

Meld. St. 10 (2016-2017) Risiko i et trygt samfunn - samfunnssikkerhet

NITO vil ta opp digitale sårbarheter og IKT-sikkerhet (kap. 6), sortert under temaene sektorovergripende regelverk, IKT- sikkerhetskompetanse og offshoring.

Sektorovergripende regelverk og styring

I dag har det enkelte fagdepartement det overordnede ansvaret for å ivareta sikkerheten i sektorens IKT-infrastruktur, og for å drive forebyggende IKT-sikkerhetsarbeid. NITO mener det har resultert i en fragmentering av hvilke krav som stilles.

- Det er behov for samordning av regelverk som omtaler IKT-sikkerhet. Når Regjeringen sier at den vil vurdere å etablere tverrsektoriell regulering innenfor IKT-sikkerhetsområdet er vi positive til dette.
- Det bør utredes hvordan IKT-sikkerhetsansvaret kan styrkes gjennom å etablere et tydeligere ansvar for dette på tvers av sektorene. Det bør være på departementalt nivå f.eks. gjennom et fast interdepartementalt utvalg med ansvar for koordinering av IKT-sikkerheten.

De ulike tilsynene møter svært ulike krav, og har i ulik grad nødvendig hjemmel til å utøve sikkerhetsrettet aktivitet. De har i tillegg hatt for lav IKT-sikkerhetskompetanse eller lav kapasitet til å gjennomføre tilsyn.

- NITO ser positivt på at det varsles at det skal tas grep for å styrke tilsynenes IKT-sikkerhetskompetanse.

IKT-sikkerhetskompetanse

Samfunnet har behov for økt kompetanse om IKT-sikkerhet. Med den mangel på generell IKT-kompetanse som er i Norge i dag, er vår erfaring at mange har mest fokus på at ting skal virke, og for lite fokus på informasjonssikkerhet.

- NITO er positiv til at Regjeringen vil følge opp Lysneutvalgets forslag om en nasjonal kompetansestrategi for IKT-sikkerhet. Det bør innføres krav til IKT-sikkerhet i alle IKT-bachelorgrader, og kapasiteten på mastergrader innen IKT-sikkerhet må styrkes.
- Vi merker oss at videreutdanning innenfor IKT-sikkerhet vil bli vektlagt i den kommende kompetansestrategien.

Offshoring

Når virksomheter benytter seg av skytjenester i sin digitale strategi er målsetningen gjerne å kutte kostnader. Det er gjort ikke tilstrekkelig vurdering av sikkerhetsmessige konsekvensene ved å flytte IKT-oppgaver ut av landet. Både offentlige og private virksomhetene må ta inn over seg at det koster å opprettholde sikkerheten.

- Offentlige virksomheter må gå foran og ha tilgang til både kompetanse og klare retningslinjer ved bruk av skytjenester.
- Alle offentlige registre som lagrer sensitive eller samfunnskritiske data må lagre data på servere i Norge, og registrene må driftes av norske selskap.
- Det må innføres en godkjenningsordning for offentlige virksomheter som ønsker å offshore f.eks. hos Datatilsynet.

Sikkerhetsloven

Sikkerhetsloven er utvidet til å gjelde nasjonale kritiske samfunnsfunksjoner. I dag mangler det kompetanse på å vurdere hva som er samfunnskritisk i egen sektor. I forlengelsen av dette har NITO spilt inn i høring til sikkerhetsutvalget at det bør utvikles en tverrsektoriell, nasjonal strategi for sikring av nasjonale kritiske samfunnsfunksjoner. En slik strategi bør sees i sammenheng med allerede eksisterende hjemmelsgrunnlag i

medhold av sikkerhetsloven. Gjennom å utarbeide en strategi vil ulike samfunnsfunksjoner kunne tilstås en form for verdi, som igjen gir grunnlag for hvilke skjermingstiltak som må settes inn for akkurat den funksjonen.