Difi
Direktoratet for
forvaltning og ikt

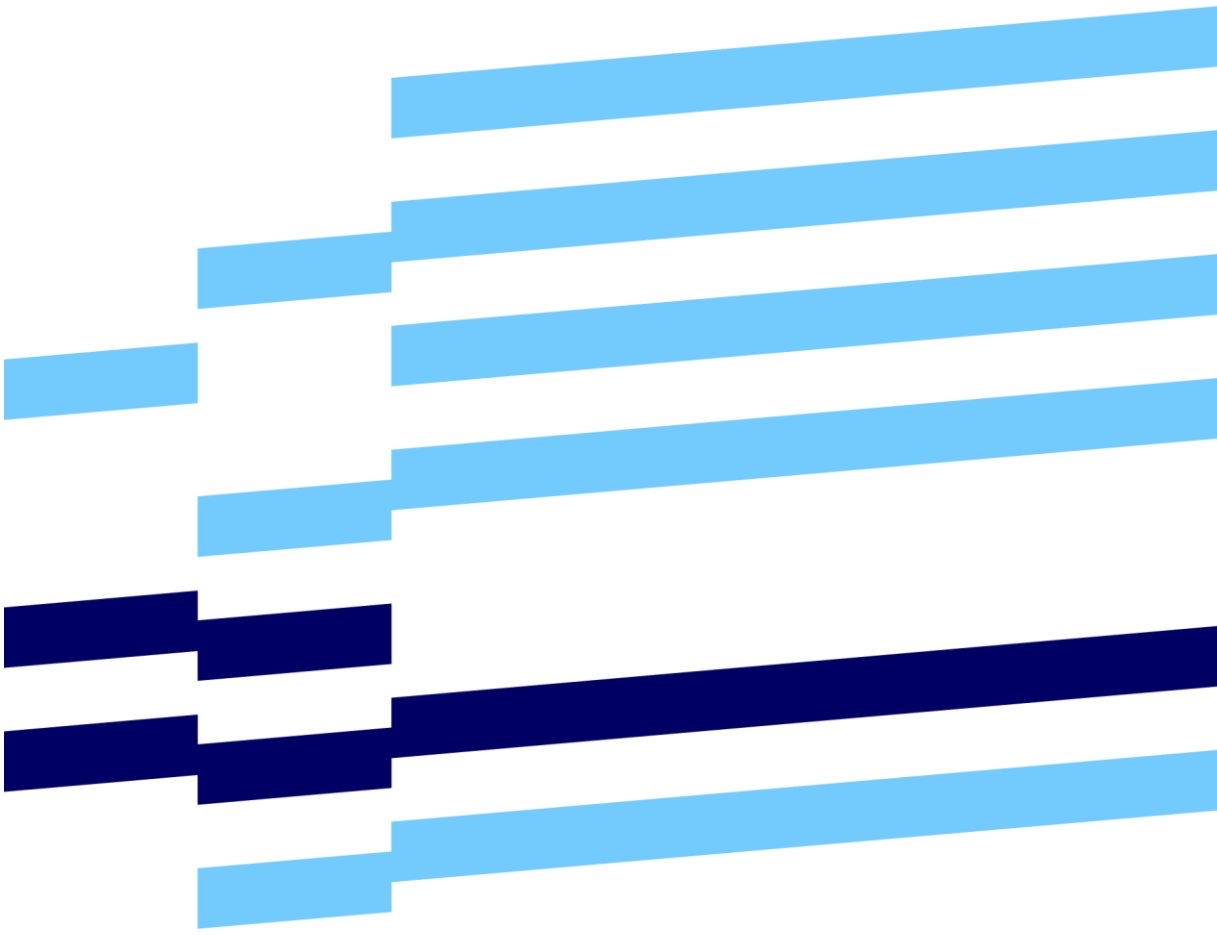
Difi-rapport

ISSN 1890-6583

2018:4

Arbeidet med informasjonssikkerhet i statsforvaltningen

Kunnskapsgrunnlag



Forord

Direktoratet for forvaltning og ikt (Difi) har på oppdrag fra Kommunal- og moderniserings-departementet (KMD) fremskaffet et kunnskapsgrunnlag på hvordan statsforvaltningen arbeider med informasjonssikkerhet.

Vi vil takke alle informantene som har besvart spørreskjema og bidratt med kunnskap og synspunkter i intervjuer.

Difi står ansvarlig for innholdet i notatet. Håkon Styri har vært prosjektleder. Barbro Lugnfors har vært ansvarlig for informasjonsinnhenting. BDO og Difi har stått for informasjons-innhenting og analysearbeid. Seksjonssjef Øyvind Grinde har vært prosjektansvarlig.

Oslo, 23.03.2018

Grete Orderud
avdelingsdirektør

Innhold

Sammendrag

Vår vurdering er at en av tre statlige virksomheter ikke har tilstrekkelig styring og kontroll på informasjonssikkerhet, og departementet etterspør i liten grad status på arbeidet med informasjonssikkerhet hos underliggende virksomheter.

Formålet med evalueringen, som Difi har gjort på oppdrag for Kommunal- og moderniseringsdepartementet (KMD), er å bidra til et mer fullstendig bilde av tilstanden på informasjonssikkerhetsarbeidet i statsforvaltningen.

KMD har bedt Difi kartlegge, evaluere og gi våre anbefalinger til arbeidet med informasjonssikkerhet i statsforvaltningens virksomheter. KMD skal legge frem en endelig rapport med anbefalinger innen sommeren 2018.

Slik har vi gjennomført oppdraget

Evalueringen belyser hvordan virksomhetene arbeider med informasjonssikkerhet, men den er ikke en kartlegging av selve sikkerhetstilstanden.

KMD sendte spørreskjema til både virksomhetsledere og fagpersoner i et representativt utvalg på 93 statlige virksomheter med ulik størrelse og organisering. 30 virksomheter og 28 etatsstyrere deltok i dybdeintervju for å supplere med kvalitativ informasjon. Vi gjennomførte også en workshop i Nettverk for informasjonssikkerhet (NIFS). Samlet gir våre funn et godt bilde av hvordan statsforvaltningen arbeider med informasjonssikkerhet.

Våre hovedfunn:

- Vår vurdering er at hver tredje statlige virksomhet ikke har tilstrekkelig styring og kontroll på informasjonssikkerheten. Det er stor variasjon på innretning og omfang på styring og kontroll i virksomhetene.
- Intervjuene viser at etatsstyrere i liten grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter. Kun 64 prosent av virksomhetene svarer at informasjonssikkerhet har vært et tema i etatsstyringsdialogen, og 7 prosent sier at det ikke en gang vil omtales i årsrapporten for 2017.
- Kun 40 prosent har kartlagt eller målt sikkerhetskulturen i virksomheten.
- Under halvparten har årlige øvelser. 27 prosent av virksomhetene mangler en IKT-beredskapsplan som er godkjent av virksomhetsleder. Det er positivt at 87 prosent likevel har håndtert hendelser basert på tydelige definerte roller, ansvar og prosedyrer.
- 68 prosent av virksomhetene svarte at de klarer å dekke opp sitt behov for fagkompetanse på området informasjonssikkerhet.
- Virksomhetene arbeider med kompetanseheving på informasjonssikkerhet, men arbeidet er i mange tilfeller lite målrettet og ikke tilpasset virksomhetens egenart og behov.
- Departementenes egenrapportering i 2016 viste at arbeidet med informasjonssikkerhet hadde høy prioritet i alle sektorer. Vår evaluering nyanserer dette bildet. Få departementer har bedt sine underliggende virksomheter analysere

status på informasjonssikkerhet. Bedre rapportering ville gjort det lettere å sammenligne status og se endringer over tid på tvers av virksomheter og sektorer.
- Virksomhetene har liten kjennskap til regelverkene som stiller krav til informasjonssikkerhet, spesielt økonomiregelverket i staten og § 15 i eForvaltningsforskriften. De fleste etatsstyrere nevner regelverket for behandling av personopplysninger som mest relevant.
- 77 prosent av virksomhetslederne mener de i stor grad gir tydelige føringer for arbeidet med informasjonssikkerhet. 51 prosent av de fagansvarlige mener at ledelsen gir tydelige føringer.
- 35 prosent av virksomhetene har retningslinjer for å akseptere risiko. Uten kriterier for hvem som kan akseptere størrelsen på risikoen, er det vanskelig å prioritere ressursbruken mot de risikoene det er viktig å håndtere.
- Mange virksomheter har utfordringer med å etablere og følge opp sikkerhetstiltak. Uten målrettede tiltak, kan tiltakene gi unødvendige kostnader og liten effekt.

Våre viktigste anbefalinger

Vi mener at arbeidet med styring og kontroll av informasjonssikkerhet i virksomhetene må styrkes for å sikre at virksomhetene oppnår tilstrekkelig modenhet og blir bedre rustet til å følge endringer i trusselbildet. Vi mener videre at departementene må stille tydeligere krav til virksomhetenes rapportering av status for å oppnå en koordinert og sektorovergripende styring av informasjonssikkerheten i statsforvaltningen

Vi har 11 anbefalinger som støtter opp under dette. Vi trekker spesielt frem fire prioriterte anbefalinger som raskt kan bidra til å forbedre dagens situasjon. Vi anbefaler at:

- Informasjonssikkerhet følges opp i styringsdialogen mellom departement og underliggende virksomhet. Etatsstyrere bør ha tilgang på veiledning om hvordan informasjonssikkerhet bør ivaretas i etatsstyringen. DFØ og Difi bør samarbeide om å gi denne veiledningen.
- Departementene stiller krav om at virksomhetene rapporterer på sikkerhetstilstanden for egen virksomhet, og status på arbeidet med styring og kontroll av informasjonssikkerhet i årsrapporten. Rapporteringen bør være lik og sammenlignbar for alle statlige virksomheter. DFØ bør i samarbeid med Difi gi veiledning om dette.
- Virksomhetene gjennomfører minst en årlig øvelse innen informasjonssikkerhet. Både planlegging og rapportering av erfaringer fra øvelsen må knyttes opp mot virksomhetens styringssystem for informasjonssikkerhet.
- Virksomheter kartlegger sin kompetanse og sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring.

Alle anbefalingene er beskrevet i kapittel 3 og gjengitt samlet i kapittel 4.1.

1 Innledning

For å treffe godt med politikkutvikling, anbefalinger og veiledere innen informasjonssikkerhet, er et godt kunnskapsgrunnlag viktig. Nasjonal strategi for informasjonssikkerhet ble lansert i desember 2012 med en handlingsplan hvor ett tiltak var etablering av Difis kompetansemiljø for informasjonssikkerhet i statsforvaltningen.

Informasjonssikkerhet er et stort område som spenner fra utvikling av kryptografiske algoritmer til juridiske betraktninger om utlevering av data. Difis rolle er forebyggende informasjonssikkerhet i statsforvaltningen, med fokus på styring og kontroll i henhold til eForvaltningsforskriften § 15, hvor Difi er pekt ut til å gi anbefalinger. Andre sentrale aktører som veileder på området er Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB), Nasjonal kommunikasjonsmyndighet (Nkom), Datatilsynet, Direktoratet for økonomistyring (DFØ). Difi er opptatt av å løse sektor-overgripende utfordringer i samarbeid med aktørene nevnt over.

I september 2015 ble Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017[1] lansert og satte tydelig retning og målsetninger for arbeidet. Handlingsplanens tre delmål er:

1. Befolkningen, næringslivet og forvaltningen skal ha tillit til at alle interne systemer og nettverk, samt alle digitale tjenester som utvikles og driftes i regi av virksomheter i offentlig sektor, er sikre og pålitelige.
2. Fagdepartementene skal ha en felles forståelse om hvilke særskilte utfordringer statsforvaltningen står overfor i forbindelse med utvikling og drift av digitale offentlige tjenester.
3. Ledere, utviklere, driftsansvarlige og brukere ansatt i statsforvaltningen skal få økt kompetanse og bevissthet omkring behovet for informasjonssikkerhet.

Handlingsplanens primære målgruppe er toppledelsen og sikkerhetsansvarlige i alle departementer, med forventning om at føringene i handlingsplanen bringes videre til underlagte virksomheter. Føringer og tiltak er fordelt over fem tiltaksområder:

- styring og kontroll
- sikkerhet i digitale tjenester
- digital beredskap
- sikkerhet i nasjonale felles komponenter
- kunnskap, kompetanse og kultur

I tråd med oppfølgingsplanen for Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017 innhentet Kommunal- og moderniseringsdepartementet (KMD) i 2016, halvveis i handlingsplanens virkeperiode, status på departementenes arbeid med handlingsplanen.

[1] https://www.regjeringen.no/no/dokumenter/handlingsplan-for-informasjonssikkerhet-i-statsforvaltningen/id2440093/

Departementenes egenrapportering viste at arbeidet med informasjonssikkerhet hadde høy prioritet i alle sektorer.

1.1 Oppdrag og mandat

KMD ba i brev av 8.9.2017 Difi om å evaluere arbeidet med informasjonssikkerhet i statsforvaltningen. Arbeidet skulle bidra til et mer fullstendig bilde av tilstanden på informasjonssikkerhetsarbeidet i statsforvaltningen, enn statusrapporten som ble utarbeidet midtveis i perioden.

En sluttrapport med anbefaling skal fremlegges for regjeringen innen sommeren 2018. KMD har bedt Difi bidra i innhentingen av opplysninger fra statsforvaltningens virksomheter, evaluering, og forslag til tiltak for videre arbeid med informasjonssikkerhet i forvaltningen.

Det legges til grunn at utfallet av evalueringsprosjektet også vil være nyttig for det videre arbeidet med ny nasjonal strategi for IKT-sikkerhet[2] og IKT-sikkerhetsutvalget[3]. Slutt-rapporten, og behandlingen av denne, vil inngå som en del av det faglige grunnlaget for de satsinger og prioriteringer regjeringen planlegger innen fagområdet informasjonssikkerhet i statsforvaltningen.

1.2 Formål og avgrensning

Difi har valgt å organisere arbeidet som et prosjekt. Formålet med prosjektet er å danne et kunnskapsgrunnlag om arbeidet med informasjonssikkerhet i statsforvaltningen slik at resultatet av handlingsplanen kan evalueres.

Overordnet vurderer prosjektet hvorvidt underliggende virksomheter i statsforvaltningen etterlever kravene til internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som stilles i eForvaltningsforskriften §15.

Spørsmålene i kartleggingen er utformet slik at de tar hensyn til at virksomhetene har ulik størrelse, formål og organisering. Ved utforming av spørsmålene har Difi tatt hensyn til hvilke opplysninger som innhentes i andre kartlegginger, som for eksempel Statistisk sentralbyrås statistikk på bruk av IKT i staten, Justis- og beredskapsdepartementets kartlegging av sikkerhetstilstanden og Norsk senter for informasjonssikrings (NorSIS) undersøkelse av sikkerhetskultur, slik at opplysninger som allerede er innhentet kan gjenbrukes.

[2] Statsminister Erna Solbergs åpningstale på Justis- og beredskapsdepartementets og Forsvarsdepartementets strategikonferanse i forbindelse med utarbeidelse av ny nasjonal strategi for IKT-sikkerhet, Høyres Hus, 6. mars 2018. https://www.regjeringen.no/no/aktuelt/nasjonal-strategi-for-ikt-sikkerhet/id2592996/

[3] https://www.regjeringen.no/no/dep/jd/org/styre-rad-og-utval/tidsbegrensede-styrer-rad-og-utvalg/IKT-sikkerhetsutvalget/id2570775/

I evalueringen er vi interessert i hvordan virksomhetene arbeider med informasjonssikkerhet, og vi har ikke analysert sikkerhetstilstanden. For eksempel har vi kartlagt hvordan virksomhetene arbeider med å oppnå den sikkerhetskulturen de ønsker, men vi har ikke forsøkt å kartlegge sikkerhetskulturen i virksomhetene.

2 Metode og gjennomføring

2.1 Overordnet metodebeskrivelse

Vi har tatt utgangspunkt i målsetningene som er formulert i handlingsplanens fem tiltaksområder:

- styring og kontroll
- sikkerhet i digitale systemer og tjenester
- digital beredskap
- nasjonale felleskomponenter
- kunnskap, kompetanse og kultur

Innhenting av informasjon

Det første tiltaksområdet, styring og kontroll, er det mest omfattende og griper også inn i de fire andre tiltaksområdene. For være i stand til å danne et godt bilde av området styring og kontroll valgte vi å hente informasjon fra tre nivåer:

- Etatsstyrere er det øverste nivået vi ønsket informasjon fra, for å få innsikt i departementenes koordinering og oppfølging på området informasjonssikkerhet.
- Virksomhetsledelse, hvor vi i utgangspunktet ønsket informasjon fra virksomhetenes direktører. Det er på dette nivået det er mulig å få bekreftet at styring og kontroll på informasjonssikkerhetsområdet har tilstrekkelig ledelsesforankring, og hvilken betydning temaet informasjonssikkerhet har i etatsstyringsdialogen.
- Teknisk og operativt nivå i statsforvaltningens virksomheter, hvor vi ønsket informasjon fra den person som er utpekt som fagansvarlig for informasjonssikkerhet i virksomheten.

Vi valgte å hente inn informasjon fra fagansvarlig for informasjonssikkerhet ved bruk av et skriftlig spørreskjema. For innhenting av informasjon fra virksomhetsledere ble det også brukt spørreskjema. Spørreundersøkelsene ble sendt ut fra KMD til et utvalg på 93 virksomheter. Denne informasjonen ble supplert med intervjuer i 30 virksomheter som utgjør en kvalitativ del av undersøkelsen. For innhenting av informasjon fra etatsstyrere var det ønskelig å intervjue etatsstyrer for hver av virksomhetene som ble intervjuet.

For utforming av spørreskjema og intervjuguider formulerte vi 11 indikatorer med grunnlag i de fem tiltaksområdene i handlingsplanen, se vedlegg 1.

Analyse

Vi har delt analysen inn i et antall vurderingstema utledet fra handlingsplanens tiltaks-områder, indikatorene som ble formulert for innhenting av informasjon og standarden ISO/IEC 27001. For en beskrivelse av hvert vurderingstema, se underkapittel 2.2. For hvert av vurderingstema har vi gjort objektive observasjoner og subjektive vurderinger. Med utgangspunkt i hver av vurderingene har vi foreslått anbefalinger for fremtidige tiltak på området.

Arbeidsmetoden for analyse av informasjonen er som beskrevet over foretatt i følgende tre trinn:

Trinn 1. Uttrekk av relevante objektive observasjoner fra innhentet informasjon
Trinn 2. Vurdering av observasjonene fra første trinn
Trinn 3. Foreslå anbefalte tiltak basert på vurderingene i annet trinn

Deretter er vurderingene for hvert tema sammenfattet i en helhetlig vurdering fulgt av et utvalg anbefalinger Difi har vurdert at bør få prioritet.

Hva denne tilnærmingen ikke dekker

Virksomhetene i statsforvaltningen dekker et stort spenn med hensyn til størrelse og organisering. Det er derfor vanskelig å utforme en metode som er egnet for analyse av alle virksomhetene. Utfordringen for modellen vi har valgt er de største etatene som er organisert med etatsledelse i et direktorat og et antall underordnede virksomheter. Et eksempel er Politietaten, hvor vår informasjonsinnhenting henvendte seg til Politidirektoratet. Dette vil gi oss et godt bilde av arbeidet med informasjonssikkerhet i direktoratet, men i svært begrenset grad gi noen innsikt i tilstanden for arbeidet med informasjonssikkerhet i etaten som helhet.

Våre forslag til anbefalte tiltak for videre arbeid med informasjonssikkerhet i forvaltningen er ikke utredet hva gjelder økonomiske og administrative konsekvenser.

2.2 Evalueringskriterier

Vår utfordring har vært å gjøre en analyse som gir et helhetlig inntrykk av arbeidet med informasjonssikkerhet i statsforvaltningen. En annen løsning ville vært å analysere hver enkelt virksomhet for seg, og vurdere i hvilken grad den etterlever et sett evalueringskriterier som kan utledes fra Difis anbefalinger og standarden NS-ISO/IEC 27001:2013. Dessverre krever denne tilnærmingen langt mer tid og ressurser enn dette prosjektet har til rådighet.

Innsamlingen av informasjon tok utgangspunkt i 11 indikatorer som er beskrevet i vedlegg 1. For bedre leselighet har vi valgt å dele analysen i følgende 7 vurderingstemaer:

- styring og kontroll (internkontroll)
- risikostyring
- beredskap, øvelser og hendelseshåndtering
- nasjonale felleskomponenter
- sikkerhetskompetanse
- sikkerhetskultur
- etatsstyringsdialogen

En detaljert beskrivelse av hvert vurderingstema finnes som innledning til hvert underkapittel i denne rapportens analysedel.

Styring og kontroll

Styring og kontroll er det mest omfattende vurderingstemaet, og de faktorer som er relevante å se på her er det vi oppfatter som kjernen i styringssystemet for informasjonssikkerhet. Vi

har sett på følgende faktorer når vi har vurdert virksomhetenes arbeid med styring og kontroll:

- **Lederforankring** («tonen på toppen») omfatter hvilke føringer som er gitt fra ledelsen og hvilke roller er definert.
- **Innretning og omfang** av virksomhetens systematiske arbeid med styring og kontroll av informasjonssikkerhet.
- **Organisering** av arbeidet med informasjonssikkerhet i virksomheten. Følger dette arbeidet linjen, og er det etablert nødvendige støttefunksjoner. Er roller og ansvar tydelige?
- **Rapportering** av arbeidet med informasjonssikkerhet til virksomhetens ledelse. Skjer det tilstrekkelig og regelmessig rapportering?
- **Oppfølging og kontinuerlig forbedring** av virksomhetens arbeid med informasjonssikkerhet. Følger ledelsen opp arbeidet med revisjoner og evalueringer, legges det til rette for forbedringer og beslutter ledelsen endringer på de områder hvor det er avdekket at det er nødvendig?
- Føres det **tilsyn** med virksomhetens arbeid med informasjonssikkerhet eller med deler av dette arbeidet?
- Hvilke **regelverk** er relevante for virksomhetens arbeid med informasjonssikkerhet?

Risikostyring

Risikostyring omfatter to faktorer som kunne vært en del av vurderingstemaet styring og kontroll, men som er trukket ut som et eget vurderingstema fordi risikostyring er et eget fag som også brukes på mange andre områder i tillegg til informasjonssikkerhet.

I denne rapporten har vi valgt å analysere to faktorer for området risikostyring:

- **Risikovurdering** gjelder kort sagt hvordan virksomhetene beskriver og vurderer operativ risiko. Vi har lagt særlig vekt på virksomhetenes tilnærming til å akseptere risiko.
- **Risikohåndtering** er hva virksomhetene gjør med hver identifiserte risiko, hva som legges til grunn for beslutninger om å akseptere en risiko og hvilken tilnærming virksomheten har til å etablere og forvalte sikkerhetstiltak for å redusere risiko.

Beredskap, øvelser og hendelseshåndtering

I dette vurderingstemaet har vi samlet tre undertema som henger tett sammen. Har virksomheten oppdaterte planer for å håndtere uønskede digitale hendelser[4] og er disse planene godkjent av virksomhetens leder? Har virksomheten definert roller, ansvar og prosedyrer for håndtering av hendelsene? Øver virksomheten regelmessig på håndtering av

[4] Tradisjonelt brukes betegnelsen IKT-hendelser, men vi skriver digitale hendelser der dette er naturlig.

uønskede digitale hendelser? Bruker virksomhetene erfaringene fra øvelser og hendelser til å forbedre planer og sikkerhetstiltak?

Nasjonale felleskomponenter

En stor del av virksomhetene i statsforvaltningen bruker en eller flere nasjonale felleskomponenter[5]. Vi ønsker å få vite hvor stor andel av virksomhetene som er kritisk avhengig av en eller flere av felleskomponentene, og om disse virksomhetene har etablert reserveløsninger som et sikkerhetstiltak mot situasjoner hvor en felleskomponent er midlertidig utilgjengelig.

Sikkerhetskultur

For dette vurderingstemaet er det sentrale spørsmålet hvilket forhold ledelsen har til sikkerhetskulturen i virksomheten. Dette kan uttrykkes som grad av modenhet. Er det gjennomført en kartlegging eller måling av sikkerhetskulturen? Har ledelsen vurdert eller gjennomført tiltak for å endre den eksisterende kulturen? Har man vurdert effekten av eventuelle tiltak?

Kompetanse

Også dette vurderingstemaet gjelder ledelsens forhold til de ansatte og sin egen kompetanse på området informasjonssikkerhet. I analysen ser vi på to typer kompetanse:

- Generell kompetanse skal bidra til risikoforståelse og sikker adferd. Har virksomheten kartlagt medarbeidernes kompetanse? Har man vurdert eller gjennomført tiltak for å heve kompetansen i hele eller deler av virksomheten? Er de kompetansehevende tiltakene generelle eller tilpasset særlige behov.
- Fagkompetanse er nødvendig for å fylle forskjellige stillinger eller utføre oppgaver innenfor fagområdet informasjonssikkerhet. Har virksomheten dekket sitt behov for fagkompetanse? Har medarbeidere behov for kompetanseheving? Får virksomheten rekruttert nye medarbeidere med tilfredsstillende kompetanse for stillingene som er utlyst?

Etatsstyringsdialogen

Etatsstyringsdialogen består av tildelingsbrev, virksomhets- og økonomiinstruks, rapportering samt den løpende dialogen mellom etatstyrer og virksomhetsleder gjennom året. Som vurderingstema ønsker vi å avdekke hvordan informasjonssikkerhet behandles i etatsstyringen og hvordan det kan påvirke prioriteringen i underliggende virksomhet. Vurderingskriteriet er i hvilken grad informasjonssikkerhet og virksomhetens styring og kontroll av denne er en del av etatsstyringsdialogen.

[5] Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter, Administrativ rapport 1 2018

2.3 Empirisk grunnlag

2.3.1 Spørreundersøkelse

Vi tok utgangspunkt i samtlige virksomheter i statsforvaltningen med unntak av den militære delen av forsvaret, og valgte ut alle virksomheter med mer enn 150 ansatte. Deretter ble det gjort et tilfeldig utvalg på åtte virksomheter av varierende størrelse med mindre enn 150 ansatte, slik at undersøkelsen også skal gi kunnskap om de mindre virksomhetene i statsforvaltningen. Deretter ble listen forelagt prosjektets referansegruppe, med deltagere fra alle departementer, for å fjerne virksomheter som var under omfattende omstilling eller som det av andre grunner ikke var ønskelig å ta med i undersøkelsen.

Det ble valgt ut 93 virksomheter. De mottok to spørreundersøkelser i form av skjema som skulle besvares skriftlig. Den ene spørreundersøkelsen besto av 15 spørsmål og var rettet til virksomhetsleder, hvor virksomhetsleder i de fleste virksomhetene har stillingen direktør. Den andre spørreundersøkelsen besto av 39 spørsmål og var rettet til fagansvarlig informasjonssikkerhet. I SSB-undersøkelsen Bruk av IKT i staten publisert i 2017 har 91,1 prosent svart at «en formelt utnevnt person er ansvarlig for informasjonssikkerheten».

Vi fikk svar på 85 prosent av spørreskjemaene rettet til virksomhetsledere. 51 prosent av svarene kom fra virksomhetens leder.

Vi fikk svar på 82 prosent av spørreskjemaene rettet til fagansvarlig informasjonssikkerhet. De 76 svarene fra fagansvarlig informasjonssikkerhet fordelte seg på virksomhetsstørrelse[6] som følger:

ansatte	1-99	100-499	500-999	1000 og flere
svar	**4**	**41**	**14**	**17**

2.3.2 Intervjuer

Av de 93 virksomhetene som fikk undersøkelsen, ble 30 plukket ut for en supplerende kvalitativ informasjonsinnhenting i form av et intervju med virksomhetsleder. Virksomhetene ble valgt ut slik at virksomheter underlagt samtlige departementer ble representert, samtidig som de representerer den samme bredden som det opprinnelige utvalget. Formålet med intervjuene var å fremskaffe utfyllende opplysninger til det som ble innhentet i spørresundesøkelsen.

For alle de 30 virksomhetene som ble intervjuet ble det også avtalt intervju med deres respektive etatsstyrere. Formålet med dette var å belyse etatsstyringsdialogen og hvordan den enkelte etatsstyrer tilrettelegger denne dialogen. 28 av intervjuene med etatsstyrere ble gjennomført.

[6] Spørreskjemaet til fagansvarlig ba om denne informasjonen ettersom virksomhetenes årsrapporter ikke publiseres før etter at dette notatet er ferdigstilt.

2.3.3 Workshop

I forbindelse med et møte i Nettverk for informasjonssikkerhet (NIFS) 21. februar 2018 ble det gjennomført en kort workshop hvor det ble diskutert tre problemstillinger fra spørreundersøkelsen: hendelseshåndtering, fire grunnleggende sikkerhetstiltak og rekruttering.

2.3.4 Dokumenter

Følgende dokumenter er brukt i forbindelse med vurderingen av de innsamlede opplysningene. Enkelte utsagn fra dokumentene er sitert som observasjoner.

- Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017. KMD, 2015
- Kartlegging av fagdepartementenes oppfølging av handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017, Difi 22. mai 2017, 14/01077-20
- Samarbeid og koordinering på informasjonssikkerhetsområdet i nasjonale felleskomponenter, Difi Notat 2017:4
- Statistisk Sentralbyrå, Bruk av IKT i staten, tabell 10852: Statlige virksomheter. Tiltak/rutiner ved administrasjon av IKT-sikkerheten, etter sysselsettingsgruppe (prosent) 2013 – 2017
- Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter, Administrativ rapport 1 2018 (2017–2018)
- Veileder i etatsstyring, Finansdepartementet, november 2011
- IKT-sikkerhet – Et felles ansvar, Meld.St. 38 (2016-2017)
- Risiko i et trygt samfunn – Samfunnssikkerhet, Meld.St. 10 (2016-2917)
- Risiko 2018, Nasjonal sikkerhetsmyndighet, 2018
- Trusselvurdering 2018, Politiets sikkerhetstjeneste, 2018
- Helhetlig IKT-risikobilde 2017, Nasjonal sikkerhetsmyndighet
- Rammeverk for håndtering av IKT-sikkerhetshendelser, NSM (versjon per 07.12.17)
- Regulering av IKT- sikkerhet, NVE rapport nr 26-2017
- Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren, Direktoratet for e-helse, Rapport nr IE-1012, 2017
- Nordmenn og sikkerhetskultur, NorSIS, 2017
- Sammenstilling etter gjennomført evaluering – Terrortrussel mot Norge i juli 2014, Rapport, Ugradert utgave, Justis og beredskapsdepartementet
- Tverrsektoriell evaluering av øvelse IKT16, Direktoratet for samfunnssikkerhet og beredskap, 2017
- IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud, NIFU Rapport 2017:32
- Cyber Europe - the programme of pan-European exercises, ENISA, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
- Hallberg et al: Informationssäkerhet och organisationskultur, Studentlitteratur, 2017

2.4 Definisjoner

2.4.1 IKT-sikkerhet

«Med IKT-sikkerhet forstås beskyttelse av informasjon, tjenester og systemer som er sårbare fordi de er koplet til eller på annen måte er avhengig av IKT. Sikkerhetsmål for IKT-sikkerhet

omfatter tilgjengelighet, integritet og konfidensialitet. IKT-sikkerhet omfatter å forebygge, avdekke og håndtere uønskede digitale hendelser.»[7]

2.4.2 Informasjonssikkerhet

Informasjonssikkerhet handler om å sikre at informasjonen:

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)[8]

2.4.3 Styring og kontroll

Vi skriver styring og kontroll når vi mener de sentrale aktivitetene som normalt inngår i styring og kontroll på informasjonssikkerhetsområdet. Vi benytter det synonymt med styringssystem, ledelsessystem eller internkontroll. Jamfør ISO/IEC 27001:2013 kapittel 4 til 10 og aktivitetene som er beskrevet i Difis veiledning «Internkontroll i praksis – informasjonssikkerhet».

2.4.4 Sikkerhetstiltak

Vi skriver gjennomgående sikkerhetstiltak når vi mener de varige tiltakene som etableres for å ivareta konfidensialitet, integritet eller tilgjengelighet i informasjonsbehandlingen. Dette er normalt tiltak som velges og etableres ved bruk av aktivitetene risikovurdering og risiko-håndtering. Det er synonymt med det engelske begrepet «security control». For eksempler, se innholdet i tiltaksbanker som ISO 27002 (ISO 27001 Annex A) og NIST SP 800-53 rev 4 Appendix F.

2.4.5 Merknad om begrepsbruk fra informasjonsinnhenting og analyse

Under arbeidet med informasjonsinnhenting og analyse har vi merket oss at det er veldig variert bruk og forståelse av begreper som informasjonssikkerhet, IKT-sikkerhet, cyber-sikkerhet og datasikkerhet. Enkelte snakker utelukkende IKT-sikkerhet, mens andre er mer bevisste på forskjellen mellom, og omfanget av, disse begrepene. Dette kan skyldes at det på overordnet nivå kan synes å være uklare skiller mellom disse begrepene. Dette gjelder både innenfor meldingsarbeid, regelverksarbeid og det nasjonale strategiarbeid.

Variert bruk og forståelse av de overnevnte begrepene har medført usikkerhet knyttet til observasjoner og vurderinger i vår analyse av arbeidet med informasjonssikkerhet i statsforvaltningen.

Difi benytter som regel begrepet «informasjonssikkerhet» om sikring av informasjons-behandling. «IKT-sikkerhet» brukes ofte synonymt med «informasjonssikkerhet», både i dagligtale og i styringen av området. I mer stringent begrepsbruk vil imidlertid «IKT-sikkerhet» kunne forstås som et sub-sett av «informasjonssikkerhet», slik at kun

[7] «Ønske om innspill til IKT-sikkerhetsutvalget», brev fra utvalget datert 9. januar 2018

[8] https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet

informasjonssikkerhetshendelser som er direkte knyttet til IKT-utstyr er omfattet. Vi skiller ikke mellom disse begrepene i våre merknader.

Når det gjelder styring og kontroll brukes begrepet informasjonssikkerhet i standarden «NS-ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet». I eForvaltningsforskriften § 15 brukes begrepet internkontroll, og i sikkerhetsloven er begrepet sikkerhetsadministrasjon definert som internkontroll. I denne rapporten har vi valgt å bruke begrepet styringssystem for informasjonssikkerhet. Her er det et behov for å samordne begrepsbruken i forskjellige regelverk.

3 Analyse av de enkelte vurderingstemaene

Evalueringen er delt inn i syv områder som er sentrale i arbeidet med informasjonssikkerhet. Hvert område er delt inn i beskrivelse av vurderingstema, observasjoner, vurderinger og anbefalinger.

Vi vurderer om virksomhetene arbeider systematisk med disse områdene for å oppnå god informasjonssikkerhet på en kostnadseffektiv måte.

3.1 Styring og kontroll

Økonomiregelverket har grunnleggende styringsprinsipper der alle virksomheter skal:

- fastsette mål og resultatkrav innenfor rammen av disponible ressurser og forutsetninger gitt av overordnet myndighet
- sikre at fastsatte mål og resultatkrav oppnås, ressursbruken er effektiv og at virksomheten drives i samsvar med gjeldende lover og regler, herunder krav til god forvaltningsskikk, habilitet og etisk adferd
- sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag

Ledere på alle nivå skal sikre at virksomheten når sine samlede mål. Dette forutsetter at ledere har tilstrekkelig kontroll på risikoene innen de mål og arbeidsoppgaver som de og deres organisatoriske enhet har ansvaret for – inkludert informasjonssikkerhetsrisiko.

På informasjonssikkerhetsområdet skal virksomhetene ifølge eForvaltningsforskriften § 15 ha:

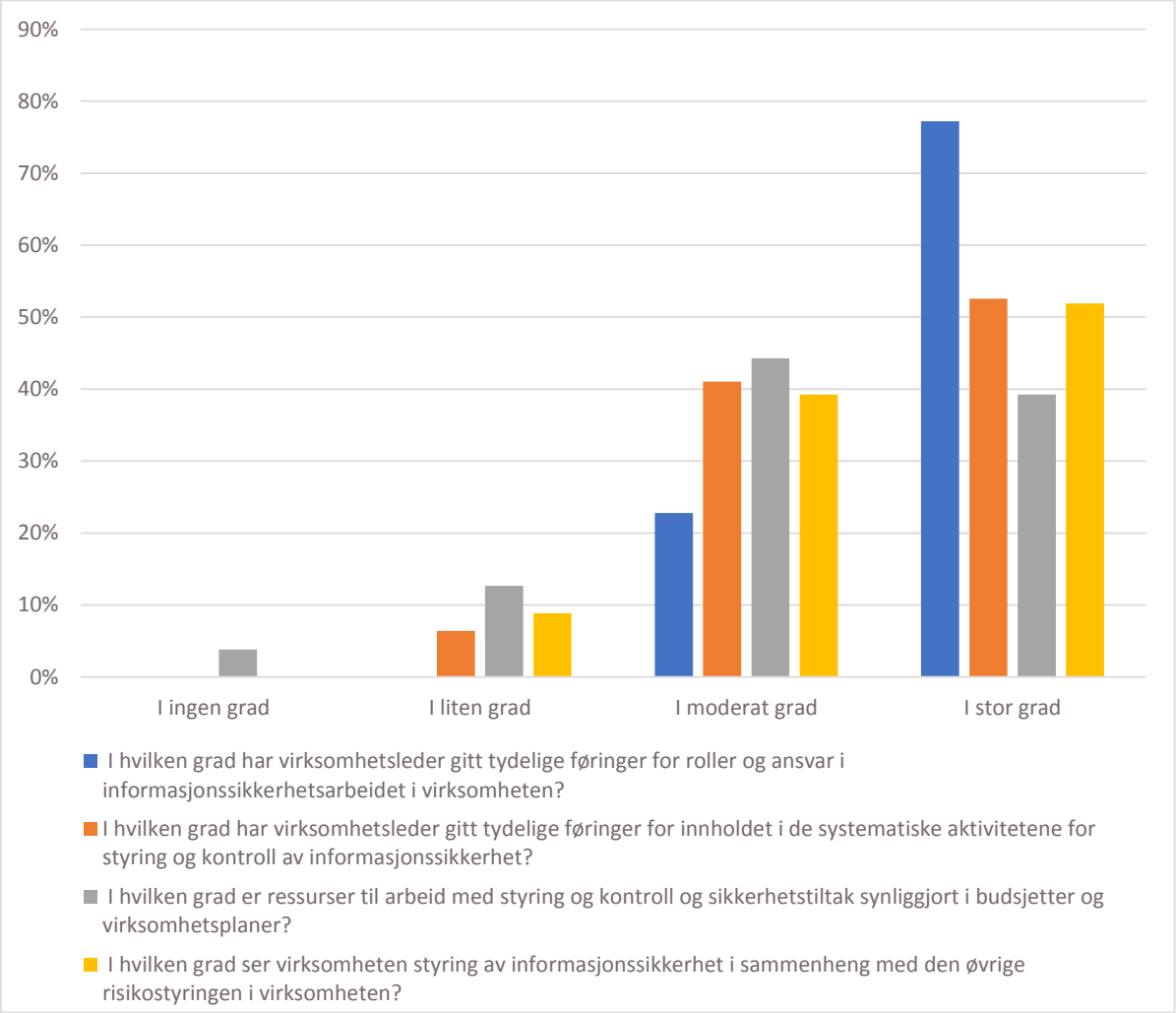
- sikkerhetsmål
- sikkerhetsstrategi
- internkontroll (styring og kontroll) basert på anerkjent standard

Bestemmelsen presiserer at internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. I praksis betyr det at internkontrollen bør ses i sammenheng med den generelle virksomhetsstyringen.

Difi er utpekt til å gi anbefalinger på området, og anbefaler i Referansekatalogen[9] å basere seg på ISO/IEC 27001:2013 og Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet».

[9] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet

3.1.1 Observasjoner for styring og kontroll



Figur 1 - Internkontrollspørsmål besvart av virksomhetsledelsen

Forankring – Tonen på toppen

Føringer fra ledelsen er avgjørende for styring og kontroll på informasjonssikkerhetsområdet. Styringssystem for informasjonssikkerhet er ledelsens verktøy for å ha tilstrekkelig styring og kontroll på området, og kan ikke være forankret eller ledet fra noe annet sted i virksomheten. Dersom ledelsen ikke tar informasjonssikkerhet på alvor, blir dette fort synlig for de ansatte. En konsekvens er da ofte at organisasjonen får problemer med å lykkes med etablering og gjennomføring av systematiske aktiviteter. Vi har følgende observasjoner knyttet til forankring av arbeidet med styring og kontroll av informasjonssikkerhet:

- 77 prosent av respondentene i spørreundersøkelsen rettet mot virksomhetsleder oppgir at de i stor grad har gitt føringer for roller og ansvar i informasjonssikkerhets-arbeidet, mens de resterende 23 prosent sier de i moderat grad har gitt slike føringer.
- Videre svarer 53 prosent av virksomhetsledere at det i moderat grad, og 41 prosent i stor grad, er gitt føringer for innholdet i de systematiske aktivitetene for styring og kontroll. De fagansvarlige svarer 49 prosent i stor grad, 46 prosent i moderat grad og

5 prosent i liten grad på tilsvarende spørsmål. I intervjuene kommer det frem at innholdet i de systematiske aktivitetene for styringen og kontroll av informasjonssikkerhet ofte kan være mangelfulle eller utydelige.
- På oppfølgingsspørsmålet «Gi gjerne noen eksempler på hvordan det er gitt tydelige føringer» trekkes det frem ulike virkemidler. Noen av de mest nevnte er informasjonssikkerhetspolicy, instrukser/retningslinjer eller andre styrende dokumenter, samt fokus på ledelsens gjennomgang og risikovurderinger.
- Difis erfarer at tonen på toppen i vesentlig grad påvirker arbeidet med styring og kontroll. I dialog med Difi gir NSM og NorSIS uttrykk for det samme.

Innretning og omfang

Ulike aspekter må inngå i en virksomhets systematiske arbeid med styring og kontroll av informasjonssikkerhet. Man må ta hensyn til ulike behov knyttet til sikring av konfidensialitet, integritet og tilgjengelighet av informasjon, og i størst mulig grad se styringen i sammenheng med den helhetlige virksomhetsstyringen. Videre må ledelsen sørge for at det tilføres tilstrekkelig ressurser – både i form av økonomiske rammer og ressurser. I tillegg bør innretningen basere seg på en anerkjent standard for styring og kontroll av informasjonssikkerhet. Vi har følgende observasjoner knyttet til disse aspektene:

- I intervjuene fremkommer det at virksomhetene styrer og leder arbeidet med informasjonssikkerhet på en rekke forskjellige måter.
- I intervjuene fremkommer det at forståelsen og omfanget av informasjonssikkerhetsarbeidet varierer relativt mye blant virksomhetene. Noen virksomheter er primært opptatt av viktigheten av å ha kritisk informasjon tilgjengelig, mens flertallet er mest opptatt av behovet for å sikre konfidensialitet. Få nevner integritet som en egenskap som skal sikres.
- I spørreundersøkelsen til både virksomhetsledere og fagmiljø svarer henholdsvis 52 prosent og 47 prosent av respondentene at de i stor grad ser styringen av informasjonssikkerhet i sammenheng med den øvrige risikostyringen i virksomheten (se Figur *2*).

Figur 2 - I hvilken grad ser virksomheten styring av informasjonssikkerhet i sammenheng med den øvrige risikostyringen i virksomheten, fordelt på virksomhetsleder og fagansvarlig

- Mens 17 prosent av respondentene i spørreundersøkelsen rettet mot virksomhetsleder oppgir at de i ingen eller liten grad synliggjør ressurser til arbeid med styring og kontroll og sikkerhetstiltak i budsjetter og virksomhetsplaner, sier 39 prosent at de i stor grad gjør dette. På oppfølgingsspørsmålet «Gi gjerne noen eksempler på hvordan arbeidet synliggjøres» er en *egen enhet* (eller egne midler) eller *utpekt dedikert personell* de virkemidlene som trekkes frem av flest respondenter (ca. 30 prosent). Enkelte respondenter trekker frem at ressurser allokert til informasjonssikkerhet inngår som en del av den ordinære driften til enhetene, og at det derfor ikke spesifiseres i budsjetter. Egne budsjetter for prosjekter og tiltak trekkes også frem som måter å synliggjøre ressursbruk på.

Organisering

Ansvaret for informasjonssikkerhet og tilhørende internkontrollarbeid bør som hovedregel følge linjen. For å understøtte ledere på forskjellige nivåer, må virksomheten etablere nødvendige støttefunksjoner. Sammen med linjen utgjør dette det man kan kalle sikkerhetsorganisasjonen i virksomheten. Roller og ansvar må være tydelige. Vi har følgende observasjoner knyttet til organiseringen av arbeidet med informasjonssikkerhet:

- I SSBs undersøkelse om bruk av IKT i staten (2017) svarer 91 prosent av virksomhetene at de formelt har utpekt en person som ansvarlig for informasjonssikkerheten. Dette stemmer overens med inntrykket fra intervjuene, men intervjuobjektene var uklare på hva rollen som fagansvarlig informasjonssikkerhet innebærer.

- I intervjuene fremkommer det store variasjoner i hvordan virksomhetene har organisert informasjonssikkerhetsarbeidet. Forskjellene gjør seg gjeldende både med tanke på hvilke roller som er definert, hvordan ansvaret er fordelt og hvordan rollene er plassert i organisasjonen. Noen har egne sikkerhetsenheter, mens andre har mer distribuerte sikkerhetsstrukturer. Enkelte virksomheter legger informasjonssikkerhets-arbeidet direkte i IT- eller IKT-avdelingen, mens andre har organisert rollen som fagansvarlig informasjonssikkerhet uavhengig av IT.
    - Hos Mattilsynet ligger det operative sikkerhetsansvaret i linjen, og informasjonssikkerhetsarbeidet løses på lavest mulig nivå. Denne virksomheten har opprettet et eget sikkerhetsutvalg med sikkerhetsleder, bestående av 5-6 personer, noe virksomheten mener har forbedret fokus på, og arbeidet med, styring av informasjonssikkerheten betraktelig.
- I spørreskjema for fagansvarlig har respondentene angitt hvor mange personer i virksomheten som arbeider med fagområdet informasjonssikkerhet. Antallet her spenner fra 0 til 24 personer, og var uavhengig av virksomhetens størrelse.

Rapportering

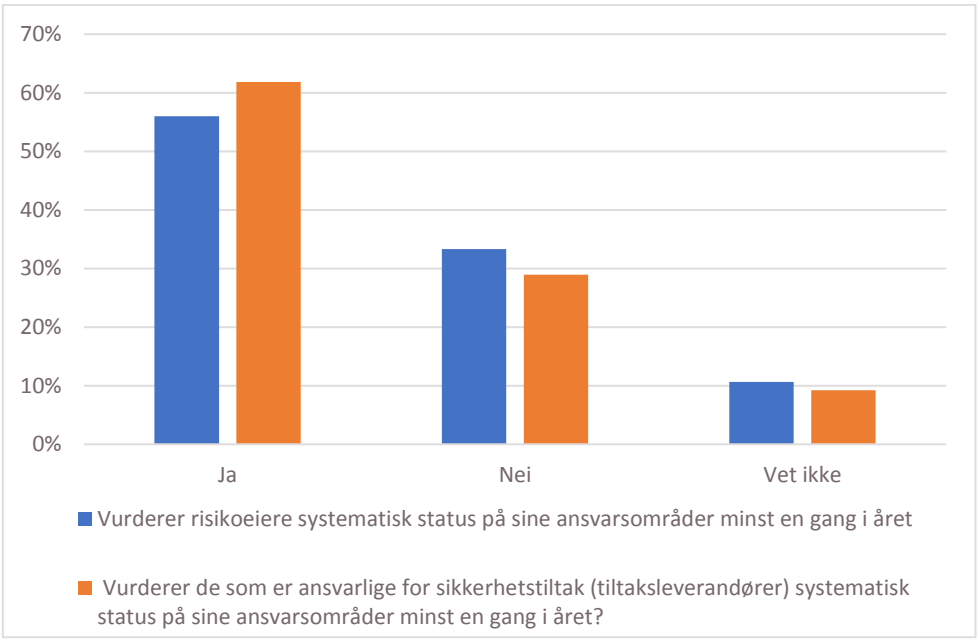
For å kunne følge opp styringssystemet sitt må ledelsen sørge for at de jevnlig, og ved behov, får tilstrekkelig informasjon om status. Det kan være på arbeidet generelt, spesifikke områder ledelsen er spesielt interessert i, og områder der det er behov for endringer, prioritering eller andre beslutninger fra ledelsen. Vi har følgende observasjoner knyttet til rapportering av arbeidet med informasjonssikkerhet til ledelsen:

- I SSBs undersøkelse om bruk av IKT i staten svarer 56,9 prosent (2017) av virksomhetene at de har årlig gjennomgang av styringssystemet for informasjonssikkerhet.
- Det er variasjon på hva intervjuobjektene kaller denne rapporteringen. Enkelte har en såkalt *ledelsens gjennomgang*, hvor statusen på informasjonssikkerhetsarbeidet skal gjennomgås i nødvendig detalj for leder. Andre sier de rapporterer på informasjons-sikkerhet i forbindelse med mer generell risikorapportering, da enten fra en sikkerhetsleder til virksomhetsstyringsenheter eller via denne og direkte til direktøren.
    - I Utdanningsdirektoratet ligger den utøvende delen av informasjonssikkerhets-arbeidet i virksomhetens avdeling for virksomhetsstyring.
    - Noen av intervjuobjektene sier de har god erfaring med årlig sikkerhetsgjennomgang for ledelsen. Utdanningsdirektoratet uttrykker, *«vi finner denne gjennomgangen veldig nyttig med gode diskusjoner».* Noen virksomheter, da spesielt de med en viss størrelse, har ofte faste lederforum, hvor det regelmessig rapporteres på informasjonssikkerhet.
- Frekvensen på rapportering av informasjonssikkerhetsarbeidet innad i virksomheter varierer betraktelig, helt fra ukentlig til årlig.
- 7 prosent av respondentene i spørreskjemaet til virksomhetsleder oppgir at informasjonssikkerhet ikke kommer til å bli omtalt i virksomhetens årsrapport til etatsstyrer. 63 prosent sier det vil bli omtalt som et eget tema, mens 30 prosent oppgir at det vil bli omtalt under et annet tema.

- I spørreskjemaet til virksomhetsleder oppgir 64 prosent at informasjonssikkerhet har vært et eget tema i etatsstyringsdialogen i 2017

Oppfølging og kontinuerlig forbedring

Viktige aspekter ved styring og kontroll er å legge til rette for forbedringer, følge opp arbeidet og gjøre endringer der det er nødvendig. Hendelseshåndtering og gjennomføring av evalueringer og revisjoner er viktige deler i dette.



Figur 3 - Regelmessig vurdering av status besvart av fagansvarlig informasjonssikkerhet

- Som vist i Figur 3, er det kun 56 prosent av risikoeiere (de som har ansvaret for mål og resultater i virksomheten) som systematisk og minst én gang i året vurderer status på sitt ansvarsområde – det vil si å gjøre en selvstendig vurdering av om de intern-kontrollaktivitetene de har ansvaret for blir forsvarlig utført, og at ansatte etterlever de retningslinjer som gjelder for dem. 11 prosent av respondentene vet ikke om slike vurderinger blir gjennomført.
- Tilsvarende svarer 62 prosent av respondentene på spørreskjemaet for fagansvarlige at de som er ansvarlige for sikkerhetstiltak gjør en vurdering av om de tiltakene de er ansvarlige for fungerer som forutsatt og avtalt. Her er det 9 prosent som svarer «vet ikke».
- 55 prosent av respondentene på spørreskjemaet for fagansvarlige oppgir at de i stor grad benytter erfaringer fra hendelseshåndtering til kontinuerlig forbedring av arbeidet med informasjonssikkerhet, 34 prosent svarer i moderat grad. 8 prosent sier at dette gjøres i liten eller ingen grad, mens 3 prosent svarer at dette ikke er relevant.
- På tilsvarende spørsmål til virksomhetsleder svarer 90 prosent «Ja» på om man benytter slik erfaring til kontinuerlig forbedring. 4 prosent svarer «Nei», og 6 prosent svarer «Vet ikke».

- I SSBs undersøkelse om bruk av IKT i staten (2017) rapporterer 59,9 prosent av virksomhetene at de har årlig interne revisjoner av styringssystemet for informasjons-sikkerhet.
    - Av alle som er intervjuet er det kun én virksomhet, Tolletaten, som nevner at den har en egen funksjon som kontrollerer om virksomheten følger opp sikkerhetsinstrukser og lignende.
    - I en av de større virksomhetene som ble intervjuet løser de interne revisjoner ved at IKT-sikkerhetsleder har ansvar for å kontrollere og følge opp etterlevelse av instrukser og retningslinjer.
- I SSBs bruk av IKT i staten for 2017 svarer 43,6 prosent at beredskapsøvelse gjennomføres minst en gang per år.

Tilsyn

- I intervjuene med virksomheter og etatsstyrere kommer det frem at Riksrevisjonens arbeid oppleves som nyttig og viktig, og at det fører til økt fokus på informasjonssikkerhet, men at det av og til blir for detaljorientert. For eksempel oppfølging av tilgangsstyring i stedet for kontinuerlig forbedring eller overordnet styring og kontroll.
- Flere respondenter har hatt tilsyn fra blant annet NSM, DSB og Datatilsynet. Tilsyn oppleves som nyttig, men det fremheves at det er viktig med dialog, fremfor bare å påpeke feil.
- I intervjuene kommer det frem at tilsyn førte til at virksomheter begynte å jobbe med implementering av styringssystem for informasjonssikkerhet, etter at mangler ble påpekt i revisjon.

Regelverk

- I intervjuene oppgir under halvparten av etatsstyrerne eForvaltningsforskriften som et av flere relevante regelverk med tanke på styring og kontroll av informasjons-sikkerhet. Regelverket for behandling av personopplysninger får god oppmerksomhet av de fleste. Det samme gjelder sikkerhetsloven med forskrifter.

Vi finner også eksempler på fravær av referanse til relevant regelverk i flere rapporter og stortingsmeldinger fra nyere tid:

- I kapittel 6.3 «Rettslig regulering på IKT-sikkerhetsområdet» i Meld. St. 38 (2016-2017) «IKT-sikkerhet» nevnes NIS-direktivet, personvernregelverk og ny sikkerhetslov.
- I kapittel 6.5.1 «Tverrsektorielt regelverk» i Meld. St. 10 (2016-2017) «Risiko i et trygt samfunn» nevnes sikkerhetsloven, NIS-direktivet og personvernregelverk. Difis anbefaling om bruk av ISO/IEC 27001 er nevnt, mens § 15 i eForvaltningsforskriften (som anbefalingen er knyttet til) er utelatt.
- I kapittel 3.1 «Juridiske vurderinger» i rapport om «Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten» fra Direktoratet for e-helse nevnes personvernregelverk, sektorregelverk og sikkerhetsloven.

- I kapittel 7 «Sektorovergripende regelverk for IKT-sikkerhet» i rapport 26-2017 «Regulering av IKT-sikkerhet» fra NVE er forvaltningsloven blant de lovene som er omtalt, og det er et eget avsnitt om eForvaltningsforskriften. Der henvises det til § 5 om formidling av taushetsbelagte opplysninger, men kravet om styring og kontroll i § 15 er ikke nevnt.

3.1.2 Vurdering for styring og kontroll

Modenhet på styringssystem for informasjonssikkerhet ser ut til å være bra når 100 prosent svarer at de har tydelige føringer (i moderat eller stor grad) for roller og ansvar, og over 90 prosent svarer at de har tydelige føringer (i moderat eller stor grad) for de systematiske aktivitetene for styring og kontroll. Imidlertid er det andre svar som trekker i motsatt retning. Under 60 prosent har årlig revisjon eller gjennomgang av styringssystemet for informasjonssikkerhet. Det er også vesentlig forskjell når vi sammenligner leder og fagansvarlige i deres oppfatning av i hvor stor grad det er gitt tydelige føringer for internkontroll og styringssystem. Mens 77 prosent av lederne mener de selv i gir tydelige føringer (i stor grad), hevder kun 51 prosent av fagansvarlige at de får tydelige føringer (i stor grad). Under 50 prosent har systematisk arbeid med øvelser. På bakgrunn av disse svarene er vår vurdering at en tredjedel av statlige virksomheter ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet.

Utilstrekkelig modenhet på styringssystemet for informasjonssikkerhet kan være et resultat av manglende kjennskap til lover og regler på området. Fravær av referanser til regelverket, der det er relevant, viser lav kjennskap til bestemmelsene som pålegger tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet. Vi tenker da primært på økonomiregelverket i staten og eForvaltningsforskriften § 15.

Regelverket sier at styring og kontroll på informasjonssikkerhetsområdet skal være basert på anerkjent standard. Difi anbefaler å basere seg på ISO 27001, og merker seg at forskrift til ny sikkerhetslov også legger seg tett opp til denne. Vi vurderer dette som en god tilnærming. Den legger til rette for å følge regelverkets anbefaling om at styring og kontroll på informasjonssikkerhetsområdet skal være en integrert del av virksomhetens helhetlige styringssystem.

Da virksomhetene har stor variasjon i samfunnsoppdrag, oppgaver og størrelse, vil det være naturlig at styring og kontroll er tilpasset disse forskjellige forutsetningene. Når vi ser på de variasjonene som er observert, og ser dem i forhold til type virksomhet, er det likevel større variasjoner enn det som er forventet når en baserer seg på anerkjente standarder. Vi opplever at dette stemmer overens med bildet som presenteres i Riksrevisjonens arbeid, NSMs tilsyn med sikkerhetsadministrasjon og Datatilsynets funn ved tilsyn etter personopplysningsloven.

Veiledning og tilsyn bidrar begge til mer enhetlig arbeid med informasjonssikkerhet. Vi observerer at tilsyn oppfattes som nyttig, men at veiledningen og tilsynet av og til vektlegger forskjellige områder.

For å heve kvaliteten på arbeidet med informasjonssikkerhet må lederne jobbe med kontinuerlig forbedring, som også er et vesentlig element i ISO 27001. For at det skal skje vurderer vi det som nødvendig at etatsstyrerne følger opp forbedringen.

Intervjuene viser at etatsstyrere i liten grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter. Kun 64 prosent av virksomhetene svarer at informasjonssikkerhet har vært et tema i etatsstyringsdialogen, og 7 prosent sier at informasjonssikkerhet ikke en gang vil omtales i årsrapporten for 2017. For å kunne styre godt på informasjonssikkerhetsområdet har etatsstyrere behov for oversikt over tilstand på arbeidet med informasjonssikkerhet. Bedre oversikt ville gjort det lettere for sentrale myndigheter å sammenligne status på tvers av virksomheter og sektorer, samt gjort det lettere å se endringer over tid.

At variasjonene er så store, både med tanke på måter å styre på og faktisk modenhet i informasjonssikkerhetsarbeidet, peker mot at det er nødvendig med sterkere styring og kontroll i virksomhetene.

3.1.3 Anbefalinger for styring og kontroll

Undersøkelsen og intervjuene viser at departementene i liten grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter. Bedre rapportering vil gjøre det lettere å sammenligne status på tvers av virksomheter og sektorer, samt gjøre det lettere å se endringer over tid.

Anbefaling 1: Departementene stiller krav om at virksomhetene rapporterer på sikkerhetstilstanden for egen virksomhet, og status på arbeidet med styring og kontroll av informasjonssikkerhet i årsrapporten. Rapporteringen bør være lik og sammenlignbar for alle statlige virksomheter. DFØ bør i samarbeid med Difi gi veiledning om dette.

Forvaltningen må forholde seg til et risikobilde i stadig endring. Informasjonssikkerhet er et område det må jobbes kontinuerlig med for å møte nye trusler.

Anbefaling 2: Informasjonssikkerhet inngår som en del av virksomhetsplanen.

3.1.4 Videre arbeid for Difi

Anbefalinger til og kriterier for revisjon av virksomheters etterlevelse av eForvaltningsforskriften § 15 bør være samstemt. Difi vil forbedre sin veileder, slik at den lettere kan brukes som støtte ved revisjonsarbeid.

Uten ledelsesforankring vil ikke informasjonssikkerheten bli ivaretatt. De siste årene har vi utarbeidet veiledninger og har ulike tilbud om opplæring og nettverk. Hovedtyngden av disse har vært innrettet mot de fagansvarlige i virksomhetene. Fremover må vi legge større vekt på virksomhetsledere, men også legge til rette for kompetansetiltak for etatsstyrere i departementene.

3.2 Risikostyring

Systematiske aktiviteter for å vurdere og håndtere risiko er sentralt i styring og kontroll av informasjonssikkerhet. Vi har skilt dette ut som et eget emne for å gi det tilstrekkelig omtale,

og for å gjøre rapporten enklere å lese. Risikostyringen på informasjonssikkerhetsområdet er en del av virksomhetens helhetlige risikostyring, men omtalen er her i hovedsak avgrenset til aktivitetene for vurdering og håndtering av risiko. I tillegg til styringsaktivitetene forbundet med risikohåndtering, er arbeidet med å styre implementering av sikkerhetstiltak for å redusere risiko også omtalt her.

Det er hverken mulig eller hensiktsmessig å gjennomføre grundige risikovurderinger på all informasjonsbehandling og alle informasjonssystem i en virksomhet. Virksomheter må ha tilstrekkelig oversikt over helheten og kunne prioritere, og jevnlig vurdere hvor det er behov for grundig vurdering av risiko. Oversikten over informasjonsbehandling bør inkludere hvilke informasjonstyper som behandles i de forskjellige arbeidsoppgavene, og potensielt konsekvensnivå ved brudd på konfidensialitet, integritet eller tilgjengelighet (ofte kalt «verdivurdering»).

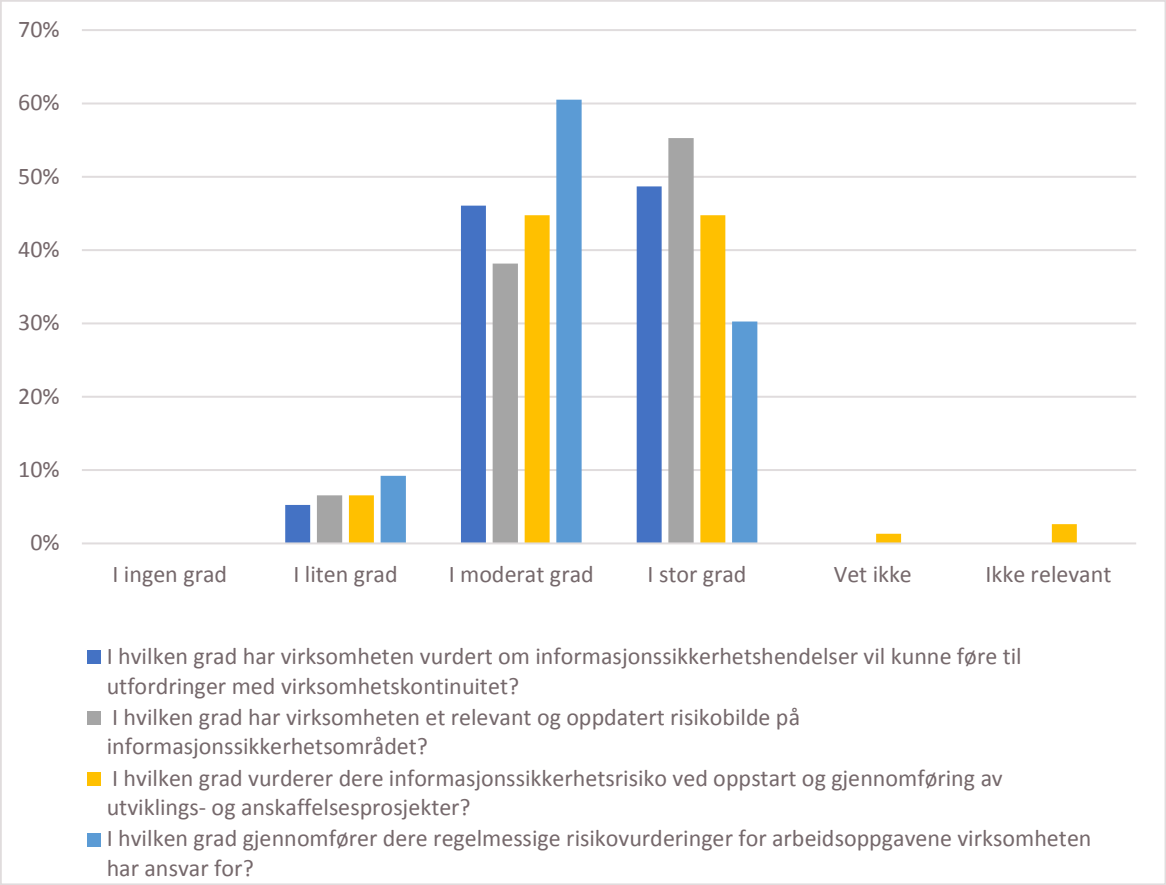
Virksomheter må ha gode føringer for planlegging og gjennomføring av risikovurderinger, som inkluderer hvordan de skal beskrive, forstå og vurdere operativ risiko. Normering av faktorer som inngår i vurderingene vil normalt inkludere konsekvensnivåer i flere kategorier, hvordan man skal estimere sannsynlighet og kriterier for å akseptere risiko.

Hensikten med risikovurdering er å identifisere risikoer som må håndteres, uansett om en potensiell uønsket hendelse er forårsaket av uhell, uaktsomhet, tilsiktede handlinger eller tilfeldige utløsende årsaker, inkludert naturhendelser.

I risikohåndteringsaktivitetene er det viktig at risikoeiere har hovedansvaret for beslutninger om håndtering av risiko, og at det finnes mekanismer i kriteriene for å akseptere risiko som sørger for at beslutninger om aksept av risiko tas på riktig nivå i virksomheten. Vurderinger om etablering av sikkerhetstiltak bør inkludere estimert effekt, kostnader og potensielle negative sideeffekter. Det er også viktig med tydelige roller og ansvar for etablering, forvaltning og annen oppfølging av sikkerhetstiltak, og at arbeidet med sikkerhetstiltak er helhetlig organisert for kostnadseffektivt sikkerhetsarbeid.

3.2.1 Observasjoner for risikostyring

Risikovurdering



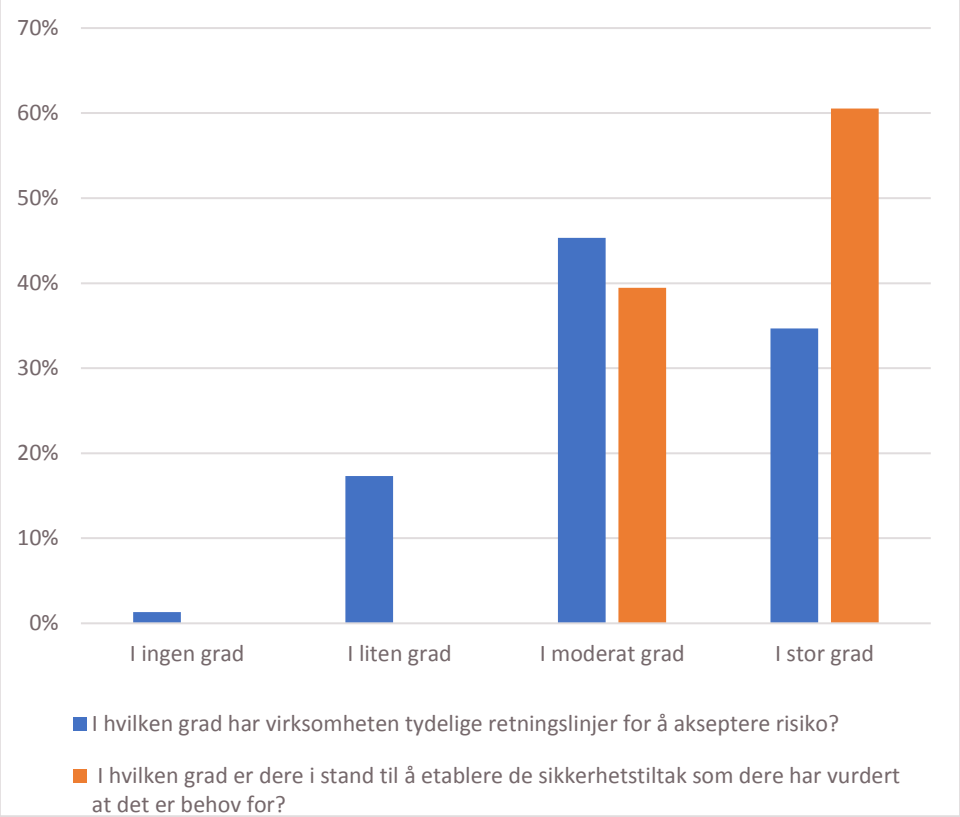
Figur 4 - Spørsmål om risiko besvart av fagansvarlig informasjonssikkerhet

- I spørreundersøkelsen svarer hele 48 prosent av virksomhetslederne at de kun i liten eller moderat grad ser styring av informasjonssikkerhet i sammenheng med den øvrige styringen av risiko i virksomheten. I spørreundersøkelsen av fagansvarlige svarer hele 51 prosent at de i moderat eller liten grad har vurdert om informasjons-sikkehetshendelser vil kunne føre til utfordringer med virksomhetskontinuitet. I disse intervjuene fremkommer det også at kun et fåtall av virksomhetene ser informasjonssikkerhetsrisiko i sammenheng med andre virksomhetsrisikoer.
- SSBs undersøkelse om bruk av IKT i staten måler at 79,2 prosent (2017) av virksomhetene gjennomfører risikovurderinger systematisk og periodisk. I vår spørreundersøkelse svarer derimot kun 61 prosent at de i moderat grad, og 9 prosent at de i liten grad, gjennomfører regelmessige risikovurderinger for arbeidsoppgavene virksomheten har ansvar for. Disse tallene avviker fra de som fremkom i intervjuene, hvor alle svarte at de gjennomfører periodiske risikovurderinger.
- Gjennom intervjuene fremkommer det også at det er store variasjoner rundt hvordan virksomhetene arbeider med risikovurdering. Det er betydelige forskjeller mellom virksomhetenes bruk av kriterier og metoder for gjennomføring av risikovurderinger.

Kun et fåtall av intervjuobjektene sier de har klare akseptkriterier for risiko innen informasjonssikkerhet, mens andre er vage hva gjelder forståelse og bruk av slike.

- I spørreundersøkelsen til virksomhetsleder fremkommer det at ansvaret for å vurdere og håndtere risiko følger linjeprinsippet i 84 prosent av virksomhetene. 82 prosent av respondentene på spørreskjemaet til fagansvarlig sier det samme. I intervjuene fremkommer det at direktøren har det overordnede ansvaret, mens avdelingsdirektørene hver for seg er ansvarlig for daglig sikkerhetsmessig ledelse av sine medarbeidere og innenfor sitt fagområde. I noen virksomheter som er intervjuet gis ansvaret helt ned på seksjons- og individnivå. I enkelte av de mindre virksomhetene er det utpekt en IT-sikkerhetsleder, som da ofte blir ansett som ansvarlig for informasjonssikkerhetsarbeidet som sådan.
- Det er også store forskjeller hva gjelder frekvens på gjennomføringer av risikovurderinger. Enkelte virksomheter gjennomfører kun overordnede vurderinger årlig sentralt, mens andre gjennomfører i linjen. Andre gjør begge deler. Et fåtall av virksomhetene som er intervjuet henviser til enkle GAP-analyser, mens noen primært gjennomfører risikovurderinger relatert til enkelte eller alle IKT-løsninger eller -prosjekter. Én virksomhet har gjennomført opp mot 300 risikovurderinger av enkeltstående systemløsninger, med en dedikert IKT-sikkerhetsstab på fire årsverk som hovedressurser for gjennomføringen av disse.
- En virksomhetsdirektør som er intervjuet ser stort forbedringspotensial i egen virksomhet hva gjelder tilgang til, og bruk av, oppdaterte risikovurderinger. I fremtiden ønsker direktøren bedre og jevnere tilgang til oppdatert informasjon som kursen kan justeres etter.
- Enkelte av virksomhetene som er intervjuet gjennomfører periodiske, eksempelvis månedlige, risikovurderinger. Disse er primært virksomheter av en viss størrelse, som behandler verdifull informasjon og har relativt høye krav fra sin sektor. Det er disse som gjør flest og mest grundige risikovurderinger.
- Flertallet bruker sannsynlighet og konsekvens (i henhold til ISO 27005 eller lignende) for vurdering av risiko på området informasjonssikkerhet, mens noen bruker en sammenstilling av verdi-, trussel- og sårbarhetsvurderinger for å vurdere og uttrykke sikringsrisiko (i henhold til NS 5832 e.l., og NSMs anbefaling om bruk av denne).

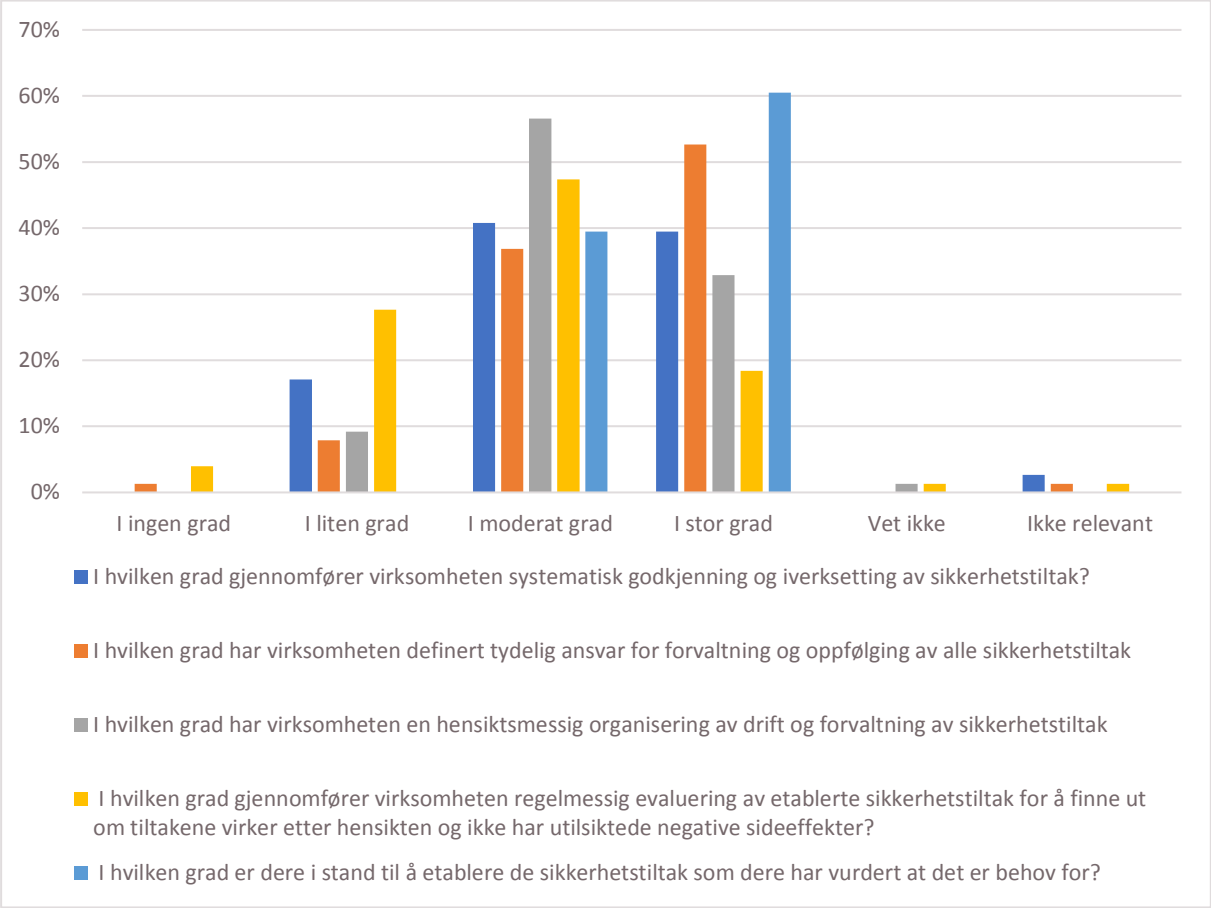
Risikohåndtering



Figur 5 - Risikohåndtering besvart av fagansvarlig informasjonssikkerhet

- I intervjuene fremkommer det store forskjeller blant virksomhetene hva gjelder eierskapet til sikkerhetsrisiko som blir identifisert. I enkelte virksomheter uttrykkes det at risiko eies i linjen, mens hos andre er det virksomhetsleder som pekes på som risikoeier.
- I intervjuene fremkommer det at risikohåndteringen knyttet til informasjonssikkerhetsrisiko skjer på ulike nivåer i virksomhetene. Det er store variasjoner i ledelsesforankringen av risikohåndteringen. Det er videre flere virksomheter som håndterer risiko stykkevis og delt, og ikke basert på en helhetlig sikkerhetsstrategi eller gitte akseptkriterier.
- De store variasjonene som er beskrevet tidligere om styring av informasjonssikkerhet generelt, gjenspeiles i styringen av risikohåndteringen hos virksomhetene som er intervjuet. I noen virksomheter er dette et linjeansvar, mens hos andre er det mer sentraliserte sikkerhetsenheter som gjennomfører risikovurdering og -håndtering relatert til informasjonssikkerhet.
- I spørreundersøkelsen rettet mot fagpersoner har to tredjedeler av virksomhetene oppgitt at de ikke har tydelige retningslinjer for å akseptere risiko. Omtrent 35 prosent oppgir at de i stor grad har dette.
- I spørreundersøkelsen rettet mot fagpersoner er det bare 40 prosent som i stor grad driver systematisk godkjenning og iverksetting av sikkerhetstiltak.

- I spørreundersøkelsen rettet mot fagpersoner er det ca. halvparten som i stor grad har tydelig ansvar for forvaltning og oppfølging av sikkerhetstiltak.
- I spørreundersøkelsen rettet mot fagpersoner har 33 prosent oppgitt at de i stor grad har hensiktsmessig organisering av drift og forvaltning av sikkerhetstiltak.
- I spørreundersøkelsen rettet mot fagpersoner er det 18 prosent som oppgir at de i stor grad regelmessig evaluerer etablerte sikkerhetstiltak. 32 prosent oppgir at de i liten eller ingen grad gjør dette.
- I spørreundersøkelsen rettet mot fagpersoner oppgir alle at de i moderat eller stor grad er i stand til å etablere de sikkerhetstiltakene de har behov for.
- I enkelte, spesielt små og IKT-orienterte, virksomheter er det ofte en IT- eller datasikkerhetsleder som har ansvar og beslutningsmyndighet, mens beslutningene i større virksomheter løftes i linjen til passende ledelsesnivå.



Figur 6 - Forvaltning av sikkerhetstiltak besvart av fagansvarlig

3.2.2 Vurdering for risikostyring

Det er behov for god ledelse, organisering, kunnskap og evne til å gjøre gode vurderinger av, og beslutninger om, risiko. Det krever tilstrekkelig fagkunnskap for å velge, etablere og forvalte hensiktsmessige sikkerhetstiltak – og for å fase ut sikkerhetstiltak som ikke er hensiktsmessige.

Regelverket på informasjonssikkerhetsområdet er i hovedsak risikobasert, og overlater til virksomheten å velge et passende nivå for usikkerhet (risiko), og å velge egnede sikkerhetstiltak. Det er stort rom for tilpasning til en virksomhets størrelse, egenart og risikobilde. Slik fleksibilitet kan være positivt, ettersom det gjør det mulig å tilpasse styring og sikkerhetstiltak til lokale behov, og sørge for at sikkerhetsarbeidet er kostnadseffektivt og understøtter virksomhetens måloppnåelse. Uansett kreves god kunnskap, kompetanse og evne for å utnytte denne fleksibiliteten og gjøre kloke vurderinger og valg.

Det er store variasjoner i hvordan disse aktivitetene er lagt opp og gjennomføres. Eksempelvis har kun 35 prosent av virksomhetene i spørreundersøkelsen svart at de i stor grad har retningslinjer for å akseptere risiko. Uten slike kriterier er det vanskelig å prioritere ressursbruken mot de risikoene det er viktig å håndtere.

Videre svarer alle virksomhetene at de i moderat eller stor grad er i stand til å etablere de sikkerhetstiltakene som de har vurdert det er behov for. Disse observasjonene indikerer store variasjoner og noen motsetninger. Selv om virksomhetene føler de etablerer tiltak etter identifiserte behov basert på vurdering av risiko, harmoniserer dette ikke med det faktum at kun et fåtall har kriterier for å akseptere risiko. Dette tyder på at det er manglende kunnskap om gjennomføring av systematiske aktiviteter for å vurdere og håndtere risiko. Dette kan føre til at etablerte sikkerhetstiltak ikke er hensiktsmessige og kostnadseffektive. Difis og NSMs erfaringer med å veilede på dette området underbygger antakelsen om manglende kunnskap og veiledning.

Mange av virksomhetene har utfordringer med etablering, forvaltning og oppfølging av sikkerhetstiltak. Kun 40 prosent oppgir at de i stor grad driver systematisk godkjenning og iverksetting av sikkerhetstiltak. Kun 33 prosent har i stor grad hensiktsmessig organisering av drift og forvaltning av sikkerhetstiltak, og bare halvparten har tydelig ansvar for forvaltning og oppfølging av sikkerhetstiltak. Disse funnene indikerer at det ikke er kostnadseffektiv forvaltning av sikkerhetstiltak, og at virksomhetene ikke har tilstrekkelig systematikk som gir tillit til at etablerte sikkerhetstiltak virker etter hensikten og har de effektene man forventer, uten uforutsette negative sideeffekter.

3.2.3 Anbefalinger for risikostyring

God risikostyring er nødvendig for å treffe godt med sikkerhetstiltak, men vi ser at kun 40 prosent av statsforvaltningen har systematisk godkjenning av sikkerhetstiltak. Risikostyring er et eget fagfelt som dekker et mye større område enn informasjonssikkerhet. Vi ser en endring i retning av mer risikobasert regelverk, der virksomhetene har mer handlingsrom til å gjøre individuelle tilpasninger, men for å gjøre de rette tilpasningene kreves det høyere kompetanse.

Anbefaling 3: Den enkelte virksomhet må sikre nødvendig kompetanse på fagfeltet risikostyring.

Dette vil føre til at virksomhetene treffer godt med de tiltak de iverksetter. Ved økt kompetanse på risikostyring vil virksomhetene gjøre bedre risikovurderinger og velge effektive sikkerhetstiltak. Det vil gi fleksibilitet til å ta i bruk ny teknologi og digitale tjenester for å oppnå politiske målsetninger om effektivisering, innovasjon og økonomisk vekst.

Den teknologiske utviklingen går fort, og det er viktig at regelverket ikke blir til hinder for utviklingen.

Anbefaling 4: Hovedprinsippet om at regelverk for informasjonssikkerhet bør være risikobasert og legge til rette for tilpasning i virksomhetene bør videreføres.

3.3 Beredskap, øvelser og hendelseshåndtering

Virksomheter må være forberedt på at sikkerhetshendelser vil inntreffe. God beredskaps-planlegging bidrar til at man håndterer uønskede hendelser på en bedre måte. Uten beredskapsplaner som beskriver hvem som har ansvar for hva vil det bli vanskeligere å håndtere hendelser på en god måte. Det å trene alene eller sammen med andre bidrar til at virksomheten gjør de rette handlingsvalgene. Ved krisehåndtering er tid kritisk for å redusere konsekvensene av en hendelse.

Hvordan man planlegger og gjennomfører øvelser og hvilke typer tema man øver på påvirker evnen til å håndtere uønskede hendelser, Virksomheten som trener på de risikoscenarier som de har avdekket gjennom ulike former for risikoanalyser, blir bedre forberedt på å gjøre de rette valgene. De virkelig modne virksomhetene viser en planlagt og forberedt risikobasert tilnærming i sitt beredskapsarbeid. De har i forkant tenkt gjennom hva som sikrer god gjennomføring av øvelser. De har trent på scenariene og handlingsalternativene som er forankret i egen risiko, fått en erfaring med hva som faktisk fungerer godt, og evaluerer øvelsene og følger opp de forbedringspunkter som ble avdekket.

3.3.1 Observasjoner for beredskap, øvelser og hendelseshåndtering

Beredskap

- De fleste som blir intervjuet svarer at hendelseshåndtering er et linjeansvar, og noen tilføyer at håndtering av IKT-hendelser er en del av dette. Svarene i spørreskjema til virksomhetsleder angir at 69 prosent har en egen IKT-beredskapsplan som er godkjent av virksomhetens leder. Dette utdypes i spørreskjema fagansvarlig der 72 prosent svarer at IKT-beredskapsplanen er evaluert og oppdatert i løpet av de siste år. Det innebærer at 28 prosent svarer at de ikke har en beredskapsplan som ivaretar IKT-håndtering.
- I spørreskjema til fagansvarlig fremkommer det at erfaringene fra øvelsene blir brukt til å forbedre sikkerhetstiltak av 88 prosent, å forbedre planverk av 83 prosent, å vurdere effekten av, og behov for, sikkerhetstiltak av 79 prosent og å vurdere behov for kompetansetiltak i virksomheten av 61 prosent.

Øvelser

- I SSBs bruk av IKT i staten svarer 43,6 prosent at de gjennomfører minst en beredskapsøvelse årlig.
- I spørreundersøkelsen svarer 18 prosent at virksomheten i stor grad jobber systematisk med øvelser innen informasjonssikkerhet, og 45 prosent har svart at de har gjennomført minst én øvelse med tema informasjonssikkerhet hvert år ifølge spørreskjema besvart av fagansvarlig.

- En virksomhet angir at de øver fire ganger i året på løsningene de forvalter, og beskriver at alle øvelsene er knyttet til informasjonssikkerhet.

Hendelseshåndtering

- Det er stor variasjon fra virksomheter som sier at de har gode forebyggende tiltak med god internkontroll og god hendelseshåndtering, til de som har forbedret hendelseshåndteringen som følge av alvorlige IKT-hendelser. Flere sier også at de har vært utsatt for inntrengningstest fra NSM, og svarer at de har fått seg noen overraskelser etter disse testene.
- Nesten alle virksomheter sier at de har tydelig definerte roller, ansvar og prosedyrer for hvordan hendelser skal håndteres. De beskriver en organisering med kriseledelse, beskrevne roller og ansvar. Noen få beskriver bruk av IKT-beredskapsplaner.
- I intervjuer kommer det frem at kontrakt med et eksternt selskap (for eksempel CERT eller en dataleverandør) kan bistå virksomheten i hendelseshåndteringen. Selskapet varsler dersom virksomheten er under et angrep, eller om det er noe som skjer som de kan være utsatt for. Flere uttrykker at det føles trygt å være tilknyttet en CERT-funksjon.
- Etter å ha vært utsatt for alvorlige IKT-hendelser sier noen at de avdekket store forbedringsområder med hensyn til varsling, logging, rapportering og oppfølging.

  Respondentene beskriver at de bruker erfaring fra hendelseshåndteringen til kontinuerlig forbedring av informasjonssikkerhetsarbeidet. 89 prosent svarer dette i spørreskjema til fagansvarlige og 89 prosent svarer dette i spørreskjema til virksomhetsleder, hvor 6 prosent har svart «vet ikke». SSB sier *«Vi plukker opp en hendelse og lærer av den.»*
- Håndtering av hendelser der informasjon om hendelsen er gradert har skapt utfordringer for virksomhetene som ikke har informasjonssystemer for å motta slik informasjon.

3.3.2 Vurdering for beredskap, øvelser og hendelseshåndtering

Når en hendelse eller en krise skal håndteres må det fattes mange beslutninger raskt og under usikkerhet. Man har ikke all den informasjonen som man gjerne skulle ønske man hadde, og det er en stor grad av forventning om å gjøre de rette tingene til rett tid. Det stiller store krav til beslutningstakerne og de som jobber tett med håndtering av selve krisen. Omtrent halvparten av de som har opplevd hendelser forteller at de ble godt håndtert, mens den andre halvparten beskriver at de fant betydelige forbedringspunkter.

I SSBs undersøkelse om bruk av IKT i staten svarer 83,7 prosent at de har oppdatert beredskapsplan de siste 2 årene. Det er usikkert om dette tallet omtaler den generelle beredskapsplanen eller om det er IKT-beredskapsplanen som er oppdatert. Usikkerhet mellom generell beredskap og spesifikk IKT-beredskap går igjen gjennom hele undersøkelsen hva gjelder beredskapsplaner og -øvelser. Noen hadde likevel integrert beredskap og informasjonssikkerhet, slik som NAV:

> *«Sikkerhetsseksjonen har informasjonssikkerhet og beredskap. Derfor trener vi helhetlig på for eksempel hva gjør vi ved nedetid på ID porten eller andre scenarioer.»*

Vi ser store variasjoner i de ulike virksomhetene som ble intervjuet hva gjelder modenhet på øvingsgjennomføring og hendelseshåndtering. Med bakgrunn i intervjuene vurderer vi at modenhet er uavhengig av virksomhetens størrelse. De virksomheter som definerte seg selv som en beredskapsetat var mer bevisst sine egne forbedringspunkt innen informasjons-sikkerhet enn de som ikke definerte seg selv som beredskapsetater.

Det er vanskelig å konkludere om temaene for øvelsene som gjennomføres er innen informasjonssikkerhet eller om de øver andre deler av beredskapsfeltet. Det er også vanskelig å se om de øver risikobasert. Tema for øvelsene var ikke en del av spørreundersøkelsen, men tilgjengelighet og kompromitterte systemer er tema som ble nevnt. Brønnøysundregistrene sier:

> *«Poenget mitt er at vi tidligere har vært veldig opptatt av stål og metall, men nå er vi mer opptatt av å utvikle gode systemer for informasjonssikkerhet.»*

Hendelser og øvelser har vært evaluert i mange år og noen av læringspunktene er de samme hver gang. DSB har gått gjennom 11 hendelser i perioden 2004 – 2014 og vurdert 53 evalueringsrapporter om de samme 11 hendelsene[10]. I alle 11 hendelsene fant man forbedringspunktene innen tema beredskapsplanverk og organisasjon. I spørreunder-søkelsen besvart av virksomhetsleder svarer hele 27 prosent at de ikke har en IKT-beredskapsplan som er godkjent av virksomhetsleder. I 9 av 11 hendelser ble det avdekket forbedring innen risiko- og sårbarhetsanalyse. Dette korresponderer godt med svarene til de fagansvarlige som mente at virksomheten ikke arbeidet systematisk med IKT-sikkerhet.

DSB har også vurdert 14 store øvelser i perioden 2006 – 2013 med påfølgende evaluerings-rapporter. Gjennomgangen viser samme resultat, de fleste forbedringspunkter gjelder svakheter i planverk, informasjonsdeling, kommunikasjon og ansvar og roller.

I øvelse SNØ IKT 16 var noe av målsettingen å få testet rammeverket for digital hendelses-håndtering[11] og å få testet bruk og samarbeid mellom de sektorvise responsmiljøene. Tilknytningen til et CERT-miljø (et responsmiljø) og den følelse av trygghet det medfører, er det kun noen få respondenter som har kommentert i vår undersøkelse. At ikke flere kommenterer bruk av responsmiljø som bidrag inn i hendelseshåndteringen kan tyde på at man ikke kjenner til disse miljøene og hvordan disse miljøene kan brukes som en del av hendelseshåndteringen. Rammeverket for digital hendelseshåndtering som ble testet under

---

10 https://www.fylkesmannen.no/Documents/Dokument%20FMTE/Samfunnssikkerhet/Beredskapsseminar/Beredskapsseminaret%202015/%C3%98velser%20-%20gjennomf%C3%B8ring%20og%20evaluering%20-%20Jan%20Aast%C3%B8.pdf

11 https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

IKT 16 inneholdt også krav til interne prosedyrer som skulle beskrive et handlingsmønster i virksomhetene ved håndtering av hendelser. At 87 prosent svarte at de håndterte hendelsen basert på tydelige definerte roller, ansvar og prosedyrer for hvordan hendelser skal håndteres, kan tyde på at dette punktet i evalueringsrapporten etter øvelse IKT 16 er fulgt opp.

Når det gjelder noen respondenters kommentarer om utfordringer ved håndtering av graderte hendelser, er dette en gjentakelse av erfaringene etter terrortrusselen 2014. Evalueringsrapporten etter denne hendelsen viser også til at mangel på graderte kommunikasjonsløsninger var en praktisk hovedutfordring [12]. Evalueringsrapporten etter IKT 16 omtaler samme utfordring. Vi ser at dette fortsatt kommenteres av virksomheter med beredskapsansvar som en utfordring når det gjelder hendelseshåndtering.

Det er en rød tråd fra mål for informasjonssikkerhetsarbeidet, gjennomføring av ulike former for risikovurderinger, utarbeidelse av beredskapsplaner og øving på scenarier hentet fra de ulike analyser av risiko som er foretatt til god hendelseshåndtering. Undersøkelsen i sin helhet viser betydelige forbedringspunkter i det systematiske arbeidet innen øvingsplanlegging og -gjennomføring hva gjelder informasjonssikkerhet.

3.3.3 Anbefalinger for beredskap, øvelser og hendelseshåndtering

Under halvparten av virksomhetene i statsforvaltningen øver årlig og 27 prosent har ikke en beredskapsplan godkjent av ledelsen. Vi ser store variasjoner i de ulike virksomhetene som ble intervjuet hva gjelder modenhet på øvingsgjennomføring og hendelseshåndtering. Å møte en alvorlig hendelse uten beredskap eller øvelse i hendelseshåndtering vil kunne hindre virksomheten i å utføre sitt samfunnsoppdrag.

Anbefaling 5: Virksomhetene gjennomfører minst en årlig øvelse innen informasjonssikkerhet. Både planlegging og rapportering av erfaringer fra øvelsen må knyttes opp mot virksomhetens styringssystem for informasjonssikkerhet.

Gode øvelser bidrar til å avdekke de viktigste forbedringspunktene. Veiledning og erfaring fra andre er hjelp til å lage gode øvelser.

Anbefaling 6: DSB bør i samarbeid med NSM og Difi tilpasse sitt kursmateriale for øvelser, slik at det blir enkelt å ta i bruk for mindre virksomheter.

Anbefaling 7: Vi anbefaler at det i sektorer (for eksempel virksomheter under et departement) eller geografiske regioner (for eksempel i et fylke) gjennomføres felles øvelser.

Anbefaling 8: Norske virksomheter bør vurdere å delta i internasjonale øvelser for å få erfaring med grenseoverskridende hendelser. ENISA har ansvar for det europeiske

12 https://www.regjeringen.no/globalassets/departementene/jd/evalueringsrapport_terrortrusselen_2014.pdf, kap 7.1.

øvingsprogrammet Cyber Euro som arrangerer øvelser hvert annet år og hvor NSM NorCERT er etablert som norsk kontaktpunkt.

Ved øvelse vil forbedringspunkter i beredskap og hendelseshåndtering avdekkes og modenheten vil øke, slik at virksomhetene er i stand til å håndtere alvorlige hendelser samtidig som de leverer på sitt samfunnsoppdrag.

3.4 Nasjonale felleskomponenter

Nasjonale felleskomponenter[13] er gjenbrukbare løsninger som dekker typiske behov på digitaliseringsområdet og er en viktig del av den nasjonale digitale infrastrukturen. Dette er felleskomponentene:

- ID-porten (Difi)
- Altinn (Brønnøysundregistrene)
- Digital postkasse til innbyggere (Difi)
- Kontakt- og reservasjonsregisteret (Difi)
- Det sentrale folkeregisteret (Skatteetaten)
- Enhetsregisteret (Brønnøysundregistrene)
- Matrikkelen (Statens kartverk)

En stor del av forvaltningen er avhengig av nasjonale felleskomponenter for å løse sitt samfunnsoppdrag.

3.4.1 Observasjoner for nasjonale felleskomponenter

Vi har spurt både virksomhetsleder og fagansvarlige om de har vurdert om de er avhengige av en nasjonal felleskomponent. I tillegg har vi spurt fagansvarlige om de er kritisk avhengige, og i så fall om de har etablert en reserveløsning.

- Andelen virksomhetsledere og fagansvarlige som svarer at de har vurdert sin avhengighet av de nasjonale felleskomponentene, er veldig lik med henholdsvis 88 prosent og 89 prosent. Det er litt flere virksomhetsledere som har svart «Vet ikke» på dette spørsmålet enn fagansvarlige (5 prosent mot 1,5 prosent).
- 48 prosent av de fagansvarlige svarer at de er kritisk avhengig av en felleskomponent.
- Bare 19 prosent av de som er kritisk avhengige av en felleskomponent har etablert en reserveløsning.

3.4.2 Vurderinger for nasjonale felleskomponenter

I Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter (Riksrevisjonens administrative Rapport nr. 1 2018) svarer 51 prosent av respondentene at de bruker én eller flere felleskomponenter i sitt arbeid. I undersøkelsen vår svarer 48 prosent av respondentene

[13] https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/felleskomponenter/id2342598/

at de er kritisk avhengige av en felleskomponent. Disse resultatene er ganske like, og kan tyde på at når virksomhetene benytter en felleskomponent, så er de kritisk avhengig av den.

Selv om det er mange virksomheter som er kritisk avhengig av en felleskomponent, er det relativt få virksomheter som har etablert reserveløsninger for felleskomponentene. En reserveløsning kan være nødvendig om internettforbindelsen faller bort eller felleskomponenten ikke er tilgjengelig. For eksempel må en fastlege kunne gjennomføre en konsultasjon, selv om ID-porten er utilgjengelig. Et alternativ kan være å lagre alle resepter lokalt inntil ID-porten er oppe igjen og reseptene kan ekspederes.

Virksomhetenes vurdering av behovet for en reserveløsning kan avspeile at de vurderer tilgjengeligheten på felleskomponentene som god nok. Dette er imidlertid ikke avdekket i våre observasjoner, og hovedspørsmålet er da firedelt:

1) Har de gjennomført en risikovurdering og funnet at risikoen kan aksepteres?
2) Har bruker og felleskomponentforvalter samsvarende oppfatning av felleskomponentens sikkerhet, og da spesielt tilgjengeligheten?
3) Finnes det ikke reserveløsninger med god nok kvalitet?
4) Er problemstillingen ikke vurdert?

Difi-notat 2017:4 om «Samarbeid og koordinering på informasjonssikkerhetsområdet i nasjonale felleskomponenter» viser at felleskomponentforvalterne er gjennomgående bevisst at mange tjenester er avhengige av deres komponent, og at de jobber internt i egen virksomhet med å sørge for god tilgjengelighet.

3.4.3 Anbefaling for nasjonale felleskomponenter

Vi har ingen anbefalinger for dette vurderingstemaet ut over det som er foreslått i Difi-notat 2017:4.

3.4.4 Videre arbeid for Difi

Difi vil undersøke hva som ligger til grunn for at kun 19 prosent av de som er kritisk avhengige av felleskomponenter, har etablert en alternativ løsning for situasjoner hvor felleskomponenten er midlertidig utilgjengelig.

3.5 Sikkerhetskultur

Sikkerhetskulturen regnes som en del av organisasjonskulturen, og handler om hvilke felles verdier og normer som ligger til grunn for risikoforståelse, den enkeltes valg for hvordan informasjon håndteres og hvordan man reagerer på avvik eller sikkerhetsbrudd. Sikkerhetskulturen i en virksomhet kan ha positive eller negative konsekvenser for informasjonssikkerheten. Det vesentlige er at kultur kan påvirkes og endres. En god sikkerhetskultur kan gi bedre effekt av sikkerhetstiltak.

3.5.1 Observasjoner for sikkerhetskultur

- I spørreundersøkelsen svarer 40 prosent at de har gjennomført kartlegging eller måling av sikkerhetskulturen.

- I spørreundersøkelsen oppgir 48 prosent av virksomhetene at informasjonssikkerhet i moderat grad har fokus og prioritet hos ledelsen, mens 52 prosent oppgir at informasjonssikkerhet i stor grad har fokus og prioritet.
- Ti av virksomhetene som ble intervjuet presiserer at de anser sikkerhetskulturen som god ut fra en skjønnsmessig vurdering. Flere av disse oppgir likevel at de ønsker å jobbe med kulturen.
- Det er et stort spenn i hvordan sikkerhetskulturen og kompetansen oppfattes i virksomhetene:
    - *Kartverket: «Generelt er vi nok i en oppvåkningsperiode når det gjelder sikkerhet og informasjonssikkerhet, som gjør at vi i større grad utvikler oppmerksomhet rundt dette.»*
    - *NAV: «Lederne ser på sikkerhet som et virkemiddel som er med på å nå måloppnåelsen.»*
    - *SSB: «De ansattes forståelse av informasjonssikkerhet er ganske god og betydningen av å ha en oppegående sikkerhetskultur er godt befestet i organisasjonen.»*
- Flertallet av de intervjuede virksomhetene påpeker at de jobber med å forbedre sikkerhetskulturen i virksomheten. Dette foregår på forskjellige måter, men bruk av e-læring/nanolæring og arrangementer i sikkerhetsmåneden går igjen hos mange. Andre måter å forbedre kulturen på er gjennom tester, deling av kompetanse og beste praksis, iverksettelse av tiltak, fokus på hva virksomheten har av verdier og informasjonsdeling over intranett.
- I intervjuene kommer det frem at endring må komme fra lederne og at de må gå foran med et godt eksempel.
- I følge intervjuene vil sikkerhetskultur og kompetanse på området informasjons-sikkerhet være særlig viktig i IKT-utviklingsprosjekter fremover.

3.5.2 Vurderinger for sikkerhetskultur

Det kan være utfordrende å si om virksomhetens kultur er god eller dårlig, og i praksis kan kulturen ha noen gode og noen negative elementer samtidig. Sikkerhetskulturen må vurderes ut fra den enkelte virksomhets oppgaver og egenart.

Hovedinntrykket når det kommer til sikkerhetskulturen i de intervjuede virksomhetene er at spennet er stort. I spørreundersøkelsen svarer 40 prosent at de har gjennomført kartlegging eller måling av sikkerhetskulturen. Noen virksomheter forteller at sikkerhet er et kjerneområde for dem og at kun det perfekte er godt nok, mens andre sier at de er i en oppvåkningsperiode. Felles for de aller fleste er imidlertid at de presiserer at det er mer fokus på dette området nå enn tidligere, og at bevisstheten rundt informasjonssikkerhet har økt.

Inntrykket er at de virksomhetene som har gjennomført en kartlegging eller måling av sikkerhetskulturen er mer bevisste hvilke svakheter de har, og dermed kan implementere mer målrettede tiltak.

I flere tilfeller virker det som at ledelsen har våknet, men at det kan være vanskelig å få de ansatte med på tankegangen. Tolletaten formulerte det slik:

> *«Sikkerhetskulturen er godt forankret hos toppledelsen, men den er ikke godt nok spredt utover i organisasjonen.»*

Dette virker særlig utbredt blant de virksomhetene som har hatt et hovedfokus på forskning og tradisjonelt sett har hatt en åpenhetskultur, selv om det også her finnes virksomheter som mener de har etablert en god sikkerhetskultur. *OsloMet sier at:*

> *«[Utdanningssektoren] har fokusert på åpenhet og deling heller enn informasjonssikkerhet.»*

Virksomheter som tradisjonelt sett har hatt en sterk organisasjonskultur, enten dette gjelder tradisjonell sikkerhet, øvelser og beredskap, generell ryddighet eller har måtte forholde seg til strenge lover og regler, virker som de gjennomgående vurderer det slik at de også har en bedre sikkerhetskultur.

3.5.3 Anbefaling for sikkerhetskultur

Sikkerhetskulturen må vurderes ut fra den enkelte virksomhets oppgaver og egenart. I spørreundersøkelsen svarer 40 prosent at de har gjennomført kartlegging eller måling av sikkerhetskulturen. Vårt inntrykk er at de virksomhetene som har gjennomført en kartlegging eller måling av sikkerhetskulturen er mer bevisste hvilke svakheter de har, og dermed kan implementere mer målrettede tiltak.

Anbefaling 9: Virksomheter kartlegger sin sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring.

3.5.4 Videre arbeid for Difi

Difi vil utvikle veiledningsmateriell for at virksomhetene skal kunne planlegge og gjennomføre kartlegging og måling av sikkerhetskultur.

3.6 Kompetanse

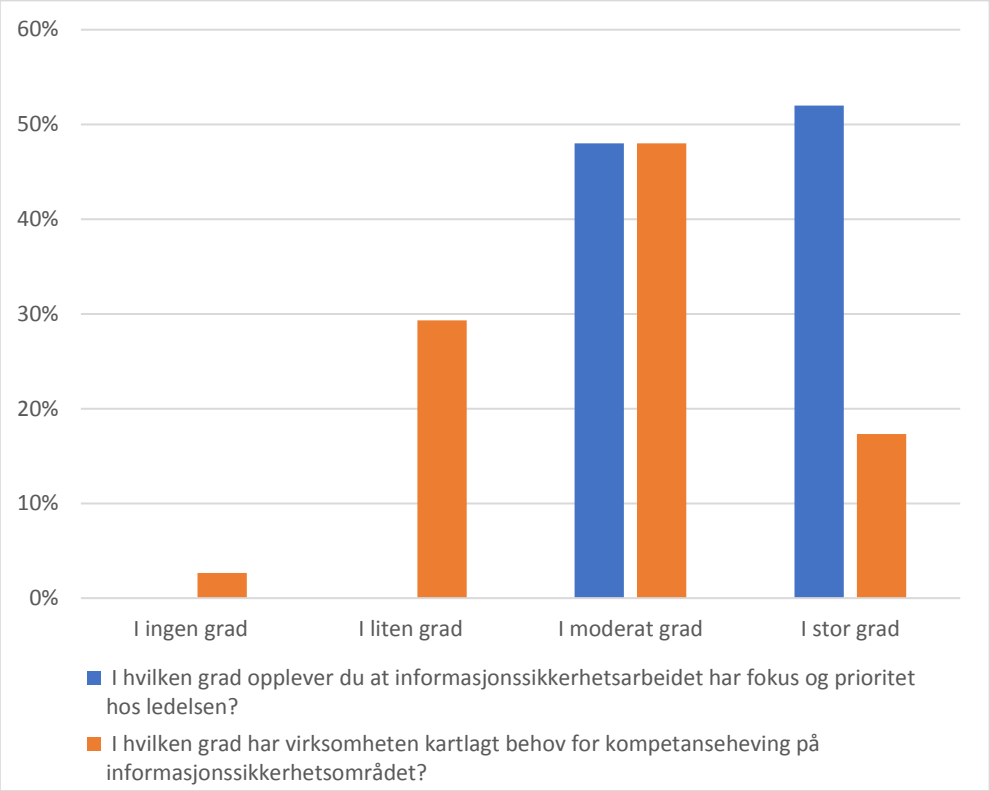
Regelverket på informasjonssikkerhetsområdet er i hovedsak risikobasert, og den nye personvernforordningen og ny sikkerhetslov drar også disse regelverkene mer i denne retningen, og det bidrar til økt krav til kompetanse. Se også kapittel 3.2 om risikostyring.

Manglende kompetanse på IKT og informasjonssikkerhet har vært oppe på den politiske dagsordenen flere ganger den siste tiden. For denne analysen deler vi sikkerhetskompetanse i to områder:

- Generell kunnskap om informasjonssikkerhet som skal bidra til risikoforståelse og at den enkelte medarbeider forstår hvorfor virksomheten har etablert rutiner, prosedyrer og tekniske sikkerhetstiltak. Denne typen kompetanse er tett knyttet virksomhetens sikkerhetskultur.
- Fagkompetanse som er nødvendig for forskjellige stillinger og oppgaver den enkelte medarbeider skal utføre. En del av denne kompetansen er knyttet til utdanning fra fagskoler, universitet og høgskoler. En annen del av denne kompetansen er knyttet til etterutdanning, kurs og sertifiseringer.

3.6.1 Observasjoner for kompetanse

- I spørreundersøkelsen oppga 68 prosent av virksomheter at de klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet, mens 27 prosent svarte at de ikke klarer det.
- Seks av de intervjuede virksomhetene anser medarbeidernes kompetanse på informasjonssikkerhetsområdet som tilstrekkelig, mens en tredjedel av virksomhetene som ble intervjuet vektla at medarbeiderne ikke har god nok kompetanse.
- 32 prosent av virksomhetene svarte i spørreundersøkelsen at de «i ingen grad» eller «i liten grad» har kartlagt behov for kompetanseheving på informasjonssikkerhetsområdet. 48 prosent av virksomhetene rapporterte at de «i moderat grad» har kartlagt behov for kompetanseheving, mens 17 prosent svarte de «i stor grad» har kartlagt behovet.
- I spørreundersøkelsen oppga 51 prosent av virksomhetene at de «i moderat grad» har tilpassede kompetansetiltak. 27 prosent av virksomhetene oppga at de «i stor grad» har tilpassede kompetansetiltak. Andelen virksomheter som svarte at de «i liten grad» har tilpassede kompetansetiltak er 16 prosent. Dette samstemmer med intervjuene, hvor en litt større andel av virksomhetene oppga at de har tilpassede kompetansehevingstiltak, enn andelen som mener de ikke har dette.
- «Det er ikke alltid avgjørende hvilke spisskompetanser kandidaten har, mener flere av informantene. Det handler i nokså høy grad om at kandidaten har en basisforståelse for et område og en attityde og et engasjement for å jobbe med IKT-sikkerhet. Da kan intern utvikling og opplæring kompensere for at kandidaten eventuelt mangler den rette spisskompetansen. Dessuten går utviklingen innen IKT-sikkerhet så fort at det uansett er et løpende behov for å tilegne seg ny viten og kompetanse.» (NIFU Rapport 2017:32)
- «Uten sikkerhetskompetanse vil det være vanskelig for en virksomhet å forstå den risikoen man utsetter verdiene sine for.» (Risiko 2018, Nasjonal sikkerhetsmyndighet)



Figur 7 - Spørsmål om kompetanse besvart av fagansvarlig informasjonssikkerhet

3.6.2 Vurdering for kompetanse

68 prosent av virksomhetene svarte i spørreundersøkelsen at de klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet. Samtidig vektlegger kun en liten del av de intervjuede virksomhetene at etatens medarbeidere har tilstrekkelig med kompetanse på området. Vi tolker dette som forskjellen mellom behov for fagkompetanse knyttet til stilling og behovet for generell kunnskap om informasjonssikkerhet som de fleste ansatte bør ha.

Generell kunnskap om informasjonssikkerhet kan økes gjennom opplæring av ansatte, mens behovet for fagkompetanse kan dekkes opp ved rekruttering, etterutdanning av medarbeidere, ved innleie av konsulenter eller ved å tjenesteutsette enkelte oppgaver.

At få virksomheter anser medarbeideres kompetanse som tilstrekkelig trenger imidlertid ikke være ensidig negativt, da det også kan bety at virksomhetene har en bedre forståelse av hva som kreves av dem og er opptatt av utviklingen som skjer på området. Som OsloMet forklarte:

> *«Vi vil aldri kunne svare ja på at vi har god nok kompetanse da informasjonssikkerhetsarbeidet er i kontinuerlige endringer på grunn av stadig nye trusler, sårbarheter og gjennomstrømning av mennesker.»*

Erkjennelse av mangel på fagkompetanse eller generell kunnskap om informasjonssikkerhet må uansett følges opp av kompetansehevende tiltak.

Manglende generell sikkerhetskunnskap hos medarbeidere kan redusere betydningen av gode sikkerhetstiltak, eller betydningen av å ha enkeltmedarbeidere med god fagkompetanse. Informasjonssikkerheten vil aldri være bedre en virksomhetens svakeste ledd.

Kunnskap om trusselbildet gjør det lettere for den ansatte å forstå behovet for informasjonssikkerhet. Kartverket knytter kompetanseutfordringer til manglende forståelse av trusselbildet i virksomheten:

> *«Det handler ikke om [manglende] kompetanse per se, men den allmenne kunnskapen i virksomheten om trusselbildet.».*

Derfor etterspør Kartverket tydeligere, relevante og tilpassede trusselvurderinger fra sikkerhetstjenestene.

Noen av virksomhetene beskriver kompetansemangelen blant medarbeiderne som stor. Samtidig beskrives vesentlige variasjoner i kompetanse på tvers av avdelinger innad i virksomhetene. Typisk sett rapporteres det at IT-miljøene sitter på den beste sikkerhets-kompetansen, mens særlig forskningsavdelinger nevnes som miljøer med manglende forståelse og interesse for informasjonssikkerhet, slik som Folkehelseinstituttet uttrykte det:

> *«Kompetansen blant mange forskere på informasjonssikkerhet er mangelfull og blir til tider overskygget av deres stoiske tro på egen kompetanse og evne til å håndtere ting på en god måte, samt deres overbevisning om hvor hellig deres forskning er. Å få forskerne i tale og ordentlig om bord på informasjonssikkerhet er utfordrende.»*

Dette funnet må ses i sammenheng med at forskningsinstitusjoner tradisjonelt har vært preget av en «åpenhetskultur», som beskrevet i avsnittet om kultur over.

I spørreundersøkelsen oppga 27 prosent av virksomhetene at de ikke klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet. Dette må ses i sammenheng med at enkelte virksomheter i intervjuene beskrev utfordringer med å få tak i personer med riktig kompetanse. Å finne riktig kompetanse nevnes i større grad som en utfordring blant virksomheter utenfor Oslo, enn for dem som befinner seg i Oslo-området. Enkelte virksomheter beskriver outsourcing av IT som utfordrende, da de er usikre på om de har tilstrekkelig og god nok kompetanse igjen internt. Det er også relevant om den enkelte virksomhet har kompetanse til å beskrive stillingsutlysninger godt nok. Informasjonssikkerhet og ikke minst IKT-sikkerhet er fagområder med mange spesialiseringer.

> *«Riktig fokus på sikkerhet i en virksomhet fordrer at man forstår og kan definere behovet for sikkerhetskompetanse i den enkelte bedrift. Her er kartlegging av allerede eksisterende kompetanse samt av kompetansegap viktig.»*[14]

[14] Risiko 2018, Nasjonal sikkerhetsmyndighet

De aller fleste virksomhetene vektla i intervjuene at de jobber kontinuerlig med generell kompetanseheving. Tiltakene varierer mellom virksomhetene, men som eksempler nevnes onboarding-programmer, phishing-kampanjer, deltakelse i sikkerhetsmåneden, e-læringskurs, lederopplæring i forbindelse med GDPR og faglunsjer. Enkelte nevner også autorisasjonssamtaler som konkrete kompetansehevingstiltak.

I spørreundersøkelsen oppga 27 prosent av virksomhetene at de i stor grad har tilpasset kompetansehevingstiltakene til konkrete arbeidsoppgaver og fagmiljøer. 51 prosent av virksomhetene oppga at de i moderat grad har tilpassede kompetansetiltak. Intervjuene viser at det er et stort spenn i hvordan virksomhetene tilpasser kompetansehevingstiltak til forskjellige arbeidsoppgaver og fagmiljøer i etaten, og at tilpassede kompetansehevingstiltak i hovedsak er rettet mot ansatte med lederansvar.

Enkelte virksomheter presiserer at de har fått en oppvåkning etter uønskede hendelser og har brukt dette til å tilpasse kompetansetiltak. Et eksempel er NVE som ble rammet av et løsepengevirus og senere la det inn som ett eksempel i sitt nano-læringskurs. Utover dette eksempelet er det imidlertid få virksomheter av dem som ble intervjuet som har brukt hendelser og/eller øvelser til å tilpasse læring og kompetanseheving.

Samlet sett er vårt inntrykk at virksomhetene arbeider med kompetanseheving på området informasjonssikkerhet, men at arbeidet hos mange er lite målrettet og tilpasset. Det er behov for bedre forståelse for hvilken fagkompetanse som kreves for å løse virksomhetens oppgaver innen fagområdet informasjonssikkerhet.

3.6.3 Anbefalinger for kompetanse

Spisskompetanse er nødvendig for å velge gode sikkerhetstiltak. Manglende generell sikkerhetskunnskap hos øvrige medarbeidere kan redusere betydningen av sikkerhetstiltak. Noen av virksomhetene beskriver kompetansemangelen blant medarbeiderne som stor. Samtidig beskrives vesentlige variasjoner i kompetanse på tvers av avdelinger innad i virksomhetene. I spørreundersøkelsen oppga 27 prosent av virksomhetene at de ikke klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet. Samlet sett er vårt inntrykk at virksomhetene arbeider med kompetanseheving på området informasjonssikkerhet, men at arbeidet hos mange er lite målrettet og tilpasset.

Anbefaling 10: Virksomhetene bør vurdere å etablere en plan for kompetanseutvikling på området informasjonssikkerhet.

Dersom medarbeidere fra virksomheter med stort behov for bedre kompetanse kan hospitere hos virksomheter med sterke sikkerhetsmiljø vil dette være en enkel og kostnadseffektiv måte å legge til rette for utveksling av viktig erfaring og kompetanse.

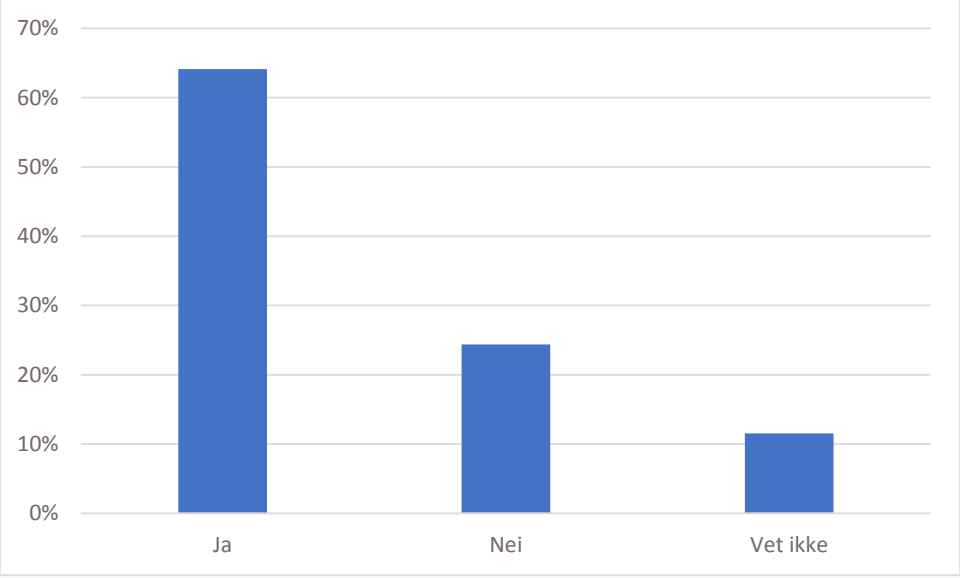
3.7 Etatsstyringsdialogen

Styringsdialogen mellom departement og underliggende virksomhet har stor betydning for hvilke områder virksomheten prioriterer å jobbe med. Etatsstyringen består av tildelingsbrev, virksomhets- og økonomiinstruks, rapportering, samt formell og uformell dialog. Vi har undersøkt hvordan informasjonssikkerhet behandles i etatsstyringen, fordi det påvirker prioriteringen i underliggende virksomhet.

3.7.1 Observasjoner for etatsstyringsdialogen

Behandling av informasjonssikkerhet i etatsstyringen

- I spørreskjemaet til virksomhetsleder oppgir 64 prosent at informasjonssikkerhet har vært et eget tema i etatsstyringsdialogen i 2017. 24 prosent svarer at det ikke har vært et eget tema, mens 12 prosent svarer «vet ikke».
- I intervjuene med etatsstyrere oppgir flertallet at det gis føringer (eventuelt krav om rapportering) for informasjonssikkerhet i tildelingsbrevet, men det synes å være stor variasjon i hvordan disse føringene er utformet, og hvor detaljert de er.
- Kun ett intervjuobjekt oppgir at det ikke gis føringer knyttet til informasjonssikkerhet i tildelingsbrevet.
- Fra intervjuene kommer det frem at etatsstyrere tilpasser oppfølgingen av informasjonssikkerhet til de ulike virksomhetenes behov og egenart.
- Intervjuene viser stor variasjon i hvordan informasjonssikkerhet behandles i etatsstyringen, fra
    - ingen oppfølging fordi underliggende virksomhet selv skal ha kontroll på arbeidet med informasjonssikkerhet, til
    - detaljert oppfølging ved spesifikke føringer.
- Én etatsstyrer oppgir at de ønsker at alle sine underliggende virksomheter skal være sertifisert etter ISO 27001.



Figur 8 - Har informasjonssikkerhet vært et eget tema i etatsstyringsdialogen i 2017?

- De færreste av etatsstyrerne har bedt sine underliggende virksomheter om å gjøre en analyse av status på informasjonssikkerhetsområdet, og rapportere på dette.
- Fra intervjuene kommer det frem at tilsyn, risikovurderinger, hendelser og håndtering av avvik er kilder til innsikt i hvordan underliggende virksomheter jobber med informasjonssikkerhet.

Helhetlig styring i sektoren

En helhetlig styring av informasjonssikkerhet i sektoren må veies opp mot tilpassing for den enkelte virksomhet.

- Det varierer i hvor stor grad arbeidet med informasjonssikkerhet samkjøres i ulike sektorer. Noen departementer har fellesføringer for alle sine underliggende virksomheter, og gir tilleggsføringer ved behov, mens andre har føringer for den enkelte virksomhet.
- Det er varierende om man har et helhetlig risikobilde i en enkelt sektor – noen baserer seg på de rapportene som kommer fra eksterne parter (f.eks. NSM).
- Fra intervjuene kommer det frem at føringer på tvers av en sektor gjøres i sektorlovgivning, tildelingsbrev eller retningslinjer i etatsstyringen.

3.7.2 Vurdering for etatsstyringsdialogen

Finansdepartementets veileder i etatsstyring sier blant annet at:

> *«Departementet kan ikke vektlegge alle oppgaver og ansvarsområder like sterkt i den operative styringen. I praksis innebærer styring at noen mål, oppgaver eller områder løftes frem og prioriteres fremfor andre, og at grunnleggende oppgaver og funksjoner forutsettes å fungere.»*

Tydelige føringer for informasjonssikkerhet i tildelingsbrev og instrukser eller på annen måte i etatsstyringsdialogen, er viktig for at arbeidet med informasjonssikkerhet skal få fokus og innarbeides i virksomhetsstyringen og understøtte virksomhetens mål.

Årsrapporter kan være en kilde til informasjon om status på arbeidet med informasjons-sikkerhet, men Difis gjennomgang av årsrapporter for 2016 konkluderte med at disse ikke ga særlig informasjon om status.

3.7.3 Anbefalinger for etatsstyringsdialogen

De færreste av etatsstyrerne har bedt sine underliggende virksomheter om å gjøre en analyse av status på informasjonssikkerhetsområdet. Dette er en forutsetning for å finne ut om omfanget og kvaliteten på informasjonssikkerhetsarbeidet er godt nok.

Anbefaling 11: Informasjonssikkerhet følges opp i styringsdialogen mellom departement og underliggende virksomhet. Etatsstyrere bør ha tilgang på veiledning om hvordan informasjonssikkerhet bør ivaretas i etatsstyringen. DFØ og Difi bør samarbeide om å gi denne veiledningen.

4 Konklusjon

Vår vurdering er at en av tre statlige virksomheter ikke har tilstrekkelig styring og kontroll på informasjonssikkerhet.

Vi mener at arbeidet med styring og kontroll av informasjonssikkerhet i virksomhetene må styrkes for å sikre at virksomhetene oppnår tilstrekkelig modenhet og blir bedre rustet til å følge endringer i trusselbildet. Vi mener videre at departementene må stille tydeligere krav til virksomhetenes rapportering av status for å oppnå en koordinert og sektorovergripende styring av informasjonssikkerheten i statsforvaltningen

Vi har 11 anbefalinger som støtter opp under dette. Teksten i underkapittel 4.1 er i sin helhet hentet fra anbefalingene som er fordelt på de syv vurderingstemaene i kapittel 3.

4.1 Anbefalingene

Styring og kontroll

Undersøkelsen og intervjuene viser at departementene i liten grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter. Bedre rapportering vil gjøre det lettere å sammenligne status på tvers av virksomheter og sektorer, samt gjøre det lettere å se endringer over tid.

Anbefaling 1: Departementene stiller krav om at virksomhetene rapporterer på sikkerhets-tilstanden for egen virksomhet, og status på arbeidet med styring og kontroll av informasjonssikkerhet i årsrapporten. Rapporteringen bør være lik og sammenlignbar for alle statlige virksomheter. DFØ bør i samarbeid med Difi gi veiledning om dette.

Forvaltningen må forholde seg til et risikobilde i stadig endring. Informasjonssikkerhet er et område det må jobbes kontinuerlig med for å møte nye trusler.

Anbefaling 2: Informasjonssikkerhet inngår som en del av virksomhetsplanen.

Risikostyring

God risikostyring er nødvendig for å treffe godt med sikkerhetstiltak, men vi ser at kun 40 prosent av statsforvaltningen har systematisk godkjenning av sikkerhetstiltak. Risikostyring er et eget fagfelt som dekker et mye større område enn informasjonssikkerhet. Vi ser en endring i retning av mer risikobasert regelverk, der virksomhetene har mer handlingsrom til å gjøre individuelle tilpasninger, men for å gjøre de rette tilpasningene kreves det høyere kompetanse.

Anbefaling 3: Den enkelte virksomhet må sikre nødvendig kompetanse på fagfeltet risikostyring.

Dette vil føre til at virksomhetene treffer godt med de tiltak de iverksetter. Ved økt kompetanse på risikostyring vil virksomhetene gjøre bedre risikovurderinger og velge effektive sikkerhetstiltak. Det vil gi fleksibilitet til å ta i bruk ny teknologi og digitale tjenester for å oppnå politiske målsetninger om effektivisering, innovasjon og økonomisk vekst.

Den teknologiske utviklingen går fort, og det er viktig at regelverket ikke blir til hinder for utviklingen.

Anbefaling 4: Hovedprinsippet om at regelverk for informasjonssikkerhet bør være risikobasert og legge til rette for tilpasning i virksomhetene bør videreføres.

Beredskap, øvelser og hendelseshåndtering

Under halvparten av virksomhetene i statsforvaltningen øver årlig og 27 prosent har ikke en beredskapsplan godkjent av ledelsen. Vi ser store variasjoner i de ulike virksomhetene som ble intervjuet hva gjelder modenhet på øvingsgjennomføring og hendelseshåndtering. Å møte en alvorlig hendelse uten beredskap eller øvelse i hendelseshåndtering vil kunne hindre virksomheten i å utføre sitt samfunnsoppdrag.

Anbefaling 5: Virksomhetene gjennomfører minst en årlig øvelse innen informasjonssikkerhet. Både planlegging og rapportering av erfaringer fra øvelsen må knyttes opp mot virksomhetens styringssystem for informasjonssikkerhet.

Gode øvelser bidrar til å avdekke de viktigste forbedringspunktene. Veiledning og erfaring fra andre er hjelp til å lage gode øvelser.

Anbefaling 6: DSB bør i samarbeid med NSM og Difi tilpasse sitt kursmateriale for øvelser, slik at det blir enkelt å ta i bruk for mindre virksomheter.

Anbefaling 7: Vi anbefaler at det i sektorer (for eksempel virksomheter under et departement) eller geografiske regioner (for eksempel i et fylke) gjennomføres felles øvelser.

Anbefaling 8: Norske virksomheter bør vurdere å delta i internasjonale øvelser for å få erfaring med grenseoverskridende hendelser. ENISA har ansvar for det europeiske øvingsprogrammet Cyber Euro som arrangerer øvelser hvert annet år og hvor NSM NorCERT er etablert som norsk kontaktpunkt.

Ved øvelse vil forbedringspunkter i beredskap og hendelseshåndtering avdekkes og modenheten vil øke, slik at virksomhetene er i stand til å håndtere alvorlige hendelser samtidig som de leverer på sitt samfunnsoppdrag.

Sikkerhetskultur

Sikkerhetskulturen må vurderes ut fra den enkelte virksomhets oppgaver og egenart. I spørreundersøkelsen svarer 40 prosent at de har gjennomført kartlegging eller måling av sikkerhetskulturen. Vårt inntrykk er at de virksomhetene som har gjennomført en kartlegging eller måling av sikkerhetskulturen er mer bevisste hvilke svakheter de har, og dermed kan implementere mer målrettede tiltak.

Anbefaling 9: Virksomheter kartlegger sin sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring.

Kompetanse

Spisskompetanse er nødvendig for å velge gode sikkerhetstiltak. Manglende generell sikkerhetskunnskap hos øvrige medarbeidere kan redusere betydningen av sikkerhetstiltak. Noen av virksomhetene beskriver kompetansemangelen blant medarbeiderne som stor. Samtidig beskrives vesentlige variasjoner i kompetanse på tvers av avdelinger innad i virksomhetene. I spørreundersøkelsen oppga 27 prosent av virksomhetene at de ikke klarer å dekke opp sitt behov for fagkompetanse på informasjonssikkerhetsområdet. Samlet sett er vårt inntrykk at virksomhetene arbeider med kompetanseheving på området informasjonssikkerhet, men at arbeidet hos mange er lite målrettet og tilpasset.

Anbefaling 10: Virksomhetene bør vurdere å etablere en plan for kompetanseutvikling på området informasjonssikkerhet.

Dersom medarbeidere fra virksomheter med stort behov for bedre kompetanse kan hospitere hos virksomheter med sterke sikkerhetsmiljø vil dette være en enkel og kostnadseffektiv måte å legge til rette for utveksling av viktig erfaring og kompetanse.

Etatsstyringsdialogen

De færreste av etatsstyrerne har bedt sine underliggende virksomheter om å gjøre en analyse av status på informasjonssikkerhetsområdet. Dette er en forutsetning for å finne ut om omfanget og kvaliteten på informasjonssikkerhetsarbeidet er godt nok.

Anbefaling 11: Informasjonssikkerhet følges opp i styringsdialogen mellom departement og underliggende virksomhet. Etatsstyrere bør ha tilgang på veiledning om hvordan informasjonssikkerhet bør ivaretas i etatsstyringen. DFØ og Difi bør samarbeide om å gi denne veiledningen.

4.2 Prioriteringer

Vi anbefaler å starte med de tiltakene som kan gi raske resultater eller som vil bidra til raskere implementering av øvrige tiltak. I den forbindelse vektlegger vi behovet for bedre informasjon om status for arbeidet med informasjonssikkerhet. Den informasjon vi nå har samlet inn, burde eksistert som et resultat av virksomhetenes etatsstyringsdialog og årsrapporter. Vi mener derfor at anbefalingene 1 og 11 bør prioriteres.

Deretter er det vår vurdering at det er viktig å styrke den digitale beredskapen. Øvelser gjør at virksomhetene er bedre forberedt til å håndtere alvorlige uønskede hendelser. Øvelser er også et virkemiddel for å gi bedre risikoforståelse og kan være et virkemiddel for å forbedre sikkerhetskulturen i virksomheten. Vi mener derfor at anbefaling 5 bør prioriteres.

Effekten av sikkerhetstiltak er som regel avhengig av en god sikkerhetskultur. En god sikkerhetskultur vil i særlig grad bidra til å redusere sårbarheter som skyldes menneskelige feil og sosial manipulering. Vi mener derfor at anbefaling 9 og 10 bør prioriteres og sammenfattes ved å legge til ordet kompetanse i anbefaling nummer 9.

4.3 Videre arbeid for Difi

Undersøkelsen gir oss god innsikt i hvordan Difi bør innrette vårt arbeid fremover med å styrke informasjonssikkerheten i statsforvaltningen. «Tonen på toppen» er avgjørende for å lykkes med informasjonssikkerhetsarbeidet. Uten ledelsesforankring vil ikke informasjonssikkerheten bli ivaretatt. De siste årene har vi utarbeidet veiledninger og har ulike tilbud om opplæring og nettverk. Hovedtyngden av disse har vært innrettet mot de fagansvarlige i virksomhetene. Fremover må vi legge større vekt på virksomhetsledere, men også legge til rette for kompetansetiltak for etatstyrere i departementene.

Virksomhetsledere må forstå hvordan de bør jobbe med informasjonssikkerhet gjennom bedre veiledning på blant annet styringssystemet, rapportering i årsrapporten og kartlegging av sikkerhetskultur. Etatsstyrere har behov for veiledning om hvordan de bør følge opp informasjonssikkerhetsområdet i etatsstyringen.

Samarbeidet mellom veiledningsaktørene på området må videreutvikles slik at virksomhetene får enhetlige råd. Vi opplever at samarbeidsformen med NSM og Datatilsynet har fungert bra og mener at denne kan utvides til å inkludere flere veiledningsaktører.

Vedlegg

Vedleggene følger som separate dokumenter.

Vedlegg 1 - Indikatorer

Liste over indikatorer over hva vi ønsket å besvare.

Vedlegg 2 - Utvalgte virksomheter

Liste over virksomheter utvalgt til intervju og spørreskjema.

Vedlegg 3 - Spørreskjema til virksomhetsleder

Spørreskjema som ble sendt til virksomhetsledere.

Vedlegg 4 - Spørreskjema til fagansvarlig informasjonssikkerhet

Spørreskjema som ble sendt til fagansvarlig informasjonssikkerhet.

Referanseark for Difi

Tittel på rapport:	Arbeidet med informasjonssikkerhet i statsforvaltningen - kunnskapsgrunnlag
Difis rapportnummer:	2018:4
Forfatter(e):	Håkon Styri med flere
Evt. eksterne samarbeidspartnere:	BDO
Saksnummer:	17/01167-23
Prosjektnummer:	17-79
Prosjektnavn:	Evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen
Prosjektleder:	Håkon Styri
Prosjektansvarlig avdeling:	Digital transformasjon
Oppdragsgiver(e):	KMD

Resymé/omtale:

Direktoratet for forvaltning og ikt (Difi) har på oppdrag fra Kommunal- og moderniseringsdepartementet (KMD) fremskaffet et kunnskapsgrunnlag på hvordan statsforvaltningen arbeider med informasjonssikkerhet.

En av tre statlige virksomheter har ikke tilstrekkelig styring og kontroll på informasjonssikkerhet, og etatsstyrere etterspør i liten grad status på arbeidet med informasjonssikkerhet hos underliggende virksomheter. Det viser vår evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen.

Emneord: informasjonssikkerhet, internkontroll, risikostyring, etatsstyring, sikkerhetskultur, beredskap, beredskapsøvelse og hendelseshåndtering.

Totalt antall sider til trykking:	
Dato for utgivelse:	

Utgiver:	Difi Postboks 8115 Dep 0032 OSLO www.difi.no