NSM

Vår saksbehandler
Ingunn Mari Skaaden

Vår dato
07.12.2022

Vår referanse
U-22/01592-5

Deres dato

Deres referanse

Antall vedlegg

Til
DIGITALISERINGSDIREKTORATET
Postboks 1382 Vika
0114 OSLO

Innspill fra NSM til DigDirs notat om Felles informasjonssikkerhet i offentlig forvaltning

Nasjonal sikkerhetsmyndighet (NSM) viser til skriv fra digitaliseringsdirektoratet (Digdir) vedrørende innspill til notat «Et nasjonalt løft for informasjonssikkerhet i offentlig sektor».

NSMs generelle betraktninger til notatet

NSM synes det er et godt initiativ og det bygger videre på prosjekter og samarbeid knyttet til informasjonssikkerhet i offentlig forvaltning som Digdir har holdt i de siste årene. NSM ønsker å bidra til å bedre sikkerheten i både offentlig og privat sektor så langt vi har mulighet, både innenfor og utenfor sikkerhetslovens virkeområde. Dette er også i tråd med vårt oppdrag fra overordnede departementer, JD og FD. Vi utarbeider blant annet risikorapporter, temarapporter og råd og anbefalinger som vil være relevante for målgruppen i notatet (www.nsm.no). Notatet henviser til flere av våre publiserte produkter, blant annet NSMs grunnprinsipper for IKT-sikkerhet. Det er viktig at norsk offentlig forvaltning utnytter hverandres kompetanse, erfaring og utgitte produkter. Vi kommer til å videreutvikle NSMs grunnprinsipper og mener det vil være det viktigste bidraget fra NSM inn mot det videre arbeidet som er beskrevet i notatet. Primærmålgruppen for grunnprinsippene er virksomheter som forvalter kritiske samfunnsfunksjoner og/eller kritisk infrastruktur, men grunnprinsippene er relevante for alle offentlige og private virksomheter, inkludert kommuner. Vi tar gjerne imot innspill og forslag til hvordan grunnprinsippene kan videreutvikles og forbedres slik at de treffer både primær- og sekundærmålgruppen enda bedre.

Behov for IT-modernisering og digital transformasjon – infrastruktur, plattform og tjenester

NSM ser enkelte områder som gjerne kunne vært omtalt mer i notatet. Det gjelder blant annet strategi for IT-modernisering og digital transformasjon. Dette går ikke direkte på virksomheters evne til å drive intern sikkerhetsstyring, men det legger mange av premissene for å få til effektive, moderne og sikre tjenester. Det hjelper lite å ha god intern, (helhetlig) styring av informasjonssikkerheten dersom IT-systemer og prosesser er avleggs og lite effektive. Alle virksomhetene bør ha en strategi og en plan for hvordan de skal gjennomføre en digital transformasjon i tiden fremover. Mange virksomheter vil i tillegg være for små til å kunne opprettholde et tilfredsstillende drifts- og sikkerhetsmiljø, som enten skal drifte og videreutvikle digitale plattformer og/eller følge opp en eller flere leverandører som gjør dette på vegne av virksomheten. I disse tilfellene vil det ofte være fornuftig å slå seg sammen med flere andre

virksomheter i samme situasjon og danne et fellesmiljø, alternativt koble seg på løsninger som eksisterer eller som tas frem av andre offentlige aktører. Staten kan (og bør) legge til rette for at det blir stordriftsfordeler slik at ikke hver enkelt lille virksomhet må gjøre all jobben selv.

Enkelte initiativer er allerede i gang. For eksempel konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste som (om en del år) kan bli aktuelt å benytte for flere av virksomhetene som omfattes av notatet. Målgruppen for KVUen er statsforvaltningen med noen unntak, og fremtidig mulighetsrom innbefatter også andre deler av offentlig sektor.

En av utfordringene vi ser er mangelen på tydelige autoritative føringer fra myndighetene om hvilke tiltak som etatene faktisk skal prioritere og hvordan disse tiltakene skal settes sammen til en helhetlig og enhetlig systemarkitektur – fortrinnsvis på tvers av staten slik at de danner en helhetlig digital grunnmur og ikke etatssiloer. Det er først når tiltak og initiativer samles i en helhetlig arkitektur som omfatter plattform, infrastruktur og tjenester at vi får nødvendig sikkerhet (balansert sikkerhetsnivå, helhetlig dekning osv.).
NSM har uttalt og skrevet om dette flere ganger, blant annet i følgende innlegg:

- https://nsm.no/aktuelt/statens-muligheter-for-it-modernisering-og-digital-transformasjon-1
- https://nsm.no/getfile.php/136483-1623398218/NSM/Filer/Dokumenter/VIRT-1902-NO%20Moderne%20IT-plattform_updated%20ver.pdf

Digdir ønsket særskilt innspill på følgende spørsmål:

- ***Er det mangler i beskrivelsen av utfordringsbildet?***

NSMer enig i mye av det som er skrevet om utfordringsbildet. Kapitlet kunne vært noe mer spisset, blant annet ved å slå sammen flere av problembeskrivelsene under tittelen «*mangelfull sikkerhetsstyring*». NSM gir ut årlige risikorapporter i form av Risiko YY og NDIG YYYY (se https://nsm.no/regelverk-og-hjelp/rapporter/). Det kan være enkelte momenter i disse rapportene som også er relevante for målgruppen for notatet, for eksempel:

- Manglende kartlegging av (nasjonale) verdier
- Manglende oversikt over trusselbildet og vanlige utnyttelsesmetoder
- Manglende oversikt over risikobildet
- Utnyttelse av sårbare verdikjeder
- Lav sikkerhetsbevissthet.

- ***Vurderer dere den beskrevne strategiske retningen som egnet for å styrke arbeidet med informasjonssikkerhet i forvaltningen?***

NSM mener det er mange gode momenter her. Vi anbefaler imidlertid at behovet for overordnet strategi for IT-modernisering og digital transformasjon inkluderes, se våre innledende kommentarer om Behov for IT-modernisering og digital transformasjon – infrastruktur, plattform og tjenester.

- ***Hvilke synspunkter har dere på en tydeligere felles referanseramme (eller «norm») for offentlige virksomheters arbeid med informasjonssikkerhet og de andre konseptene som beskrives?***

Det finnes allerede en rekke ulike veiledere og støttemateriell for offentlig sektor som er tilgjengelig for bruk. Det er viktig at man hele tiden jobber for at dette skal være relevant, oppdatert og tilpasset brukerne. Det kan være utfordrende for den enkelte virksomhet å holde oversikt over tilgjengelige veiledere og støttemateriell hos de ulike veiledningsaktører. En felles referanseramme kan være en god måte å hjelpe virksomheter i dette arbeidet. NSMs hovedbidrag inn i en mulig felles referanseramme vil trolig være videreutvikling av grunnprinsippene slik at dette kan benyttes som en tiltaksbank for virksomheter, se for øvrig innledende kommentarer. Videreutvikling av grunnprinsippene vil være en separat aktivitet som

NSM er ansvarlig for og det er ønskelig med innspill fra målgruppen i notatet underveis i utviklingsarbeidet.

- ***Hvordan vurderer dere behovet for samarbeid for å nå målsetningene som beskrives i notatet, og har dere innspill på hvordan et slikt samarbeid bør innrettes og organiseres?***

NSM antar at Digdir fortsetter med de etablerte samarbeidsarenaene som blant annet omfatter «nettverk for veiledningsaktører» og «nettverk for informasjonssikkerhet». Dette er nyttige arenaer der informasjon utveksles og diskuteres. NSM holder gjerne innlegg om aktuelle områder og informerer gjerne om pågående aktiviteter og prosjekter. Utover dette har vi på nåværende tidspunkt ikke innspill på hvordan et samarbeid bør innrettes og organiseres.

- ***Hvilke andre initiativer det er viktig å ta hensyn til i videre arbeid?***

Se innledende kommentarer om behov for IT-modernisering og digital transformasjon.

Med hilsen

Ingunn Mari Skaaden
underdirektør

Geir Løvnes
seksjonssjef

Dette dokumentet er elektronisk godkjent hos Nasjonal sikkerhetsmyndighet og sendes uten signatur.

Kopi til:
JUSTIS- OG BEREDSKAPSDEPARTEMENTET (JD)