

Høring av NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet

Vi viser til Justis- og beredskapsdepartementets brev av 21.12.2018 om høring av;

- 1.) Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018:14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.
- 2.) Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

Under følger våre kommentarer:

1.) Utredning fra IKT-sikkerhetsutvalget

Utvalget ble gitt i oppdrag å vurdere om dagens regulering av IKT-sikkerhet er hensiktsmessig gitt de utfordringene Norge står ovenfor. Utvalget har gitt følgende anbefalinger:

- Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
- Krav til IKT-sikkerhet ved alle offentlige anskaffelser
- Nasjonalt IKT-sikkerhetssenter
- Tydeligere regulering av og ansvar for tilkoblede produkter og tjenester
- Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet

Statens jernbanetilsyn støtter utvalgets anbefalinger og har ingen ytterligere kommentarer utover dette.

2.) Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

Under følger Statens jernbanetilsyn svar på spørsmålene som Justis- og beredskapsdepartementet har bedt om tilbakemelding på:

- *I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring eller internkontroll?*

Statens jernbanetilsyn har implementert et styringssystem for informasjonssikkerhet som følger ISO 27000-serien. Tilsynet legger ikke opp til en sertifisering etter ISO-standard men følger standarden på de vesentligste områdene i sin interne styring av informasjonssikkerhet. Tilsynet er dermed av den oppfatning at det arbeides systematisk med IKT-sikkerhet.

- *Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.*

Tilsynet er ikke en tilbyder av samfunnsviktige tjenester slik de er definert i NIS-direktivet, og vil dermed ikke bli direkte berørt av direktivet knyttet til den interne driften.

Når det gjelder tilsynets rolle som en eventuell utpekt tilsynsmyndighet etter den nye loven, ser vi det som positivt at nytt regelverk vil sette konkrete krav og føringer for informasjonssikkerhetsarbeidet i sektoren. Eksisterende regelverk i sektoren dekker informasjonssikring, men tilsynet har sett at praksis og bevissthet knyttet til informasjonssikkerhet varierer mellom de ulike aktørene. Tilsynet mener et nytt regelverk vil

bidra positivt ved at det settes eksplisitte krav til vurderinger av risikoer i nettverk og informasjonssystemer noe som vil bidra til økt bevissthet og bedre informasjonssikkerhet.

- Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.

For tilsynets interne drift vil ikke gjennomføringen av direktivet få verken positive eller negative konsekvenser, jf. kommentar over.

For vårt myndighetsområde som tilsynsmyndighet er det vanskelig å vurdere konsekvensene basert på lovforslaget, men det er sannsynlig at dette vil medføre økt ressursbehov, både i form av opplæring i det nye regelverket og for utøvelsen av tilsynsrollen. Et eventuelt økt ressursbehov vil avhenge av faktorer som tilsynsregimet som blir lagt til grunn for oppfyllelse av § 12 (frekvens, hvilke virksomheter som blir omfattet mv.) og tolkninger av spesielt §§ 7 og 8 i form av veiledere eller lignende. Veiledere til loven vil kunne legge føringer som krever økte ressurser fra oss som en eventuell tilsynsmyndighet.

- Er din virksomhet per i dag underlagt krav til IKT-sikkerhet og varsling? Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?

Statens Jernbanetilsyn er underlagt krav til informasjonssikkerhet eksempelvis gjennom regelverk som GDPR, Jernbaneloven, Sikringsforskriften, Arkivloven og Sikkerhetsloven. Statens jernbanetilsyn har i sine interne styrende dokumenter definert at varsling skal følge Rammeverk for håndtering av IKT-sikkerhetshendelser.

- Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?

Selv om jernbaneforetak har krav i eksisterende regelverk knyttet til informasjonssikkerhet, er Statens jernbanetilsyn positiv til at en lov om sikkerhet i nettverk og informasjonssystemer blir vedtatt. Økt digitalisering i sektoren skaper nye typer sårbarheter og et regelverk som setter krav til informasjonssikkerheten i nettverk og informasjonssystemer er etter vårt syn viktig for å sikre informasjonssikkerheten i nye løsninger og ytterligere øke fokus og bevissthet på området. Vi vil avslutningsvis understreke viktigheten av at en eventuell implementering av nytt regelverk tidlig blir fulgt opp med relevante veiledere, spesielt knyttet til §§ 7 og 8 i lovforslaget.