Til Justis- og beredskapsdepartementet

22. mars 2019

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

Tekna er den største foreningen i Akademikerne med over 77 000 medlemmer. Våre medlemmer består av naturvitere og teknologer, høyt utdannede med master eller mer. Mange av våre medlemmer innehar unik kompetanse innen IKT-sikkerhet og mange fler arbeider i bransjer der sikkerhet i IKT-systemene er helt avgjørende. Vi ønsker derfor å komme med innspill til NOU 2018: 14 og forslaget om utkastet til ny lov som gjennomfører NIS-direktivet i norsk rett.

Kommentarer til NOU 2018: 14 IKT-sikkerhet i alle ledd

Tekna mener at Holte-utvalget har levert en god utredning som synliggjør svakheter i dagens regelverk knyttet til IKT-sikkerhet som vi lenge har ment bør gjennomgås nærmere. Tydelige krav for IKT-sikkerhet i alle ledd, god samhandling mellom tilsynsorganene og ikke minst økt kompetanse innen IKT-sikkerhet er avgjørende for å sikre norske innbyggere og virksomheter fra digitale trusler også referert til i Digital21. Tekna har følgende kommentarer til tiltakene som foreslås.

Forslag om ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Tekna har lenge etterlyst et felles sektorovergripende regelverk, og mener utvalgets forslag kan berede grunnen for utviklingen av en mer overordnet og helhetlig sikkerhetspraksis innen det digitale området.

Tekna er særlig opptatt av at de ulike tilsynsorganenes roller og fullmakter avklares og at de opererer mer enhetlig i sine tilsyn med IKT-sikkerhet. Særlig må man vurdere om man har tilstrekkelig hjemmel til å føre tilsyn med underleverandører og å føre teknisk IKT-tilsyn. Dette er godt omtalt i NOUens kap. 15.4.1.

Tekna er også positive til utvalgets forslag om å nedsette et utvalg som skal utrede lovforslag som stiller krav til IKT-sikkerhet i alle norske virksomheter. Tekna tar ikke stilling til om det burde innføres krav for alle norske virksomheter, men vi frykter at enkelte virksomheter som eksisterer i et grenseland kan falle utenfor lovens krav til IKT-sikkerhet. Vi viser i denne sammenhengen til våre tidligere innspill til ny sikkerhetslov der vi understrekte følgende punkter:

- *at det må etableres klare krav til forebyggende sikkerhet av de virksomheter som ikke faller inn under sikkerhetsloven, men som er i et grenseland*
- *at det må settes av tilstrekkelig med ressurser hos sikkerhetsmyndigheten og andre egnede organer og myndigheter til å gi veiledning til virksomheter som ligger utenfor sikkerhetslovens virkeområde, men i «gråsonen»* [1]

[1] https://www.tekna.no/globalassets/filer/politikkdokumenter/horingsdokumenter/2018/20180928-innspill---forskrifter-ny-sikkerhetslov.pdf

Krav om IKT-sikkerhet ved anskaffelser

Tekna støtter utvalgets forslag om krav til sikkerhet ved anskaffelser gjennom endringer i anskaffelsesregelverket og i standardkontraktene. Hovedutfordringen med lovkrav er å definere disse på en måte som står seg over tid. Den digitale og teknologiske utviklingen går raskt. Lovarbeid, utvikling av veiledningstilbud og materiell, tar tid. Vi tror derfor **det kan være en løsning at loven definerer krav til vurderinger fremfor å skissere konkret innhold i produktet eller tjenesten som skal anskaffes.**

Tekna vil også understreke at bestiller-kompetanse innen IKT-sikkerhet vil være avgjørende dersom loven skal definere krav til vurderinger fremfor å skissere konkret innhold i produktet eller tjenesten som skal anskaffes.

Etablere et nasjonalt IKT-sikkerhetssenter

Etableringen av et nytt nasjonalt IKT-sikkerhetssenter må vurderes i lys av etablering av Nasjonalt Cyber-sikkerhetssenter underlagt NSM. Cyber-sikkerhetssenteret som nå etableres skal være et nasjonalt kontaktpunkt og nav for IKT-sikkerhet i Norge. I tillegg etableres nasjonalt cyberkrimsenter underlagt KRIPOS.

Tekna ser utfordringen som ligger i at NSM er underlagt to departementer, henholdsvis justis- og forsvarsdepartementet, og at prioritering av oppgaver og mulig uklar rolleforståelse kan gi uheldige utslag for de ulike sektorene. Tekna vil derfor ikke avvise at det kan være behov for et eget senter som ivaretar den sivile delen av sikkerhetsarbeidet.

Tekna mener det er viktig med en behovsanalyse og en vurdering av om mandatet og fullmaktene til Cybersikkerhetssenteret kan og bør justeres, eller om senteret kan omorganiseres i en sivil og en militær del for å møte de behovene som utvalget skisserer.

Tekna har over tid uttrykt sterk bekymring for det store kompetansegapet vi har når det gjelder avansert IKT-sikkerhetskompetanse. Det er derfor viktig at man i vurderingen av etablering av nye, frittstående sentre på dette området vurderer den kapasiteten vi har til å bemanne opp disse hver for seg. For mange sentre bidrar til fragmentering av kompetansemiljøer.

Tydelig regulering og ansvar for tilkoblede produkter og tjenester

Tekna er enig i at ansvaret for IKT-sikkerhet på dette området i større grad bør flyttes fra forbrukeren til produsentene og leverandørene gjennom krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester. Både sertifiseringsordning eller omfattende standardisering kan være en alternativ vei å gå for å imøtekomme et slikt krav.

Tekna er enig med utvalget i at det er bedre å bidra til et oppdatert, harmonisert regelverk på EU-nivå enn at Norge unilateralt endrer regelverket på feltet. Tekna er svært opptatt av at Norge holder seg godt orientert om det arbeidet som gjøres i Brussel på dette området og kommer med innspill som bidrar til et for Norge akseptabelt sikkerhetsnivå for norske borgere og virksomheter balansert opp mot mulighetene for næringsutvikling blant produsentene av varer og tjenester.

Tekna mener, som utvalget, at det må etableres et tettere samarbeid mellom tilsynsmyndigheter som Datatilsynet, Forbrukertilsynet, DSB og Nkom når det gjelder tilkoblede produkter og tjenester.

Tekna er enig i at myndighetene må sørge for at produkter uten tilstrekkelig IKT-sikkerhet kan oppdages, varsles om og tilbakekalles. Forbrukerne må kunne heve kjøp av produkter og tjenester som ikke har tilstrekkelig IKT-sikkerhet. DSB bør få klare fullmakter når det gjelder varsling, rapportering, tilbakekalling og håndtering i forbindelse med manglende IKT-sikkerhet i tilkoblede produkter og tjenester.

En problemstilling som dukker opp når man omtaler krav til sikkerhet i tilkoblede produkter, er hvor langt ned i leverandørkjeden kravene skal rettes og hvor ansvaret for underleverandørene skal ligge. I forlengelsen av dette må man også løfte spørsmålet om hvem som skal føre tilsyn med underleverandørene og om det skal føres tilsyn med disse.

Tekna mener ansvaret må plasseres i første ledd, hos leverandøren av produktet og tjenesten.

Tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet

Tekna viser til at regjeringen nå er utvidet med to nye ministre, en digitaliseringsminister og en minister for samfunnssikkerhet. Tekna mener det er viktig at den statsråden som har en koordinerende rolle innen samfunnssikkerhet også har et overordnet ansvar for å utvikle et overgripende og helhetlig rammeverk, og fullmakter til å gi pålegg og ansvar for å påse at sektorene lever og leverer i tråd med overordnede føringer og politiske signaler.

Tekna ønsker en tydeliggjøring av ansvarsområdene for de to nye ministrene.

Kommentarer til lov som gjennomfører NIS-direktivet i norsk rett:

Angående forslaget til lov som gjennomfører NIS-direktivet i norsk rett er Tekna bekymret for at implementeringen av denne, i etterkant kan gjøre det mer krevende å utarbeide et nytt lovforslag i tråd med anbefalingene i NOUen.

Ettersom lovforslaget kun ivaretar minimumskravene i direktivet er det også problematisk dersom dette skulle svekke den etablerte standarden på nasjonalt nivå dersom dette gis forrang foran annen nasjonal regulering og praksis innen IKT-sikkerhet.

Lovforslaget definerer krav om sikkerhet og varsling for tilbydere av samfunnsviktige tjenester innen definerte sektorer, samt tilbydere av digitale tjenester som har sitt hovedforetak i Norge. For Tekna er det uklart om loven gjelder alle tilbydere av digitale tjenester, eller om det kun dreier seg om de som tilbyr skytjenester, digitale markedsplasser og digitale søkemotorer innenfor området samfunnsviktige tjenester.

Hva gjelder krav til sikkerhet, er kravet at **sikkerhetsnivået skal være tilpasset risikoen.** Hva gjelder krav om varsling, er kravet at hendelsen skal ha **betydelig innvirkning på tjenesteleveransen.** Det er gitt forskriftshjemler til bestemmelsene. Tekna påpeker at de rettslige standarder som her er brukt krever presiseringer som det er mulig å forholde seg til på tvers av sektorer. Man må ha en omforent forståelse av når et sikkerhetsnivå er tilpasset risikoen og hva som skal til for at en hendelse har betydelig innvirkning på tjenesteloven for å kunne møte lovkravene. Tekna mener det er uklart hvorfor man har en oppramsing av elementer man skal ta hensyn til i lovens § 9. andre ledd, mens tilsvarende opplisting av elementer ikke er lagt inn i lovens § 7.

I dag har vi en rekke reguleringer som strekker seg lenger enn å ivareta et *forsvarlig* sikkerhetsnivå og det er viktig at man ikke firer på kravene gjennom å definere et minimumsnivå på IKT-sikkerheten i ny lov. Sektorregelverk skal sørge for at vi har så godt sikkerhetsnivå som mulig, og det er svært viktig at det ikke sendes signaler ut om at et tilstrekkelighetskrav er godt nok. ***Tekna ber om at dette fremkommer klart ved utformingen av forskriftene til loven.***

Utkast til lov skal forplikte virksomheter som har en særlig viktig rolle i opprettholdelsen av et funksjonelt indre marked til å gjennomføre IKT-sikkerhetstiltak og varsle om alvorlige hendelser. Disse virksomhetene faller inn i to kategorier:

1. Tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur.
2. Tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

Tekna viser til at dette er en snevrere definisjon enn det som Direktoratet for samfunnssikkerhet og beredskap (DSB) definerer å falle inn under samfunnskritiske virksomheter. Det fremgår av høringsnotatet at det er opp til medlemslandene å definere samfunnsviktige tjenester, og ***Tekna mener det hadde vært hensiktsmessig at man opererte med de samme definisjoner som DSB opererer med når direktivet implementeres i norsk lov.***

Tekna viser til Holte-utvalgets forslag om ny lov om samfunnssikkerhet. Her foreslås at en slik lov skal gjelde samfunnskritiske virksomheter, offentlig forvaltning og NIS-direktivet. Holte-utvalgets forslag har dermed et videre virkeområde enn dette lovforslaget. ***Tekna mener man bør gjøre en grundigere vurdering av om loven bør ha et utvidet virkeområde enn det NIS-direktivet legger opp til og er i tråd med Holte-utvalget før man kan vedta et lovforslag.***

I direktivet legges det opp til at det er den enkelte virksomhet som selv skal vurdere om man er underlagt regelverket. Med de relativt åpne definisjonene man har her, samt med kjennskap til at man i forskjellige medlemsland ikke nødvendigvis legger samme praksis til grunn, er Tekna bekymret for at det vil være virksomheter der ute som enten definerer seg inn under og pådrar seg kostnader unødvendig eller som definerer seg ut selv om de ikke burde være det og dermed ikke har tilstrekkelig sikkerhet. Det vil også være vanskelig for tilsynsmyndigheten(e) å følge opp når det ikke er klart hvem som er underlagt eller ikke. **Selv om det vil være kostbart for departementene, mener Tekna at det må være et organ som fatter vedtak (forskrift eller enkeltvedtak) som nærmere definerer hvem som er underlagt.**

I lovforslagets § 9 ligger det i andre ledd en oppramsing av elementer som skal med i vurderingen av et «passende sikkerhetsnivå». Tekna mener at elementet i pkt. e. om **anerkjente internasjonale standarder,** er svært vanskelig å forstå. Det er et enormt antall standarder i IT-verdenen og det er høyst uklart hva som faller inn under kategorien av å være anerkjent. **Tekna ber departementet om å redegjøre for hvordan dette elementet er ment å forstå.**

Til tross for dette er sårbarheten innen IKT såpass stor og det haster med å innføre nasjonale og internasjonale krav til sikkerhet. **Med de forbehold som er nevnt over støtter Tekna derfor at det vedtas en lov i tråd med NIS-direktivet,** gitt at dette blir vedtatt implementert i forhandlingene mellom EU og EFTA. Det er likevel viktig at man følger opp med et mer omfattende forslag til lovendringer som tar stilling til forslagene i NOUen heller enn å begrense seg til direktivets minimumskrav.

Generelle betraktninger:

Den digitale og teknologiske utviklingen går raskt. Lovarbeid, utvikling av veiledningstilbud og materiell, tar tid. Tekna ber departementet vurdere hensiktsmessige og tidsbesparende virkemidler for å få opp den allmenne forståelse av fremtidige krav og forventninger til IKT-sikkerhet, særlig blant produsenter og leverandører av digitale produkter og tjenester.

Tekna har over tid påpekt behovet for tydelige grep for å øke den nasjonale IKT-sikkerhetskompetansen og har fokusert på dette gjennom representasjon i Digital 21. Vi har sett et økt engasjement for dette fra regjeringen og Tekna er svært glad for de økte bevilgninger til å bygge kapasitet og de føringer som er gitt UH-sektoren om å legge IKT-sikkerhet inn i

utdanningsprogrammene. Det er likevel et betydelig behov for etter- og videreutdanning innen IKT-sikkerhet, og Tekna mener regjeringens fremlagte "Nasjonal strategi for digital sikkerhetskompetanse" er svært tynn hva gjelder konkrete tiltak for å ruste de som er i jobb.

Tekna etterlyser konkrete tiltak for å sikre at det i virksomhetene og i offentlig sektor er tilstrekkelig IKT-sikkerhetskompetanse til å møte de kravene som det legges opp til i denne NOUen og i forslag til nye reguleringer. Det må lages et etter- og videreutdanningsløp innen dette området.

Tekna mener regulering og styring av IKT-sikkerhet må ivareta et næringsperspektiv. Næringsaktører som skal levere digitale tjenester og teknologisk løsninger til samfunnskritiske virksomheter og offentlig forvaltning, må kunne utvikle og levere tjenester til alle sektorer. Til det kreves et felles rammeverk på tvers av sektorer som sikrer at det ikke utvikler seg ulik forståelse av lovverket og ulike krav til produktene og tjenestene. Det blir krevende for næringslivet å utvikle gode tjenester for sektorer som ikke har sektorovergripende felles rammeverk. Dette svekker god næringsutvikling.

Med vennlig hilsen
Tekna – Teknisk- og naturvitenskapelig forening

Line Henriette Holten
Generalsekretær