Utenriks- og forsvarskomiteen

Høring Lov om nasjonal sikkerhet (sikkerhetsloven)

Innspill til sikkerhetsloven.

Kritisk digital infrastruktur og lovens virkeområde

Tekna støtter i hovedsak innretningen på forslaget til ny sikkerhetslov, og mener at dette vil legge til rette for en bedring av sikkerheten og en god utvikling av denne. Tekna ønsker imidlertid å bemerke at det er behov for mer sektorovergripende reguleringer enn det lovforslaget legger opp til med tanke på kravene til hvordan sikkerhets- og sårbarhetsanalyser gjennomføres for digitale systemer og -infrastruktur.

Tekna ser at det forestående forskriftsarbeidet med konkretisering av hva som faller inn under lovens virkeområde vil bli av stor betydning. Det er svært positivt at digital infrastruktur nå skal omfattes av loven. Det er likevel ennå høyst uklart hva som vil falle inn under definisjonen kritisk digital infrastruktur og hvilke kriterier som skal brukes til å definere hva som faller innenfor lovens virkeområde. Dette må tydeliggjøres gjennom det foreliggende forskriftsarbeidet. Tekna ønsker å understreke at det også er behov for sikkerhetsarbeid, klare rammer og reguleringer for systemer og infrastruktur som faller utenfor sikkerhetslovens virkeområde, men som likevel kan defineres som kritisk infrastruktur. Her er det i dag en gråsone som skaper usikkerhet blant både myndigheter og private aktører som håndterer slik infrastruktur.

Tekna vil

- *At Stortinget tydeliggjør kriteriene for lovens virkeområde.*
- *At Stortinget understreker viktigheten av klare regler og rammer for sikkerhets- og sårbarhetsvurderinger i virksomheter som forvalter kritisk infrastruktur, men som faller utenfor lovens virkeområde.*

Lovforslaget er tenkt å gi rom for løpende tilpasninger til endringer i bruk av digitale løsninger. Økt digitalisering bidrar til at stadig flere av samfunnets kritiske funksjoner er avhengige av digitale systemer som ved misbruk vil utgjøre en trussel mot *nasjonens suverenitet, territorielle integritet og demokratiske styreform*. Det legges i lovforslaget opp til at sektordepartementene har en løpende vurdering av egen sektors digitale infrastruktur opp mot sikkerhetslovens virkeområde. Tekna vil påpeke at det her kan være behov for sektorovergripende anbefalinger for gjennomføring av grunnleggende sikkerhets- og sårbarhetsanalyser av digitale systemer.

www.tekna.no

Org.nr.: 971 420 782
MVA

Tekna mener det er et stort behov for tydeligere retningslinjer og direktiver for slike sikkerhetsvurderinger. Dette vil være klargjørende for alle involverte aktører.

Tekna vil

- *At Stortinget fremmer forslag om at regjeringen må igangsette et arbeid med å utarbeide et tydelig rammeverk og klare nasjonale retningslinjer for å regulere hvordan sikkerhets- og sårbarhetsvurderinger av digitale systemer og infrastruktur skal gjennomføres.*

Utkontraktering av IT-oppgaver til utlandet/utenlandske selskaper

Tekna er ikke prinsipielt motstander av utkontraktering av tjenester, men er opptatt av den sårbarheten slik utkontraktering kan medføre. Dette er bredt omtalt i Lysne-I utvalgets rapport[1] og er senere presisert i en rekke uttalelser fra fagmiljøene og nasjonale sikkerhetsmyndigheter. Er man underlagt sikkerhetsloven, er adgangen til utkontraktering ut av landet sterkt begrenset.

Forebyggende sikkerhetsarbeid er av stor verdi, og behovet for slikt arbeid vil øke når lovens virkeområde utvides. Tekna mener et betydelig kompetanseløft er avgjørende for å få dette på plass. Tilstrekkelig og høy nasjonal sikkerhetskompetanse er nødvendig for å kunne følge opp det nasjonale sikkerhetsarbeidet. Dette er videre omtalt under avsnittet om kompetanse.

Tekna vil

- *At det stilles klare krav til bestillerkompetanse i virksomheter underlagt sikkerhetsloven.*
- *At regjeringen orienterer Stortinget om de kompetansemessige konsekvensene av omfattende utkontraktering og bruk av innleid utenlandsk arbeidskraft til utvikling og drift av viktige nasjonale IKT-tjenester og systemer.*

Manglende sikkerhets og sårbarhetsvurderinger ved utkontraktering

Gode risikovurderinger er essensielt ved utkontraktering av IT-tjenester og systemdrift. Det har de siste årene vært mange diskusjoner og en rekke mediesaker knyttet til sikkerhet og sårbarhet i digital infrastruktur, og det finnes en rekke eksempler på at manglende risikovurderinger i forkant av utkontraktering har ført til manglende sikkerhetstiltak. Dette har igjen ledet til økt sårbarhet. Statoil gjennomførte på en prisverdig måte en ny risikovurdering etter Mongstadsaken, og konkluderte da med at enkelte tjenester skulle hentes hjem til Norge fordi risikoen var for høy. Nasjonal kommunikasjonsmyndighet konkluderte i tilsynsrapporten fra nødnettsaken med at det ikke var gjennomført tilstrekkelige risikovurderinger. Denne saken ble henlagt av PST med henvisning til at regelverket var uklart. Den private aktøren som her hadde utkontraktert virksomhet i strid med sikkerhetsloven har i den forbindelse kommentert manglende veiledning og uklart

[1] NOU 2015: 13

regelverk. Saken med utkontraktering i Helse Sør-Øst bidrar også til bildet om uklare regler og retningslinjer.
Det er med andre ord et stort behov for en klargjøring av regelverket rundt risikovurderinger ved utkontraktering. Stortinget har gjennom det pågående lovarbeidet og tilhørende forskrifter mulighet til å gjøre noe med dette.

Tekna vil

- *Ha nasjonale krav til vurdering av sikkerhet og sårbarhet ved utkontraktering av IT-tjenester i virksomheter som forvalter kritisk infrastruktur.*

Systemdrift og datalagring

Tekna mener at drift av systemer som håndterer sensitive personopplysninger, som faller innenfor definisjonen kritisk digital infrastruktur, og som ligger innenfor lovens virkeområde, skal driftes i Norge. Tekna tar ikke stilling til hvor data lagres utover at selskapet og personalet som drifter løsningen må være lokalisert i Norge, og underlagt norsk lov og regelverk. Nærhet er viktig for løpende sikkerhetsvedlikehold og driftsoppgaver. Ved en eventuell lagring av data i et annet land, må risiko- og sikkerhetsvurderingen også omfatte en vurdering av lovverk og sikkerhetssituasjon i landet der dataene lagres. Svært sensitive persondata som kan være mål for eksempelvis utpressing, mener Tekna bør lagres i Norge.

Tekna vil

- *Pålegge datalagring i Norge av data knyttet til nasjonale sikkerhetsinteresser.*
- *At drift av systemer som håndterer sensitive personopplysninger, er innenfor sikkerhetslovens virkeområde, og som defineres som kritisk infrastruktur, skal gjøres i Norge.*

Behov for kompetanse

Tekna er kjent med at regjeringen har igangsatt en kartlegging av fremtidig behov for IT-sikkerhetskompetanse. Oppdraget er satt ut til NIFU, som leverte sin foreløpige rapport i juni i år. I rapporten fremgår et kompetansegap frem til 2030 på 4 100 personer med IKT-sikkerhetskompetansen[2]. Tekna mener nasjonale myndigheter har hatt mangelfull bevissthet på viktigheten av nasjonal sikkerhetskompetanse. Dette gjelder både i virksomheter som faller innenfor sikkerhetslovens anvendelsesområde og de som faller utenfor, men som defineres som kritisk infrastruktur. Siden sikkerhet må inkluderes allerede i designfasen av systemet har alle IT-utdanninger behov for sikkerhetskompetanse.

[2] NIFU Arbeidsnotat 2017:8
IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud

For å løse dette omfattende kompetansebehovet er det etter Teknas mening helt nødvendig å utvide kapasiteten på eksisterende IT-utdanninger, men også å etablere relevante etter- og videreutdanningstilbud for høyt utdannede IKT-medarbeidere på IT-sikkerhet.

Tekna vil

- *Ha en full gjennomgang av all IKT-utdanning med tanke på kapasitet og behov.*
- *Legge inn sikkerhet og risikovurderinger som en obligatorisk del i IKT-studieprogrammene.*
- *At læreplaner og utdanningsprogrammer må utvikles i tett samarbeid med sektorer og myndigheter som forvalter og operasjonaliserer nasjonale sikkerhetstiltak og som fører tilsyn med sårbare virksomheter.*
- *At universitets- og høyskole-sektoren utvikler etter- og videreutdanningstilbud innen informasjonssikkerhet.*
- *At Stortinget ber regjeringen igangsette konkrete tiltak for å øke rekrutteringen av sikkerhetsklarerbare PhD-kandidater til sikkerhets- og sårbarhetsforskning.*