 4. februar 2022].
[485] Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT* [Hentedato 4. februar 2022].
[486] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[487] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.

til virksomheter uten klarering, eller som ikke har systemer for å motta sikkerhetsgradert informasjon.[488]

Medlemskap i VDI-nettverket er basert på samtykke. I henhold til virksomhetssikkerhetsforskriften § 64 kan imidlertid Nasjonal sikkerhetsmyndighet pålegge virksomheter som er underlagt sikkerhetsloven, å knytte seg til VDI. Nasjonal sikkerhetsmyndighet forteller imidlertid at hjemmelen hittil ikke har vært benyttet.[489] Nasjonal sikkerhetsmyndighet forteller at virksomhetene blir medlem av VDI-nettverket av ulike grunner. Alle virksomheter kan sende inn en formell søknad til Nasjonal sikkerhetsmyndighet om medlemskap i nettverket.[490] Virksomhetene betaler selv for installasjonen av sensoren, og private virksomheter må betale en årlig avgift utover dette.

Nasjonal sikkerhetsmyndighet anser dekningen av VDI-sensorer som lavere enn ønsket i en del sektorer, men opplyser at det arbeides systematisk med å forbedre dekningsgraden.[491] I Prop. 78 S (2021−2022) *Endringer i Statsbudsjettet (økonomiske tiltak som følge av krigen i Ukraina)*, jf. Innst. 270 S (2021−2022), ble det bevilget til sammen 28,3 millioner kroner for å øke antall stillinger i Nasjonalt cybersikkerhetssenter med det formål å bedre kapasiteten for analyse og hendelseshåndtering og øke dekningsgraden av VDI. For å øke antall virksomheter som er med i VDI-nettverket, ble det bestemt at staten skal overta finansieringen av VDI-nettverket, slik at private virksomheter ikke lenger skal betale årlige avgifter eller etableringskostnader for VDI. Midlene ble imidlertid ikke videreført for 2023, og private virksomheter må betale for tjenesten etter årsskiftet.[492]

Ukjente angrepsmønstre vil foreløpig ikke bli oppdaget av VDI, da sensorene i dag kun fanger opp kjente signaturer[493]. Nasjonal sikkerhetsmyndighet forteller at det har blitt vanskeligere for VDI å oppdage uønskede digitale hendelser fordi de digitale truslene har blir mer kompliserte og fordi mer informasjon krypteres.[494] Det er imidlertid ikke alle virksomhetene i VDI-nettverket som er kjent med VDIs begrensede evne til avdekking av trusler. Noen av virksomhetene vi intervjuet, opplever VDI som en trygghet, mens andre er bekymret for hva VDI faktisk fanger opp. Én virksomhet uttrykker bekymring for at dagens VDI-løsning ikke fanger opp relevant aktivitet fra trusselaktører. Virksomheten peker på økt bruk av skytjenester og større grad av kryptert datatrafikk som forklaringer på VDIs begrensede deteksjonsevne. Virksomheten forteller at de i flere tilfeller har fanget opp trusler selv, gjennom egne systemer, og at de deretter har varslet Nasjonalt cybersikkerhetssenter.[495] En annen virksomhet opplever at VDI spilte en viktigere rolle før enn det gjør nå. Virksomheten beskriver VDI som én av flere kilder for å fange opp trusler. De opplever det likevel som en trygghet å ta del i VDI-nettverket.[496] To andre virksomheter har positive erfaringer med VDI-nettverket. Den ene virksomheten har erfart at Nasjonal sikkerhetsmyndighet varsler om trusler raskere enn det sektorvise responsmiljøet. Den andre virksomheten synes det er betryggende at ikke det hviler på virksomheten alene å oppdage uønsket aktivitet fra trusselaktører. Flertallet av de digitale uønskede hendelsene i virksomheten, har blitt fanget opp og varslet av Nasjonalt cybersikkerhetssenter.[497]

Nasjonal sikkerhetsmyndighet bemerker at VDI er et supplement, og ikke en erstatning for virksomhetens egne sikkerhetstiltak. VDI skal primært bidra til myndighetenes situasjonsforståelse når

[488] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[489] Verifisert intervju med Nasjonal sikkerhetsmyndighet (BEGRENSET), 1. desember 2021, utdraget det henvises til, er UGRADERT.
[490] Nasjonal sikkerhetsmyndighet (2020) *Varslingssystemet for digital infrastruktur (VDI)* [Hentedato 6. mai 2022].
[491] Verifisert intervju med Nasjonal sikkerhetsmyndighet (BEGRENSET), 1. desember 2021, utdraget det henvises til, er UGRADERT.
[492] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[493] Signaturer i VDI er å anse som digitale fingeravtrykk fra kjente trusselaktører eller måter de jobber på.
[494] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[495] Riksrevisjonens dybdeundersøkelser.
[496] Riksrevisjonens dybdeundersøkelser.
[497] Riksrevisjonens dybdeundersøkelser.

det gjelder sikkerhet i det digitale rom. Det er en forutsetning for VDI-medlemskap at virksomheten har en adekvat sikkerhetsorganisasjon med egne sikkerhetstiltak.[498]

Videreutviklingen av VDI

Nasjonal sikkerhetsmyndighet og Forsvarsdepartementet er ansvarlige for arbeidet med å utvikle ny sensorteknologi til bruk i VDI.[499] Bakgrunnen er at mesteparten av nettverkstrafikken i dag er kryptert, og at krypteringsgraden øker. Dermed blir synligheten i nettet dårligere, og VDI-sensorene fanger opp mindre. Nasjonal sikkerhetsmyndighet utvider derfor VDI med flere ulike komponenter, herunder kunstig intelligens og maskinlæring, som er designet for å fungere sammen og styrke situasjonsbildet for det digitale domenet. Dette er ment å styrke analysekapasiteten til VDI betydelig, slik at mer data kan innhentes, for eksempel fra skytjenester og sikkerhetslogger. Slik kan dataene fra ulike kilder kobles sammen, og uønsket aktivitet kan oppdages i større grad enn tidligere.[500] Neste generasjons VDI-sensor vil også ha mulighet til å støtte graderte signaturer og indikatorer og vil dekke et behov for raskere varsling. Tiltaket ses også opp mot arbeidet med sikret offentlig nett (SON), som er et annet tiltak i den nasjonale strategien. SON er tenkt som en sentral komponent i den nye VDI-løsningen.[501]

Forsvarsdepartementet forteller at ideen til et videreutviklet VDI-nettverk oppstod i 2012 som følge av et behov for å etablere et eget sensornettverk for Forsvaret. Da det på et senere tidspunkt ble klart at det også var behov for å oppgradere Nasjonal sikkerhetsmyndighets eksisterende VDI-sensornettverk, anbefalte departementet å slå de to prosjektene sammen. Videreutviklingen av VDI skal gjennomføres som et samarbeid mellom Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet og skal ferdigstilles i 2023.[502]

Forsvarsdepartementet bemerker i intervju at trusselsituasjonen var en annen da den opprinnelige prosjektideen først ble fremmet i 2012, og at behovet for funksjonalitet og teknologiske muligheter i VDI har endret seg over tid. Et viktig argument for en felles løsning med sivil sektor er blant annet at utviklingen som har skjedd innenfor maskinlæring, vil gi et langt større data-tilfang, som kan brukes til maskinlæring. Ved å være tilknyttet en felles løsning kan forsvarssektoren dra lærdom av hendelser i sivil sektor og omvendt. En annen viktig grunn til at Forsvarsdepartementet finansierer et tverrsektorielt investeringsprosjekt av denne typen, handler om totalforsvaret. I lys av forsvarssektorens avhengigheter av sivile virksomheter er det viktig for departementet å bidra til et styrket sikkerhetsnivå også på sivil side.[503]

Flere og flere virksomheter bruker i dag skyløsninger. VDI-sensorene kan per i dag ikke fange opp trafikken som går direkte fra klienter til servere i skyen, og dermed kan de ikke fange opp angrep via disse datastrømmene. Forsvarsdepartementet forteller at det på nåværende tidspunkt ikke er gjort noen vurdering av hvilke konsekvenser bruken av skytjenester har for VDI. De viser imidlertid til at et av målene med prosjektet er å utvikle nasjonal sensordekning som gjør det mulig å fange opp trusler i framtidig infrastruktur som er basert på skytjenester og gradert/kryptert informasjon. Dette forutsetter også en videreutvikling av hjemmelsgrunnlaget for VDI og nasjonal responsfunksjon. Økt bruk av skytjenester er tematisert i en rekke sammenhenger, blant annet i risikovurderingene til etterretnings- og sikkerhetstjenestene. Nasjonal sikkerhetsmyndighet antar imidlertid at VDI i lys av det digitale trusselbildet må videreutvikles ytterligere etter 2023.[504]

[498] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022.
[499] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[500] Nasjonal sikkerhetsmyndighet (2020) *Varslingssystemet for digital infrastruktur (VDI)* [Hentedato 6. mai 2022].
[501] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[502] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[503] Verifisert intervju med Forsvarsdepartementet (BEGRENSET), 19. januar 2022, utdraget det henvises til, er UGRADERT.
[504] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.

6.4.2 Sårbarhetskartleggingsverktøyet Allvis NOR

Videreutvikling og oppskalering av sårbarhetskartleggingsverktøyet Allvis NOR er ett av flere nasjonale tekniske sikkerhetstiltak i *Nasjonal strategi for digital sikkerhet* (2019). Nasjonal sikkerhetsmyndighet er ansvarlig for tiltaket. Formålet med Allvis NOR er å øke sikkerheten i offentlige virksomheter og hos eiere av kritisk infrastruktur, herunder virksomheter som er underlagt sikkerhetsloven. Allvis NOR er en samtykkebasert tjeneste som skanner etter kjente tekniske sårbarheter i systemer koblet opp mot internett. Tjenesten er gratis og tilbys til virksomheter underlagt sikkerhetsloven og virksomheter som eier eller forvalter samfunnskritisk infrastruktur eller tjenester. Tjenesten kartlegger potensielle sårbarheter som kan utnyttes av en trusselaktør. Tjenesten ble etablert i 2018 og driftes av Nasjonal sikkerhetsmyndighet. Allvis NOR driftes ikke av Nasjonalt cybersikkerhetssenter, men av en annen avdeling i Nasjonal sikkerhetsmyndighet. Det er virksomhetene som melder inn IP-adressene til Nasjonal sikkerhetsmyndighet, som de ønsker å skanne.[505]

Nasjonal sikkerhetsmyndighet har registrert følgende fordeling av virksomheter som er tilknyttet Allvis NOR:[506]

- offentlige virksomheter: 202
- private virksomheter: 35

Allvis NOR skal etter planen videreutvikles og oppskaleres slik at tjenesten kan avdekke flere sårbarheter i flere virksomheter enn den gjør i dag.[507]

Flere av virksomhetene i vår undersøkelse er tilknyttet Allvis NOR. Intervjuer med disse viser at det er en del sårbarheter i virksomhetenes systemer som ikke fanges opp av Allvis NOR:

- En av virksomhetene i dybdeundersøkelsene oppgir at de aldri har mottatt noe varsel fra Allvis NOR, selv om de har benyttet seg av tjenesten i mange år. Virksomheten har selv oppdaget flere sårbarheter som ikke ble fanget opp av Allvis NOR. Virksomheten synes dessuten det er utfordrende at Nasjonalt cybersikkerhetssenter administrerer VDI, mens en annen del av Nasjonal sikkerhetsmyndighet administrerer Allvis NOR. De opplever ikke at partene deler informasjon om sårbarheter fra de to varslingssystemene slik de burde.[508]
- En annen virksomhet oppgir at de bare har mottatt to varsler fra Allvis NOR i løpet av de siste årene. Videre viser virksomheten til at de samarbeider med et responsmiljø for håndtering av digitale sikkerhetshendelser som benytter en annen sårbarhetsskanner. Ifølge virksomheten har denne skanneren fanget opp flere sårbarheter hos virksomheten som ikke har blitt fanget opp av Allvis NOR.[509]
- En tredje virksomhet har kun blitt varslet om én sak via Allvis NOR i løpet av de årene de har vært tilknyttet skanneren.[510]
- En fjerde virksomhet opplever at de fanger opp langt flere sårbarheter selv enn dem som avdekkes gjennom Allvis NOR.[511]

6.4.3 Arbeidet med en tverssektoriell cyberreserve er forsinket

Som tiltak 44 i *Nasjonal strategi for digital sikkerhet* (2019) viser til, skal Nasjonal sikkerhetsmyndighet i perioden 2018−2019 utrede en tverrsektoriell cyberreserve for hendelseshåndtering ved spesielt store kriser som krever innsats utover ordinær bemanning. I utredningen skal de se på hvilke krav som må stilles til personell i en slik modell, og hvilke miljøer eller personer det er naturlig å benytte til

[505] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[506] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[507] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*
[508] Riksrevisjonens dybdeundersøkelser.
[509] Riksrevisjonens dybdeundersøkelser.
[510] Riksrevisjonens dybdeundersøkelser.
[511] Riksrevisjonens dybdeundersøkelser.

et slikt tiltak. Blant andre momenter som må avklares er juridiske forhold, behov for klarering av personell og øvelser og trening for å opprettholde den digitale sikkerhetskompetansen.

Nasjonal sikkerhetsmyndighet jobber med en utredning av en tverrsektoriell cyberreserve. Justis- og beredskapsdepartementet har kommet med innspill, men på grunn av koronapandemien og utbruddet av krigen i Ukraina har arbeidet tatt lengre tid enn planlagt.[512] Departementet forteller at Nasjonal sikkerhetsmyndighet nå har tatt opp igjen arbeidet, og at de venter å få tilsendt et utkast fra direktoratet innen kort tid. Justis- og beredskapsdepartementet forteller at de ikke opplever noen umiddelbare konsekvenser av forsinkelsen. De antar at hendelser har blitt håndtert slik de skal, og at forsinkelsen ikke har hatt noen innvirkning på håndteringen. Justis- og beredskapsdepartementet bemerker at det ikke er noen klar prioritering mellom tiltakene i strategien, og at departementet derfor har mulighet til å gjøre løpende vurderinger av prioriteringer.

Det foreligger ingen framdriftsplan for tiltak 44.[513] Dette skyldes ifølge Justis- og beredskapsdepartementet andre prioriteringer, blant annet som følge av pandemien. Justis- og beredskapsdepartementet vil følge opp arbeidet i Nasjonal sikkerhetsmyndighet, som er ansvarlige for tiltaket, innen kort tid.[514]

6.4.4 Rammeverk for håndtering av IKT-sikkerhetshendelser er ikke revidert og øvet

Nasjonal sikkerhetsmyndighet utga *Rammeverk for håndtering av IKT-sikkerhetshendelser* i 2017. Utviklingen av rammeverket ble gjort parallelt med planleggingen av den nasjonale øvelsen IKT16 og første versjon av rammeverket ble deretter testet ut under øvelsen i 2016.[515] Formålet med rammeverket er å 1) skape en god situasjonsoversikt ved å aggregere og koordinere informasjon om alle relevante IKT-sikkerhetshendelser, 2) effektivt håndtere alvorlige IKT-sikkerhetshendelser fra virksomhetsnivå til politisk nivå gjennom god utnyttelse av samfunnets samlede ressurser, og 3) sørge for at Norge framstår koordinert overfor andre land og internasjonale organisasjoner.[516]

Rammeverket er rettet mot Nasjonalt cybersikkerhetssenter, sektorvise responsmiljøer og virksomheter, og beskriver de ulike etatenes oppgaver og ansvarsområder ved en hendelse. Rammeverket er strukturert i samsvar med ulike faser innenfor digital hendelseshåndtering. Se faktaboks 26. Det er i tillegg utarbeidet fem vedlegg til rammeverket, herunder prinsippskisser for håndtering av to scenarioer, en mal for aktørkart på sektornivå, en begrepsliste og en taksonomi for klassifisering av IKT-sikkerhetshendelser.[517]

Faktaboks 26 Faser innen digital hendelseshåndtering

1) Planlegging og forberedelse
2) Deteksjon og vurdering av omfang og alvorlighetsgrad
3) Varsling av relevante parter
4) Iverksetting av prosesser og tiltak for å håndtere hendelsen
5) Situasjonsrapportering
6) Tilbakeføring og læring av hendelsen

Kilde: Nasjonal sikkerhetsmyndighet (2017), *Rammeverk for håndtering av IKT-hendelser* og ISO2700

[512] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022
[513] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022
[514] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022
[515] Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022
[516] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser*
[517] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser*

Nasjonal sikkerhetsmyndighet forteller at rammeverket gjelder for statlige organer, men at innholdet i rammeverket oppfattes som en implisitt forutsetning for god hendelseshåndtering også blant private virksomheter. Ifølge Nasjonal sikkerhetsmyndighet benyttes rammeverket av flere sektorvise responsmiljøer og av virksomhetene som er tilknyttet disse miljøene. Nasjonal sikkerhetsmyndighet har imidlertid ikke oversikt over den eksakte bruken av rammeverket, men viser til at flere sektorer henviser til rammeverket som standard prosedyre ved hendelseshandtering.[518]

Forsvarets forskningsinstitutt evaluerte i 2020 håndteringen av de digitale angrepene mot fylkesmannsembetene og Helse Sør-Øst. I den forbindelse anbefalte de å videreutvikle *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017). Ifølge Forsvarets forskningsinstitutt gir rammeverket et godt utgangspunkt for å få en felles forståelse av fagbegreper, roller og ansvar, men det løser ikke det de anser som de største svakhetene når det gjelder digitale sikkerhetshendelser – forebygging, forberedelser og oversikt over egne verdier, sårbarheter og systemer. Evalueringen viste også at rammeverket ikke ble benyttet i det hele tatt under håndteringen av de to hendelsene. Forsvarets forskningsinstitutt antar at dette skyldes at de tre aktørtypene som omfattes av rammeverket (Nasjonal sikkerhetsmyndighet, sektorvise responsmiljøer og virksomheter), langt fra er tilstrekkelig med tanke på større og/eller sektorovergripende digitale sikkerhetshendelser, slik angrepene på fylkesmannsembetene og Helse Sør-Øst er eksempler på. Ved større angrep vil flere aktører være involvert.[519]

Rammeverk for håndtering av IKT-sikkerhetshendelser er dynamisk og skal revideres hvert annet år eller hyppigere ved behov.[520] Rammeverket har ikke vært revidert siden 2017. I tildelingsbrevet til Nasjonal sikkerhetsmyndighet for 2021 er revisjon av rammeverket et resultatkrav, uten at dette er fullført ennå. Ifølge Justis- og beredskapsdepartementet har det imidlertid vært en allmenn oppfatning at rammeverket er dynamisk, som gjør at det revideres fortløpende når erfaringer fra hendelseshåndtering tilsier det.[521]

I arbeidet med revisjonen av rammeverket har Nasjonal sikkerhetsmyndighet bedt alle partene som omfattes av rammeverket, om å komme med innspill til endringer. I tillegg gjennomførte KPMG våren 2022 en evaluering av ordningen med sektorvise responsmiljøer. Denne rapporten vil inngå i det videre arbeidet til Justis- og beredskapsdepartementet med å oppdatere og utvikle rammeverket[522].

Under Øvelse Digital 2020 skulle man etter planen øve på å bruke *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017).[523] Øvelse Digital 2020 ble imidlertid nedskalert, og erfaringene med rammeverket ble derfor ikke innhentet slik det var tiltenkt. Nasjonal sikkerhetsmyndighet mener det hadde vært bra å få øvet rammeverket i spilløvelsen, og at en slik øvelse kunne vært en nyttig erfaring å ha med seg i arbeidet med revisjonen av rammeverket.[524] Revisjonen av rammeverket skulle etter planen være ferdig i løpet av første kvartal 2022, men Justis- og beredskapsdepartementet opplyser i intervju at arbeidet fortsatt pågår.[525]

6.4.5 Systemer for sikkerhetsgradert kommunikasjon mellom beredskapsaktører

Mulighetene til å kommunisere og utveksle sikkerhetsgradert data og informasjon er en betingelse for effektiv hendelseshåndtering i krisesituasjoner, herunder alvorlige eller omfattende digitale angrep. Handlingsplanen til *Nasjonal strategi for informasjonssikkerhet* fra 2012 hadde et tiltak om å innføre et system for høygradert datakommunikasjon mellom departementene, underliggende etater og andre

[518] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[519] Forsvarets forskningsinstitutt (2020) *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene.*
[520] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser.*
[521] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[522] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.
[523] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 21. mai 2021.
[524] Verifisert intervju med Nasjonal sikkerhetsmyndighet, 1. desember 2021.
[525] Verifisert intervju med Justis- og beredskapsdepartementet, 28. juni 2022.

sentrale beredskapsaktører.[526] Det ble ikke satt noen frist for gjennomføring av tiltaket i 2012-strategien. Lysneutvalget påpekte i 2015 at det var utfordringer knyttet til utvekslingen av sikkerhetsgradert informasjon mellom beredskapsaktører, blant annet på grunn av manglende sikkerhetsgraderte kommunikasjonssystemer.[527] Systemer for sikkerhetsgradert kommunikasjon er videreført som et tiltak i *Nasjonal strategi for digital sikkerhet* fra 2019, hvor det går fram at Forsvarsdepartementet skal utvikle og drifte et Nasjonalt BEGRENSET nett for lavgradert kommunikasjon og et Nasjonalt HEMMELIG nett for høygradert kommunikasjon. Tiltaket skulle etter planen være gjennomført i 2019. Nasjonalt BEGRENSET nett er etablert og tatt i bruk. Nasjonalt HEMMELIG nett er ikke rullet ut til beredskapsaktørene ennå.[528]

Ytterligere detaljer om av etableringen av systemer for sikkerhetsgradert kommunikasjon mellom beredskapsaktører er rapportert i sikkerhetsgradert vedlegg til denne rapporten.

[526] Justis og beredskapsdepartementet (2012) *Nasjonal strategi for informasjonssikkerhet (2012*) – *Handlingsplan.*
[527] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*, s. 262.
[528] Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.*

7 Vurderinger

Justis- og beredskapsdepartementets pådriver- og samordningsrolle innenfor digital sikkerhet innebærer blant annet å initiere og koordinere prosesser på tvers av departementer, veilede departementene i deres arbeid på området og sørge for at problemstillinger på tvers av sektorer blir håndtert. Videre skal Justis- og beredskapsdepartementet utforme regjeringens politikk for IKT-sikkerhet, herunder etablere nasjonale krav og anbefalinger på IKT-sikkerhetsområdet både for offentlige og private virksomheter.

Den siste tiden har det vært betydelige endringer i det sikkerhetspolitiske bildet, særlig etter utbruddet av krigen i Ukraina i februar 2022. Gjennom den teknologiske utviklingen får trusselaktører stadig nye verktøy og metoder. Etterretnings- og sikkerhetstjenestene melder om en økning av digitale angrep mot norske virksomheter. Økende grad av digitalisering og samarbeid på tvers av sektorer og landegrenser gjør samfunnet mer sårbart. Et digitalt angrep kan få store negative konsekvenser for Norges stats- og samfunnssikkerhet. Grunnleggende nasjonale funksjoner og kritiske samfunnsfunksjoner som blant annet kraftforsyningen, elektronisk kommunikasjon og transport kan bli rammet. Arbeidet med digital sikkerhet krever derfor samordning av aktører og virkemidler på tvers av sektorer. Justis- og beredskapsdepartementet opplever at samordningen mellom etatene innenfor området digital sikkerhet har hatt en positiv utvikling, både på departements- og etatsnivå. Departementet viser samtidig til at sektorprinsippet, varierende prioritering av sikkerhetsarbeidet i departementene og samarbeidsutfordringer mellom departementene gjør samordningen krevende.

Vår undersøkelse viser at det er flere utfordringer med samordningen av arbeidet med digital sikkerhet som ikke har blitt håndtert. Justis- og beredskapsdepartementet har ikke sørget for god nok samordning av roller, ansvar og krav i arbeidet med digital sikkerhet. Vi har også funnet mangler i departementets oversikt over den nasjonale digitale sikkerhetstilstanden, noe som særlig skyldes den langsomme implementeringen av sikkerhetsloven. Justis- og beredskapsdepartementet følger i liten grad opp effekten av tiltakene i nasjonale strategier og har siden 2016 ikke sørget for at det på nasjonalt nivå har blitt øvd godt nok på å håndtere alvorlige digitale angrep på nasjonalt nivå som treffer flere sektorer. Samlet sett kan disse svakhetene ha negative konsekvenser for den nasjonale digitale sikkerheten. Vår vurdering er at Justis- og beredskapsdepartementet ikke utnytter sitt pådriver- og samordningsansvar godt nok til å møte utfordringene på det digitale sikkerhetsområdet.

7.1 Svak samordning av roller, ansvar og krav gjør arbeidet med digital sikkerhet krevende for virksomhetene

Vi har undersøkt samordningen av aktører, regelverk og veiledning på det digitale sikkerhetsområdet. Samordningen av disse skal bidra til at etatene som har ansvar for oppfølgingen av den digitale sikkerheten, opptrer koordinert overfor brukerne, både når det gjelder rådgivning og veiledning og ved tilsyn. Det er et mål at all rådgivning og veiledning som myndighetene tilbyr brukerne, skal være harmonisert og ensrettet.[529]

7.1.1 Sentrale samordningsarenaer er lite forpliktende for deltakerne og bidrar i varierende grad til samordning

Det er etablert mange samordningsarenaer innenfor myndighetenes arbeid med digital sikkerhet. Formålet med arenaene er å øke samordningen mellom aktørene på området ved å legge til rette for at de skal kunne utveksle kunnskap og erfaringer. Vi har undersøkt de samordningsarenaene som er presentert som tiltak til *Nasjonal strategi for digital sikkerhet* (2019). Dette er *Felles*

[529] Meld. St. 5 (2020–2021) S*amfunnssikkerhet i en usikker verden*.

cyberkoordineringssenter, Forum for digital sikkerhet, *Forum for IKT-tilsyn*, *Nasjonalt cybersikkerhetssenter*, *Nettverk for nasjonal IKT-sikkerhet* og *Nettverk for veiledningsaktører innen styring og kontroll*. I tillegg trekkes *Samhandlingsarena for sektortilsyn med sikkerhetsloven* fram i *samfunnssikkerhetsmeldingen* (2020) som sentral for samordning av myndigheter med ansvar for å føre tilsyn etter sikkerhetsloven. Se Tabell 2 (på side 30) for en oversikt over deltakere i og formål for disse arenaene. Vår undersøkelse har vist at arenaene i varierende grad bidrar til samordning av aktørene.

Nasjonalt cybersikkerhetssenter har oppgaver knyttet til både forebyggende sikkerhetsarbeid og hendelseshåndtering. Når det gjelder arbeidet med forebyggende sikkerhet, oppleves *Nasjonalt cybersikkerhetssenter* i all hovedsak som en velfungerende samordningsarena av virksomhetene vi har intervjuet. *Nasjonalt cybersikkerhetssenter* arrangerer jevnlige og hyppige møter med partnerne i nettverket og disponerer lokaler som partnerne kan benytte etter ønske og behov. Vår undersøkelse viser imidlertid at det er noen utfordringer knyttet til hendelseshåndtering i *Nasjonalt cybersikkerhetssenter* og i *Felles cyberkoordineringssenter*. Disse omtales i kapittel 7.4.

De øvrige gjennomgåtte samordningsarenaene beskrives av intervjuede virksomheter i hovedsak som nyttige. Likevel viser undersøkelsen at arenaene er kjennetegnet av lav grad av forpliktelse, engasjement og systematikk i arbeidet. Det er gjennomgående lav møteaktivitet i samordningsarenaene. For eksempel har det i *Nettverk for veiledningsaktører innen styring og kontroll* kun blitt avholdt fire møter siden desember 2020. I *Forum for digital sikkerhet* har det siden Nasjonal sikkerhetsmyndighet overtok ansvaret i 2021 blitt avholdt tre møter. Den lave møteaktiviteten i de øvrige arenaene skyldes delvis konsekvensene koronapandemien fikk både med tanke på prioriteringer av ressurser og restriksjoner for fysiske møter.

Videre har sammensetningen av deltakere i arenaene, og deres engasjement og forpliktelse vært gjenstand for diskusjon. Evalueringen av *Forum for digital sikkerhet* fra 2019 viste for eksempel at det var ønskelig med flere aktører som representerer kritisk infrastruktur og kritiske samfunnsfunksjoner i forumet. Det var også ønske om at Nasjonal sikkerhetsmyndighet, Kommunal- og distriktsdepartementet og Digitaliseringsdirektoratet skulle delta i forumet. Justis- og beredskapsdepartementet gjorde på bakgrunn av evalueringen en endring i forumets sammensetning og mandat. Dette vurderes som positivt. Det vurderes også som positivt at det i *Nettverk for veiledningsaktører innen styring og kontroll* er gjort en gjennomgang av deltakerne, og at flere nye, relevante aktører har kommet inn i nettverket etter etableringen.

Også *Nettverk for nasjonal IKT-sikkerhet* ble evaluert i 2020. Både denne evalueringen og evalueringen av *Forum for digital sikkerhet* fant at deltakelsen og engasjementet i samordningsarenaene er varierende. For *Forum for digital sikkerhet* viste evalueringen også at erfaringsgrunnlaget blant deltakerne oppleves for tynt til å kunne diskutere nasjonale sikkerhetsspørsmål på strategisk nivå. Basert på evalueringen av *Nettverk for nasjonal IKT-sikkerhet* ble det besluttet å slå nettverket sammen med *Departementenes samordningsråd for samfunnssikkerhet*. Formålet er å styrke koblingen mellom det nasjonale og internasjonale perspektivet, og redusere antallet samordningsarenaer. Grunnet pandemien har ikke evalueringen per november 2022 medført noen endringer.

For å gi en indikasjon på graden av samordning i arenaene har vi som nevnt benyttet Direktoratet for forvaltning og økonomistyrings samordningsstige. Første trinn i samordningsstigen er begrenset til utveksling av informasjon, erfaringer og kunnskap, altså et lavt ambisjonsnivå for samordning. På bakgrunn av denne utvekslingen kan aktørene samarbeide om å utvikle problem- og løsningsforslag (trinn to). Trinn tre går ut på at aktørene, på bakgrunn av dialog, endrer planer eller policyer for ikke å svekke andres måloppnåelse. Det siste trinnet i stigen, der ambisjonsnivået for samordning er høyest, handler om å utvikle felles planer eller tiltak på tvers av sektorene for å oppnå synergieffekter.

Med utgangspunkt i samordningsstigen til Direktoratet for forvaltning og økonomistyring ser det ut til at samordningsgraden i arenaene vi har undersøkt, hovedsakelig samsvarer med trinn én (dele informasjon) og i noen tilfeller med trinn to (utvikle felles forståelse). Arenaene brukes i hovedsak til å opplyse og orientere hverandre om pågående arbeid. Dette er også formålet til arenaene; å dele kunnskap og erfaringer. I eksempelvis *Nettverk for nasjonal IKT-sikkerhet* og *Forum for digital sikkerhet* har man utover å utveksle erfaringer også arbeidet med *Nasjonal strategi for digital sikkerhet* (2019). Å utvikle felles planer/strategier samsvarer til et høyere nivå i samordningsstigen. Slik samordningsarenaenes mandater er utformet i dag er det ikke å forvente at deltakerne i arenaene skal drive operativt arbeid for økt samordning av det digitale sikkerhetsarbeidet. Det foregår også mye samarbeid mellom deltakerne i arenaene, utover de planlagte møtene. Vi vurderer det likevel slik at aktørene i de fire overnevnte samordningsarenaene – *Nettverk for nasjonal IKT-sikkerhet*, *Forum for digital sikkerhet, Forum for IKT-tilsyn* og *Nettverk for veiledningsaktører innen styring og kontroll* – i større grad kunne utnyttet sitt potensial for samordning av det nasjonale digitale sikkerhetsarbeidet. Arenaene kunne eksempelvis vært benyttet til å utvikle tiltak på tvers av sektorer, for eksempel for å samordne skriftlig veiledningsmateriell.

7.1.2 Det er krevende for brukere å holde oversikt over regelverk og veiledning

Det har gjennom årene har vært nedsatt flere utvalg som har undersøkt lovgivningen på det digitale sikkerhetsområdet. Omfang og overlapp i regelverk har vært trukket fram som en utfordring av flere av utvalgene.[530] Videre påpekte IKT-sikkerhetsutvalget i 2018 overlapp mellom veiledere fra ulike aktører innen arbeidet med digital sikkerhet som en utfordring.[531]

Vår undersøkelse viser at omfanget av regelverk fortsatt er stort og at flere av regelverkene og veilederne på det digitale sikkerhetsområdet overlapper tematisk. Undersøkelsen viser også at veiledningsaktører som veileder om de samme emnene i noen tilfeller bruker ulike standarder og begreper og gir ulike anbefalinger. Dette gjør det krevende for virksomhetene å forstå hvilke anbefalinger og standarder de skal bruke, og hvordan de skal etterleve regelverket. Digitaliseringsdirektoratet har forsøkt å løse noen av disse utfordringene gjennom en nettside der de har samlet en rekke veiledere til regelverk for digital sikkerhet i offentlig sektor. Nettsiden er et resultat av tiltak om sikker digitalisering i offentlig sektor i *Nasjonal strategi for digital sikkerhet* (2019). Ifølge brukere vi har intervjuet, er imidlertid ikke denne nettsiden oversiktlig nok. Fra et brukerperspektiv oppleves veiledningen fortsatt ikke som samordnet og tilgjengelig.

Når rolle- og ansvarsfordelingen mellom aktørene på det digitale sikkerhetsområdet framstår uklar og veiledningen oppleves lite tilgjengelig, er det krevende for brukerne å holde oversikt over relevant regelverk og veiledningsmateriell. Regelverket for digital sikkerhet, inkludert den nye sikkerhetsloven, har dessuten gått fra å være kravsbasert til å bli mer funksjonsbasert. Det krever mer kompetanse og kapasitet å etterleve et funksjonsbasert regelverk. Da er det desto viktigere at veiledningen oppleves god og tilgjengelig. Etter vår vurdering har ikke myndighetene lagt godt nok til rette for at virksomhetene skal kunne etterleve regelverket for digital sikkerhet på en god måte, det vil si gjennom mer tilgjengelig og samordnet veiledning.

Når det gjelder regelverk og veiledning, vurderer vi graden av samordning mellom aktørene som lav til moderat, da den stort sett begrenser seg til utveksling av informasjon, erfaring og kunnskap mellom aktørene (trinn én i samordningsstigen) og tidvis omfatter utvikling av felles forståelse (trinn to), der man for eksempel henviser til hverandres veiledere eller til de samme standardene. For å oppnå målet om samordnet veiledning burde veiledningsaktørene ideelt sett vært på trinn fire i stigen, der man sammen utvikler tiltak, strategier og materiell for å samordne veiledningen.

[530] NOU (1986:12) *Datateknikk og samfunnets sårbarhet* (Seip-utvalget); Rapport fra styrings- og arbeidsgruppene for samordning av regelverk for beskyttelse av informasjon, nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet (1991); NOU (2000: 24) *Et sårbart samfunn. Utfordringer for sikkerhets og beredskapsarbeid i samfunnet* (Willoch-utvalget); NOU (2018: 14) *IKT-sikkerhet i alle ledd.*
[531] NOU (2018: 14) *IKT-sikkerhet i alle ledd.*

Konsekvensene av at roller, ansvar og krav er svakt samordnet, er at virksomhetene finner det krevende å avklare hvilke regelverk de *omfattes* av, hvilke myndighetsaktører de skal forholde seg til, og hvilke veiledere de skal benytte i sikkerhetsarbeidet. Dette gjør at implementeringen av relevant regelverk, særlig sikkerhetsloven, er forsinket og mangelfull. I verste fall kan dette føre til at verdier ikke sikres tilstrekkelig, og dermed svekke den digitale sikkerheten i virksomhetene og samfunnet for øvrig.

7.1.3 Tilsynsmyndighetene er lite samordnet, og arbeidet med felles tilsynsmetodikk er ikke kommet i gang

Tilsyn er et sentralt virkemiddel når Justis- og beredskapsdepartementet og øvrige myndigheter skal kontrollere at regelverk implementeres og overholdes. Nasjonal sikkerhetsmyndighet har fått i oppdrag å koordinere arbeidet mellom myndigheter som fører tilsyn med den digitale sikkerheten, og skal legge til rette for hensiktsmessig samhandling mellom disse. Det er etablert to samordningsarenaer som skal bidra til bedre koordinering av tilsynene med digital sikkerhet, *Forum for IKT-tilsyn* og *Samhandlingsarena for sektortilsyn etter sikkerhetsloven*.

Samhandlingsarena for sektortilsyn etter sikkerhetsloven ble opprettet i 2019 for at aktørene som fører tilsyn etter sikkerhetsloven, skal ha en samordnet tilsynspraksis. Arenaen består av tre aktører, Nasjonal sikkerhetsmyndighet, NVE og Nasjonal kommunikasjonsmyndighet. Ifølge deltakerne fungerer samarbeidet godt. Hittil har aktørene inngått samarbeidsavtaler og avholdt møter for å sikre en enhetlig kontroll av at sikkerhetslovens bestemmelser etterleves. Nasjonal sikkerhetsmyndighet har også utarbeidet en veileder for sikkerhetsstyring, *Veileder for tilsyn med forebyggende sikkerhetsarbeid* og nettkurs til virksomheter i gjennomføring av tilsyn. NVE og Nasjonal kommunikasjonsmyndighet har ennå ikke ført tilsyn etter sikkerhetsloven i egne sektorer, og vi har derfor ikke informasjon om hvordan samordningen påvirker tilsynspraksisen.

Forum for IKT-tilsyn ble etablert i 2019 og omfatter en rekke tilsynsmyndigheter som fører tilsyn med den digitale sikkerheten i egen sektor. Formålet med forumet er å dele informasjon og utarbeide en enhetlig metode for å føre tilsyn med den digitale sikkerheten. Da forumet ble etablert, ble det ikke gjennomført en systematisk kartlegging av hvilke myndigheter som fører tilsyn med den digitale sikkerheten i de ulike sektorene, og som derfor burde være deltaker i forumet. Dette er heller ikke gjort på et senere tidspunkt. Det er videre avholdt få møter i forumet, og det er lite konkrete samordningsaktiviteter utover å informasjons- og erfaringsutveksling. Både Datatilsynet og NVE har startet arbeidet med å utvikle sine respektive tilsynsmetoder uten at det er koordinert med tilsynsmyndighetene gjennom *Forum for IKT-tilsyn*.

Det finnes også andre initiativ som skal bidra til samordning mellom tilsynsmyndighetene. Kommunal- og distriktsdepartementet arrangerer for eksempel møter om koordinering av tilsyn, mens Datatilsynet samordner kommunetilsynene med statsforvalterne gjennom felles tilsynskalendre. Nasjonal sikkerhetsmyndighet utveksler tilsynskalendre med Direktoratet for samfunnssikkerhet og beredskap, men ikke med andre tilsynsmyndigheter.

Behovet for å samordne tilsynsmetodikk og tilsyn med digital sikkerhet ble påpekt allerede i 2005 av Koordineringsutvalget for informasjonssikkerhet. Det pågår noe samhandling mellom tilsynsmyndighetene, men arbeidet i *Samarbeidsarena for sektortilsyn etter sikkerhetsloven* har etter vår vurdering kommet sent i gang og virker for lite målrettet. Tilsynene har startet informasjonsutveksling, men det er ikke satt i gang konkrete aktiviteter for å oppnå en enhetlig tilsynspraksis.

Justis- og beredskapsdepartementet har ikke evaluert *Forum for IKT-tilsyn* eller innretningen av tilsyn med den digitale sikkerheten på tvers av tilsynsmyndighetene. Departementet har dermed ikke

informasjon om hvordan tilsynspraksisen er. Vår vurdering er at departementet mangler informasjon som kunne ha bidratt til bedre samordning av tilsynene og dermed til en mer effektiv tilsynsvirksomhet.

Arbeidet med å etablere rutiner for samordning av tilsynene har ikke kommet i gang, verken når det gjelder utvikling av metodikk eller planer for gjennomføring av tilsyn. Vi vurderer graden av samordning av tilsyn med den digitale sikkerheten som lav (tilsvarende trinn én i Direktoratet for forvaltning og økonomistyrings samordningsstige), da aktørene kun i begrensede tilfeller deler informasjon, erfaringer og kunnskap. Mangelen på samordning kan føre til at tilsynsmyndighetene har ulik oppfatning av hva som er godt nok for å etterleve samme type krav, for eksempel hvordan virksomhetene skal gjennomføre risikoanalyser og iverksette tiltak. Dette kan føre til ulik etterlevelse av regelverkskravene og dermed til ulik grad av digital sikkerhet mellom sektorene.

7.2 Det er mangler i Justis- og beredskapsdepartementets oversikt over den nasjonale digitale sikkerhetstilstanden

Justis- og beredskapsdepartementet benytter en rekke kilder for å holde oversikt over den nasjonale digitale sikkerhetstilstanden, blant annet sikkerhets- og tilsynsrapporteringer fra Nasjonal sikkerhetsmyndighet og status- og tilstandsvurderinger fra departementene med ansvar for kritiske samfunnsfunksjoner. Departementet viser til at de mener at de har tilstrekkelig oversikt til å identifisere behov på nasjonalt nivå og til å sette retning og prioritere tversektorielle tiltak. Denne undersøkelsen viser imidlertid at det er flere utfordringer med kildene departementet benytter, og at det er mangler i Justis- og beredskapsdepartementets informasjonsgrunnlag.

7.2.1 Justis- og beredskapsdepartementet har ikke fullstendig oversikt over hvilke verdier som skal sikres

Sikkerhetsloven trådte i kraft 1. januar 2019. Justis- og beredskapsdepartementet utarbeidet da en milepælsplan for implementering av loven, som blant annet innebærer å identifisere grunnleggende nasjonale funksjoner og virksomhetene, systemene og infrastrukturen som disse funksjonene er avhengige av for å fungere. I henhold til milepælsplanen skulle alle departementene ha identifisert grunnleggende nasjonale funksjoner innenfor sitt ansvarsområde i løpet av august 2020, men dette arbeidet ble først fullført høsten 2021.

Fordi identifiseringen av grunnleggende nasjonale funksjoner er en forutsetning for det videre arbeidet med å implementere sikkerhetsloven, har også arbeidet med kartlegge avhengigheter blitt forsinket. I henhold til milepælsplanen skulle arbeidet med kartlegging avhengigheter være ferdig i juli 2021. Departementene arbeider fortsatt med å kartlegge hvilke andre virksomheter de grunnleggende nasjonale funksjonene er avhengige av for å fungere som de skal, slik at også disse virksomhetene iverksetter tiltak i henhold til krav i sikkerhetsloven. Myndighetene har ikke oversikt over alle avhengigheter mellom de grunnleggende nasjonale funksjonene. På grunn av den manglende oversikten er det fare for at virksomheter, systemer eller infrastruktur som de grunnleggende nasjonale funksjonene er avhengige av, ikke er tilstrekkelig sikret. Dette øker risikoen for at grunnleggende nasjonale funksjoner kan settes ut av funksjon ved digitale angrep på infrastruktur og systemer lenger ut i verdikjeden.

Både Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at arbeidet som følger av sikkerhetsloven går sakte. Manglende kapasitet og sikkerhetskompetanse i departementer og virksomheter som omfattes av sikkerhetsloven trekkes fram som en medvirkende årsak. Ifølge Justis- og beredskapsdepartementet kan dette kan medføre at viktige verdier ikke er tilstrekkelig sikret.

Det har lenge vært klart at arbeidet som følger av ny sikkerhetslov er kraftig forsinket, men Justis- og beredskapsdepartementet har likevel ikke satt nye frister for gjennomføringen av arbeidet. Riksrevisjonen ser at det er begrensninger for Justis- og beredskapsdepartementets samordningsrolle på samfunnssikkerhetsområdet. Det enkelte departement har ansvar for samfunnssikkerhet i egen sektor. Samtidig må det være slik at når fremdriften i departementenes implementeringen av sikkerhetsloven går tregt, så må Justis- og beredskapsdepartementet følge dette tydelig opp. Riksrevisjonen vil her peke på de alvorlige konsekvensene manglende implementering av sikkerhetsloven kan ha for nasjonal sikkerhet. Etter vår vurdering har Justis- og beredskapsdepartementet i liten grad brukt pådriver- og samordningsrollen til å få fart på dette arbeidet.

7.2.2 Justis- og beredskapsdepartementet har ikke sørget for at sentral rapportering fra departementene kan brukes for å holde oversikt over sikkerhetstilstanden

En samfunnsfunksjon defineres som kritisk hvis bortfall av den får konsekvenser som truer befolkningens og samfunnets grunnleggende behov, herunder ivaretakelse av grunnleggende samfunnsverdier som liv og helse, natur og miljø, økonomi, samfunnsstabilitet, styringsevne og kontroll. Det er identifisert 16 kritiske samfunnsfunksjoner. Departementene med hovedansvar for disse gjennomførte status- og tilstandsvurderinger for funksjonene i perioden 2017−2021. Disse vurderingene var imidlertid av varierende omfang og kvalitet, og de ble gjennomført på ulike måter. Dette gir etter vår vurdering ikke et godt utgangspunkt for å trekke noen overordnede konklusjoner om den digitale sikkerhetstilstanden i de samfunnskritiske funksjonene. Justis- og beredskapsdepartementet har ennå ikke kommet fram til en ny, enhetlig måte å gjennomføre status- og tilstandsvurderinger på som gjør vurderingene mer egnet til å holde en samlet og oppdatert oversikt over tilstanden i samfunnets kritiske funksjoner.

I henhold til samfunnssikkerhetsinstruksen skal alle departementene gjennomføre risiko- og sårbarhetsanalyser for samfunnskritiske funksjoner innenfor deres ansvarsområde. Analysene skal omfatte risiko knyttet til digital sikkerhet. Justis- og beredskapsdepartementet opplyser at de ikke bruker informasjonen fra departementenes risiko- og sårbarhetsanalyser til å holde oversikt over den digitale sikkerhetstilstanden. Årsaken til dette er ifølge departementet at analysene er gjort på så ulike måter at en sammenstilling ville være for ressurskrevende sammenlignet med hva de mener de kunne ha fått ut av det. Gjennom Justis- og beredskapsdepartementets samordningsansvar for samfunnssikkerhet, herunder digital sikkerhet, kan de gi føringer for hvordan departementene skal gjennomføre risiko- og sårbarhetsanalyser. Departementet har ikke gjort dette, og de har dermed ikke lagt til rette for at analysene kan gjennomføres og utformes på en måte som gjør at analysene kan sammenstilles på et overordnet nivå. Vi mener at risiko- og sårbarhetsanalysene kunne ha vært en nyttig kilde til informasjon om risikoen på det digitale sikkerhetsområdet i hver enkelt sektor, noe Justis- og beredskapsdepartementet i dag mangler.

Samlet sett medfører svakhetene som er påpekt i kildene Justis- og beredskapsdepartementet bruker, at det er mangler i bildet av den digitale sikkerhetstilstanden. Justis- og beredskapsdepartementet har ikke lagt til rette for at arbeidet med risiko- og sårbarhetsanalyser og status- og tilstandsvurderinger blir gjennomført på en enhetlig måte. Etter vår vurdering ville en enhetlig gjennomføring muliggjort en sammenstilling av analysene, som kunne gitt departementet viktig informasjon om den nasjonale digitale sikkerhetstilstanden.

7.2.3 Det gjennomføres få tilsyn med digital sikkerheten

Tilsyn er et sentralt virkemiddel når Justis- og beredskapsdepartementets og øvrige myndigheter skal kontrollere at regelverk implementeres og overholdes. Tilsyn skal bidra til å forbedre arbeidet med digital sikkerhet i virksomhetene, og for myndighetene er tilsynsrapporter en viktig kilde til å få innsikt i statusen for arbeidet på et område, i en sektor eller i samfunnet som helhet. Mangelfull

tilsynsvirksomhet kan derfor føre til at den digitale sikkerheten får mindre oppmerksomhet i virksomheter og departementer, noe som igjen kan svekke den digitale sikkerheten i samfunnet.

Arbeid med digital sikkerhet er regulert gjennom en rekke lover og regler, berører de fleste virksomheter og kontrolleres av flere ulike tilsynsmyndigheter. Likevel finner vi at det gjennomføres forholdvis få tilsyn hvor digital sikkerhet er tema.

Det er et stort antall tilsynsobjekter som omfattes av de generelle regelverkene, som sikkerhetsloven og personvernregelverket. Nasjonal sikkerhetsmyndighet har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller pliktene de har etter sikkerhetsloven. Nasjonal sikkerhetsmyndighet påpeker i Kontrollmeldingen for 2019 at antall tilsyn per år er begrenset sett opp mot antall tilsynsobjekter. Som følge av koronapandemien ble det gjennomført relativt få tilsyn i 2020 og 2021, men antallet tilsyn økte i 2022 og antas av sikkerhetsmyndigheten å øke videre framover. For å tilpasse tilsynene bedre etter sektor og øke antall tilsyn etter sikkerhetsloven ble Nasjonal kommunikasjonsmyndighet og NVE i 2019 utpekt som sektortilsyn. Verken Nasjonal kommunikasjonsmyndighet eller NVE har imidlertid kommet i gang med slike tilsyn. Datatilsynet gjennomfører tilsyn etter personvernregelverket. I 2021 planla Datatilsynet å gjennomføre 14 egeninitierte tilsyn, men bare 5 ble startet opp, og kun 3 ble gjennomført.

Tilsynene som gjennomføres av ovennevnte tilsynsmyndigheter, er i stor grad dokumenttilsyn av styringssystemene som danner grunnlaget for det digitale sikkerhetsarbeidet. Disse tilsynene omfatter i liten grad undersøkelser av hvordan styringssystemene etterleves i praksis og omfatter ikke vurderinger av den tekniske sikkerhetstilstanden i virksomhetene.

Samfunnssikkerhetsinstruksen og sivilbeskyttelsesloven stiller krav til henholdsvis departementenes og kommunenes samfunnssikkerhetsarbeid. Digital sikkerhet er en integrert del av samfunns-sikkerhetsarbeidet og inngår i regelverkenes virkeområde. Justis- og beredskapsdepartementet har ansvar for at det gjennomføres tilsyn med den digitale sikkerheten. Direktoratet for samfunnssikkerhet og beredskap fører tilsyn med departementene, mens statsforvalterne fører tilsyn med kommunene. Tema i tilsynene skal velges ut fra en risiko- og vesentlighetsvurdering. I Helse- og omsorgsdepartementets rapport om Justis- og beredskapsdepartements gjennomføring av tilsyn på området fra 2013 går det fram at tilsynene i større grad framstår som brede gjennomganger enn som tilsyn som er spisset mot risiko og vesentlighet. Vår gjennomgang viser at tilsynene fortsatt omfatter departementenes og kommunenes samfunnssikkerhetsarbeid generelt, og at arbeidet med digital sikkerhet ikke er valgt ut som tema i tilsynene. Rapportene fra disse tilsynene gir dermed ikke informasjon om statusen for arbeidet med digital sikkerhet i departementene og kommunene til tross for at trusler i det digitale rom gjennom en årrekke har vært framhevet blant annet i Nasjonal sikkerhetsmyndighets publikasjoner.

7.3 Justis- og beredskapsdepartementet utnytter ikke potensialet i nasjonale strategier for digital sikkerhet godt nok

Som en del av pådriver- og samordningsrollen på samfunnssikkerhetsområdet har Justis- og beredskapsdepartementet ansvar for å utarbeide nasjonale strategier for arbeidet med digital sikkerhet.

I 2019 utarbeidet Justis- og beredskapsdepartementet i samarbeid med Forsvarsdepartementet og Kunnskapsdepartementet *Nasjonal strategi for digital sikkerhet* og *Nasjonal strategi for digital sikkerhetskompetanse*. Dette var fjerde gang det ble gitt ut en nasjonal strategi for digital sikkerhet (de tidligere strategiene ble gitt ut i 2003, 2007 og 2012), og første gang det ble gitt ut en egen delstrategi for digital sikkerhetskompetanse. I *samfunnssikkerhetsmeldingen* (2020) trekkes strategien fram som et sentralt virkemiddel i myndighetenes arbeid med digital sikkerhet. Etter vår vurdering utnytter

imidlertid ikke Justis- og beredskapsdepartementet potensialet som ligger i dette virkemiddelet godt nok i samordningen av arbeidet med den digitale sikkerheten nasjonalt.

7.3.1 Justis- og beredskapsdepartementet har ikke sørget for god nok informasjon om virkningen av nasjonale strategier og tilhørende tiltak

Justis- og beredskapsdepartementet viser til at en systematisk og kunnskapsbasert tilnærming ligger til grunn for utarbeidelsen av *Nasjonal strategi for digital sikkerhet* (2019). Etter at Justis- og beredskapsdepartementet overtok ansvaret for digital sikkerhet i 2013 er det utarbeidet flere utredninger og styrende dokumenter. Blant annet har det vært nedsatt to nasjonale utvalg for å utrede særskilte forhold knyttet til nasjonal digital sikkerhet. I 2017 kom også den første stortingsmeldingen som utelukkende omhandler digital sikkerhet. Riksrevisjonen vurderer dette arbeidet som positivt. Justis- og beredskapsdepartementet viser også til at det i forkant av utgivelsen av *Nasjonal strategi for digital sikkerhet* (2019) ble gjennomført en omfattende prosess for å få innspill til strategien fra et så bredt utvalg av aktører som mulig.

En gjennomgang av de tidligere strategiene viser at flere av de identifiserte utfordringene på det digitale området har vært vedvarende over tid. Her kan nevnes blant annet mangel på digital sikkerhetskompetanse, behov for økt evne til å avdekke og håndtere digitale angrep, og bedre styring av den digitale sikkerheten i offentlig sektor. De prioriterte satsningsområdene i *Nasjonal strategi for digital sikkerhet* fra 2019 er i stor grad de samme som i 2012-strategien, og flere av tiltakene er videreført fra 2012 til 2019. Justis- og beredskapsdepartementet bemerker at grunnen til at mange av utfordringene strategiene er ment å løse, som å for eksempel styrke den digitale sikkerhetskompetansen, vedvarer over tid er stor utvikling på det digitale sikkerhetsområdet. I 2019-strategien legges imidlertid mer vekt på sivilt-militært og offentlig-privat samarbeid, og virksomheters egenbeskyttelse mot digital trusler og angrep enn det er gjort i tidligere strategier.

Våren 2021 gjennomførte Justis- og beredskapsdepartementet en statusoppdatering på *Nasjonal strategi for digital sikkerhet* (2019) og i den forbindelse innhentet de rapportering om status for strategien fra departementene. I en oppsummering av disse rapportene påpeker Justis- og beredskapsdepartementet at kvaliteten på rapporteringen varierer, og at den sier lite om hvilken effekt tiltakene i strategien har hatt på den digitale sikkerheten i underliggende virksomheter. Justis- og beredskapsdepartementet har likevel ikke etterspurt informasjon som kan bidra til å utdype dette. Til tross for at departementet påpekte de samme utfordringene når det gjaldt statusrapporteringen på strategien fra 2012, har ikke rapporteringsmetoden blitt endret for å møte disse utfordringene. Etter vår vurdering har ikke departementet sørget for å få god nok informasjon om virkningen av tiltakene i strategien. Siden departementet har en samordningsrolle, mener vi at slik informasjon er viktig, både fordi den gjør det mulig å vurdere effekten av tiltakene, og fordi den kan danne grunnlag for å oppdatere tiltaksoversikten med nye tiltak eller endringer i pågående tiltak.

7.3.2 Justis- og beredskapsdepartementet har ikke en samlet og oppdatert oversikt over tiltak for å ivareta den digitale sikkerheten

Nasjonal strategi for digital sikkerhet (2019) er ledsaget av en oversikt over tiltak som skal understøtte strategiens mål. Selv om det ikke kommer tydelig fram i strategidokumentet, var tiltakene som beskrives i oversikten, i hovedsak allerede planlagt og finansiert av de enkelte departementene før strategien ble utarbeidet. Enkelte tiltak ble imidlertid planlagt og finansiert parallelt med strategiprosessen. Justis- og beredskapsdepartementet forklarer at dette er vanlig praksis i forvaltningen, og at det skyldes at departementene ikke har mulighet til å lage tiltaksplaner som krever framtidige investeringer som det ikke er vedtatt midler til. Tiltaksplanen beskrives derfor som et øyeblikksbilde av hva som var besluttet på tidspunktet da strategien ble utgitt.

Tiltaksoversikten skal revideres ved behov, men ifølge Justis- og beredskapsdepartementet vil ikke oversikten bli oppdatert med nye tiltak eller endringer i eksisterende tiltak til tross for at det er identifisert behov for nye tiltak knyttet til både hovedstrategien og delstrategien om kompetanse. Departementet opplyser at nye tiltak vil bli presentert på annen måte, for eksempel gjennom stortingsmeldinger. Våren 2022 ble det i forbindelse med krigen i Ukraina vedtatt å bevilge midler til å styrke flere av tiltakene i strategien, blant annet Nasjonal sikkerhetsmyndighets kapasitet til hendelseshåndtering og videreutvikling av tekniske systemer for å avdekke digitale angrep. Dette er sentrale tiltak i strategien, og tiltaksoversikten kunne ha vært oppdatert med disse endringene.

I tiltaksoversikten står det at tiltakene skal understøtte målene i strategien, men det går ikke fram i hvilken grad tiltakene er tilstrekkelige til å nå målene i strategien, eller om det er deler av strategien hvor det ikke er planlagt eller iverksatt tilstrekkelige tiltak. Etter vår vurdering burde det ha vært gjort en vurdering av hvordan tiltakene understøtter målene i strategien. Det burde også ha gått klart fram om det er områder i strategien hvor det mangler tiltak.

Justis- og beredskapsdepartementet har ikke oppdatert tiltaksoversikten med nye tiltak eller endringer i pågående tiltak. Dette ville gitt myndighetsaktørene en bedre samlet oversikt over sentrale tiltak som er iverksatt for å ivareta og styrke den nasjonale digitale sikkerheten

7.3.3 Satsingen på kompetanse er mindre målrettet enn *Nasjonal strategi for digital sikkerhet* tilsier

Behovet for økt digital sikkerhetskompetanse er trukket fram som en av de største utfordringene på det digital sikkerhetsområdet. Å styrke den digitale sikkerhetskompetansen i samfunnet er derfor et overordnet mål i *Nasjonal strategi for digital sikkerhet* (2019). Kompetansemålene utdypes i en egen delstrategi − *Nasjonal strategi for digital sikkerhetskompetanse* – fra samme år. Justis- og beredskapsdepartementet bemerker at dette ble gjort for å løfte fram et særlig behov og vie kompetanseområdet ekstra oppmerksomhet. Siden de fleste av tiltakene i kompetansestrategien er rettet mot forsknings- og utdanningsinstitusjoner, er det Kunnskapsdepartementet som har hovedansvaret for oppfølgingen og gjennomføringen av disse.

I tiltaksoversikten til *Nasjonal strategi for digital sikkerhet* (2019) vises det til prioriteringer på kompetanseområdet på over 800 millioner kroner. Også i *samfunnssikkerhetsmeldingen* (2020) vises det til at 800 millioner kroner er satt av til å styrke den digitale sikkerhetskompetansen. Vår undersøkelse viser imidlertid at flere av tiltakene i strategien er ikke rettet direkte mot å øke den digitale sikkerhetskompetansen dette omfatter tiltak for å øke den digitale kompetansen i samfunnet generelt, og ikke den digitale sikkerhetskompetansen spesielt. Satsingen på digital sikkerhetskompetanse er dermed mindre målrettet enn det som opprinnelig ble beskrevet i strategidokumentet.

Dette gjelder blant annet Forskningsrådets to programmer IKTPLUSS og SAMRISK, som trekkes fram som sentrale for å øke den digitale sikkerhetskompetansen i samfunnet. Av de totale bevilgningene til de to programmene gikk i perioden 2018–2021 kun en mindre prosentandel til prosjekter under temaet digital sikkerhet. Et annet eksempel er Kompetanseprogrammet, som er en del av kompetansereformen (St. Meld. 14 (2019−2020)). Programmet presenteres i kompetansestrategien som et av de meste sentrale tiltakene knyttet til satsingsområdet *Etter- og videreutdanningstilbud innenfor IKT og digital sikkerhet*. Til tross for at det er bevilget store beløp til kompetanseprogrammet, kan ikke Kunnskapsdepartementet slå fast at tiltaket vil bidra til å øke den digitale sikkerhetskompetansen.

7.3.4 Løpende oppfølging av tiltak i kompetansestrategien hadde gjort det mulig å identifisere behov for nye tiltak

Nasjonal strategi for digital sikkerhetskompetanse har per august 2022 ikke blitt evaluert i sin helhet. Justis- og beredskapsdepartementet og Kunnskapsdepartementet begrunner dette med at tiltakene i kompetansestrategien er av langsiktig karakter, og at det fortsatt er for tidlig å stadfeste den fulle effekten av tiltakene. Også Direktoratet for høyere utdanning og kompetanse konkluderte i en rapport fra 2021, der tiltak som skal bidra til å øke den digitale kompetansen vurderes, med at det er for tidlig å vurdere effekten av de iverksatte tiltakene.[532]

I henhold til tiltak i kompetansestrategien skal de to ansvarlige departementene sørge for oppdaterte tall og statistikk for å følge med på forholdet mellom samfunnets tilgang til og behov for digital sikkerhetskompetanse. NIFU-rapporten[533], som utgjør kunnskapsgrunnlaget for strategien på kompetanseområdet, ble utgitt i 2017. Etter dette har det ikke blitt innhentet oppdaterte data og analyser om kompetansegapet på det digitale sikkerhetsområdet. Sentrale aktører på det digitale sikkerhetsområdet har beskrevet kunnskapsgrunnlaget for kompetansestrategien som utdatert.

Videre er det identifisert risiko for at enkelte tiltak ikke møter målene i kompetansestrategien. Dette gjelder for eksempel rekruttering til utdanning og forskning innen digital sikkerhet. Både Justis- og beredskapsdepartementet og Kunnskapsdepartementet er kjent med denne risikoen. Til tross for dette har det ikke blitt innhentet tilstrekkelig informasjon for å løpende kunne vurdere effekten av tiltak i kompetansestrategien der dette hadde vært mulig. Denne informasjonen ville ha vært et viktig grunnlag for å justere og iverksette nye tiltak på et område der mangelen på kompetanse har eksistert og vært økende over lang tid.

7.4 Justis- og beredskapsdepartementet har ikke lagt godt nok til rette for tverssektoriell hendelseshåndtering

Som en del av samordningsrollen på samfunnssikkerhetsområdet har Justis- og beredskapsdepartementet også ansvar for å gjennomføre nasjonale øvelser og sørge for at problemstillinger på tvers av flere sektorer blir håndtert. Sentrale tiltak for å møte slike problemstillinger omfatter blant annet felles rammeverk for digital hendelseshåndtering og tekniske systemer for varsling av uønsket aktivitet og kommunikasjon mellom beredskapsaktører.

7.4.1 Det er svakheter ved Nasjonal sikkerhetsmyndighets evne til å oppdage og håndtere digitale hendelser

Nasjonal sikkerhetsmyndighet skal i henhold til sikkerhetsloven drifte en nasjonal responsfunksjon som skal oppdage digitale trusler og bistå virksomheter med å håndtere digitale angrep. I 2019 ble Nasjonalt cybersikkerhetssenter opprettet for å ivareta denne funksjonen. Nasjonalt cybersikkerhetssenter bruker Varslingssystem for digital infrastruktur (VDI) for å avdekke sårbarheter og digitale trusler mot norske virksomheter.

Våre dybdeundersøkelser viser at de intervjuede virksomhetene gjennomgående har vært fornøyde med bistanden de har fått fra Nasjonalt cybersikkerhetssenter ved håndtering av digitale hendelser. Alle disse virksomhetene understøtter en grunnleggende nasjonal funksjon, og er tildelt en fast kontaktperson i Nasjonalt cybersikkerhetssenter. Ikke alle virksomheter har en fast kontaktperson, og intervjuede representanter fra kommunesektoren bemerket at noen kommuner opplever det som

[532] Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av tiltak*. Rapport nr. 03/2021.
[533] Mark, Michael Spjelkavik, Cathrine Tømte, Terje Næss og Trude Røsdal (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud*. NIFU-rapport 2017: 32.

vanskelig å komme i kontakt med og få bistand fra Nasjonalt cybersikkerhetssenter både ved digitale hendelser og ved normaltilstand.

Vår undersøkelse har avdekket utfordringer med Nasjonal sikkerhetsmyndighets tekniske systemer VDI og Allvis NOR. Både Nasjonal sikkerhetsmyndighet og Nasjonalt cybersikkerhetssenter bruker disse til å overvåke uønsket aktivitet og kartlegge sårbarheter. VDI-nettverket dekker ikke alle relevante virksomheter og har flere utfordringer med å fange opp relevant datatrafikk, for eksempel datatrafikk til skybaserte tjenesteløsninger. Utfordringene knyttet til VDI utdypes i sikkerhetsgradert vedlegg til rapporten.

Det har også kommet fram gjennom vår undersøkelse at Allvis NOR har begrenset evne til å fange opp sårbarheter. Dette fører til at virksomheter kan være utsatt for digitale trusler eller angrep og ha sårbarheter i systemene som ikke fanges opp av verktøyet.

Det har siden 2012 pågått et stort prosjekt som skal oppgradere funksjonaliteten og øke omfanget av VDI. Prosjektet skal ferdigstilles i 2023. Som en konsekvens av krigen i Ukraina ble det våren 2022 bevilget ekstra midler for å øke analysekapasiteten i Nasjonalt cybersikkerhetssenter, forbedre dekningen av VDI-sensorer og anskaffe teknisk utstyr som skal styrke evnen til å håndtere graderte signaturer. Tiltakene i utviklingsprosjektet og de ekstra bevilgingene løser bare delvis de utfordringene som VDI har med å oppdage digitale angrep. For eksempel er det fortsatt ikke utviklet en løsning for å overvåke datatrafikk i skybaserte løsninger som virksomhetene benytter. Justis- og beredskapsdepartementet bemerker imidlertid at det er både tekniske og regulatoriske utfordringer ved å få på plass en slik løsning. Vi vurderer det som positivt at det er satt i gang tiltak for å videreutvikle de tekniske verktøyene VDI og Allvis NOR, men vil samtidig påpeke at det er risiko for at tiltakene ikke løser alle kjente utfordringer med systemene.

Flere utfordringer med VDI og konsekvensene av disse utdypes i sikkerhetsgradert vedlegg til denne rapporten.

7.4.2 Formålet med etableringen av Felles cyberkoordineringssenter er ikke fullstendig oppnådd, og vedvarende utfordringer er ikke håndtert

På oppdrag fra Justis- og beredskapsdepartementet og Forsvarsdepartementet ble Felles cyberkoordineringssenter etablert i 2017. Felles cyberkoordineringssenter er et permanent, samlokalisert fagmiljø med representanter fra Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos. Det er Nasjonal sikkerhetsmyndighet som er gitt ansvaret for å lede senterets arbeid. Utfordringer knyttet til senterets arbeid beskrives mer inngående i et sikkerhetsgradert vedlegg til denne rapporten.

Formålet med Felles cyberkoordineringssenter er å 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 rom. I henhold til *Retningslinjer for cybersamarbeid* (2022) skal dette oppnås gjennom senterets åtte hovedoppgaver. Partene i senteret har i hovedsak prioritert fire av hovedoppgavene. Videre er det gjennom denne undersøkelsen blant annet identifisert utfordringer knyttet til ressurssituasjon og bemanning i Felles cyberkoordineringssenter. Vedvarende utfordringer som partene selv ikke har evnet å utbedre har ikke blitt rapportert til Justis- og beredskapsdepartementet.

Utfordringene som er identifisert gjennom undersøkelse framkom også i partenes egen evaluering av Felles cyberkoordineringssenter i 2019. Partene utarbeidet da en handlingsplan for å imøtekomme de identifiserte utfordringene, men flere av disse vedvarer. En evalueringsrapport ble oversendt til Justis- og beredskapsdepartementet og Forsvarsdepartementet i etterkant av evalueringen. Rapporten inneholdt imidlertid ingen informasjon om hverken utfordringer knyttet til arbeidet eller tiltak for å

imøtekomme utfordringene. Justis- og beredskapsdepartementet opplyser at de etterspurte mer informasjon om resultatene av evalueringen, men at enkelte av partene ikke ønsket å dele dette med departementet. Justis- og beredskapsdepartementet fulgte ikke dette opp videre.

Justis- og beredskapsdepartementet har ikke gjennom etatsstyringen blitt gjort kjent med senterets utfordringer. Justis- og beredskapsdepartementet viser til at det er partene selv som er ansvarlige for ressurssetting av senteret. Videre viser departementet til at Nasjonal sikkerhetsmyndighet er gitt en lederfunksjon for Felles cyberkoordineringssenter. Departementet mener det følger av denne funksjonen blant annet å sørge for at senteret har gode rutiner for hendelseshåndtering.

Det er vår vurdering at de identifiserte utfordringene begrenser måloppnåelsen med etableringen av Felles cyber koordineringssenter. Videre mener vi Justis- og beredskapsdepartementet skulle ha gjort mer for å sikre seg relevant informasjon om måloppnåelsen i Felles cyberkoordineringssenter. En mer aktiv styring fra departementets side kunne ha bidratt til å løse utfordringene tidligere, og dermed gitt en bedre måloppnåelse for Felles cyberkoordineringssenter.

7.4.3 Det er behov for mer øving av tverrsektoriell håndtering av hendelser på nasjonalt nivå

Justis- og beredskapsdepartementet skal som en del av samordningsansvaret planlegge, gjennomføre og evaluere nasjonale øvelser i sivil sektor. Formålet med øvelser er å sørge for at aktører som kan bli involvert i hendelseshåndtering, vet hva de skal gjøre og hvem de skal samhandle med dersom det oppstår en reell hendelse. Det er også viktig å gjennomføre øvelser for å avdekke om det er noe i planverket eller i aktørenes rolle- og ansvarsforståelse, kompetanse eller kapasitet som ikke fungerer godt nok.

Høsten 2020 skulle Øvelse Digital 2020 avholdes, men på grunn av koronarestriksjoner ble øvelsen gjennomført i sterkt redusert omfang, både med tanke på hvilke aktører som deltok, scenarioet i øvelsen og øvelsens varighet. Spesielt nedskaleringen av spilløvelsen, en av øvelsens tre deler, fikk stor betydning fordi dette medførte at tverrsektoriell hendelseshåndtering på nasjonalt nivå i ikke ble øvet. Erfaringene fra spilløvelsen skulle også brukes i revisjonen av *Rammeverk for håndtering av IKT-sikkerhetshendelser* (2017).

Direktorat for samfunnssikkerhet- og beredskap konkluderer i evalueringen av Øvelse Digital 2020 med at øvingsprosjektet som helhet har møtte hensikten med øvelsen. Dette til tross for at ikke alle øvingsmålene ble innfridd. Direktoratet viser imidlertid til at det fortsatt er behov for bedre oversikt over aktørbildet innenfor det digitale sikkerhetsområdet, økt samhandling på tvers av sektorer og mer koordinert kommunikasjonshåndtering. Direktoratet ser også behov for flere og hyppigere øvelser innen digital sikkerhet. Også Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet har uttalt at det var uheldig av øvelsen ble nedskalert og at viktige elementer ikke ble øvet.

Justis- og beredskapsdepartementet opplyser i intervju at det ikke er planlagt å gjennomføre en ny spilløvelse som erstatning for Øvelse Digital 2020. Departementet viser til at det øves på digitale hendelser internt i de sektorene, og at Norge deltar i en rekke internasjonale øvelser på det digitale området. De sentrale hendelseshåndteringsmiljøene, som Nasjonalt cybersikkerhetssenter og Felles cyberkoordineringssenter, håndterer dessuten jevnlig reelle hendelser, og har gjennom det fått god erfaring med digital hendelseshåndtering. Videre bemerker departementet at det generiske systemet for sentral krisehåndtering øves ofte, selv om disse øvelsene ikke alltid er knyttet spesifikt til digital sikkerhet.

Det er positivt at Norge deltar i internasjonale øvelser, og at det øves på krisehåndtering på strategisk nivå. Slike øvelser øver imidlertid ikke digital hendelseshåndtering på tvers av sektorer i Norge, og det er derfor uheldig at Øvelse digital 2020 ikke ble gjennomført i fullskala. Fra vår undersøkelse

framkommer også at ved gjennomføring av sektorinterne øvelser blir ofte scenarioer som omhandler digital sikkerhet nedprioritert. Dette gjelder særlig i kommunene. Til tross for at departementet uttaler at det gjennomføres en rekke sektorinterne øvelser har ikke departementet en oversikt over dette. Det er derfor usikkerhet knyttet til hvor mye det faktisk øves på dette området.

7.4.4 Viktige tverrsektorielle tiltak for å håndtere digitale angrep er forsinket

I 2012 ble det bestemt at alle sektorer skulle etablere egne sektorvise responsmiljøer som skal bistå virksomhetene i sektoren ved digitale angrep. Det ble ikke lagt føringer for hvordan disse responsmiljøene skulle organiseres eller finansieres, og resultatet er at det er stor variasjon i responsmiljøenes struktur og virkemåte. Det er heller ikke alle sektorer som har fått på plass et eget responsmiljø. De sektorvise responsmiljøene skal blant annet fungere som bindeledd mellom Nasjonalt cybersikkerhetssenter og virksomhetene i sektoren. Vår undersøkelse viser imidlertid at responsmiljøene i enkelte sektorer bidrar til forsinkelser i håndtering og informasjonsflyt, og at virksomhetene foretrekker å ha direkte kontakt med Nasjonalt cybersikkerhetssenter framfor å gå via det sektorvise responsmiljøet. En evaluering av ordningen med sektorvise responsmiljøer som ble gjennomført av KPMG i 2022, viser også til flere utfordringer med ordningen, blant annet uklar ansvars- og rolleforståelse og mangel på tilgang til relevant kompetanse. Vi ser det som positivt at Justis- og beredskapsdepartementet våren 2022 satte i gang en prosess for å evaluere og forbedre ordningen med sektorvise responsmiljøer.

Rammeverk for håndtering av IKT-sikkerhetshendelser (2017) skal bidra til å skape god situasjonsoversikt og er et viktig verktøy som angir roller, ansvar og oppgaver ved håndtering av digitale angrep. Videre skal det bidra til at informasjon om alle relevante IKT-sikkerhetshendelser koordineres, og til at alvorlige IKT-sikkerhetshendelser – fra virksomhetsnivå til politisk nivå – håndteres effektivt gjennom god utnyttelse av samfunnets samlede ressurser.[534] Rammeverket ble utformet i 2017 og skal revideres annethvert år eller hyppigere ved behov. Nasjonal sikkerhetsmyndighet jobber for øyeblikket med å revidere rammeverket, som ikke har blitt revidert siden 2017. Da Forsvarets forskningsinstitutt undersøkte hvordan angrepene mot fylkesmannsembetene og Helse Sør-Øst i 2018 ble håndtert, fant de at rammeverket ikke ble brukt. Nasjonal sikkerhetsmyndighet har ikke oversikt over hvor utbredt bruken av rammeverket er i dag, men viser til at flere sektorer henviser til rammeverket som standard prosedyre ved hendelseshandtering. Etter planen skulle man øve på å bruke rammeverket under den store nasjonale øvelsen Øvelse Digital 2020. Ettersom denne ikke ble gjennomført som planlagt, ble ikke dette til. Planen var at øvelsen skulle gi viktige innspill til revisjonen av rammeverket.

For å øke den nasjonale kapasiteten til å håndtere store digitale angrep er det i *Nasjonal strategi for digital sikkerhet* (2019) et tiltak om å utrede behovet og mulighetene for en tverrsektoriell cyberreserve. En tverrsektoriell cyberreserve skal være en nasjonal kapasitet som kan bistå med hendelseshåndtering ved spesielt store kriser som krever innsats utover ordinær bemanning. Utredningen skulle gjennomføres i perioden 2018−2019, men arbeidet er ennå ikke ferdigstilt. Justis- og beredskapsdepartementet forventer en utredning fra Nasjonal sikkerhetsmyndighet i løpet av høsten 2022. Det er uheldig at arbeidet med en tverrsektoriell cyberreserve er såpass forsinket ettersom kapasiteten i hendelseshåndteringen har vært en utfordring over lengre tid.

Det har siden 2012 vært iverksatt tiltak for å utvikle et system for høygradert datakommunikasjon mellom departementene, underliggende etater og andre sentrale beredskapsaktører.[535] Manglende muligheter for å kunne kommunisere via sikkerhetsgradert informasjonssystemer har blitt pekt på som hindrer for effektiv hendelseshåndtering av både Lysneutvalget i 2015 og Forsvarets forskningsinstitutt i 2020.[536] I henhold til *Nasjonal strategi for digital sikkerhet* (2019) skal Forsvarsdepartementet utvikle

[534] Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser*.
[535] Nasjonal strategi for informasjonssikkerhet (2012) - Handlingsplan
[536] Forsvarets forskningsinstitutt (2020) *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene.*

og drifte et nasjonalt begrenset nett (NBN) for lavgradert kommunikasjon, og et nasjonalt hemmelig nett (NHN) for høygradert kommunikasjon. Tiltaket var i strategien planlagt gjennomført i 2019. Nasjonal BEGRENSET Nett er etablert og tatt i bruk. Nasjonalt HEMMELIG Nett er ikke rullet ut til beredskapsaktørene ennå. Det er vår vurdering at etableringen av Nasjonalt Hemmelig Nett ikke har kommet langt nok i forhold til målet i strategien. Dette kan i verste fall få negative konsekvenser for håndteringen av alvorlige digitale angrep, på grunn av treg eller manglende kommunikasjon av sikkerhetsgradert informasjon mellom beredskapsaktører.

Detaljer om enkelte tiltak som gjelder hendelseshåndtering, omtales i eget sikkerhetsgradert vedlegg til denne rapporten. Dette omfatter detaljer om varslingssystemet for digital infrastruktur (VDI), systemer for gradert kommunikasjon mellom beredskapsaktører og Felles cyberkoordineringssenter.

8 Referanseliste

Regelverk

Lover

- *Lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m.* (jernbaneloven) (1. juli 1993)
- *Lov om arbeids- og velferdsforvaltningen* (arbeids- og velferdsforvaltningsloven) [NAV-loven] (1. juli 2006)
- *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv.* (arbeidsmiljøloven) (1. januar 2006)
- *Lov om arkiv* (arkivloven) (1. januar 1999)
- *Lov om behandling av helseopplysninger ved ytelse av helsehjelp* (pasientjournalloven) (1. januar 2015)
- *Lov om behandling av opplysninger i politiet og påtalemyndigheten* (politiregisterloven) (1. juli 2014)
- *Lov om behandlingsmåten i forvaltningssaker* (forvaltningsloven) (1. januar 1970)
- *Lov om betalingssystemer mv.* (betalingssystemloven) (14. april 2000)
- *Lov om elektronisk kommunikasjon* (ekomloven) (25. juli 2003)
- *Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked* (lov om elektroniske tillitstjenester) (15. juni 2018)
- *Lov om helsemessig og sosial beredskap* (helseberedskapsloven) (1. juli 2001)
- *Lov om helseregistre og behandling av helseopplysninger* (helseregisterloven) (1. januar 2015)
- *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret* (sivilbeskyttelsesloven) (25. juni 2010)
- *Lov om luftfart* (luftfartsloven) (1. april 1994)
- *Lov om matproduksjon og mattrygghet mv.* (matloven) (1. januar 2004)
- *Lov om medisinsk og helsefaglig forskning* (helseforskningsloven) (1. juli 2009)
- *Lov om nasjonal sikkerhet* (sikkerhetsloven) (1. januar 2019)
- *Lov om personopplysninger* (personopplysningsloven) (20. juli 2018)
- *Lov om petroleumsvirksomhet* (petroleumsloven) (1. juli 1997)
- *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energiloven) (29. juni 1990)
- *Lov om skipssikkerhet* (skipssikkerhetsloven) (1. juli 2007)
- *Lov om tilsynet med finansforetak mv.* (finanstilsynsloven) (7. desember 1956)
- *Lov om universiteter og høyskoler* (universitets- og høyskoleloven) (1. april 2005)

Kongelige resolusjoner

- Kgl.res. av 10. mars 2017 nr. 312 *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet*
- Kgl.res. av 20. desember 2018 *Ikraftsetting av lov 1. juni 2018 nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.*
- Kgl. res 24. juni 2005 om DSBs generelle koordineringsansvar og ansvaret for koordinering av tilsyn med aktiviteter, objekter og virksomheter med potensial for store ulykker, herunder ansvar for koordinering av tilsyn med virksomheter som omfattes av storulykkeforskriften

Forskrifter

- *Forskrift om behandling av opplysninger i politiet og påtalemyndigheten* (politiregisterforskriften) (20. september 2013)
- *Forskrift om behandling av personopplysninger* (personopplysningsforskriften) (1. januar 2001)
- *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)* (1. januar 2003)

- *Forskrift om elektronisk kommunikasjon med og i forvaltningen* (eForvaltningsforskriften) (1. juli 2004)
- *Forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett* (klassifiseringsforskrifta) (1. januar 2013)
- *Forskrift om kommunal beredskapsplikt* (kommunalberedskapsforskriften) (7. oktober 2011)
- *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (virksomhetssikkerhetsforskriften) (1. januar 2019)
- *Forskrift om sikkerhet og beredskap i kraftforsyningen* (kraftberedskapsforskriften) (1. januar 2013)
- *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)* [Forskrift om IKT-systemer i banker mv.] (1. august 2003)

Reglement
- *Bevilgningsreglementet* vedtatt gjennom St.prp. nr. 48 (2004−2005) *Om bevilgningsreglementet*, jf. Innst. S. nr. 187 (2004-2005)
- *Reglement for økonomistyring i staten* fastsatt 12. desember 2003 med endringer, senest 31. august 2021 (økonomireglementet)
- *Bestemmelse for økonomistyring i staten* fastsatt 12. desember 2003 med endringer, senest 31. august 2021 (økonomibestemmelsene)

Instrukser
- *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen) (1. september 2017)

Stortingsdokumenter

Stortingsmeldinger
- Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*
- Meld. St. 14 (2019–2020) *Kompetansereformen – Lære hele livet*
- Meld. St. 10 (2016−2017) *Risiko i et trygt samfunn*
- Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*
- Meld. St. 27 (2015–2016) *Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet*
- Meld. St. 29 (2011−2012) *Samfunnssikkerhet*, jf. Innst. 426 S (2012−2013)

Innstillinger
- Innst. 275 S (2020−2021) *Innstilling fra justiskomiteen om Samfunnssikkerhet i en usikker verden*
- Innst. 370 S (2019−2020) *Innstilling fra utdannings- og forskningskomiteen om Kompetansereformen – Lære hele livet*
- Innst. 103 L (2017–2018) *Innstilling fra utenriks- og forsvarskomiteen om Lov om nasjonal sikkerhet (sikkerhetsloven)*
- Innst. 187 S (2017−2018) *Innstilling fra justiskomiteen om IKT-sikkerhet. Et felles ansvar*
- Innst. 84 S (2016−2017) *Innstilling fra transport- og kommunikasjonskomiteen om Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*
- Innst. 426 S (2012−2013) *Innstilling fra justiskomiteen om samfunnssikkerhet*

Stortingsproposisjoner
- Prop. 1 S (2020–2021) Justis- og beredskapsdepartementet
- Prop. 78 S (2021–2022) *Endringer i statsbudsjettet 2022 under Kunnskapsdepartementet, Kultur- og likestillingsdepartementet, Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet, Arbeids- og inkluderingsdepartementet, Helse- og omsorgsdepartementet, Barne- og familiedepartementet, Nærings- og fiskeridepartementet, Finansdepartementet og Forsvarsdepartementet (økonomiske tiltak som følge av krigen i Ukraina)*

- Prop. 153 L (2016−2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*

Rapporter fra Riksrevisjonen

- Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelser av angrep mot IKT-systemer i politiet*
- Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelse av sikring mot dataangrep i Utenriksdepartementet*
- Del av Dokument 1 (2019–2020) *Riksrevisjonens undersøkelse av sikring mot dataangrep i Oljedirektoratet*
- Dokument 1 (2010–2011) *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2009*
- Dokument 1 (2014–2015) *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2014*
- Del av Dokument nr. 3:2 (2020–2021) *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer*
- Del av Dokument nr. 3:2 (2020–2021) *Riksrevisjonens undersøkelse av informasjonssikkerhet i Norfund*
- Dokument nr. 3:4 (2005–2006) *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur*
- Dokument nr. 3:5 (2020–2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT*
- Dokument nr. 3:7 (2020–2021) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*

Høringsuttalelser

- Justis- og beredskapsdepartementet (2018) Høring – NOU 2018: 14 *IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*

Styringsdokumenter

- Direktoratet for e-helse (2021) *Mandat for styringsgruppen for norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren*, 1. januar 2021
- Justis- og beredskapsdepartementet og Forsvarsdepartementet (2019) *Hovedinstruks for Nasjonal sikkerhetsmyndighet*
- Nasjonal sikkerhetsmyndighet (2019) *Samarbeidsavtale med Nasjonal kommunikasjonsmyndighet om tilsyn med sikkerhetsloven*, signert 19. desember 2019
- *Samarbeidsavtale om tilsyn inngått mellom Nasjonal sikkerhetsmyndighet og Nasjonal kommunikasjonsmyndighet*, signert 19. desember 2019

Tildelingsbrev

- Justis- og beredskapsdepartementet (2021) *Tildelingsbrev til Direktoratet for samfunnssikkerhet og beredskap*
- Kommunal- og distriktsdepartementet (2021) *Tildelingsbrev til Nasjonal kommunikasjonsmyndighet*
- Olje- og energidepartementet (2021) *Tildelingsbrev til Norges vassdrags- og energidirektorat*

Rapportering

- Kunnskapsdepartementet (2021) *Oppfølging av tiltak i strategi for digital sikkerhetskompetanse*
- Justis- og beredskapsdepartementet (2014) *Rapportering fra departementene om informasjonssikkerhet, sikkerhetstilstanden i departementet og underlagte virksomheter og øvelser.* UNNTATT OFFENTLIGHET
- Justis- og beredskapsdepartementet (2021) *Notat – Oppfølging og rapportering på digital sikkerhet*

Rundskriv, veiledere og retningslinjer

Retningslinjer

- Forsvarsdepartementet (2014) *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren*
- Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Kripos (2022) *Retningslinjer for cybersamarbeid*

Veiledere

- Arbeidstilsynet, m.fl. (2019) *Veileder om kontroll og overvåking i arbeidslivet.* Veileder publisert på Arbeidstilsynets nettsider. [Hentedato 5. desember 2021]
- Datatilsynet (2018) *Etablere internkontroll.* Veileder publisert på Datatilsynets nettsider. [Hentedato 23. november 2021]
- Digitaliseringsdirektoratet (u.å.) *Internkontroll i praksis, versjon 2.0.* Veileder publisert på direktoratets nettsider. [Hentedato 25. november 2021]
- Digitaliseringsdirektoratet (u.å.) *Regelverkskrav og anbefalinger – Internkontroll informasjonssikkerhet.* Veileder publisert på direktoratets nettsider. [Hentedato 23. september 2021]
- Digitaliseringsdirektoratet (u.å) *Veiledning om etatsstyring og oppfølging av virksomheter.* Veileder publisert på direktoratets nettsider. [Hentedato 23. november 2021]
- Direktoratet for e-helse (2020) *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger.* Veileder publisert på direktoratets nettsider. [Hentedato 2. desember 2021]
- Direktoratet for forvaltning og økonomistyring (2021) *Støtte til styringsdialogen om informasjonssikkerhet.* Veileder publisert på direktoratets nettsider. [Hentedato 23. november 2021]
- Direktoratet for forvaltning og økonomistyring (2021) *Veiledning i risikostyring i staten.* Veileder publisert på direktoratets nettsider. [Hentedato 23. november 2021]
- Direktoratet for samfunnssikkerhet og beredskap (2016) *Veileder i krisekommunikasjon.* Veileder publisert på direktoratets nettsider. [Hentedato 24. september 2021]
- Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*. Veileder publisert på regjeringens nettsider. [Hentedato 21. september 2021]
- Direktoratet for samfunnssikkerhet og beredskap (2020) *Samfunnssikkerhetsinstruksen for departementene − Vurderingskriterier for tilsyn av 6. mars 2020.* Veileder publisert på direktoratets nettsider. [Hentedato 24. september 2021]
- Direktoratet for samfunnssikkerhet og beredskap (2020) *Veileder for fylkesmannens arbeid med risiko- og sårbarhetsanalyser* (versjon 4, mars 2020). Veileder publisert på direktoratets nettsider [Hentedato 17. november 2022]
- Direktoratet for sikkerhet og beredskap (2021) *Veileder til forskrift om kommunal beredskapsplikt, versjon 2*. Veileder publisert på direktoratets nettsider. [Hentedato 22. september 2021]
- European Securities and Markets Authority (u.å.) *Guidelines on outsourcing to cloud service providers.* Veileder publisert på European Securities and Markets Authoritys nettsider. [Hentedato 23. september 2021]
- Finanstilsynet (2006) *Veiledning i etterlevelse av IKT-forskriften for mindre foretak.* Veileder publisert på Finanstilsynets nettsider. [Hentedato 21. september 2021]
- Forsvarets forskningsinstitutt (2020) *Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger.* Veileder publisert på instituttets nettsider. [Hentedato 21. september 2021]
- Justis- og beredskapsdepartementet (u.å.) *Prosesstrinn tilsyn v 5(1).* Veileder publisert på departementets nettsider. [Hentedato 2. mars 2022]
- Kredittilsynet (2006) *Veiledning i etterlevelse av IKT-forskriften for mindre sparebanker.* Veileder publisert på Kredittilsynets nettsider. [Hentedato 23. september 2021]

- Kystverket (2013) *Veiledning til forskrift om sikring av havneanlegg.* Veileder publisert på Kystverkets nettsider. [Hentedato 5. mars 2022]
- Mattilsynet (2021) *Veileder til drikkevannsforskriften.* Veileder publisert på Mattilsynets nettsider. [Hentedato 5. mars 2022]
- Nasjonal kommunikasjonsmyndighet (2017) *Veileder for ekomtilbydere.* Veileder publisert på etatens nettsider. [Hentedato 6. desember 2021]
- Nasjonal kommunikasjonsmyndighet (2018) *Veileder – Tillitstjenester i Norge.* Veileder publisert på etatens nettsider. [Hentedato 6. desember 2021]
- Nasjonal sikkerhetsmyndighet (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Grunnprinsipper for IKT-sikkerhet 2.0*. Veileder publisert på direktoratets nettsider. [Hentedato 23. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Håndbok i skadevurdering.* Veileder publisert på direktoratets nettsider. [Hentedato 24. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Håndbok i verdivurdering av informasjon og veileder for godkjenning av informasjonssystemer.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Veileder i anskaffelser etter sikkerhetsloven.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Veileder i sikkerhetsstyring*. Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Veileder for tilsyn med forebyggende sikkerhetsarbeid.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2020) *Veileder i verdivurdering av informasjon.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (2021) *Håndbok i klassifisering*. Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (u.å.) *Grunnprinsipper for sikkerhetsstyring.* Veileder publisert på direktoratets nettsider. [Hentedato 21. september 2021]
- Nasjonal sikkerhetsmyndighet (u.å.) *Personellsikkerhet.* Veileder publisert på direktoratets nettsider. [Hentedato 23. september 2021]
- Norges vassdrag- og energidirektorat (2020) *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen.* Veileder publisert på direktoratets nettsider. [Hentedato 7. mars 2022]
- Norges vassdrag- og energidirektorat (u.å.) *Veileder til kraftberedskapsforskriften kapittel 6.* Veileder publisert på direktoratets nettsider. [Hentedato 24. september 2021]

Rapporter, planer og utredninger

Offentlige utredninger

- NOU (1986: 12) *Datateknikk og samfunnets sårbarhet*
- NOU (2000: 24) *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*
- NOU (2006: 6) *Når sikkerheten er viktigst*
- NOU (2015: 13) *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*
- NOU (2018: 2) *Fremtidige kompetansebehov 1. Kunnskapsgrunnlaget*
- NOU (2018: 14) *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*
- NOU (2019: 2) *Fremtidige kompetansebehov II. Utfordringer for kompetansepolitikken*
- NOU (2020: 2) *Fremtidig kompetansebehov III. Læring og kompetanse i alle ledd*

Strategier

- Nærings- og handelsdepartementet, Forsvarsdepartementet og Justis- og politidepartementet (2003) *Nasjonal strategi for informasjonssikkerhet*
- Fornyings-, administrasjons- og kirkedepartementet, Samferdselsdepartementet, Forsvarsdepartementet og Justis- og beredskapsdepartementet (2007) *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010*
- Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Fornyings-, administrasjons- og kirkedepartementet (2012) *Nasjonal strategi for informasjonssikkerhet*
- Justis og beredskapsdepartementet (2012) *Nasjonal strategi for informasjonssikkerhet (2012*) – *Handlingsplan*
- Kripos (2016) *Strategi 2016−2025*
- Justis- og beredskapsdepartementet og Forsvarsdepartementet (2019) *Nasjonal strategi for digital sikkerhet*
- Justis- og beredskapsdepartementet og Kunnskapsdepartementet (2019) *Nasjonal strategi for digital sikkerhetskompetanse*
- Justis- og beredskapsdepartementet (2019) *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*

Øvrige rapporter og utredninger

- A-2 Norge AS (2021) *Kartlegging av drift og forvaltning av IKT-løsninger i statlige virksomheter*
- Agder kommunerevisjon IKS (2019) *Samfunnssikkerhet og beredskap i Songdalen kommune*
- Arbeidsgruppen regelverk og informasjonssikkerhet; *oversikt og forslag til KIS AE/MHa 21.09.2005*
- Bergen kommune (2020) *Overordnet beredskapsplan for Bergen kommune. Administrativ del*
- Bindal kommune (2021) *Tilsyn*
- Datatilsynet (2020) *Årsrapport 2020*
- Digitaliseringsdirektoratet (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen.* Difi-rapport 2018:4
- Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i kommuner og fylkeskommuner*
- Direktoratet for forvaltning og økonomistyring (2014) *Mot alle odds? Veier til samordning i norsk forvaltning*
- Direktoratet for forvaltning og økonomistyring (2020) *Statlig tilsyn med kommunene, Kartlegging av omfang, samordning og nytte.* DFØ-rapport 2020:9
- Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av kunnskapsgrunnlaget*. Rapport nr. 01/2021 (utgitt september 2022)
- Direktoratet for høyere utdanning og kompetanse (2021) *Behovet for IKT-kompetanse i Norge. En vurdering av tiltak*. Rapport nr. 03/2021 (utgitt november 2022)
- Direktoratet for samfunnssikkerhet og beredskap (2016) *Samfunnets kritiske funksjoner, versjon 1.0*
- Direktoratet for samfunnssikkerhet og beredskap (2016) *Metodehefte: spilløvelse*
- Direktoratet for samfunnssikkerhet og beredskap (2019) *Analyser av krisescenarioer 2019*
- Direktoratet for samfunnssikkerhet og beredskap (2020) *Rapport fra tilsyn med Olje- og energidepartementets samfunnssikkerhetsarbeid, 2. juni 2020*
- Direktoratet for samfunnssikkerhet og beredskap (2021) *Rapport: Tilsyn med Nærings- og fiskeridepartementets arbeid med samfunnssikkerhet, 23. mars 2022*
- Direktoratet for samfunnssikkerhet og beredskap (2021) *Rapport: Tilsyn med Klima- og miljødepartementets arbeid med samfunnssikkerhet, 31. august 2021*
- Direktoratet for samfunnssikkerhet og beredskap (2021) *Øvelse Digital 2020 Evalueringsrapport.* UNNTATT OFFENTLIGHET
- Etterretningstjenesten (2022) *Fokus 2022*

- Europol (2021) *Iocta 2021 unveils the most recent cyber threat revolutions*
- Finanstilsynet (2019) *Rapportering av IKT-hendelser til kredittilsynet*
- Forskningsrådet (2018) *Programplan for SAMRISK 2018-2027*
- Forsvarets forskningsinstitutt (2020) *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene*
- Forsvarets forskningsinstitutt og Direktoratet for forvaltning og IKT (2017) *Evaluering av tilsyn med departementenes samfunnssikkerhets- og beredskapsarbeid - tredje tilsynsrunde.* Difi-rapport 2017:4
- Arbeidsgruppe nedsatt av Forsvarsdepartementet, Justisdepartementet og Arbeids- og administrasjonsdepartementet (1991) *Samordning av regelverk for beskyttelse av informasjon*
- Fylkesmannen i Oppland (2012) *Rapport fra tilsyn med samfunnssikkerhet og beredskap i Lillehammer kommune*
- Helsetilsynet (2012) *Rapport fra tilsyn med samfunnssikkerhets- og beredskapsarbeidet i Lardal kommune 2012*
- Helsetilsynet (2014) *Rapport fra tilsyn med samfunnssikkerhets- og beredskapsarbeidet i Justis- og beredskapsdepartementet. Inkludert undersøkelser i Direktoratet for samfunnssikkerhet og beredskap, Politidirektoratet og to politidistrikter*
- Helsetilsynet (2021) *Tilsyn med kommunal beredskapsplikt og helseberedskap Åfjord kommune 2021*
- Justis- og beredskapsdepartementet (2019) *Evaluering av «Forum for nasjonal IKT-sikkerhet»*
- Justis- og beredskapsdepartementet (2020) *Nettverk for nasjonal IKT-sikkerhet – forslag om innlemmelse i Departementenes samordningsråd for samfunnssikkerhet*
- Koordineringsutvalget for informasjonssikkerhet (2005) *Forprosjektrapport fra arbeidsgruppen Regelverk og informasjonssikkerhet til Koordineringsutvalget for informasjonssikkerhet (KIS)*
- Kompetansebehovutvalget (2022) *Fremtidige kompetansebehov: Høyere yrkesfaglig utdanning for et arbeidsliv i endring*
- KPMG (2022) *Rapport: Evaluering av sektorvise responsmiljøer.* Sak 21/6916
- KS (2018) *Kartlegging av digital modenhet i kommunesektoren*
- Mark, Michael Spjelkavik, Cathrine Tømte, Terje Næss og Trude Røsdal (2017) *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud*. NIFU-rapport 2017: 32
- Meløy kommune (2020) *Plan for oppfølging av samfunnssikkerhet og beredskap 2020-2023*
- Nasjonal sikkerhetsmyndighet (2018) *Risiko 2018*
- Nasjonal sikkerhetsmyndighet (2019) *Helhetlig digitalt risikobilde 2019*
- Nasjonal sikkerhetsmyndighet (2019) *Risiko 2019*
- Nasjonal sikkerhetsmyndighet (2020) *Kontroll av nasjonal sikkerhet – Kontrollmeldingen 2020*
- Nasjonal sikkerhetsmyndighet (2020) *Risiko 2020*
- Nasjonal sikkerhetsmyndighet (2020) *Helhetlig digitalt risikobilde 2020*
- Nasjonal sikkerhetsmyndighet (2021) *IKT-risikobilde 2021*
- Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021*
- Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022*
- Nasjonal sikkerhetsmyndighet (2022) *Nasjonalt digitalt risikobilde* 2022.
- Norsk senter for informasjonssikring (2017) *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)*
- Norsk senter for informasjonssikring (2019) *Trusler og trender 2018/2019*
- Norsk senter for informasjonssikring (2020) *Trusler og trender 2020*
- Norsk senter for informasjonssikring (2021) *Trusler og trender 2021*
- Næringslivets sikkerhetsråd (2018) *Mørketallsundersøkelsen 2018*
- Næringslivets sikkerhetsråd (2020) *Mørketallsundersøkelsen 2020*
- Næringslivets sikkerhetsråd (2021) *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2021*

- Næringslivets sikkerhetsråd (2921) *Hybridundersøkelsen − hybride trusler og hendelser mot norsk næringsliv*
- Oslo kommune (2021) *Kommunalt risikobilde 2021*
- Politiets sikkerhetstjeneste (2018) *PSTs trusselvurdering 2018*
- Politiets sikkerhetstjeneste (2021) *Nasjonal trusselvurdering 2021*
- Politiets sikkerhetstjeneste (2022) *Nasjonal trusselvurdering 2022*
- Sarpsborg kommune (2019) *Helhetlig risiko- og sårbarhetsanalyse*
- Sopra Steria (2021) *Evaluering av tilskudd til NorSIS*
- Telenor (2020) *Digital sikkerhet 2020*
- Telenor (2021) *Digital sikkerhet 2021*
- Viken kommunerevisjon IKS (2020) *Samfunnssikkerhet og beredskap – 2020*
- Østre Viken kommunerevisjon (2020) *Samfunnssikkerhet og beredskap*

Faglitteratur

- Klijn, Erik-Hans (2008) *Governance and Governance Networks in Europe.* I: Public Management Review, 10(4), s. 505–525. DOI: 10.1080/14719030802263954
- Klijn, Erik-Hans og Joop Koppenjan (2014) *Complexity in governance network theory.* I: *Complexity, Governance & Networks.* 1(1), s. 61–70
- Kooiman, Jan (1993) *Modern Governance. New Government - Society Interactions*. London: SAGE
- Peters, Guy B. (2018) *The challenge of policy coordination.* I: *Policy Design and Practice*, 1(1), s. 1–11, DOI: 10.1080/25741292.2018.1437946
- Schartum, Dag Wiese (2005) *Norsk regelverk vedrørende informasjonssikkerhet – oversikt og struktur vurdert i lys av ønsket om samordning.* I: Nordisk Årbok i rettsinformatikk, Norstedts forlag
- Trondal, Jarle (2017) *The Rise of Common Political Order.* Storbritannia: Edward Elgar Publishing

Brev, notater og nettkilder

Brev/e-post

- Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022
- Justis- og beredskapsdepartementet (2022) *Hovedanalyserapport Samordning av digital sikkerhet_JDs innspill*. Vedlegg til Justis- og beredskapsdepartementet (2022) *Riksrevisjonens undersøkelse om myndighetenes samordning av arbeidet med digital sikkerhet.* Brev til Riksrevisjonen, 11. november 2022
- Kunnskapsdepartementet (2022) *Svar på oppfølgingsspørsmål om Nasjonal strategi for digital sikkerhetskompetanse*. E-post til Riksrevisjonen, 26. august 2022
- Norges vassdrags- og energidirektorat (2022) *SV: Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet*. E-poster til Riksrevisjonen, 19. og 23. mai 2022
- Svar på skriftlige spørsmål fra Digitaliseringsdirektoratet, besvart 6. mai 2022
- Svar på skriftlige spørsmål fra Direktoratet for sikkerhet og beredskap, besvart 9. mai 2022

Møtereferater

- Justis- og beredskapsdepartementet (2017–2022) *Tilsendte møtereferater fra Nettverk for nasjonal IKT-sikkerhet*
- Justis- og beredskapsdepartementet (2020) *Møtereferat 22. september 2020, Nettverk for nasjonal IKT-sikkerhet*
- Justis- og beredskapsdepartementet (2022) *Referat fra møte i Nettverk for nasjonal IKT-sikkerhet*, 9. mars 2022
- Nasjonal sikkerhetsmyndighet (2021) *Referat SIG Digital Brief, 3. september 2021*

Nettkilder

- Datatilsynet (2018) *Skytjenester.* Nettartikkel, 23. juni 2018 [Hentedato 4. april 2022]
- Datatilsynet (2019) *Risikovurdering.* Nettartikkel, 16. juli 2019 [Hentedato 6. april 2022]
- Datatilsynet (2020) *Hva er phishing?* Nettartikkel, 17. juli 2020 [Hentedato 6. april 2022]
- Datatilsynet (2022) *«Tilsyn kommune»* Nettsøk [Søk gjennomført 4. mai 2022]
- Datatilsynet (2022) *Tilsynsvirksomheten vår i 2022.* Nettartikkel, 20. januar 2022 [Hentedato 16. juni 2022]
- Digi.no (2004) *Statlig utvalg skal koordinere norsk IT-sikkerhet.* Nettartikkel, 21. mai 2004 [Hentedato 30. august 2022]
- Digitaliseringsdirektoratet (u.å.) *Begrepsliste.* Nettartikkel [Hentedato 4. april 2022]
- Digitaliseringsdirektoratet (u.å.) *Hva vil det si å jobbe helhetlig?* Nettartikkel [Hentedato 2. juni 2022]
- Digitaliseringsdirektoratet (u.å.) *Kva er Digitaliseringsdirektoratet?* [Hentedato 15. november 2021]
- Digitaliseringsdirektoratet (u.å.) *Nettverk for veiledningsaktører - styring og kontroll* [Hentedato 10. november 2022]
- Direktoratet for forvaltning og økonomistyring (2021) *Samordning.* Nettartikkel, 27. april 2022 [Hentedato 10. juni 2021]
- E24 (2021) *Nortura utsatt for dataangrep.* Nettartikkel, 22.desember 2021 [Hentedato 7. oktober 2022]
- Enisa (2006) *CSIRT Setting up Guide in English.* Nettartikkel, 22. desember 2006 [Hentedato 5. april 2022]
- EØS-notatbasen (2016) *NIS-direktivet.* Nettartikkel, 16. desember 2016 [Hentedato 22. mars 2022]
- First (u.å.) *First Teams (Norway).* Nettartikkel [Hentedato 10. juni 2021]
- Forskningsrådet (u.å.) *Prosjektbanken − søkeord «digital sikkerhet»* [Hentedato 3. august 2022]
- Forsvaret (2020) *Forsvarets fellestjenester.* Nettartikkel, 6. juli 2022 [Hentedato 15. november 2021]
- Forsvaret (2021) *Cyberforsvaret.* Nettartikkel, 18. juni 2021 [Hentedato 16. november 2021]
- Forsvaret (2022) *Etterretningstjenesten.* Nettartikkel, 21. juni 2022 [Hentedato 16. november 2021]
- Furberg, Petter-Børre, *Beredskap og sikkerhet må planlegges for selv de verste dager*. Innlegg på Nasjonal sikkerhetsmyndighets sikkerhetskonferanse i 2022. Nettkilde. [Hentedato: 19. november 2022]
- Gausen, Sigrid, Torgeir Knudsen, Solveig Ruud og Torgeir Strandberg (10.03.2021) *Stortinget utsatt for IT-angrep: «Et angrep på vårt demokrati».* I: Aftenposten, nettutgave <https://www.aftenposten.no/norge/i/PRnGRX/stortinget-utsatt-for-it-angrep-et-angrep-paa-vaart-demokrati> [Hentedato 7. oktober 2022]
- Honningsøy, Kirsti Haga (28. desember 2021) *Amedia utsatt for alvorlig dataangrep*. I: NRK, nettutgave. < https://www.nrk.no/norge/amedia-utsatt-for-alvorlig-dataangrep-1.15788535> [Hentedato 7. oktober 2022]
- Johansen, Per Anders (13.10.2020) *Regjeringen: Russland stod bak dataangrep på Stortinget.* I: Aftenposten, nettutgave <https://www.aftenposten.no/norge/i/39JXme/regjeringen-russland-sto-bak-dataangrep-paa-stortinget> [Hentedato 7. oktober 2022]
- Kommunal- og distriktsdepartementet (2021) *Tilsynskalender for samordning av planlagde statlege tilsynsaktivitetar.* Nettartikkel, 5. januar 2021 [Hentedato 6. april 2022]
- Kommunal- og distriktsdepartementet (u.å.) *Notat samfunnssikkerhet og beredskap* [Hentedato 4. april 2022]
- KS (2021) *ROS-analyse* Nettartikkel. Nettartikkel, 18. januar 2019 [Hentedato 4. april 2022]
- Nasjonal sikkerhetsmyndighet (2020) *Hendelseshåndtering.* Nettartikkel, 24. juni 2020 [Hentedato 7. april 2022]

- Nasjonal sikkerhetsmyndighet (2020) *Råd om IKT-sikkerhetstiltak, basert på erfaringer fra 2020.* Nettartikkel, 29. august 2020 [Hentedato 8. april 2022]
- Nasjonal sikkerhetsmyndighet (2020) *Varslingssystemet for digital infrastruktur (VDI).* Nettartikkel, 3. juni 2020 [Hentedato 6. mai 2022]
- Nasjonal sikkerhetsmyndighet (2021) *Oversikt over innmeldte grunnleggende nasjonale funksjoner.* Nettartikkel, 15. oktober 2021 [Hentedato 8. mars 2022]
- Nasjonal sikkerhetsmyndighet (u.å.) *Nasjonalt cybersikkerhetssenter (NCSC) og NorCERT* Nettartikkel [Hentedato 4. februar 2022]
- Nasjonal sikkerhetsmyndighet (u.å.) *Virksomheter av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner.* Nettartikkel [Hentedato 1. september 2022]
- NATO (2019) *Resilience: the first line of defence.* Nettartikkel, 27. februar 2019 [Hentedato 22. mars 2022]
- Nettvett.no (2021) *Løsepengevirus.* Nettartikkel, 19. mai 2021 [Hentedato 6. april 2022]
- NorDangruppen (2022) *Bevissthet og åpenhet rundt dataangrep*. Nettartikkel [Hentet 7. oktober 2022]
- Norges teknisk-naturvitenskapelig universitet (2022) *Center for Cyber and Information Security*. Nettkilde. [Hentedato: 11.11.22]
- Norges vassdrag- og energidirektorat (2022) *NVE følger opp Riksrevisjonens rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen.* Nettartikkel, 7. februar 2022 [Hentedato 16. juni 2022]
- Næringslivets sikkerhetsråd (u.å.) *Næringslivets sikkerhetsråd.* Nettartikkel [Hentedato 22. oktober 2021]
- Petroleumstilsynet (2019) *Hvilket regelverk gjelder?* Nettartikkel, 11. februar 2019 [Hentedato 2. juni 2022]
- Politiet (u.å.) *Nettsvindel.* Nettartikkel [Hentedato 6. april 2022]
- Politiets sikkerhetstjeneste (2017) *Hva gjør vi?* Nettartikkel, 10. oktober 2017 [Hentedato 11. november 2021]
- Store norske leksikon (2019) *Sårbarhet (IT).* Nettartikkel, 2. desember 2019 [Hentedato 4. april 2022]
- Store norske leksikon (2021) *Internkontroll.* Nettartikkel, 6. juli 2021 [Hentedato 7. april 2022]
- Store norske leksikon (2022) *Informasjonssikkerhet.* Nettartikkel, 5. august 2022 [Hentedato 9. september 2022]
- Store norske leksikon (2022) *Trusselaktør.* Nettartikkel, 21. februar 2022 [Hentedato 4. april 2022]
- Triple-S (2021) *Redundante løsninger: Hva det er og hvordan du kommer i gang.* Nettartikkel, 24. november 2021 [Hentedato 7. april 2022]
- Universitet i Bergen (2022) *Simula@UiB*. Nettkilde. [Hentedato: 11.11.2022]
- Universitet i Oslo (2019) *Begreper og definisjoner.* Nettartikkel, 7. mars 2019 [Hentedato 7. april 2022]

9 Vedlegg

Vedlegg 1: Utdypende informasjon om sentrale tiltak for håndtering av alvorlige digitale hendelser (BEGRENSET).

Vi har levert et sikkerhetsgradert vedlegg til Stortinget om detaljer om utfordringene rundt hendelseshåndtering. Vedlegget er ikke offentlig.