Norsk senter for informasjonssikring
Studievegen 2, 2815 Gjøvik

Telefon +47 40 00 58 99
post@norsis.no | www.norsis.no NO 995 195 003 MVA

Digitaliseringsdirektoratet
Postboks 1382
0114 Oslo

Gjøvik, 25.08.2022

Innspill til høring om notat Felles sikkerhet i forvaltningen

1. Bakgrunn

Norsk senter for informasjonssikring (NorSIS) viser til mottatte brev fra Digitaliseringsdirektoratet, hvor det bes om høringsinnspill til notat om Felles sikkerhet i forvaltningen. Dette brevet representerer NorSIS sine kommentarer til det utsendte notat.

2. Drøfting

NorSIS vil forsøke å besvare de konkrete spørsmålene som er listet i invitasjonsbrevet. I tillegg vil det bli gitt noen generelle kommentarer i det etterfølgende:

2.1 Generelt

NorSIS støtter behovet for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning.

2.1.1. Begrepsapparat

I Norge har et manglende felles begrepsapparat vært en betydelig utfordring i mange år. Dette har spesielt kommet til uttrykk etter at relativt nye ord og uttrykk som cyber og digitalisering har blitt introdusert. I enkelte sammenhenger er det forsøkt å tilpasse og oversette engelskspråklige definisjoner, samt ord og uttrykk til norsk, men i andre tilfeller blir de engelske ordene tatt inn i det norske språk. Det er svært bra at det gjøres et forsøk på å beskrive og definere relevante ord og uttrykk. Dette er ofte en forutsetning for effektiv samhandling og samstyring.

Informasjonsbehandling er et sentralt og gjennomgående tema i hele notatet. Det ser ut som om det er gjort forsøk på å beskrive og definere begrepet flere steder i dokumentet. Det bør legges ytterligere vekt på å utforme en entydig og autorativ definisjon av dette begrepet.

Et annet sentralt begrep er informasjonssikkerhet. Slik det fremgår i dokumentet, benyttes ofte informasjonssikkerhet, cybersikkerhet, datasikkerhet, IT-sikkerhet, IKT-sikkerhet, digital sikkerhet om hverandre, selv om disse begrepene kan ha forskjellig innhold og betydning. Et eksempel på dette kan være at det i notatet er beskrevet følgende: «informasjonssikkerhet handler om å sikre informasjonsbehandlingen i de oppgavene og tjenestene som offentlige virksomheter har ansvaret for.» I mange sammenhenger blir informasjonssikkerhet benyttet om forhold som har med sikkerheten til selve informasjonen å gjøre, og ikke de mer prosessuelle forhold som kan knyttes til informasjonsbehandlingsbegrepet. Når det har vært gjort forsøk på å definere begreper og uttrykk innenfor dette fagområdet, har det i flere sammenhenger vært henvist til von Solms og van Niekerk sine modeller og beskrivelser fra 2013. Selv om det har skjedd en viss utvikling av fagområdet siden 2013, kan både modellene og beskrivelsene fortsatt nyttes som hensiktsmessige referanser.

Gitt de utfordringene som er knyttet til begrepsforståelsen av en del sentrale begreper anbefales det at disse utdypes og tydeliggjøres ytterligere.

I pkt 4.3 er det beskrevet at virksomhetene skal ha gode grunner for ikke å følge anbefalingene som er gitt, og at anbefalingene i realiteten er bør-krav. Med dette som utgangspunkt, bør det vurderes om ikke bruken av begrepet anbefaling bør justeres.

2.2 Innspill til konkrete spørsmål

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

  Utfordringsbildet er uten tvil omfattende, sammensatt og komplisert. Beskrivelsen i notatet favner bredt og ivaretar mange viktige og sentrale problemstillinger og utfordringer.

  Det som imidlertid kan være litt utfordrende er å identifisere de bakenforliggende årsakene til de beskrevne problemene.
  Hvis vi for eksempel tar for oss problemstilling 1: «Svake eller manglende styringsaktiviteter».
  Er årsaken til svake eller manglende styringsaktiviteter at kompetanse om styring i forvaltningen er for dårlig, skyldes det svak eller manglende kompetanse om informasjonssikkerhet, eller kan det skyldes generell dårlig ledelse?
  For å kunne iverksette gode og effektive korrektive tiltak, kan det generelt sett være behov for å identifisere årsakene til opplevde problemene på et noe mer detaljert nivå. På enkelte områder kan nok de beskrevne utfordringer og problemer være anerkjent og akseptert av de involverte og berørte aktørene, mens på andre områder kan det være et potensiale for at de beskrevne utfordringene blir oppfattet som udokumenterte påstander.

  Spørsmålet er også hvordan utfordringsbildet skal struktureres. Det finnes helt sikkert mange måter å gjøre dette på, noe avhengig av den enkelte virksomhet og sektors erfaringer og fremtidige behov. I enkelte sammenhenger har det vist seg at det kan være hensiktsmessig å beskrive utfordringsbildet, knyttet til forskjellige personellkategorier som for eksempel ledere, medarbeidere (kan evt deles opp i HR, økonomi, logistikk, fagmedarbeidere osv, IT-driftspersonell, sikkerhetspersonell.

  I beskrivelsen av utfordringsbildet, finnes det ingen eksplisitt fremstilling av trusselbildet, herunder aktuelle trusselaktører, og de mest sannsynlige angrepsmåter/-vektorer som potensielt kan ramme aktører innenfor offentlig forvaltning. Det er selvfølgelig en vurdering om dette er nødvendig, og vil kunne ha en sammenheng med hvorvidt de sikkerhetsmessige tiltak skal utformes helt generisk, eller mer spesifikt, basert på den gjeldende trussel eller den enkelte virksomhet sine særegenheter.

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

  Den beskrevne strategiske retningen vil kunne bidra til å styrke arbeidet med informasjonssikkerhet i offentlige virksomheter og med samarbeidene virksomheter. En felles veiledning og referanseramme, vil kunne bidra til å legge grunnlaget for et bedre samarbeid, både vertikalt og horisontalt på tvers av både etater, direktorater og ikke minst mellom nivåene. Den beskrevne retningen kan også bidra til at digital sikkerhet kan bli bedre integrert i annen offentlig virksomhet, som for eksempel i arbeidet med å ytterligere forbedre digitaliseringsarbeidet. Videre kan den strategiske retningen som er beskrevet bidra til at informasjons- og digital sikkerhet, kan bli en naturlig del av virksomhetsstyringen, hvor det kan utformes relevante måle- og styringsparametre.

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

  Sannsynligvis vil en tydeligere felles referanseramme bidra til å forenkle et til dels komplisert fagområde. Ikke minst kan det bidra til forenkling for virksomhetsledere, uten spesifikk digital sikkerhetskompetanse.

  På den andre siden kan det være en viss fare for at sikkerhetsarbeidet kan bli for generisk, og en «sovepute» for virksomhetene, ved at de respektive aktører kan si seg fornøyd med å innføre generiske tiltak. Dermed kan sikkerhetsarbeidet i større grad bli «compliance»-basert, snarere enn risikobasert som er en klart uttrykt målsetting.

  Erfaring har vist at det for enkelte kan være komplisert og noe abstrakt å forholde seg til risikovurderinger. Beskrivelsen av kategorier og nivåer av konsekvenser, slik det er beskrevet i dokumentet, vil være til god hjelp for å gjøre det enklere å komme i gang med denne typen vurderinger, samt å skape en større grad av felles forståelse av risiko

  Det kan imidlertid bli utfordrende og krevende å forvalte innholdet i basisnivåene over tid med relevant og oppdatert innhold.

  Tilgjengeliggjøring av felles tjenester og felles tjenesteutvikling er en god tanke, vil definitivt kunne bidra til å forenkle og forbedre sikkerhetsarbeidet.

  Det er også svært positivt at forholdene rundt oppfølging og kravstilling til eksterne eller tredjeparts tjenesteleverandører blir beskrevet i et informasjonssikkerhetsperspektiv.

  Faktiske undersøkelser viser at kompetansenivået til ansatte i både privat og offentlig sektor er svært varierende. I tillegg er det i mange virksomheter mangel på tilrettelagte opplærings- og utdanningsaktiviteter. Basert på dette, bør det vurderes å legge mer vekt på krav til opplæring og sertifisering, og arbeid med digital sikkerhetskultur som helhet

- **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?**

  Samarbeid på tvers anses som helt vesentlig for å nå målsettingene om både økt digitalisering og forbedret sikkerhet i offentlig sektor.

  For å oppnå et ønsket samarbeid, er det en forutsetning at det etableres nødvendig tillit mellom aktørene. Dette krever at det skapes forutsigbarhet og langsiktighet for alle involverte aktører. Den enkelte må tenke utover eget ansvar og funksjonsperiode. Det er viktig at de ikke er kamp om makt, innflytelse, oppgaver og ressurser mellom aktørene. Dette kan kreve en tydelig oppdeling og definering av roller, ansvar og myndighet. Tilrettelegging for størst mulig åpenhet og transparens i forvaltning er også svært viktig, for å kunne oppnå et godt samarbeid. Det kan i denne sammenheng oppnås positive effekter ved å tillegge et styrings- og ledelsesansvar til en aktør som ikke har egeninteresser i arbeidet.

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

  Generelt bør det videre arbeid ses i sammenheng med digitaliseringsarbeidet i Staten. I tillegg bør det legges opp til en kontinuerlig oppdateringsprosess, hvor resultatet av risiko-, trussel og sårbarhetsrapporter, samt andre relevante analyser og undersøkelser blir lagt til grunn.

Det er naturligvis nødvendig at eventuelle justering av nasjonale strategier og policyer innenfor cyber- og digital sikkerhet, blir hensyntatt.

Det bør også undersøkes om det pågår relevant forskningsaktivitet i Norge og eventuelt i utlandet, hvor resultatene kan benyttes i det videre arbeidet.

3. Avslutning

NorSIS takker for invitasjonen til å bidra i arbeidet med en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning. Selv om offentlige virksomheter ikke faller inn under hovedmålgruppene til NorSIS, anses det verdifullt å få muligheten til å bidra i det videre arbeidet.

Med vennlig hilsen

Knut Ivar Rønning
Seniorrådgiver
NorSIS

Karoline Hultman Tømte
Faglig leder
NorSIS