

Direktoratet for e-helse

Vår ref: BJ

Oslo 21. september 2017

Innspill til gjennomgang av informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren

Tekna representerer 73 000 medlemmer med master eller doktorgrad innen teknologi og/eller naturvitenskap og er Akademikernes største organisasjon. Våre medlemmer er representert i offentlig og privat sektor og en stor andel jobber med teknologiutvikling og IT.

1. Hvilke kriterier, betingelser og tiltak anser organisasjonene som nødvendig for å kunne benytte private underleverandører på en trygg og ansvarlig måte?

Tekna oppfatter oppdraget til å handle om kjøp av alt fra helseteknologi, applikasjoner og programvare, driftssystemer og infrastruktur, drift og utvikling av disse fra private leverandører inkludert underleverandører. Oppdraget til direktoratet, jfr. tillegg til tildelingsbrev nr 4, omhandler informasjonssikkerhet knyttet til behandling av personsensitive helseopplysninger.

Det er i dag et stort mangfold av IT-tjenester som håndterer personopplysninger, og det er krevende å gi ett sett av kriterier og betingelser som skal gjelde for alle. Det er også utfordrende å implementere ett sett av kriterier som skal gjelde alle anskaffelser uavhengig av type produkt eller tjeneste.

En første vurdering er å avklare om virksomheten falle inn under sikkerhetslovens virkeområde. I så fall trer en hel del krav til virksomheten inn. I dagens sikkerhetslov er det enkelte sektordepartement som avgjøre om underliggende organer faller innenfor eller utenfor lovens virkeområde.

Regjeringen har oversendt et forslag til Stortinget til ny sikkerhetslov med forslag til utvidet virkeområde. Det er viktig at direktoratet i dette arbeidet gjennomgår lovforslag for å vurdere om

www.tekna.no

Org.nr.: 971 420 782
MVA

sikkerhetsnivået i helse- og omsorgssektorens IT-virksomhet er dekket. Tekna er opptatt av at den nye loven ivaretar sikkerhetsutfordringen i helse sektoren på en best mulig måte og er åpen for å få innspill på områder som bør forbedres i god tid før Stortinget avgir innstilling i saken.

Personopplysninger skal behandles i tråd med personopplysningslovens rammer (konfidensialitet). Disse rammene er i endring med implementering av ny personvernforordning (GDPR) fra mai neste år. Deretter må man sørge for at dataene er korrekte og ikke kan manipuleres (integritet) Det er avgjørende for helsevesen at IT-løsningene til enhver tid fungerer på en slik måte at det er mulig å gi nødvendig helsehjelp (tilgjengelighet). Systemet må derfor være robust mot ytre angrep.

For å ivareta dette forhold kreves oppdatert og riktig kompetanse, samt tilstrekkelig kapasitet hos anskaffer. Det gjelder kompetanse knyttet til forståelse av lovverk (personopplysningslov, sikkerhetslov, lov om helsetjenester osv.), god system- og teknologiforståelse samt god innsikt og kunnskap om de leverandører som opererer i markedet. Med andre ord må det være god kompetanse *in house* før man går ut og gjør en anskaffelse. I tillegg er det avgjørende at man har en god plan for oppfølging, implementering og drift i etterkant. Tekna er opptatt av det sikkerhetsvedlikeholdet som må skje i etterkant av anskaffelsen. Et kontinuerlig fokus på retting, feilsøking og videreutvikling av tjenesten eller produktet etter levering, krever en klar plan for oppfølging. Å bygge ned et eksisterende kompetansemiljø i offentlig virksomhet ved utkontraktering av tjenester, vil kunne svekke det løpende sikkerhetsarbeidet i etterkant.

For små kommuner og tilbydere av helse- og omsorgstjenester i offentlig og privat regi som fastleger, tannleger, psykologer, drivere av omsorgsboliger osv., er det en betydelig utfordring å ha en fullgod forståelse av sårbarheten i egne digitale løsninger. Slik innsikt og forståelse er nødvendig for å kunne gjøre en god ROS-analyse (risiko- og sårbarhetsvurdering) av anskaffelser. Tekna mener departementet må vurdere å innføre en form for kvalifisering av private leverandører og en sertifisering av tjenester og produkter for å sikre at det leveres i tråd med kravene til personopplysninger.

Videre mener Tekna at det må utarbeides klare nasjonale retningslinjer for hvordan slike risikovurderinger skal gjennomføres. Nasjonale sikkerhetsmyndigheter må bistå med veiledning og informasjon som kan sikre kvaliteten i vurderingene. Datatilsynet er også en aktør som har en naturlig rolle i veiledningen av aktører som ikke har tilstrekkelig kompetanse.

Tekna mener sikkerhet må være en integrert del i utviklingen av all ny teknologi og IT-systemer. Tekna er også opptatt av at sikkerhet skal være en integrert del av all IKT-utdanning. Tekna mener vi i altfor liten grad har vektlagt sikkerhet i utviklingsfasen av IT-systemer.

2. Er det tjenester som ikke bør overlates til private underleverandører, og hvilke kriterier legger en til grunn for denne anbefalingen?

Tekna viser til Lysne I-utvalgets NOU¹ hvor man trekker frem at utkontraktering til et annet land kan representere en økt sårbarhet i seg selv. Her bør nasjonale myndigheter stille tydelige krav til overordnede sikkerhetsvurderingene.

Tekna mener at drift av det som faller innenfor definisjonen av kritisk infrastruktur og som ligger innenfor sikkerhetslovens virkeområde ikke skal settes ut til utenlandske selskaper.

NSM har en klar rådgivende funksjon når det gjelder sikkerhets- og sårbarhetsvurderinger. Ved større anskaffelser innen områder som krever høy grad av sikkerhet, bør man alltid konferere med NSM. Tekna mener det må utarbeides nasjonale krav til sikkerhet- og sårbarhetsvurderinger. NSM kan da gis myndighet til å beslutte om risikoen er større enn forsvarlig nivå, og dermed pålegge at tjenesten ikke kan utkontrakteres.

De mange diskusjonene og mediasaker knyttet til sikkerhet og sårbarhet i digitale løsninger og infrastruktur viser at det er behov for å legge større vekt på å utvikle en bedre sikkerhetskultur i virksomhetene. Det krever økt kompetanse i virksomhetenes ledelse for å forstå de muligheter og begrensninger som ligger i systemene. Helse- og omsorgssektoren står overfor en omfattende digitalisering som vil utfordre arbeide rundt sikkerhet- og sårbarhets vurderinger. Tillit til det offentlige helsevesen vil raskt kunne svekkes hvis man ikke har et bevisst forhold til hvordan man skal møte disse utfordringene.

Tekna ser frem til rapporten fra Direktoratet for E-helse ferdigstilles. Tekna håper at alle innspill til dette viktige arbeidet blir tilgjengeliggjort sammen med den ferdige rapporten.

Er det behov for mer informasjon vedrørende Teknas innspill kan seniorrådgiver Birgitte Jordahl, birgitte.jordahl@tekna.no, kontaktes.

Med vennlig hilsen



Terje Sletnes
Direktør for samfunnspolitikk

Birgitte Jordahl (el.sign)
Seniorrådgiver

¹ NOU 2015 Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden