Digdir

SAKSFRAMLEGG

Forum: Skate Møtedato: 23.03.2022

Sak 2/2022 Status og utfordringer i offentlig sektor mht. styring og kontroll på informasjonssikkerhetsområdet – Råd fra Skate
Behandlingssak

Historikk/bakgrunn
Nasjonal strategi for digital sikkerhet ble lansert i januar 2019. Kommunal og moderniserings-departementet (KMD) og Difi (senere Digdir) hadde ansvaret for tiltak 5 i tiltaksoversikten: «Sikker digitalisering i offentlig sektor». Kapittel 9 «Digital sikkerhet» i digitaliseringsstrategien «En digital offentlig sektor» gjengir blant innholdet i dette tiltaket. Tiltaket ble ferdigstilt i 2021.

Undersøkelser Digdir v/Statens kompetansemiljø for informasjonssikkerhet har gjennomført viser at det er store utfordringer knyttet til styring av informasjonssikkerhet i både stat[1], kommune og fylkeskommune[2]. Informasjon fra andre myndigheter, blant annet Nasjonal sikkerhetsmyndighet, peker på det samme.

Digdir har høsten og vinteren 2021/2022 gjort en kartlegging av utfordingsbildet, og vurdert mulige tiltak og anbefalinger[3]. Som del av denne prosessen har vi hatt dialog med Nasjonal sikkerhetsmyndighet, KS, Datatilsynet, Direktoratet for forvaltning og økonomistyring, Direktoratet for e-helse, KiNS, NorSIS og Skatteetaten. Samtlige har vært positive til at det startes et arbeid som beskrevet i denne saken.

Digdir ønsker nå Skates råd knyttet til den strategiske retningen for det videre arbeidet for en styrket og helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning. Vi ser at dette kan styrke arbeidet i små og mellomstore virksomheter, og også i forbindelse med utvikling av sammenhengende tjenester. Dette arbeidet er hovedsakelig avgrenset til den enkelte virksomhets systematiske arbeid med å vurdere og håndtere risiko, og omhandler ikke initiativer knyttet til, CERT-funksjoner, hendelseshåndtering på tvers av virksomheter eller lignende.

Det er ønskelig at Skate inntar perspektivet til små og mellomstore kommuner når saken diskuteres.

Forslag til beslutning:
- Skate anbefaler at denne tilnærmingen – et tversektorielt samarbeid for å etablere en brukerorientert, felles referanseramme for offentlige virksomheters arbeid med informasjonssikkerhet – legges til grunn for videre arbeid.
- Digdir merker seg for øvrig Skates råd i videre arbeid.

Presentasjon av saken
Til tross for at det de siste årene er utviklet en rekke nye veiledere og hjelpemidler[4], og tall fra SSB[5] viser forbedring på en del områder, er det fortsatt store utfordringer knyttet til det offentliges arbeid med informasjonssikkerhet. Den siste tiden har også et økende antall hendelser vist hvor store konsekvenser informasjonssikkerhetsbrudd kan få. Både hendelser og tilsyn fra myndigheter avdekker at det er utfordringer på mange områder, for eksempel:

- Ledelsens forståelse av betydningen av informasjonssikkerhet, og hvilke konsekvenser informasjonssikkerhetsbrudd kan få
- Tilstrekkelig oversikt over oppgaver og tjenester, informasjonsbehandlingen i disse og behovet for informasjonssikkerhet
- Avhengigheter mellom tjenester, hvor svikt et sted i kjeden påvirker mange andre
- Helt grunnleggende sikkerhetstiltak er ikke etablert

[1] Difi Rapport 2018:4 «Arbeidet med informasjonssikkerhet i statsforvaltningen»
[2] Digdir Rapport 2020:3 «Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner»
[3] Se vedlegg 1 for sammendrag av Digdirs utkast til notat «Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning».
[4] Se vedlegg 2 for en oversikt over funn og anbefalinger i Difi rapport 2018:4 «Arbeidet med informasjonssikkerhet i statsforvaltningen», og leveransene i samarbeidsprosjektet som ble gjennomført som oppfølging av rapporten
[5] «Digitalisering og IKT i offentlig sektor», tabell 12042: https://www.ssb.no/statbank/table/12042/

Digdir

Svært mange av regelverkene som stiller krav til arbeidet med informasjonssikkerhet er funksjonsbaserte. Det vil si at det stiller krav til hva som skal oppnås, men er fleksibelt med tanke på de spesifikke detaljene i hvordan det skal oppnås. Slike funksjonsbaserte regelverk kan være krevende å etterleve, fordi virksomhetene må ha tilstrekkelig kompetanse og evne til å vurdere hva som ligger innenfor regelverkets krav, og hva som er myndighetenes forventninger.

Det finnes mye veiledning innenfor informasjonssikkerhetsområdet, fra ulike aktører[6]. I tillegg finnes det en rekke rammeverk en virksomhet kan benytte i arbeidet. Kompleksiteten av dette, og behovet for kompetanse som følger av det, gjør at det for mange virksomheter er vanskelig å benytte seg av det materialet som finnes. Siden mye av lovverket er funksjonsbasert, legger også den veiledningen som er tilgjengelig opp til at virksomheten må gjøre en del vurderinger selv. Hver enkelt virksomhet må gjøre egne vurderinger av omfang og innretning på både styringsaktiviteter og sikkerhetstiltak. I mange virksomheter er modenheten lav, og kompetansen på informasjonssikkerhetsområdet varierende. Det gjør at det er utfordrende å gjøre de nødvendige vurderingene og tilpasningene på en måte som passer virksomhetens egenart og risiko.

Forslag til strategisk retning

Felles sikkerhet i forvaltningen

Digdir foreslår et tverrsektorielt samarbeid for å etablere en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter. En felles referanseramme beskriver hvordan veiledning på ulike områder henger sammen, og gir virksomhetene et klarere bilde av hvilke vurderinger som må gjøres. (Se eksempel på bruk av referanserammen nedenfor.)

Digdirs målsetning er en styrket og helhetlig tilnærming til informasjonssikkerhet i det offentlige. Mer brukerorienterte hjelpemidler vil gjøre virksomheter i bedre i stand til å vurdere risiko og gjennomføre andre styringsaktiviteter, og basert på det, etablere tiltak som er egnet til å redusere den risikoen de står overfor.

Eksisterende veiledning er i stor grad generisk. Mer konkretiserte råd og veiledning vil gjøre arbeidet med informasjonssikkerhet lettere for virksomheter med lav modenhet på informasjonssikkerhetsområdet. Sentraliserte faglige vurderinger vil effektivisere arbeidet i hver enkelt virksomhet, gjøre det enklere for virksomhetene å ivareta sitt ansvar, og gi bedre sikkerhet.

I mange tilfeller er oppgavene og tjenestene som leveres, og informasjonen som behandles i disse oppgavene, i stor grad like. Dette gjelder særlig på kommunalt forvaltningsnivå, der kommunene i stor grad leverer de samme tjenestene til sine innbyggere. Selv om det kan være stor variasjon i hvordan oppgavene utføres, gjør dette at konsekvensene av informasjonssikkerhetsbrudd er sammenlignbare, og at det er mulig å standardisere en del av anbefalingene knyttet til sikkerhetstiltak.

Ved å koble oppgaver og tjenester, og informasjonsbehandlingen i disse, opp mot konsekvensnivåer og nivåer av sikkerhetstiltak, kan man oppnå bedre sikkerhet i hele forvaltningen. Dette vil også styrke arbeidet med samfunnssikkerhet og beredskap. Virksomhetene vil få et utgangspunkt de kan bygge videre på for å jobbe godt og risikobasert med informasjonssikkerhet i sin virksomhet.

Eksempel på mulig bruk av referanserammen: Det etableres en katalog over oppgaver og tjenester[7] som utføres i kommuner, og informasjonsbehandlingen i disse. En kommune kan slå opp i denne katalogen, finne konsekvensnivåer for de ulike oppgavene/tjenestene, og en tiltaksbank med anbefalinger for hvilke sikkerhetstiltak som bør etableres for å oppnå tilstrekkelig sikkerhet for informasjonsbehandlingen. Dette kan brukes som utgangspunkt for virksomhetens egne vurderinger.

Målgruppe

Det er naturlig å starte med de små og mellomstore kommunene. Der er likhetene relativt store, og utfordringene størst. Det er også stort gjenbrukspotensiale på tvers av kommuner. På sikt er det naturlig å se på synergier mot statlige virksomheter og andre deler av forvaltningen.

[6] Se vedlegg 3 for et utvalg av veiledningsaktører på informasjonssikkerhetsområdet.

[7] Det kan vurderes om det er mulig å ta utgangspunkt i tjenestebeskrivelsene i Nasjonal tjenestekatalog fra Kommuneforlaget AS (KF).

Bygger på eksisterende veiledning

Ved å ta utgangspunkt i eksisterende anbefalinger og tilføre noen nye elementer, kan det bygges opp en slik felles referanseramme for arbeidet med informasjonssikkerhet. Referanserammen vil støttes opp av eksisterende veiledning fra ulike aktører. Det kan bygges en bro mellom veiledning om styring av informasjonssikkerhet og veiledning om sikkerhetstiltak, fremfor å utvikle nye veiledningsprodukter. Det gir kommunene en enklere hverdag når de skal arbeide med informasjonssikkerhet.

Utarbeides over tid

Et slikt arbeid vil måtte skje over tid, og vi tar sikte på å involvere flere aktører. Det vil være hensiktsmessig å bygge sten på sten, og bygge opp referanserammen over tid. Arbeidet er i en tidlig fase, og det er derfor ikke mulig å på dette tidspunktet si eksakt hvilke aktører som vil være involvert, eller hva som vil være varigheten. KS vil imidlertid naturlig være en sentral samarbeidspartner. Det samme vil ulike aktører med veiledningsansvar på informasjonssikkerhetsområdet.

Mulige gevinster

Digdir ser en rekke mulige gevinster ved etablering av en slik felles referanseramme. Gevinstene vil være avhengig av omfang på arbeidet, og samarbeid og koordinering knyttet til utvikling, formidling og utbredelse av resultatet. Mulige gevinster er at arbeidet med informasjonssikkerhet vil bli mer kostnadseffektivt, og at man får en styrket grunnleggende sikkerhet for hele forvaltningen.

Det vil i tillegg gjøre det enklere å utvikle sammenhengende tjenester og dele data. Det at ting gjøres mer likt og felles på tvers av forvaltningen styrker evnen til samarbeid og samstyring, og bidrar til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre. En mer utfyllende liste over gevinster finnes i vedlegg 1.

Råd fra Skate

Digdir ønsker følgende råd fra Skate:

- Stiller Skate seg bak forslaget til strategisk retning?
- Hvilke justeringer bør Digdir eventuelt gjøre for å treffe offentlige virksomheters behov best mulig?

3 vedlegg.

Saken vil bli framlagt av Knut Bjørgaas
Saksframlegget er utarbeidet av Digitaliseringsdirektoratet
Oslo, 07.03.22