NITO

Justis- og beredskapsdepartementet

25.03.2019

Vår ref. Lars Øystein Eriksen Deres ref.

Høringsinnspill IKT-sikkerhet i alle ledd
NITO - Norges Ingeniør- og Teknologorganisasjon - er Norges største organisasjon for ingeniører og teknologer på alle nivå; bachelor, master og høyere. Vi har over 88.000 medlemmer i alle sektorer, herunder ca. 10 000 innen IKT.

NITO har over lengere tid etterlyst bedre regulering av IKT-sikkerhet, og er positiv til at regjeringen nedsatte IKT-sikkerhetsutvalget. NITO merker seg at utvalget legger som overordnet prinsipp at IKT-sikkerhet må balanseres opp mot brukervennlighet, økonomi og menneskerettigheter. NITO vil påpeke at når det gjelder balanse mot økonomi må det være *samfunnsøkonomisk* og ikke *bedriftsøkonomisk* lønnsomhet som må ligge til grunn. Utover dette støtter NITO en slik balanse.

Støtte til tydeligere regulering av IKT-sikkerhet
NITO ønsker mer sektorovergripende regulering av IKT-sikkerhet. Regelverk som omtaler IKT-sikkerhet i dag er fragmentert, og det er et klart behov for samordning. NITO stiller seg derfor positiv til forslaget om en egen lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning. Videre bør definisjonen av hva som er samfunnskritiske virksomheter basere seg på DSBs beskrivelse av samfunnskritiske funksjoner.

Utvalget forslår at den nye loven skal stille krav til forsvarlig IKT-sikkerhet. Mange offentlige myndigheter baserer seg på veiledninger, slik som *Norm for informasjonssikkerhet i helsesektoren*. NITO mener disse veilederne i for stor grad åpner for frivillighet. NITO mener at en ny lov må etablere krav til sektorovergripende minstestandard for beskyttelse av kritisk infrastruktur. Minstekrav må følges av krav til kompenserende tiltak og avviksrapportering.

I dag omtaler omlag 150 lover og forskrifter IKT-sikkerhet. Utvalget viser til at IKT-sikkerhetsregelverket har uensartet tilnærming til regulering noe som igjen gjør det krevende å få oversikt over faktiske krav. Det vil være mye enklere for den enkelte virksomhet å forholde seg til ett sektorovergripende regelverk for IKT-sikkerhet. I tillegg må det ryddes opp i begrepsbruk i tråd med ordlyden som benyttes i en ny lov. I dag brukes ulike begreper for å beskrive det samme, samtidig som samme begrep brukes for å beskrive ulike krav.

Utvalget tar opp hvorvidt loven bør være bredere og omfatte alle virksomheter. NITO mener dette kan være nødvendig, men at det er hensiktsmessig med et eget lovutvalg som kan vurdere dette.

Sikkerhet ved bruk av skytjenester
NITO vil understreke at sikkerhetskompetanse hos leverandører av skytjenester er svært uensartet. NITO mener det bør opprettes et felles minimumskrav for tilbydere av skytjenester til offentlig sektor med standarder for bl. a. grensesnitt og sikkerhetsnivå. Dette skal sørge for at det opprettholdes et gitt sikkerhetsmessig nivå. Det vil samtidig gjøre det enklere for det offentlige å bytte leverandør.

NITO vil påpeke at det totale omfanget av utkontraktering fra Norge til utlandet vil påvirke samfunnssikkerheten, slik Digitalt Sårbarhetsutvalg også la vekt på. Selv om utkontraktering kan være innenfor akseptabel risiko for den enkelte virksomhet, kan det få store konsekvenser for samlet risiko dersom mange virksomheter flytter sin IKT-virksomhet ut av landet. Utstrakt bruk av utkontraktering kan også bidra til å svekke den nasjonale evnen til utvikling og oppfølging på sentrale kompetanseområder.

Tilstrekkelig IKT-sikkerhetskompetanse til å styre selv
Rapporten viser til at juridisk dokumentasjon kan gi en etterlevelsesillusjon. Altså at overholdelse av lov og forskrift bare er i form og ikke innhold. Aktivt bruk av tilsyn er nødvendig for å forhindre dette. Samtidig må det satses betydelig på økt IKT-sikkerhetskompetanse både fra myndigheter og blant private virksomheter.

Det tilligger virksomheter som håndterer samfunnskritiske funksjoner et stort ansvar for å utvikle solid sikkerhetskultur og kompetansemiljøer på IKT-sikkerhet, slik at de evner å følge god anskaffelsespraksis og relevant sikkerhetslovgivning i praksis og ikke bare i form. Et prinsipp må være at private virksomheter med ansvar for samfunnskritiske funksjoner har tilstrekkelig kompetanse til å styre digitaliseringen og integrere de digitale løsningene i de interne virksomhetsprosessene. Sikkerhet og kvalitet må ikke gå på bekostning av lav innkjøpspris.

IKT-sikkerhet ved anskaffelser
Offentlige virksomheter må stille større krav til IKT-sikkerhet i forbindelse med innkjøp. NITO støtter at forslaget om ny lov om IKT-sikkerhet også må inkluderer plikt til å vurdere IKT-sikkerheten ved bruk av anskaffelser.

Etablering av et nasjonalt IKT-sikkerhetssenter
Råd og veiledning fra myndigheter er for lite koordinert mellom etatene. For å koordinere uønskede hendelser og dele informasjon som gjelder IKT-sikkerhet foreslår utvalget et nytt nasjonalt IKT-sikkerhetssenter. Behovet for slik koordinering er viktig og ble også avdekket i Digitalt Sårbarhetsutvalg. Det har i ettertid blitt etablert flere sentre for cybersikkerhet.[1] Målet med etableringen av et nytt senter må derfor være tydelige. NITO mener at en forutsetning for å opprette et nytt senter må være at det faktisk skaper bedre oversikt. De ulike sentrene må ha tydelige rollefordeling seg imellom.

Regulering og ansvar for tilkoblede produkter og tjenester (IoT)
Utvalget påpeker at det finnes få retningslinjer for IKT-sikkerhet for produkter og tjenester som er koblet til internett. Selskaper og produsenter velger sine egne tilnærminger og dette igjen fører til

[1] 1. Nasjonalt cybersikkerhetssenter under NSM. 2. Nasjonalt Cyberkrimssenter (NC3) under Politiet.
3. Felles Cyberkoordineringssenter som er et samarbeid mellom NSM, E-tjenesten, PST og KRIPOS knyttet til alvorlige angrep og vurdering av risikobildet.

ulike IKT-sikkerhetsutfordringer. NITO støtter utvalget i at ansvaret må flyttes over fra forbruker til leverandører og produsenter. Det må være mulig å kreve tilbakekalling av produkter med for lav IKT-sikkerhet. NITO mener det må stilles krav om innebygget sikkerhet, såkalt security by design.

Alle nye Internet of Things (IoT)-leverandører må for øvrig sørge for at de har tilstrekkelig IKT-sikkerhetskompetanse selv. Det gir en helt annen kontinuitet og trygghet i utvikling av IoT-produkter. IoT-produkter som er koblet med en skykonto - for eksempel for å styres fra mobiltelefonen - har en ekstra sårbarhet: Hackere kan gjette passordet og overta kontrollen over IoT-produktet. I slike tilfeller har produsenten et ekstra ansvar for å beskytte tilgangen til produktet.

NITO støtter også Forbrukerrådets høringssvar om tilkoblede produkter og tjenester. Det gjelder:

- Bindende minstekrav for IKT-sikkerhet i tilkoblede forbrukerprodukter.
- Tydeligere rollefordeling og samarbeid mellom relevante sektortilsyn.
- Tilrettelagt samarbeid mellom relevante bransjeaktører og myndigheter, for å bidra med veiledning og råd.
- Koordinerte mekanismer for å ivareta og respondere på varsler om sikkerhetsbrister.
- Norske myndigheter må støtte EU-prosesser for å sikre framtidsrettet regulering for IKT-sikkerhet i tilkoblede forbrukerprodukter.

Med vennlig hilsen

Trond Markussen
President

Steinar Sørlie
Generalsekretær