



Justis- og beredskapsdepartementet - JD
Postboks 8005 Dep.
0030 OSLO

Vår referanse: 15/01824-2
Arkivkode: X00
Saksbehandler: Anne Mette Dørum
Deres referanse: 15/8216
Dato: 15.03.2016

Høring - Digital sårbarhet - sikkert samfunn - Nou 2015-13

Lysne-utvalget har nylig lagt fram NOU 2015: 13 Digital sårbarhet - sikkert samfunn.), med høringsfrist 15. mars 2016.

Utvalget maler med bred pensel og har kartlagt samfunnets digitale sårbarhet og foreslått tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utredningen gjennomgår digitale sårbarheter innenfor samfunnsfunksjonene elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, olje og gass, vannforsyning, finansielle tjenester, helse og omsorg, transport, kompetanse, fellesfunksjoner, styring og kriseledelse og avdekke og håndtere digitale angrep. Utvalget har satt digitalisering både i et samfunnsperspektiv og i et informasjonssikkerhetsperspektiv.

Utredningen inneholder flere analyser og forslag som har betydning for kommunesektoren. Et særlig viktig forslag er at det bør etableres en mekanisme for deteksjon og håndtering av IKT-sikkerhetshendelser i kommunesektoren - et kommuneCERT eller kommune CSIRT. Begrepet CSIRT er til fri benyttelse og mest anvendelig i kommunal sammenheng. Behovet for en kommuneCSIRT er omtalt flere steder i utredningen.

KS vil i dette høringssvaret avgrense merknadene til anbefalingene om å etablere kommuneCERT/kommuneCSIRT .

Merknader til kapitlet om vannforsyning

Det er allerede flere CERT-er i Norge, ett nasjonalt CERT (NSM NorCert) og fem sektorCERT. Det planlegges å etablere et NkomCSIRT og i utredningen foreslås det å etablere et CERT for vannforsyning. Når det gjelder vannforsyning er det nevnt tre alternativer for etablering av felles responsmiljø for hendelseshåndtering:

- 1) Kommunene oppretter en egen kommuneCERT som også omfatter vannforsyning
- 2) Fylkesmannen tar initiativ til en regional plan for hendelseshåndtering i kommunale vannverk
- 3) At vannverkene knytter seg opp mot allerede eksisterende hendelseshåndteringsmiljø

Lysne-utvalget anbefaler at Helse- og omsorgsdepartementet, i samråd med Justis- og beredskapsdepartementet og Kommunal- og regionaldepartementet, utreder muligheten for et responsmiljø for hendelseshåndtering som ivaretar vann og avløp.

KS kan vanskelig si seg uenig i de problemstillingene som løftes i kapittel 15 om vannforsyning. Det er en åpenbar utfordring om vann blir borte over lengre tid, ikke minst i større byer, ettersom vann også er grunnlaget for alt avløp. KS vil likevel påpeke at vann og avløp har tett sammenheng med tilgang på energi. Forsvinner strøm, forsvinner raskt både grunnlaget for vann og avløp.

KS støtter Lysne-utvalgets anbefaling om at Helse- og omsorgsdepartementet, i samråd med Justis- og beredskapsdepartementet og Kommunal- og regionaldepartementet, utreder muligheten for et resposmiljø for hendelsehåndtering som ivaretar vann og avløp. KS mener at det er nødvendig at kommunesektoren selv er part i denne utredningen. Videre mener KS at utredningen bør belyse hvilken rolle resposmiljøene for både vannkraft (KraftCERT) og helsesektoren (HelseCERT) bør ha.

Merknader til anbefaling om etablering av kommuneCERT/kommuneCSIRT

NorSIS-rapporten «KommuneCERT – utredning av behov og muligheter», som det vises til i NOU-en, påpeker at mange kommuner har liten evne til å håndtere cyber-trusler, samtidig som alle kommunale tjenesteområder er fullstendig avhengig av IKT. Datakriminalitet, sabotasje eller hærverk på kommunale IKT-systemer vil derfor kunne få store samfunnsmessige konsekvenser. Kommunene står overfor et komplekst trusselbilde som kan ramme bredt. Evne til forebygging og håndtering av cyber-hendelser er en forutsetning for å opprettholde kommunale tjenester. Mangelfull cyber-sikkerhetsberedskap står derfor i sterk kontrast til den betydelige innsats som legges ned i digitalisering av sektoren.

NorSIS foreslår organisering av KommuneCSIRT som en koordinerende kapasitet. NOU-en viderefører denne anbefalingen.

Behovet for en variant av et KommuneCSIRT synes veldokumentert, både i NOU 2015:13 og i NorSIS-rapporten. NorSIS-rapporten gir i tillegg et godt bilde av utfordringer og aktuelle oppgaver. KS støtter de vurderingene som er gjort i NOU-en og av NorSIS om at det er behov for et samlet løft for kommunesektorens informasjonssikkerhet. Gjennom en CERT-funksjon vil kommuner og fylkeskommuner bli mer bevisst på egen informasjonssikkerhet, og de vil få tilgang til en koordinerende funksjon, et resposmiljø, som har kompetanse på området.

KS mener at det gjenstår en del avklaringer før et eventuelt KommuneCSIRT kan etableres:

- Utrede relasjonen mellom KommuneCSIRT og øvrig kommunal avviks- og krisehåndtering, herunder konkretisere hvilke oppgaver en KommuneCSIRT bør tillegges, for å ivareta sin rådgivende funksjon.
- Utrede ulike organisasjonsmodeller og organisasjonstilknytning, og det må tas stilling til endelig anbefalt modell.
- Utrede aktuelle finansieringsmodeller og konsekvenser av disse. Statlig finansiering må avklares.
- Forholdet til andre sektor-CERTer må avklares herunder spesielt HelseCERT. Alle kommuner er tilknyttet helsenetttet og har mulighet til å benytte tjenester fra HelseCERT.

KS mener at Lysne-utvalgets foreslåtte utredningen om etablering av felles responsmiljø for hendelseshåndtering innen vannforsyning bør utvides til å omfatte utredning av behov for et eget KommuneCERT. KS mener at det er nødvendig at kommunesektoren selv er part i denne utredningen. Videre mener KS at utredningen bør belyse hvilken rolle responsmiljøene for både vannkraft (KraftCERT), helsesektoren (HelseCERT) og de øvrige sektorCERT-ene bør ha.

Konklusjon

NOU-en peker på mange sentrale og viktige utfordringer. KS mener at kommunesektoren har behov for en kompetanse- og koordineringsfunksjon på informasjonssikkerhetsområdet. Funksjonen bør informere kommunene om trusler mv. og koordinere og «oversette» varsler til kommunen som kommer fra andre norske eller internasjonale CERT-er.

KS ser et klart behov for samordning og prioritering på tvers av kommunale tjenesteområder ved IKT-hendelser. Et KommuneCSIRT bør derfor være i stand til å gi råd til kommunenes ledelse om tiltak og prioriteringer for å redusere risiko slik at kommunale tjenester kan opprettholdes. Varsler og sensorinformasjon kan trolig innhentes eller anskaffes fra sektorCERTer og andre IKT-leverandører som grunnlag for KommuneCSIRT sine analyse- og rådgivningstjenester.

Kommunesektoren har i dag organisert seg ulikt på informasjonssikkerhetsområdet og flere kommuner benytter seg av tjenester fra UninettCERT og HelseCERT. Disse CERT-ene koordinerer ikke kommunesektoren, det er ikke innenfor dagens ansvarsområde for disse responsmiljøene. Det må utredes hvordan disse kan understøtte en fremtidig KommuneCSIRT funksjon.

Behovet for en kommunal responsfunksjon er veldokumentert. Kompetanse og samordningsbehovet på tvers av kommunale tjenesteområder er betydelig ved IKT-hendelser. Organisering, relasjoner til andre sektorvise CERTer og finansieringsmodell bør derimot utredes nærmere. Juridiske implikasjoner ved ulike organisasjonsformer må inngå i utredningen.

Mottaker	Adresse	Post	Kontaktperson
Justis- og beredskapsdepartementet - JD	Postboks 8005 Dep.	0030 OSLO	