Direktoratet for e-helse

Justis- og beredskapsdepartementet
Christian Frederik Mathiessen
Postboks 8005 Dep
0030 OSLO

Deres ref.:
Vår ref.: 18/1100-2
Saksbehandler: Jan Gunnar Broch
Dato: 19.03.2019

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

Vedlagt følger høringsuttalelse fra Direktoratet for e-helse til Høringsuttalelse- NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet.

Vi takker for mulighet til å svare på høringen.

Vennlig hilsen

Christine Bergland e.f.
direktør

Karl Stener Vestli
divisjonsdirektør

Dokumentet er godkjent elektronisk

Vedlegg: 1

Direktoratet for e-helse
E-helse Avdeling juridisk
Jan Gunnar Broch, tlf.:
Postboks 221 Skøyen, 0213 OSLO • Besøksadresse: Verkstedveien 1 • Tlf.: 21 49 50 70
Org.nr.: 915 933 149 • postmottak@ehelse.no • www.ehelse.no

Direktoratet for e-helse

Høringsuttalelse

NOU 2018: 14 (Holte-utvalget) og Regjeringens utkast til lov som gjennomfører NIS-direktivet i norsk rett.

Frist: 22.03.2019

Direktoratet for e-helse viser til felles høring om IKT-sikkerhetsutvalgets utredning (Holte-utvalget) NOU 2018: 14 og Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett fra Justis- og beredskapsdepartementet (JD).

Direktoratet for e-helse stiller seg i all hovedsak positiv til lovutkastet om gjennomføring av NIS-direktivet. Dette vil gi et enhetlig regelverk i EU/EØS. For å kunne møte et mer krevende trusselbilde er det viktig med et harmonisert sikkerhetsnivå uten svakeste ledd. Et enhetlig regelverk legger også grunnlaget for like konkurransevilkår.

Videre mener direktoratet at NOU 2018:14 "IKT-sikkerhet i alle ledd" er en god drøfting av nåsituasjon, rammebetingelser og mulig tiltak i arbeidet med organisering og regulering av nasjonal IKT-sikkerhet.

Innspill og kommentarer til NOU 2018: 14 (Holte-utvalget)

Direktoratet for e-helse mener utvalget har kommet med gode og viktige tiltak som potensielt vil gi en mer helhetlig tilnærming til nasjonal IKT-sikkerhet enn hva som foreligger i dag. Samtidig ønsker vi å påpeke viktigheten av at alle tiltakene må sees i sammenheng og tas i riktig rekkefølge. Tydeliggjøringen av styring og myndighetenes organisering rundt IKT-sikkerhet mener vi er det første tiltaket som må sees på, og dette må på plass for å legge riktig grunnlag for påfølgende tiltak.

Direktoratet for e-helse støtter også anbefalingen om et nytt nasjonalt IKT-sikkerhetssenter, forutsatt at man samordner dagens fragmenterte funksjoner og at det nye senteret kan fremstå som et helthetlig kompetansesenter for offentlige og private aktører. Som NOU 2018:14 også påpeker er tilgang på IKT-sikkerhetskompetanse en stor utfordring lokalt, nasjonalt og globalt. Derfor er det viktig å få samlet innsatsen fra myndighetsressursene på en god måte slik at man får jobbet mer effektivt og unngår offentlige instanser som jobber overlappende på dette området.

Samtidig er det viktig for helse- og omsorgssektoren at sektorinnsatsen på dette viktige området ikke svekkes for kompetansekapasitet. Vår sektor består av mange små virksomheter som har behov for f.eks tilpasset veiledning. Slik veiledning mener direktoratet vil ytes best sektorvis.

Det er også viktig at innsatsen til myndighetene på dette området fremstår som tydelige for de som håndterer IKT-hendelser både på et operativt og strategisk nivå ute hos offentlige og private virksomheter. Strukturene som vil komme med et nytt nasjonalt IKT-sikkerhetssenter må gjenspeiles på alle nivå, og være enhetlig og tydelig for alle aktører. Dette gjelder særlig rapporteringsveier. En viktig utfordring som Direktoratet ser og som utvalget påpeker, er grenseoppgangen mellom et nytt nasjonalt IKT-sikkerhetssenter (inkludert NSM NorCERT), sektor CERT og nasjonalt cyberkrimsenteret.

Angrep og innbrudd i IKT-systemer faller fort under politiets jurisdiksjon, så her bør man få på plass klare ansvarslinjer så virksomhetene til enhver tid vet hva og hvem de skal forholde seg til.

Innspill og kommentarer til regjeringens utkast til lov som gjennomfører NIS-direktivet i norsk rett.

Direktoratet for e-helse har følgende innspill til regjeringens utkast til lov om gjennomføring av NIS direktivet i norsk rett.

Vi støtter prinsippet om å benytte eksisterende tilsynsmyndigheter for tilsyn med etterlevelse av NIS-direktivet. Det er imidlertid viktig at departementet er oppmerksom på eventuell overlapp i tilsynsmyndighetenes roller, og vi mener at dette må klargjøres nærmere.

Det vil være nødvendig med godt veiledningsmateriell og sektorspesifikke veiledere, ikke minst på grunn av forskjellig regelverk som regulerer IKT-sikkerhet og dels legger opp til overlappende vurderinger. Dette kommer for eksempel særlig til syne i grenseoppgangen mellom sikkerhetsloven og NIS-loven, der det skal identifiseres «grunnleggende nasjonale funksjoner (GNF)» etter sikkerhetsloven og «samfunnsviktige funksjoner» etter NIS-loven. Formålene med vurderingene som skal gjøres er ikke de samme, men vurderingene vil trolig være overlappende. Dette vil skape et behov for veiledning som ser lovreguleringen på IKT-sikkerhetsfeltet i sammenheng.

Innspill til Kap 7.1.11:

Vi støtter i hovedsak behovet for at virksomheter i helse- og omsorgssektoren utvider omfanget av risikostyring og sikkerhetstiltak til også å omfatte annen kritisk infrastruktur, dette er en viktig og nødvendig utvidelse. For vår sektor kan dette for eksempel være styringssystemer for teknisk infrastruktur.

Innspill til Kap 7.3

Slik vi leser forslaget i kap 7.3 må hver virksomhet vurdere hvilke informasjonssystemer som omfattes av direktivet og kravene som direktivet stiller, i tillegg til vurderinger og sikkerhetstiltak som følger av annet regelverk for sektoren. Direktoratet for e-helse mener at slike konkrete vurderinger på løsningsnivå kan bli overlappende, omfattende, ressurskrevende og økonomisk belastende, særlig for mindre virksomheter. Et slik arbeid vil også kunne ta fokuset vekk fra andre viktige oppgaver virksomheten har. For å kunne oppnå gode resultater ser vi det som nødvendig at godt veiledningsmateriale utarbeides og tilgjengeliggjøres for alle virksomheter.

Innspill til kap 9 Responsmiljøer (kap 9)

I helse- og omsorgstjenesten er det i dag HelseCERT som er sektorens nasjonale senter for informasjonssikkerhet. Ved en beslutning om hvilke virksomheter som skal kunne ta imot varsler etter loven bør allerede etablerte responsmiljøer tas i betraktning. Det bør vurderes om det er hensiktsmessig å legge rapporteringen til en etablert nasjonal funksjon eller til fagmiljøene som deretter rapportere oppad.

Innspill Kap 11.3

Direktoratet for e-helse ønsker at departementet presiserer nærmere i forskrift eller veiledning sammenhengen mellom sanksjonsbestemmelsene i NIS- loven og sanksjonsbestemmelsene i personvernforordningen, og hvilke sanksjonsbestemmelser som skal gjelde når begge regelverk kan anvendes. Dette kan for eksempel bli aktuelt i de tilfeller der det foreligger brudd på tilgjengelighet eller integritet. Det må være tydelig hvilket regelverk som kommer til anvendelse, både av hensyn til forutsigbarhet og eventuelle bøtesatser.

Svar på høringsbrevets spørsmål

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

Det jobbes systematisk med IKT-sikkerhet i Direktoratet for e-helse. Det har blant annet blitt etablert et nytt ledelsessystem for informasjonssikkerhet i henhold til standarden ISO 27001:2013. Det benyttes også en beste praksis for å sikre innebygd programvaresikkerhet og personvern. I tillegg gjennomføres jevnlige egenkontroller, revisjoner og inntrengningstester. Direktoratet legger kravene i Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten til grunn. Det kan også nevnes at sekretariatet for Normen ligger i Direktoratet for e-helse.

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

Det er positivt at direktivet setter krav. Krav til hver medlemsstat om å etablere en nasjonal strategi for IKT-sikkerhet gir tydelige føringer om at IKT-sikkerhet er et viktig område som skal prioriteres. Krav til en nasjonal kompetent sikkerhetsmyndighet gir en sparringpartner og en myndighet som kan utarbeide relevante krav, veilede og tilby opplæring. Videre vil et nasjonalt kontaktpunkt og en nasjonal enhet som skal håndtere digitale sikkerhetshendelser være et godt kontaktpunkt for utveksling av trusselinformasjon og håndtering avgrenseoverskridende digitale sikkerhetshendelser

Det er også positivt at direktivet stiller krav om at virksomheten skal gjennomføre en vurdering av risikoen tilknyttet IKT-systemene virksomheten bruker for å levere samfunnsviktige tjenester, og iverksette egnede tiltak for å redusere risikoen. Helsesektoren har krav om dette allerede gjennom Normen og personvernforordningen, men å tydeliggjøre kravene i direktivet ses likevel på som positivt.

Det stilles også krav om å iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensen av hendelser. Det ses særlig positivt på at også elementene avdekke og redusere trekkes frem.

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

Flere av kravene i direktivet er allerede krav som må følges av Direktoratet for e-helse (se spørsmål 4). Hvis regelverket tolkes ulikt av de ulike tilsynsmyndighetene kan dette skape utfordringer for virksomhetene. Flere tilsynsmyndigheter fører tilsyn med direktoratet, herunder Helsetilsynet,

Datatilsynet, NSM og NKOM. Hvis overlappende regelverk tolkes ulikt av de ulike tilsynsmyndighetene kan dette skape utfordringer for virksomhetene.

4. 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?

Ja. Personopplysningsloven og personvernforordningen, pasientjournalloven, helseregisterloven, helsetilsynsloven, forvaltningsloven, sikkerhetsloven, lov om elektroniske tillitstjenester mv. I tillegg er Direktoratet for e-helse blant annet underlagt reseptformidlerforskriften, kjernejournalforskriften, e-forvaltningsforskriften ogNorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.

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

Ja. Særlig på grunn av de positive konsekvensene beskrevet under spørsmål 2.