

Vår saksbehandler
Synne Solgaard Evensen

Dokumentdato
13.12.2024
Deres dato

Vår referanse
2024/10752-4
Deres referanse

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Postboks 8005 Dep.
0030 OSLO

Høringsinnspill til forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

DSB viser til brev 11. september 2024 om høring av forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften). Vi takker for muligheten til å komme med innspill til høringen og utsatt frist for å gi innspill til 13. desember. DSB har noen innspill til høringen, men støtter i all hovedsak forslaget og departementets vurderinger.

DSB har innspill til kapittel 2 hvor det gis en beskrivelse av NIS1-direktivet og hva som omfattes av dette. Det fremkommer at direktivet gjelder for tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Det fremkommer videre at tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester, omfattes. Vi savner en nærmere forklaring på hva dette siste konkret omfatter.

DSB har innspill til kapittel 4 om lovens virkeområde. Lov om digital sikkerhet har som mål å styrke den digitale sikkerheten i viktige virksomheter for å beskytte samfunnet mot digitale angrep og uønskede hendelser. Loven er ment å treffe virksomheter som har en særlig viktig rolle for å opprettholde leveransen av samfunnsviktige tjenester. Formålet med forskriften er å klargjøre hvilke virksomheter som er underlagt lov om digital sikkerhet. I høringsnotatet er det foreslått terskler for å avgjøre hvilke virksomheter som skal anses som tilbydere av samfunnsviktige tjenester.

DSB er opptatt av at loven og forskriften treffer de virksomhetene som er så viktige for samfunnet at en hendelse hos virksomheten får negativ innvirkning for samfunnets leveranse av viktige tjenester og derfor må stilles krav til. For noen samfunnsviktige tjenester, ser DSB at tersklene kan slå uheldig ut og DSB legger til grunn at vedtakskompetansen i § 4 vil bli benyttet. For eksempel er helse- og omsorgstjenester i økende grad avhengige av digitale systemer for journalføring, kommunikasjon, medisiner og overvåking. En hendelse som rammer disse systemene kan føre til forsinkelser i behandling, feilmedisinering, og i verste fall tap av liv. Selv små enheter innen helse- og omsorg, kan ha stor betydning for lokalbefolkningen i deler av landet, men vil ikke omfattes av denne loven med mindre de blir pekt ut av ansvarlig departement ved enkeltvedtak. Et annet eksempel er at vannverk, uavhengig av størrelse, blir stadig mer digitaliserte og avhengige av IKT-systemer for drift og overvåking. Dette øker sårbarheten for digitale angrep og hendelser som kan forstyrre vannforsyningen. Selv om et vannverk forsyner færre enn 10.000 innbyggere, kan bortfall av tjenesten ha betydelige konsekvenser for det berørte samfunnet. Mindre vannverk omfattes ikke av loven med mindre de blir pekt ut av departementene ved enkeltvedtak.

DSB har konkret innspill til kapittel 4.2.2.3 Olje- og gassforsyning.

Postadresse
Direktoratet for
samfunnssikkerhet og beredskap

Postboks 2014
3103 Tønsberg

Besøksadresse
Rambergveien 9, 3115 Tønsberg

E-post
Postmottak@dsb.no

Telefon
33 41 25 00

Internett
www.dsb.no

Organisasjonsnummer
974 760 983

Høringsnotatet tar for seg olje- og gassforsyning i forbindelse med digital sikkerhet. Det presiseres at NIS1-direktivet ikke gjelder for virksomhet på kontinentalsokkelen, i henhold til EØS-avtalen artikkel 126. Dermed faller oppstrøms olje- og gassanlegg, som i stor grad befinner seg på kontinentalsokkelen, utenfor lovens virkeområde. Dette inkluderer også landanlegg.

Departementet anerkjenner at norsk oppstrøms olje- og gassproduksjon er av stor betydning for landet og mener at det på sikt bør etableres et nasjonalt regelverk for sikkerhet i nettverk og informasjonssystemer for denne typen virksomhet. DSB støtter dette. Energi er definert som en kritisk samfunnsfunksjon og kritisk infrastruktur ut fra flere rammeverk. Sikker forsyning av energi er høyt på dagsordenen både i Norge og internasjonalt. Petroleumsvirksomheten i Nordsjøen har stor betydning både for norsk forsyningssikkerhet og for europeisk energisikkerhet. I kommende nasjonalt regelverk som gjennomfører NIS2- og CER-direktivene bør derfor virksomhet på kontinentalsokkelen omfattes. DSB mener det er viktig at dette regelverket kommer på plass så raskt som mulig, for å sikre at både fysisk og digital motstandsdyktighet ivaretas.

Når det gjelder drivstofflager, foreslår departementet at hovedtankanlegg for petroleumbasert drivstoff anses som en samfunnsviktig tilbyder innenfor olje- og gassforsyningen. Disse tankanleggene faller inn under brann- og eksplosjonsvernloven med tilhørende forskrifter, slik som forskrift om håndtering av farlig stoff og storulykkesforskriften. DSB er både fag, - forvaltnings, - og tilsynsmyndighet for dette regelverket og følgelig også for nevnte anlegg. I kap. 4.2.4 som omhandler innmelding av samfunnsviktige tjenester ber departementet særlig om høringsinstansenes syn på forslaget om at det er virksomheten som tilbyr den samfunnsviktige tjenesten som selv må melde dette inn både til tilsynsmyndigheten og til Nasjonal sikkerhetsmyndighet.

Vi er enig i dette forslaget. Selv om det er en risiko for at enkelte virksomheter ikke får med seg denne innmeldingsplikten, er virksomhetene nærmest til å ha oversikt over tjenestene de tilbyr, og det er viktig at de ansvarliggjøres. Etter vår vurdering er det ikke hensiktsmessig at det er myndighetene som skal utpeke tilbyderne.

Vi forutsetter at det utvikles en felles digital løsning for denne innmeldingen, slik at sektormyndighetene får tilgang til informasjon om "sine" virksomheter, mens NSM har oversikt over samtlige virksomheter.

I kapittel 4.2.5 beskrives unntaket for små virksomheter, som er definert som virksomheter med færre enn 50 ansatte, og som har en årlig omsetning eller årsbalanse som ikke overstiger 100 millioner kroner. Vi stiller spørsmål ved om disse grensene er så høye at det kan være virksomheter som burde vært omfattet av bestemmelsen om sikkerhetskrav for tilbydere av digitale tjenester og om bestemmelsen om varslingsplikt. Dette spilles inn generelt og på bakgrunn av vår forståelse om at vedtakskompetansen i § 4 ikke kan benyttes på disse digitale tjenestetilbyderne.

DSB har innspill til kapittel 5. På generelt grunnlag og der det er relevant, samsvarer forslaget godt med hvordan en forutsetter at virksomheter jobbet systematisk for å ivareta helse- miljø og sikkerhet etter internkontrollforskriften, og kravene som stilles i storulykkesforskriften til virksomhetenes styringssystem. Det er viktig at virksomhetene kan integrere digital sikkerhet i de styringssystemene de allerede har.

I forslag til § 7 lister departementet opp minimumskrav til risikovurderinger. DSB ser at § 7 mangler noen vesentlige krav til risikovurderinger, blant annet basert på NS ISO 31000:2018 Risikostyring og NS 5814:2021 Krav til risikovurderinger. Dette gjelder beskrivelse av sikkerhetsmål og evalueringskriterier samt usikkerhet knyttet til kunnskapsgrunnlaget for risikovurderingen. DSB ber departementet vurdere å ta inn disse kravene i bestemmelsen. For ordens skyld be merkes at bokstavangivelsene i forskriftsforslaget § 7 vel skal være "a-f".

I kapittel 5.3.4 om risikohåndtering ber departementet om høringsinstansenes syn på at det foreslås at §§ 9-14 suppleres med veiledningsmateriale fra Nasjonal sikkerhetsmyndighet, som i kombinasjon med anerkjente standarder støtter virksomhetene i arbeidet. Vi er enig i dette, og ser at det i tillegg kanskje også kan være behov for veiledning fra relevant sektormyndighet.

I kap. 5.3.5.2 om teknologiske sikkerhetstiltak ber departementet om høringsinstansenes syn på om det bør tas inn en bestemmelse som gir myndighetene kompetanse til å gi unntak fra enkelte krav. Vi støtter at det innføres en slik bestemmelse, og at myndigheten i særlige tilfeller kan gjøre unntak.

Til kapittel 5.3.6 om hendelseshåndtering og beredskap og § 13 tredje ledd, vil DSB understreke viktigheten av å lære av øvelser og hendelser og at erfaringer fra øvelser og håndtering av hendelser blir tatt med i kunnskapsgrunnlaget for vurdering av sikkerhetstiltak.

Når det gjelder kapittel 5.3.7 om oppfølgingsplikt, støtter DSB departementet og mener det er viktig at det er stilt krav om å følge opp egne underleverandører og ha oversikt over kjeden av leverandører og andre kontraktører. Ved gjennomføring av tilsyn vil myndigheten kunne ha behov for å gjøre undersøkelser opp mot underleverandører. Når underleverandører ikke er omfattet av lovens virkeområde, kan ikke DSB se at § 22 gir tilsynsmyndighetene hjemmel til å kreve opplysninger fra underleverandør. DSB kan heller ikke se at "tilgang til lokaler" gjenspeiles i bestemmelsen og pliktsubjektet i bestemmelsen er også uklart. DSB støtter departementets vurdering av sårbarhet i leverandørkjeden og anser det som viktig å sikre at virksomheter underlagt loven har oversikt over og nødvendig innflytelse over sine underleverandører og deres sikkerhetskrav. Dette bør sikres enten gjennom tydeligere hjemmel eller tydeligere krav til virksomheten.

I § 20 andre ledd er inntatt en hjemmel til å benytte bistand ved tilsyn. I kapittel 9.3.1 er det vurdert at denne bestemmelsen kan være praktisk der tilsynsmyndigheten ikke har den nødvendige spisskompetanse innenfor et fagområde eller det av andre grunner kan være behov for å benytte bistand. DSB stiller spørsmål ved hvilke krav som må stilles til den som eventuelt skal yte bistand til tilsynsmyndighetene ved tilsyn, og hvem som i så fall skal betale for denne bistanden.

Departementet ber i kapittel 13 om innspill på konsekvensene som forslagene vil få for høringsinstansene. Som tilsynsmyndighet for sikkerheten knyttet til håndtering av farlige stoffer slik som petroleumprodukter, ser vi at vi også kan bli tillagt oppgaven med å føre tilsyn etter digitalsikkerhetsforskriften. Selv om vi er kjent med krav til systematisk sikkerhetsarbeid og styringssystemer så vil digital sikkerhet være et nytt og ukjent tilsynsystem for oss. Vi kjenner oss derfor igjen i departementets beskrivelse av konsekvenser. Dersom vi skal tallfeste dette nærmere antar vi at forslaget innebærer en kostnad relatert til tre nye årsverk for å kunne ivareta oppgaven på en tilfredsstillende måte.

Med hilsen

Direktoratet for samfunnssikkerhet og beredskap
Juridisk

Elisabeth Sørbøe Aarsæther
direktør

Ingvild Martinsen
seksjonssjef

Dokumentet er godkjent elektronisk og sendes derfor uten underskrift.