Foreningen kommunal informasjonssikkerhet
Daglig leder Harald Torbjørnsen
Telefon +47 489 94 701

Innspill til høring om notat Felles sikkerhet i forvaltningen

KiNS takker for muligheten til å gi innspill til notat om felles sikkerhet i forvaltningen. Vi er en medlems- og interesseorganisasjon primært for kommuner, fylkeskommuner og kommunale/offentlige virksomheter, men har også en del bedriftsmedlemmer.

Spørsmålene Digitaliseringsdirektoratet ber oss besvare ut er:

1. Er det mangler i beskrivelsen av utfordringsbildet?
2. Vurderer dere den beskrevne strategiske retningen som egnet for å styrke arbeidet med informasjonssikkerhet i forvaltningen?
3. Hvilke synspunkter har dere på en tydeligere felles referanseramme (eller «norm») for offentlige virksomheters arbeid med informasjonssikkerhet og de andre konseptene som beskrives?
4. 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?
5. Hvilke andre initiativer det er viktig å ta hensyn til i videre arbeid?

I tillegg vil KiNS å gi noen spesifikke tilbakemeldinger rundt tiltakene som er foreslått.

Generell tilbakemelding

KiNS arbeider for å styrke kommunal sektor i sitt arbeide med informasjonssikkerhet og personvern. Vi er positive til initiativet om et felles løft for informasjonssikkerhet i offentlig forvaltning. For gjennomslagskraften er det viktig at økonomiske og administrative konsekvenser utredes og kommuniseres ut i en tidlig fase av arbeidet.

Vi mener det er viktig å få fram at informasjonssikkerhet er en investering og ikke en kostnad. For mange virksomheter og organisasjoner i offentlig sektor vil arbeidet med å komme opp på basisnivå 1 kreve store investeringer både økonomisk, organisatorisk og kvalitativt.

KiNS mener det er viktig at arbeidet med et felles referanseverk kan fungere som en katalysator for bedre digitale løsninger for å håndtere informasjonssikkerhet og personvern lokalt. I den forbindelse er det viktig at notatets anbefalinger som foreksempel katalog over informasjonstyper, tiltaksbank og lignende, tilbyr standardiserte APIer for bruk inn mot leverandørbransjen og virksomheter i offentlig sektor.

KiNS anser det som en svakhet at Utdanningsdirektoratet ikke er høringsinstans for notatet. Direktoratet for høyere utdanning og kompetanse er oppført som høringsinstans, men de treffer i liten grad oppvekstsektoren i kommuner og fylkeskommuner. Oppvekst og helse er kommunenes største sektorer og vil være avgjørende for kommuner og fylkeskommuner sin evne til å nå de beskrevne sikkerhetsnivåene. Arbeidet med informasjonssikkerhet og personvern i grunnopplæringen er et ansvar KiNS mener Utdanningsdirektoratet må ta forvaltningsmessige grep om i sin sektor på lik linje som Direktoratet for e-helse har gjort overfor helsesektoren. Det er derfor viktig at Utdanningsdirektoratet inkluderes i det videre arbeidet.

I beskrivelsen av situasjonsbildet bli det påpekt mangler relatert til styringsaktiviteter, grunnleggende sikkerhetstiltak, oversikt over informasjonsbehandlingen og utfordringer med helhetlig tilnærming i virksomhetene. Ett tiltak som KiNS mener kan være med på å øke bevisstheten til virksomhetenes- og organisasjonenes toppledelse, er et krav om jevnlig standardisert rapportering til toppledelsen om disse elementene. På lik linje som at toppledelsen jevnlig får rapporter om økonomi og andre virksomhetskritiske elementer. Dette er et tiltak som vi anbefaler inkluderes i et nasjonalt referanseverk for informasjonssikkerhet.

Er det mangler i beskrivelsen av utfordringsbildet?

KiNS mener utfordringsbildet er godt beskrevet og får fram alvoret i, og omfanget av situasjonen som kommuner og fylkeskommuner generelt befinner seg i.

Kommuner og fylkeskommuner har som primæroppgave å levere gode og relevante kommunale tjenester til innbyggerne. Dette forutsetter blant annet tilfredsstillende informasjonssikkerhet, digital sikkerhet og et godt personvern. KiNS sin kommentar på Digitaliseringsdirektoratet beskrivelse er at kommunal sektor ikke er rigget for å håndtere dette ansvaret fult ut, da flere vurderinger som skal gjøres er utenfor kommunal sektor sin kontroll. Det være seg tekniske, juridiske og forvaltningsmessige problemstillinger som f.eks manglende overføringsgrunnlag til land utenfor EU og globale aktører som selger løsninger til kommunal sektor. Utfordringsbildet løses ikke alene med å tilføre kommunal sektor mer kompetanse i alle ledd, det må også gjøres forvaltningsmessige grep i styringslinja, på tvers av sektorene i offentlig forvaltning, slik at hele forvaltningen har en enhetlig rigg for å løse utfordringsbildet.

Personvern må inkluderes som et viktig element i en helhetlig rigg for forvaltning og styring da dette er fagområder som lokalt må inkluderes i samme styringssystem.

KiNS ser det som avgjørende at et felles referanseverk bygger på, og er kompatible og i samsvar med kjente standarder som allerede er rådende i offentlig sektor. Eksempelvis ISO 27xxx, NSM grunnprinsipper ol.

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

KiNS stiller seg bak den beskrevne strategiske retningen og mener det et presserende behov for et nasjonalt løft for informasjonssikkerhet generelt og digital sikkerhet spesielt. Viktig at arbeidet bygges på det som allerede finnes og utvikles i samarbeid med andre aktører i forvaltningen. KiNS mener det er avgjørende at Digitaliseringsdirektoratet får på plass et godt mandat som gir arbeidet nødvendig tyngde og forankring, slik at hele offentlig forvaltning vil hensynta et nasjonalt løft. Vi må arbeide sammen på tvers av sektorene, styrke hverandre osv., men en aktør må ha mandat til å skjære igjennom ved behov. For KiNS er Digitaliseringsdirektoratet et naturlig valg for den rollen.

Foreningen kommunal informasjonssikkerhet
Daglig leder Harald Torbjørnsen
Telefon +47 489 94 701

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

KiNS mener det er av største nødvendighet at arbeidet med felles referanseverk så raskt som mulig oppgraderes til et normgivende og ikke bare rådgivende arbeid. Aller helst skulle vi sett at arbeidet fikk status som rammeverk for informasjonssikkerhet i offentlig forvalting, inkludert kommunal sektor, med en tydelig politisk forankring. Det pågår flere initiativ i parallell både i stat og kommune for å gjøre situasjonen for sin sektor/sine virksomheter bedre. Behovet for koordinering og et overordnet rammeverk som forplikter er derfor prekært.

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 for å nå målsetningene er avgjørende. Et produktivt samarbeid for å nå målbildene avhenger av et tydelig og kraftfullt mandat som medfører at alle aktuelle samarbeidspartnere opplever at de har stor egeninteresse av å delta i arbeidet for å kunne realisere gevinstbildene i sine sektorer og for sine organisasjoner.

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

Det blir viktig å hensyn ta politisk valgte løsninger som Feide, Altinn og Markedsplassen for skytjenester i offentlig sektor. Videre må blant annet KS og deres arbeid ut mot kommunesektoren trekkes inn, tilsvarende for arbeidet som foregår i regi av Direktoratet for e-helse, Utdanningsdirektoratet, Direktoratet for høyrer utdanning og forskning, Nasjonal sikkerhetsmyndighet, Datatilsynet, NorSIS og Direktoratet for samfunnssikkerhet og beredskap.

KiNS har to pågående prosjekter som det er aktuelt å ha dialog rundt og eventuelt trekke inn i det videre arbeid. Det ene prosjektet er en ressurs for å generere relevante og standardiserte krav til digital sikkerhet og informasjonssikkerhet ved innkjøp. Det andre prosjektet er en ressursbank for risikoscenarier og tiltak til bruk i arbeidet med gjennomføring av risikovurderinger og personvernkonsekvensvurderinger.

Tilbakemelding på foreslåtte tiltak

Generelt er det gode tiltak. Der er elementer som kan kommenteres på alle foreslåtte tiltak, men KiNS velger å kommentere på kun to av de foreslåtte tiltakene for spisse tilbakemeldingen.

T3 Basisnivåer

Et tiltak med potensiale til å forenkle og effektiviser arbeidsprosesser ute i kommuner, fylkeskommuner og resten av offentlig sektor. Modell og prinsipper er gode, men vi finner det

nødvendig å korrigere et viktig moment. Det grunnleggende basisnivået vil for mange offentlige virksomheter være svært krevende både teknisk, organisatorisk og økonomisk. På grunn av stort strekk i laget vil investeringsbehovet her variere stort, men det er rimelig å anta, ut ifra tilbakemeldinger KiNS mottar fra våre medlemmer, at investeringskostnaden vil kunne være spesielt omfattende for svært mange kommuner. Informasjonssikkerhet og personvern er en investering og ikke en kostnad. Det er et viktig prinsipp som må gjennomsyre kommunikasjonen rundt felles referanseverk og basisnivåene. Har en offentlig virksomhet først gjort det tunge løftet opp til basis nivå nr. 1 så vil videre investeringer for å komme på basisnivå 2 og 3 være mindre kostnadskrevende for organisasjonen som helhet.

T4 felle tiltaksbank for offentlig sektor

Felles tiltaksbank for offentlig sektor bør basere seg på arbeid som alt gjøres eller er gjort. KiNS har i samarbeid med flere medlemmer og samarbeidspartnere startet et arbeid med å utvikle en katalog over relevante risikoscenarioer og tiltak for kommuner og FK, som har stor overføringsverdi til resten av offentlig sektor. En hovedutfordring med felles tiltaksbank er vedlikehold og forvaltning over tid.

KiNS ber derfor om at det gjennomføres konkret dialog mellom KiNS og Digitaliseringsdirektoratet i det videre arbeidet knyttet til felles tiltaksbank, da mye standardiseringsarbeid allerede er gjennomført mot kommunal sektor. Et arbeid medlemmer av KiNS ber oss utvikle videre i dialog med våre samarbeidspartnere.