Vedlegg 2 – Funn, anbefalinger og oppfølging av Difi Rapport 2018:4 «Arbeidet med informasjonssikkerhet i statsforvaltningen»

Innhold

Oppsummering av Difi Rapport 2018:4

(fra nyhetsartikkel publisert 21. juni 2018: https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen/2044)

Vår vurdering er at én 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.

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.

Våre hovedfunn

- Hver tredje statlige virksomhet har ikke tilstrekkelig styring og kontroll på informasjonssikkerheten. Det er stor variasjon på innretning og omfang på styring og kontroll i virksomhetene.
- Etatsstyrere etterspør i liten grad status på arbeidet med informasjonssikkerhet hos underliggende virksomheter.
- 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.
- Få departementer har bedt sine underliggende virksomheter analysere status på informasjonssikkerhet.
- 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

Rapporten presenterer 11 anbefalinger. Vi trekker her spesielt frem fire prioriterte anbefalinger som raskt kan bidra til å forbedre dagens situasjon:

- 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.

Leveranser fra samarbeidsprosjekt for oppfølging av Difi rapport 2018:4 «Arbeid med informasjonssikkerhet i statsforvaltningen»

Samarbeidsprosjekt besto av fem delprosjekter der det er produsert nye hjelpemidler for offentlige virksomheter.

Delprosjekt 1 – Informasjonssikkerhet i etatsstyringen (DFØ, Digdir, NSM)
Det ble utviklet en veileder med et tilhørende dialogverktøy skal bedre oppfølgingen av informasjonssikkerhet i styringsdialogen mellom departementer og underliggende virksomheter. Veilederen og dialogverktøyet er tilgjengelig på DFØs nettsider.

Delprosjekt 2 – Øvelser for bedre informasjonssikkerhet (DSB, Digdir, NSM)
Det ble utarbeidet undervisningsmateriell i form av 12 diskusjonsøvelser basert på ulike scenarier. Disse er tilgjengeliggjort på den nye portalen for øvelser innen digital sikkerhet, ovelse.no.

Delprosjekt 3 – Sikkerhetskultur (NorSIS, Digdir)
Det ble utarbeidet en metode for kartlegging av digital sikkerhetskultur med tilhørende veiledning, tilpasset bruk i statsforvaltningen, og Difis eksisterende veileder i kompetanse- og kulturutvikling ble revidert. Materialet er tilgjengelig på Digdirs nettsider.

Delprosjekt 4 – Kompetanse (Digdir, med NSM, DFØ, DSB og NorSIS i fokusgruppe)
Det ble utarbeidet kompetansebeskrivelser som beskriver hvilket ansvar, arbeidsoppgaver og kompetansebehov som kan inngå i ulike roller innen styring og kontroll av informasjonssikkerhet. Kompetansebeskrivelsene er tilgjengelige på Digdirs nettsider.

Delprosjekt 5 – Styring og kontroll av informasjonssikkerhet (Digdir, NSM og DFØ)
Digdir, DFØ og NSM samarbeidet om å utarbeide felles veiledning som skal hjelpe virksomheter til å lykkes med helhetlig styring og kontroll av informasjonssikkerhet. Datatilsynet og KS bidra også på relevante deler. Veiledningen gir brukerne svar på spørsmål som

- hva vil det si å jobbe helhetlig?
- hva er fellestrekkene når man arbeider med styring og kontroll?
- hvordan gir ulike fagområder og regelverk ulike perspektiver?
- hvilke veiledningsaktører kan hjelpe?

Veiledningen er tilgjengelig på Digdirs nettsider.