

## Vedlegg E – Metode og datagrunnlag

### Innhold

Datagrunnlag og metode .....	2
Gjennomgang av dokumenter og statistikk .....	2
Norges offentlige utredninger .....	2
Stortingsmeldinger .....	2
Rapporter .....	2
Veiledere, normer, rammeverk .....	2
Strategier .....	3
Andre relevante kilder .....	3
Statistikk .....	3
Samtaler og samarbeid med kommunal sektor .....	3
Dialog i sektoren før 2022 .....	4
Møtevirksomhet våren/sommeren 2022 .....	4
Nasjonalt program for informasjonssikkerhet (NPISK) .....	4
Innspillsrunder .....	4
Analyse og konklusjon fra dokumentasjonsgjennomgang og sektordialog .....	5
Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet .....	5
Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne .....	7
Oppsummering .....	9

## Datagrunnlag og metode

Rapporten finner sitt kunnskapsgrunnlag i offisielle og publiserte dokumenter, samtaler, workshops og innspillsrunder med kommunal sektor og erfaringsgrunnlag fra innspillet til nasjonalt program for informasjonssikkerhet i kommunal sektor (NPISK). I det følgende redegjøres det for hvilke dokumenter som har vært gjenstand for dokumentanalyse, og hvilke samarbeid og initiativ som har skapt kunnskapsgrunnlaget for rapporten.

## Gjennomgang av dokumenter og statistikk

I forbindelse med rapporten har sentrale dokumenter som regulerer rammer og ansvar for arbeid med digital sikkerhet, beredskap og personvern blitt gjennomgått. Dette omfatter veiledningsmaterieell, konseptutredninger, rammeverk, strategier, etterretnings- og sikkerhetstjenestens risikovurderinger, årsrapporter, gjennomførte kartlegginger i kommunal sektor og lovverk. Gjennomgåtte dokumenter er fra perioden 2015-2023.

### Norges offentlige utredninger

- NOU 2015:13 Digital sårbarhet – sikkert samfunn.
- NOU 2018:14 IKT-sikkerhet i alle ledd.
- NOU 2022:11 Ditt personvern – vårt felles ansvar — Tid for en personvernpolitikk.
- NOU 2023:4 Tid for handling Personellet i en bærekraftig helse- og omsorgstjeneste.
- NOU 2016:19 - Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.

### Stortingsmeldinger

- Meld. St. 10 (2016-2017) Risiko i et trygt samfunn. Samfunnssikkerhet.
- Meld. St. 38 (2016-2017) IKT-sikkerhet. Et felles ansvar.
- Meld St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden.
- Meld. St. 9 (2022 –2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.

### Rapporter

- Risiko 2022 (NSM, 2022).
- Risiko 2021 (NSM, 2021).
- Nasjonal trusselvurdering 2022 (PST, 2022).
- Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor (Riksrevisjonen, 2023).
- Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner (Digitaliseringsdirektoratet 2020).
- Personvern- og informasjonssikkerhet (DigiVestland, 2021-2022).
- Kartlegging av digital modenhet i kommunal sektor (KS, 2018).
- Fremtidig organisering av KS digitale fellestjenester (KS, 2022).
- Kommune CERT – utredning av behov og muligheter (NorSIS, 2015).

### Veiledere, normer, rammeverk

- Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen).
- Hvordan jobbe med informasjonssikkerhet (Digitaliseringsdirektoratet).
- Grunnprinsipper for IKT-sikkerhet (NSM).

- Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet – orden i eget hus (KS).
- Rammeverk for håndtering av IKT-sikkerhetshendelser.

## Strategier

- Internasjonal cyberstrategi for Norge (2017).
- Nasjonal strategi for digital sikkerhet (2019).
- Nasjonal strategi for digital sikkerhetskompetanse (2019).
- Digitaliseringsstrategien for offentlig sektor (2019-2025) – Én digital offentlig sektor

## Andre relevante kilder

- Proposisjon 78 S (2021–2022).
- Felles sikkerhet i forvaltningen. Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning (Digitaliseringsdirektoratet, 2022).
- Offentlige og private tilbydere av SOC og CERT tjenester (DFØ, Markedsplassen).

## Statistikk

Tabeller fra SSBs statistikk «Bruk av IKT i offentlig sektor»:

- Tabell 12041: «Tiltak/rutiner ved administrasjon av IKT-sikkerheten, etter antall innbyggere (Fylkeskommuner, kommuner)».
- Tabell 12038: «Rekruttering av IKT-spesialister (prosent), etter forvaltningsnivå, statistikkvariabel og år».
- Tabell 2019: «IKT-strategier (prosent), etter status for strategi, forvaltningsnivå, statistikkvariabel og år».
- Tabell 12036: «Hindringer for utvikling av elektroniske tjenester (prosent), etter statistikkvariabel, grad av hindring, forvaltningsnivå og år».
- Tabell 12617: «IKT-sikkerhetsproblemer (prosent), etter statistikkvariabel, status for sikkerhetsproblemet, forvaltningsnivå og år».
- Tabell 12618: «Tiltak for IKT-sikkerheten (prosent), etter statistikkvariabel, status for tiltak, forvaltningsnivå og år».

## Samtaler og samarbeid med kommunal sektor

Kommunal sektor har over lang tid samarbeidet om ulike tiltak for å bedre digital robusthet. I KS har for eksempel Fagrådet for informasjonssikkerhet og personvern arbeidet med problemstillinger på området i en årrekke innenfor samstyringsstrukturen, i tillegg til at SNIP-nettverket og de regionale digitaliseringsnettverkene har gitt sine bidrag.

Prosjekter og aktiviteter i kommunal sektor har også hatt en tydelig involvering av informasjonssikkerhet og personvern, herunder utvikling av kompetansepakker, SkoleSec, og større prosjekter som Akson. Gjennom disse har kommunal sektor både kartlagt status innen digital robust, og samtidig fremme behov for tiltak, selv om dette arbeidet ikke har vært samlet under en felles paraply.

Det ble i løpet av året 2022 igangsatt flere initiativ og samarbeid, inkludert NPISK, arbeids- og avklaringsmøter, og samtaler med kommuner og fylkeskommuner i forbindelse med utvikling av grunnlaget for og arbeidet med rapporten. Innspillene fra sektoren har vært avgjørende for å beskrive utfordringsbildet i sektoren i dag, samt identifikasjon av målrettede og treffsikre tiltak.

## Dialog i sektoren før 2022

I forbindelse med Akson-prosjektet ble det gjennomført mer enn 25 møter i perioden januar - juni 2020 for å utarbeide referansearkitektur for sikkerhet, beredskap og personvern for kommunal sektor (RSB) i forbindelse med Aksonprosjektet.

Ved utarbeidelsen av RSB ble det vektlagt hvordan utfordringene innen digital sikkerhet som kommunal sektor står ovenfor på kort og lang sikt kan møtes effektivt.

Det henvises til vedlegg I - *RSB - versjon 1.0 - Referansearkitektur sikkerhet beredskap og personvern* over hvilke kommuner som deltok i arbeidet og selve arbeidet.

## Møtevirksomhet våren/sommeren 2022

Det har vært gjennomført mer enn 30 møter og workshops med kommuner, myndigheter og interessenter i løpet av våren/sommeren 2022. Møtene og workshopene har satt søkelys på status og behov for kommunene. Sentrale aktører har vært kommuner i SNIP-nettverket (tilnærmet alle kommuner) i workshops, samt NSM, HelseCERT, Kommune-CSIRT, Kraft/InfraCERT, JustisCERT og DFØ. Disse aktørene har også deltatt på flere oppfølgingsmøter.

I workshops med kommunene er det noen hovedmomenter om behov som spesielt går igjen:

- Innføre trusselovervåking og monitorering (SOC), og responsmiljø (IRT).
- Gjennomføre penetrasjonstester.
- Redusere ressursbruk på ROS og DPIA, forenkling av verktøy.
- Redusere ressursbruk på leverandøroppfølging og mulig –sertifisering.
- Redusere ressursbruk på teknisk forvaltning av infrastruktur (standardoppsett etc.).
- Støtte til tolkning og implementering av rammeverk (ISO, NSM grunnprinsipper etc.).
- Gjennomføre opplæring og kompetansebygging.
- Tydeliggjøring av ansvar og roller blant aktørene.
- Samarbeid for innkjøp og felles bestillingskompetanse.

Status i forbindelse med innspillet til nasjonalt program for informasjonssikkerhet i kommunal sektor har også vært gitt til KommIT, Digitaliseringsutvalget, Fagrådet og diginetttverkene.

## Nasjonalt program for informasjonssikkerhet (NPISK)

KS har sammen med fagekspertene fra medlemmene, og i dialog med Kommunal- og distriktsdepartementet (KDD), utarbeidet et forslag til program for IKT-sikkerhet i kommunal sektor (NPISK). KS søker samarbeid med ulike aktører for å gjennomføre en rekke aktiviteter i tråd med Stortingets vedtak.

I utarbeidelsen av foreslåtte tiltak i NPISK ble det satt sammen en faggruppe med hensikt om å foreslå og utarbeide tiltak. Arbeidet pågikk fra mai 2022 – september 2022. Kunnskapsgrunnlaget fra NPISK har vært viktig for innsikt i utfordringene de enkelte kommunene står i, og hvilke strakstiltak som er nødvendig å innføre.

## Innspillsrunder

I løpet av høsten 2022 ble første utkast av rapporten ferdigstilt. Rapporten ble delt og videresendt til store deler av sektoren, og inndelt i følgende arbeidsgrupper:

- Faggruppe innen digitalisering, informasjonssikkerhet og personvern. Faggruppen besto av medlemmer fra flere kommuner og fylkeskommuner.

- Diginettverkslederene. Alle Diginettverkslederene deltok.
- Strategisk faggruppe. Representanter med strategisk styringskompetanse innen digitalisering deltok.

Det ble gjennomført to arbeidsmøter på 3 timer med faggruppen. Basert på innspillene fra faggruppen, ble rapporten justert for å hensynta innspill og tilbakemeldinger. Det ble særlig satt søkelys på utarbeidelsen av målrettede tiltak i sektoren.

Det ble gjennomført ett møte med diginettverkslederene, med særlig søkelys på implementering og operasjonalisering av tiltakene i sektoren. Diginettverkslederene ga tilbakemeldinger skriftlig i etterkant av møtet.

Strategisk faggruppe deltok i 3 møter for å gi innspill på innretningen og tiltakene i rapporten.

## Analyse og konklusjon fra dokumentasjonsgjennomgang og sektordialog

Dokumentasjonsgjennomgangen sammenholdt med sektordialogen har gitt et godt grunnlag for å forstå kommunenes situasjon innen informasjonssikkerhet og personvern. Selv om funnene og beskrivelsene spriker når man ser kommunene under ett, viser behovsbeskrivelsene etter workshops med kommunene at *behovene* i stor grad er de samme.

### Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet

KS sin kartlegging av digital modenhet i kommunesektoren fra 2018<sup>1</sup> viser at 86% av fylkeskommunene og kommunene har organisert arbeidet med informasjonssikkerhet gjennom en form for rolle/sikkerhetsfunksjon med ansvar for informasjonssikkerhet. Disse rollene varierer mellom å være en «dedikert sikkerhetsfunksjon som rapporterer til rådmann» (54 %), informasjonssikkerhetsfunksjon som rapporterer til IKT-ansvarlige» (13 %), «sikkerhetsfunksjon i hver enkelt virksomhet» (10 %) og en «tilfeldig utvalgt ressurs» (9 %).

Ved å sammenstille de ovennevnte data med SSB tabell 12041<sup>2</sup> gir denne en indikasjon på både sikkerhetsarbeidet og organisering i kommunal sektor:

12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år									
	Har en skriftlig informasjonssikkerhetspolicy som er forankret i ledelsen		En formelt utnevnt person er fagansvarlig for informasjonssikkerheten		Risikovurderinger gjennomføres systematisk og periodisk		Ved nye risikovurderinger iverksettes nødvendig risikohåndtering		
	2018	2022	2018	2022	2018	2022	2018	2022	
Fylkeskom 50 000 innbyggere eller flere	87,5	70,0	87,5	90,0	68,8	80,0	87,5	100,0	
Kommune 0 - 1 999 innbyggere	57,8	58,4	54,2	59,7	36,1	44,2	60,2	71,4	
2 000 - 4 999 innbyggere	56,5	57,9	60,2	73,7	30,6	66,3	57,4	84,2	
5 000 - 9 999 innbyggere	55,7	74,6	57,0	81,7	45,6	63,4	69,6	87,3	
10 000 - 19 999 innbyggere	78,4	72,3	76,5	80,9	51,0	66,0	78,4	91,5	
20 000 - 29 999 innbyggere	84,0	82,8	72,0	82,8	44,0	75,9	88,0	86,2	
30 000 - 49 999 innbyggere	87,5	73,3	81,3	86,7	56,3	73,3	68,8	86,7	
50 000 innbyggere eller flere	86,7	80,0	93,3	85,0	86,7	95,0	100,0	95,0	

Dataene er kun en indikasjon på sikkerhetsarbeid og organisering i kommunal sektor da de ikke inneholder informasjon om grundigheten av risikovurderingene, kompetanse- eller ressurskapasitetsnivå til fagpersonene, eller kvaliteten på informasjonssikkerhetspolicy.

<sup>1</sup> <https://www.ks.no/contentassets/3f544fbc44c1404a8b81f7f98737509f/digital-modenhet.pdf>

<sup>2</sup> <https://www.ssb.no/statbank/table/12041/tableViewLayout1/>

Denne indikasjonen støttes også opp av SSB tabell 12038<sup>3</sup>, se nedenfor, om rekruttering.

I følge «Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner» (Digitaliseringsdirektoratet, 2020), basert på DSBs tall fra 2018 er bildet mer underbygget med data: «Observasjonene viser at 44 % av kommunene har informasjonssikkerhet som et fast punkt i styringsdialogen i egen organisasjon. At under halvparten av kommunene har dette kan tyde på at informasjonssikkerhet ikke har tilstrekkelig plass i styringsdialogen hos kommunene.»

Rapporten fra Digdir peker videre på at:

«Observasjonene viser at over 75 % av fylkeskommunene i tidsperioden 2018-2019 svarte at de har evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Under 65 % av kommunene svarer tilsvarende i tidsperioden 2018-2020. [...] Observasjonene viser videre at under 75 % av fylkeskommune i tidsperioden 2018- 2019 svarte at de rapporterte erfaringer fra håndtering av uønskede hendelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten. Under 55 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. [...] Observasjonene viser videre at under 40 % av fylkeskommunene svarte at de rapporterte erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten i tidsperioden 2018 - 2019. Under 30 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. Dette kan indikere at fylkeskommuner og kommuner i liten grad rapporterer erfaringer fra øvelser til bruk i risikovurderinger».

Disse observasjonene sammen underbygger hypotesen om at styringsevnen til kommunene, som må ha en tilbakemeldingsløyfe fra oppdateringer, risikovurderinger og øvelser for å være til tilstrekkelig, ikke er tilstrekkelig innen informasjonssikkerhet og personvern.

I følge Digdirs rapport viser vurderinger Datatilsynet har gjort «at noen større kommuner ikke har tilstrekkelige tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet om personopplysninger. I enkelttilfeller har kommunen heller ikke hatt nok kompetanse rundt gjennomføringen av risikovurderinger. Dette indikerer at også blant store kommuner kan det i enkelttilfeller være utfordringer med risikostyring. Veiledning knyttet til kompetanseheving på risikovurdering og risikohåndtering bør spesielt rettes mot små og mellomstore kommuner.»

I forbindelse med workshops med kommunene fremkom også behovet for kompetanse i forbindelse med gjennomføring av risikovurderinger tydelig.

### 12038: Rekruttering av IKT-spesialister (prosent), etter forvaltningsnivå, statistikkvariabel og år

✓ Informasjon om tabellen	↶ Rotér mot venstre	↷ Rotér mot høyre	↻ Rotér manuelt	📄 Excel (xlsx)	↗ Fullskjerm	
✓ Endre visning						
✓ Rediger og beregne						
✓ Lagre data som						
✓ Lagre spørring						
	Har forsøkt å rekruttere IKT-spesialister i løpet av det siste året			Hadde problemer med å rekruttere IKT-spesialister i løpet av det siste året		
	2018	2020	2022	2018	2020	2022
Fylkeskommuner	75,0	:	80,0	33,3	:	62,5
Kommuner	29,2	35,4	51,4	31,8	50,4	56,0

<sup>3</sup> <https://www.ssb.no/statbank/table/12038/tableViewLayout1/>

Tabell 12038 kan ses i sammenheng med tabell 12019<sup>4</sup>, se nedenfor, som angår digitaliseringsstrategi. Denne tabell er lagt til grunn som en indikasjon da den ikke gir ytterligere verdier om kvalitet og grundighetsnivå på strategien. Det er også interessant å legge merke til at i 2022 hadde 84,8% av kommunene strategi for skytjenester mens 74,3% hadde digitaliseringsstrategi.

### 12019: IKT-strategier (prosent), etter status for strategi, forvaltningsnivå, statistikkvariabel og år

<ul style="list-style-type: none"> <li>✓ Informasjon om tabellen</li> <li>✓ Endre visning</li> <li>✓ Rediger og beregne</li> <li>✓ Lagre data som</li> <li>✓ Lagre spørring</li> </ul>	<span>Rotér mot venstre</span> <span>Rotér mot høyre</span> <span>Rotér manuelt</span> <span>Excel (xlsx)</span> <span>Fullskjerm</span>																																																																
	<table border="1"> <thead> <tr> <th rowspan="2"></th> <th colspan="3">Har IKT-/digitaliseringsstrategi</th> <th colspan="3">IKT-infrastruktur</th> <th colspan="3">Informasjonssikkerhet</th> <th colspan="3">Skytjenester</th> </tr> <tr> <th>2018</th> <th>2020</th> <th>2022</th> <th>2018</th> <th>2020</th> <th>2022</th> <th>2018</th> <th>2020</th> <th>2022</th> <th>2018</th> <th>2020</th> <th>2022</th> </tr> </thead> <tbody> <tr> <td>Har strategien</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Fylkeskommuner</td> <td>93,8</td><td>87,5</td><td>60,0</td><td>86,7</td><td>100,0</td><td>66,7</td><td>93,3</td><td>100,0</td><td>83,3</td><td>80,0</td><td>85,7</td><td>83,3</td> </tr> <tr> <td>Kommuner</td> <td>67,9</td><td>73,8</td><td>74,3</td><td>89,5</td><td>85,8</td><td>80,6</td><td>93,8</td><td>94,2</td><td>94,7</td><td>76,6</td><td>84,2</td><td>84,8</td> </tr> </tbody> </table>		Har IKT-/digitaliseringsstrategi			IKT-infrastruktur			Informasjonssikkerhet			Skytjenester			2018	2020	2022	2018	2020	2022	2018	2020	2022	2018	2020	2022	Har strategien													Fylkeskommuner	93,8	87,5	60,0	86,7	100,0	66,7	93,3	100,0	83,3	80,0	85,7	83,3	Kommuner	67,9	73,8	74,3	89,5	85,8	80,6	93,8	94,2	94,7	76,6	84,2	84,8
	Har IKT-/digitaliseringsstrategi			IKT-infrastruktur			Informasjonssikkerhet			Skytjenester																																																							
	2018	2020	2022	2018	2020	2022	2018	2020	2022	2018	2020	2022																																																					
Har strategien																																																																	
Fylkeskommuner	93,8	87,5	60,0	86,7	100,0	66,7	93,3	100,0	83,3	80,0	85,7	83,3																																																					
Kommuner	67,9	73,8	74,3	89,5	85,8	80,6	93,8	94,2	94,7	76,6	84,2	84,8																																																					

Tabell 12036<sup>5</sup> gir også et annet perspektiv på digitalisering i kommunal sektor, nemlig hindringer for utvikling av elektroniske tjenester.

12036: Hindringer for utvikling av elektroniske tjenester (prosent), etter statistikkvariabel, grad av hindring, forvaltningsnivå og år		Er i stor eller ganske stor grad en hindring	
		2020	2022
Mangel på politiske føringer	Fylkeskommuner	..	..
	Kommuner	14,5	8,2
Mangel på engasjement hos ledelsen	Fylkeskommuner	..	10,0
	Kommuner	12,6	12,1
Lovgivning og regler mangler tilpasning	Fylkeskommuner	12,5	50,0
	Kommuner	19,1	19,2
Mangel på felles standarder for datautveksling	Fylkeskommuner	37,5	40,0
	Kommuner	44,9	34,2
Mangel på felles offentlige løsninger og infrastruktur	Fylkeskommuner	25,0	40,0
	Kommuner	50,2	44,9
Vanskelig å integrere eksisterende IT- og fagsystemer med digital forvaltning	Fylkeskommuner	62,5	40,0
	Kommuner	46,8	47,7
Vanskelig å frigjøre ressurser til utvikling	Fylkeskommuner	87,5	70,0
	Kommuner	74,8	72,9
IKT-utgifter høyere enn forventet	Fylkeskommuner	25,0	40,0
	Kommuner	43,4	54,0
Manglende kompetanse i virksomheten	Fylkeskommuner	62,5	30,0
	Kommuner	45,8	49,7
Avhengig av utvikling hos andre virksomheter	Fylkeskommuner	37,5	40,0
	Kommuner	58,5	47,7

Ved å se disse tre tabellene under ett og koble dette med tilbakemeldingene fra kommunene gjennom kunnskapsinnhenting og dialog i forbindelse med denne rapporten, er det mulig å konkludere med at kommunal sektor har behov for å styrke kompetansenivået på dette området. Dette inkluderer behov for bistand til hvordan man kan innføre og utfase teknologi på en god måte som både understøtter og utvikler kommunal virksomhet.

### Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelsehåndtering og beredskaps- og gjenopprettingsevne

I media kan man nærmest daglig lese om dataangrep og hendelser mot norske virksomheter, herunder også kommuner.

<sup>4</sup> <https://www.ssb.no/statbank/table/12019/tableViewLayout1/>

<sup>5</sup> <https://www.ssb.no/statbank/table/12036/tableViewLayout1/>



Tabell 12617<sup>6</sup> under gir en indikasjon på sikkerhetsproblemer i kommunal sektor.

12617: IKT-sikkerhetsproblemer (prosent), etter statistikkvariabel, status for sikkerhetsproblemet, forvaltningsnivå og år		Har vært utsatt for sikkerhetsproblemet		Ukjent/ikke relevant	
		2019	2022	2019	2022
Sammenbrudd i forbindelsen til internett eller andre eksterne nettverk	Fylkeskommuner	18,8	30,0	..	..
	Kommuner	17,3	17,8	5,0	3,4
Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid	Fylkeskommuner	6,3	10,0	..	..
	Kommuner	10,5	2,0	8,0	5,6
Angrep av typen 'denial of service'	Fylkeskommuner	62,5	30,0	..	..
	Kommuner	11,3	9,6	13,3	8,8
Uautorisert tilgang til systemer eller data	Fylkeskommuner	31,3	50,0	6,3	10,0
	Kommuner	6,3	16,4	20,3	13,8
Datatap pga manglende backup	Fylkeskommuner	..	10,0	..	..
	Kommuner	4,5	0,8	8,8	4,8
IT-misbruk av økonomisk karakter	Fylkeskommuner	..	10,0	..	..
	Kommuner	6,8	7,9	10,0	6,8
Forsøk på identitetstyveri (phishing)	Fylkeskommuner	68,8	90,0	6,3	..
	Kommuner	52,1	65,3	17,8	13,0
Virksomhetens IKT-utstyr har kommet på avveie	Fylkeskommuner	50,0	50,0	37,5	10,0
	Kommuner	19,3	18,9	16,3	15,8

Det er altså hevet over enhver tvil at kommunene er, og har vært utsatt for sikkerhetsproblemer, jf dataangrep og hendelser i kommunal sektor. Det som også er interessant er andelen av kommuner som melder at sikkerhetsproblemer er ukjent. At det er ukjent om hendelser har oppstått eller ikke er en indikator på manglende rapporteringsmetodikk og/eller evne til å fange opp hendelser, noe som også underbygger funnene beskrevet under styringsevne over.

Tabell 12618<sup>7</sup> nedenfor gir en indikasjon på hvilke tiltak kommunal sektor har gjort for å øke sikkerheten og robustheten. Tiltakene i tabellen stemmer i stor grad med NSM sine grunnprinsipper<sup>8</sup> for IT-sikkerhet. Tabellen gir ikke informasjon om dybden eller effekten av tiltakene.

12618: Tiltak for IKT-sikkerheten (prosent), etter statistikkvariabel, status for tiltak, forvaltningsnivå og år		%	
		2019	2021
Oppbevaring av backup på annen lokalitet enn driftsmiljøet	Fylkeskommuner	100,0	100,0
	Kommuner	90,5	82,6
Rutinemessige tester som verifiserer at back-up ikke er korrupt eller manipulert	Fylkeskommuner	87,5	60,0
	Kommuner	60,9	65,5
Nødstrømsanlegg	Fylkeskommuner	75,0	90,0
	Kommuner	75,4	77,5
Program for avdekking og varsling av uønsket/uventet trafikk	Fylkeskommuner	75,0	80,0
	Kommuner	60,9	59,8
Program for avdekking av identitetstyveri (phishing)	Fylkeskommuner	68,8	80,0
	Kommuner	51,9	60,4
Rutinemessige penetrasjonstester på interne systemer	Fylkeskommuner	37,5	40,0
	Kommuner	29,3	30,8
Rutiner for installering av sikkerhetspatcher på systemer	Fylkeskommuner	100,0	100,0
	Kommuner	80,5	82,9
Nødløsning for kommunikasjon (alternativer for data- og telekommunikasjoner)	Fylkeskommuner	68,8	80,0
	Kommuner	73,7	73,8
Tofaktor-autentisering for ansatte ved ekstern innlogging til virksomhetens IKT-systemer	Fylkeskommuner	81,3	90,0
	Kommuner	59,4	77,8
Rollebasert brukersystem: en ansatt skal bare ha tilgang til området han/hun arbeider med (Least privilege prinsipp)	Fylkeskommuner	100,0	80,0
	Kommuner	86,2	84,9
Sentrale loggtjenester	Fylkeskommuner	87,5	60,0
	Kommuner	60,2	61,5
Tekniske tiltak for behandling av sensitive data (f. eks. kryptering, digital signering)	Fylkeskommuner	87,5	90,0
	Kommuner	70,2	74,6
Kryptering av virksomhetens bærbare IKT-utstyr	Fylkeskommuner	50,0	40,0
	Kommuner	20,8	28,5

Situasjonsbeskrivelsen som kommer frem ved å analysere tabellen kan sies å være noe bedre enn det som fremsettes muntlig i dialog med kommunene. Samtidig viser tabellen med all tydelighet at selv i 2021 er det mer enn 60 kommuner som ikke har noe så grunnleggende som rutiner for installering av sikkerhetspatcher på systemer på plass, og mer en 240 kommuner har ikke

<sup>6</sup> <https://www.ssb.no/statbank/table/12617/tableViewLayout1/>

<sup>7</sup> <https://www.ssb.no/statbank/table/12618/tableViewLayout1/>

<sup>8</sup> <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt>



rutinemessig penetrasjonstesting internt. Fravær av det første tiltaket øker sårbarhetsflaten og det vil være sannsynlig at disse kommunene kan bli rammet av for eksempel løsepengevirus. Hvis man regner disse kommunene inn i de som ikke gjennomfører penetrasjonstesting internt er det fortsatt mer enn 150 kommuner som ikke kjenner til sin faktiske tilstand på infrastrukturen.

Digdirs rapport fra 2020 trekker også frem tall fra 2018 som DSB har innhentet. Disse tallene er trolig bedre i 2023, men i dialog med kommunene har det kommet frem at situasjonen fra 2018 ikke har endret seg betydelig: «At under 25 % av både fylkeskommuner og kommuner gjennomfører beredskapsøvelser knyttet til informasjonssikkerhet, indikerer at øvelser ikke gjennomføres i tilstrekkelig grad. Dette indikerer at både fylkeskommuner og kommuner i stor grad trenger hjelp til å komme i gang med å gjennomføre jevnlig øvelser knyttet til informasjonssikkerhet.»

## Oppsummering

Det er i stor grad sammenfall mellom de funn Riksrevisjonen, Digitaliseringsdirektoratet, DSB og KS har av funn og det kommunene selv rapporterer som behov. Situasjonen og dermed behovet for den enkelte kommune divergerer fra andre, og det er dermed ikke mulig å trekke en enkelt konklusjon på tilstand. Tiltak som bør innføres må dermed adressere alle behov. Dette innebærer at det i gjennomføring av tiltak må tas høyde for kommunenes ulike situasjon.