DET KONGELIGE
FORSVARSDEPARTEMENT

Justis- og beredskapsdepartementet
Postboks 8005 Dep.
0030 OSLO

Deres ref.:	Vår ref.:	Dato:
	2019/110-4/FD I 2/MIH	22.03.2019

Svar på høring av NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett

Forsvarsdepartementet (FD) viser til Justis- og beredskapsdepartementets (JD) høring av NOU 2018:14 *IKT-sikkerhet i alle ledd* og utkast til lov som gjennomfører EUs direktiv for sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett. I det videre følger FDs kommentarer til høringen.

Forslag til lov som implementerer NIS-direktivet i norsk rett
IKT-sikkerhetsutvalget anbefaler at det utarbeides en tverrsektoriell IKT-sikkerhetslov som skal gjelde for samfunnskritiske virksomheter og offentlig forvaltning. Utvalget mener videre at den samme loven skal implementere NIS-direktivet i norsk rett. JD har utarbeidet et høringsnotat og forslag til lov som viser hvordan en slik lov vil kunne se ut. FD og etatene i forsvarssektoren vil ikke være underlagt loven, slik dennes virkeområde er angitt. Vi ønsker likevel å knytte noen kommentarer til lovforslaget og høringsnotatet.

Om lov om nasjonal sikkerhet (sikkerhetsloven)
I høringsnotatet redegjøres det for gjeldende rett og krav til sikring av informasjonssystemer. Her skrives det blant annet at sikkerhetsloven stiller krav til sikring av skjermingsverdige informasjonssystemer, i motsetning til direktivet, som stiller krav om at virksomheter sikrer informasjonssystemer de benytter for å levere en samfunnsviktig tjeneste. Omtalen av skjermingsverdige informasjonssystemer etter sikkerhetslovens bestemmelser er ikke korrekt. Sikkerhetsloven stiller krav til skjerming av informasjonssystemer også dersom systemet *i seg selv* har avgjørende betydning for grunnleggende nasjonale funksjoner (GNF).

For øvrig bør referanser til den gamle sikkerhetsloven tas ut av en eventuell lovproposisjon.

Postadresse:
Postboks 8126 Dep.
0032 Oslo

Kontoradresse:
Glacisgata 1
Oslo

Telefon:
23 09 80 00

Saksbehandler:
seniorrådgiver Mia Harlyng
Seksjon for forebyggende sikkerhet

E-postadresse:
postmottak@fd.dep.no

Webside:
www.regjeringen.no/fd

Org.nr.:
972 417 823

Om behovet for en tverrsektoriell lov om digital sikkerhet
Forsvaret er avhengig av at samfunnet fungerer, også i krise og under væpnet konflikt. Samfunnssikkerheten påvirker i betydelig grad Forsvarets evne til å ivareta statssikkerheten. Både sivile leverandører som understøtter Forsvaret, og Forsvaret selv, er dessuten avhengige av basistjenester som kraftforsyning og annen sivil infrastruktur og tjenesteproduksjon.

Den nye sikkerhetsloven er innrettet mot beskyttelse av grunnleggende nasjonale funksjoner mot sikkerhetstruende virksomhet. Det legges til grunn at prosessen med å identifisere GNF vil innebære en utvidelse av sikkerhetslovens virkeområde. Samtidig vil det, som påpekt av både IKT-sikkerhetsutvalget og i høringsnotatet fra JD, være en rekke virksomheter som *ikke* omfattes av sikkerhetslovens bestemmelser, men som like fullt er av betydning for samfunnssikkerheten. Videre omfatter lovforslaget, i motsetning til sikkerhetsloven, både tilsiktede og utilsiktede hendelser. FD støtter derfor at det legges frem forslag til en tverrsektoriell lov for digital sikkerhet med et bredere nedslagsfelt enn sikkerhetsloven i norsk rett.

Utkastet til lov om sikkerhet i nettverk og informasjonssystemer stiller krav til sikkerhetsnivå basert på risikovurdering. Lovutkastet understreker samtidig at dersom virksomheten er underlagt andre lover, som stiller krav om sikkerhet og varsling som minst tilsvarer kravene i loven, skal annen lov benyttes. FD støtter denne tilnærmingen, da sikkerhetstiltak i ulike sektorer vil kunne kreve forskjellig tilnærming og utforming av krav til sikring.

Utpeking av responsmiljøer og tilsynsmyndigheter
I lovforslaget fremkommer det at utpeking av responsmiljøer som skal kunne motta varsler etter loven, og tilsynsmyndigheter som skal føre tilsyn med tilbydere av samfunnsviktige digitale tjenester, skal utpekes av Kongen i statsråd.

I høringsnotatet fremkommer det at den nasjonale responsfunksjonen for alvorlige digitale angrep Nasjonal sikkerhetsmyndighet (NSM) er pålagt å drive etter sikkerhetsloven, skal vurderes opp mot NIS-direktivets krav. Gitt at forslaget til lov tar utgangspunkt i NIS-direktivet, som både omfatter tilsiktede og utilsiktede hendelser, vil en beslutning om å utpeke NSM som responsmiljø kunne innebære en dreining av den eksisterende responsfunksjonens virkeområde og en forskyvning i fokus fra denne responsfunksjonens allerede lovpålagte oppgaver.

FD vil samtidig understreke at for å sikre en god hendelseshåndtering, er det viktig å vurdere muligheten for å bygge på kompetanse i eksisterende responsmiljøer, slik som NSM NorCERT. NSM NorCERT er det responsmiljøet i Norge som har lengst og bredest erfaring fra å håndtere tilsiktede digitale sikkerhetshendelser. FD forutsetter samtidig at konsekvensene av en eventuell beslutning om å tillegge NSM rollen som varlingsinstans etter lovforslaget fullfinansieres. Det forutsettes også at en slik eventuell beslutning ikke påvirker direktoratets oppgaveløsning innenfor sikkerhetslovens virkeområde negativt. Tilsvarende gjelder en eventuell beslutning om å utpeke NSM som tilsynsmyndighet etter lov om sikkerhet i nettverk og informasjonssystemer.

NOU 2018:14 *IKT-sikkerhet i alle ledd*

IKT-sikkerhetsutvalget har hatt som oppdrag å vurdere rettslig regulering på IKT-sikkerhets-området og organisering av tverrsektorielt ansvar på etatsnivå, med utgangspunkt i tre problemstillinger. Det fremkommer også av mandatet at utvalgets utredning skal være avgrenset mot bestemmelser, organisering og myndighet som fulgte av tidligere sikkerhetslov og ny sikkerhetslov. Utvalget har valgt å forstå dette som at det ikke skal foreslås endringer i sikkerhetsloven.

Om ny lovregulering – omtale av sikkerhetsloven

Sikkerhetsloven trådte i kraft 1. januar 2019, og er p.t. «gjeldende sikkerhetslov». IKT-sikkerhetsutvalget skriver også at det, med hjemmel i den nye loven, utarbeides forskrifter om «myndighetenes ansvar, virksomhetenes ansvar og klarering av leverandører og personell». Det er ikke fastsatt en forskrift om myndighetenes ansvar, men forskrifter om virksomhetenes arbeid med forebyggende sikkerhet og klarering av leverandører og personell er fastsatt. I vedlegg 1 punkt 1.1 andre ledd, omtaler for øvrig utvalget gammel lov som «gjeldende sikkerhetslov».

Utvalgets anbefalinger

IKT-sikkerhetsutvalget legger frem fem anbefalinger i sin rapport:

- Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning
- Krav om IKT-sikkerhet ved anskaffelser
- Etablere et nasjonalt IKT-sikkerhetssenter
- Tydelig regulering og ansvar for tilkoblede produkter og tjenester
- Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

FD støtter anbefalingene om krav til IKT-sikkerhet ved anskaffelser, og har ingen ytterligere kommentarer til denne. Departementet har heller ingen kommentarer relatert til regulering og ansvar for tilkoblede produkter og tjenester.

Ny lov

Når det gjelder anbefalingen om ny lov om IKT-sikkerhet, viser FD til tidligere kommentarer til høringsnotat og utkast til lov om sikkerhet i nettverk og informasjonssystemer. Utvalget foreslår også at det settes ned et lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter. Forslaget til lov som implementerer NIS-direktivet i norsk rett, angis av JD å være en *minimumsgjennomføring* av direktivet. Som del av en utredning om behovet for en generell, tverrsektoriell lov for digital sikkerhet, som gjelder for alle virksomheter, bør det vurderes om en utvidelse av lovforslagets virkeområde kan være et alternativ til en ytterligere lov.

Et nasjonalt IKT-sikkerhetssenter

IKT-sikkerhetsutvalget anbefaler at det utredes å etablere et nasjonalt IKT-sikkerhetssenter som skal ivareta mange oppgaver med stor bredde og stort nedslagsfelt. NSM har allerede ansvar for enkelte av oppgavene som foreslås lagt til et slikt senter, herunder ansvar for en nasjonalt responsfunksjon for alvorlige digitale angrep.

Beslutningen om å etablere nasjonalt cybersikkerhetssenter i NSM i 2019 innebærer en samlokalisering av NSMs egne, relevante fagmiljøer innenfor digital sikkerhet. Senteret etableres innenfor NSMs gjeldende mandat, og innebærer ikke noen utvidelse av direktoratets ansvars- eller myndighetsområde. Det er også lagt til grunn at etableringen av nasjonalt cybersikkerhetssenter skal foregå innenfor NSMs gjeldende budsjettrammer.

Det er av avgjørende betydning at NSMs kapasitet og evne til å utføre sine oppgaver relatert til statssikkerheten ikke blir svekket som følge av en eventuell beslutning om å videreutvikle nasjonalt cybersikkerhetssenter i tråd med IKT-sikkerhetsutvalgets anbefaling. FD mener dette hensynet også må veie tungt dersom det besluttes å utrede et nasjonalt IKT-sikkerhetssenter med oppgaveportefølje og nedslagsfelt som anbefalt av IKT-sikkerhetsutvalget.

Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet
Regjeringen besluttet 22. januar 2019 å overføre det administrative ansvaret for NSM og sikkerhetsloven til Justis- og beredskapsdepartementet. FD mener prosessen som p.t. pågår relatert til overføringen, må anses å ivareta utvalgets anbefaling om en gjennomgang av direktoratets styringsmodell for å sikre at IKT-sikkerhet i sivil sektor blir bedre ivaretatt.

Med hilsen

Jens T. Thorsen
ekspedisjonssjef

Ole Felix Dahl
avdelingsdirektør

Dokumentet er elektronisk godkjent og signert, og har derfor ikke håndskrevne signaturer.