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 underlevererandører på en trygg og ansvarlig måte?**

Direktoratet for e-helse etterlyser kriterier, betingelser og tiltak som er nødvendige for å kunne benytte private underleverandører i helse- og omsorgssektoren.

Vi oppfatter at det her er snakk om kjøp av alt fra helseteknologi, applikasjoner og programvare, driftssystemer og infrastruktur samt drift og utvikling av disse fra private aktører, og avgrenses ikke bare til underleverandører. Vi tolker oppdraget til direktoratet, jfr. tillegg til tildelingsbrev nr 4, å dreie seg om hvordan man kan ivareta informasjonssikkerhet knyttet til behandling av personsensitive helseopplysninger.

Det er et stort mangfold av IT-tjenester som på ulike måter vil måtte håndtere personopplysninger, og det er ikke mulig å gi ett sett av kriterier og betingelser som skal gjelde for alle. Det er heller ikke mulig å gi ett sett av kriterier som skal gjelde alle anskaffelser uavhengig av hva slags produkt eller tjeneste man kjøper.

Som en første vurdering må man avklare om virksomheten vil falle inn under sikkerhetslovens virkeområde. I så fall trer en hel del krav til virksomheten inn. Det er det enkelte sektordepartement som skal avgjøre om underliggende organer faller innenfor eller utenfor lovens virkeområde.

Regjeringen har oversendt til Stortinget forslag til ny sikkerhetslov med et utvidet virkeområde. Det er viktig at direktoratet i dette arbeidet går grundig gjennom foreliggende lovforslag og ser om dette vil svare på de utfordringer som kan ligge i vurderingen av sikkerhetsnivået i helse- og omsorgssektorens IT-virksomhet. Det er mulig å få gjennomslag for eventuelle endringer i forelagte lovforslag i stortingsbehandlingen. Tekna ber om å bli orientert hvis man gjennom arbeidet ser svakheter i det lovforslaget som er forelagt Stortinget 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 fra mai neste år. Deretter må man sørge for at man kan ivareta sikkerheten knyttet til integritet, at dataene er korrekte og ikke kan manipuleres (integritet). Til slutt er det helt avgjørende for et moderne helsevesen at IT-løsningene til enhver tid fungerer på en slik måte at det er mulig å gi nødvendig helsehjelp (tilgjengelighet). Systemet må være robust mot ytre angrep.

For å ivareta alle disse forhold kreves høy 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 pulverisere et eksisterende kompetansemiljø i offentlig virksomhet ved utkontraktering av tjenester, vil kunne svekke det løpende sikkerhetsarbeidet i etterkant.

Det er åpenbart at mange, kanskje særlig mindre aktører som små kommuner, små tilbydere av helse- og omsorgstjenester i offentlig og privat regi som fastleger, tannleger, psykologer, drivere av omsorgsboliger osv., ikke har en fullgod forståelse av sårbarheten i sine digitale løsninger. Slik innsikt og forståelse er nødvendig for å kunne gjøre en nødvendig og god ROS-analyse (risiko- og sårbarhetsvurdering) av en anskaffelse fra privat aktør. 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. Det bør også vurderes å stille krav til særskilt kompetanse hos anskaffer.

Videre mener Tekna at det må utarbeides klare nasjonale retningslinjer for hvordan slike risikovurderinger skal gjøres. 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 i eget hus.

Tekna er bekymret for at sikkerheten og sårbarheten i teknologien og i IT-løsningene ikke blir bakt inn allerede i designfasen. Sikkerhet må være en integrert del i utviklingen av all ny teknologi og IT-systemer. I den sammenheng kan nevnes at Tekna er særdeles opptatt av at sikkerhet skal være en integrert del av all IKT-utdanning. Tekna mener vi i altfor liten grad har vektlagt sikkerhet på utviklerstadiet.

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

Det må alltid vurderes hvilket sikkerhetsnivå man må ligge på før man gjør avtale om en anskaffelse. Skal man kjøpe IT og eller teknologitjenester fra private norske eller utenlandske selskaper, vil man måtte vurdere om en slik utkontraktering i seg selv, utgjør en økt sikkerhetsutfordring. ROS-analyser av kjøp av tjenester innen det vi kan definere som kritisk nasjonal infrastruktur, må underlegges klare retningslinjer for vurdering av risiko fra nasjonale myndigheter. I så fall vil ROS-analysen måtte avdekke om det er tilstrekkelig trygghet for at man kan kjøpe tjenesten uten at man svekker sikkerheten.

NSM har en klar rådgivende funksjon når det gjelder sikkerhets- og sårbarhetsvurderinger. Ved større anskaffelser innen områder som krever høy grad av sikkerhet, kan man tenke seg at man alltid skal ha konferert NSM. NSM kan da gis myndighet til å beslutte om risikoen er større enn forsvarlig nivå, og dermed pålegge at tjenesten må utføres i egen regi eller i det minste av et ikke-utenlandsk selskap.

Tekna viser til Lysne I-utvalgets NOU[1] hvor man trekker frem at utkontraktering til et annet land kan representere en økt sårbarhet i seg selv. Det påligger derfor et ansvar for virksomhetene å ha kunnskap om den nasjonen og den virksomheten som får oppdraget for å gjøre en fullgod ROS-analyse. Her bør nasjonale myndigheter stille tydelige krav til de overordnede nasjonale sikkerhetsvurderingene.

Tekna mener at drift av systemer med sensitiv pasientinformasjon, som faller innenfor definisjonen av kritisk infrastruktur og som ligger innenfor sikkerhetslovens virkeområde, skal gjøres i Norge. Nærhet er viktig for slike driftsoppgaver. Tekna tar ikke stilling til hvor data lagres, utover at selskapet og personalet som drifter løsningen må være lokalisert i Norge, og underlagt Norsk lov og regelverk. Ved en eventuell lagring av data i et annet land, må risiko og sikkerhetsvurderingen også omfatte en vurdering av lovverk og sikkerhetssituasjon i landet der dataene lagres. Svært sensitive persondata mener Tekna bør lagres i Norge.

Rammene for hva som faller innenfor kritisk infrastruktur må klargjøres av nasjonale myndigheter. Ny sikkerhetslov som nå er til behandling i Stortinget vil bidra her når arbeidet med tilhørende

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

retningslinjer er ferdigstilt. Når man bruker og behandler pasientinformasjon er det avgjørende å sikre integritet, konfidensialitet og tilgjengelighet. Tekna mener derfor at det bør utarbeides nasjonale retningslinjer til bruk i arbeidet med sikkerhet og sårbarhetsvurderinger. Dette for å sikre at alle forhold systematisk blir gjennomgått og belyst før virksomheter fatter beslutninger om drift og lagring av data.

Avslutningsvis ønsker Tekna å trekke frem at de mange diskusjonene og stadig nye mediesaker knyttet til sikkerhet og sårbarhet i digital infrastruktur og teknologiske og digitale løsninger, fordrer sterk vekt på utvikling av en sikkerhetskultur i virksomhetene. Det krever en betydelig innsikt i ledelsen for å forstå de muligheter og begrensninger som ligger i systemene, og ledelsen må prioritere dette arbeidet. Tekna mener helse- og omsorgssektoren står overfor en kraftig vekst i sikkerhets- og sårbarhetsutfordringer, og at den tillit vi har til offentlig helsevesen raskt vil 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 ønsker gjerne å se innspillene fra de andre aktørene, enten oversendt direkte til oss, eller som vedlegg til den ferdige rapporten.

Er det behov for ytterligere samarbeid, oppklarende runder eller diskusjoner rundt dette temaet, kan seniorrådgiver Birgitte Jordahl, birgitte.jordahl@tekna.no, kontaktes.

Med vennlig hilsen

Terje Sletnes
Direktør for samfunnspolitikk

Birgitte Jordahl (el.sign)
Seniorrådgiver