Høringssvarskjema: Innspill til kommende stortingsmelding om helseberedskap – tema: Digital sikkerhet

Høringsutkastet består av fem hoveddeler som Direktoratet for e-helse ønsker tilbakemelding på:

- En oversikt over hva som gjøres i sektoren i dag knyttet til digital sikkerhet, med hovedfokus på beredskap, herunder forebyggende arbeid
    - Hva gjøres i sektoren i dag – kapittel 2
    - Oversikt over eksisterende tiltak knyttet til digital sikkerhet i sektoren – vedlegg A
- En beskrivelse av de største utfordringene sektoren står overfor på området – kapittel 3
- Et forslag til mål for digital sikkerhet og beredskap i helse- og omsorgssektoren – kapittel 4
- Et forslag til innsatsområder i arbeidet med digital sikkerhet, med forslag til tiltak for hvert innsatsområde – kapittel 5

Der høringsinstansen har innspill, er det ønskelig med en kort begrunnelse og gjerne konkrete forslag til endringer.

Skjemaet sendes til postmottak@ehelse.no og merkes med saksnummer 22/448.

Frist: 09.09.2022

Kontaktinformasjon
Navn på virksomhet: Oslo kommune
Kontaktperson: Kirsti Pedersen
E-postadresse: kirsti.pedersen@byr.oslo.kommune.no

1) Er det mangler i beskrivelsen av pågående initiativer knyttet til digital sikkerhet i nasjonal helseberedskap (kapittel 2), i form av initiativer som ikke er beskrevet, eller mangler i eksisterende beskrivelser? Utdyp gjerne i fritekstfeltet.

   ☒ Ja ☐ Nei ☐ Har ingen kommentar

   Under punktet om innføring av NIS direktivet i norsk lov kan det også nevnes at EU arbeider med en 2.0 versjon av NIS direktivet og at man avventer vedtak for formell adopsjon ila de neste månedene.
   https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

2) Er det mangler i vedlegget med oversikt over eksisterende tiltak knyttet til digital sikkerhet i sektoren (vedlegg A) i form av tiltak som ikke er beskrevet, eller mangler i eksisterende beskrivelser? Utdyp gjerne i fritekstfeltet.

   ☐ Ja ☐ Nei ☒ Har ingen kommentar

Ved utdypning, angi tiltak, ansvarlig, relevant for, beskrivelse:

3) Er beskrivelsen av utfordringsbildet (kapittel 3) i tilstrekkelig grad dekkende for den reelle situasjonen? Utdyp gjerne i fritekstfeltet.

☐ Ja ☒ Nei ☐ Har ingen kommentar

Her savner vi en tydeligere beskrivelse av mulige utfordringer ved at flere digitale tjenestene flyttes ut i sky, og hvordan Schrems II og verdenssituasjonen har medført at man må tenke nytt rundt skytjenester.

4) Beskriver de foreslåtte målene for digital sikkerhet og beredskap i helse- og omsorgssektoren (kapittel 4) et passende og dekkende målbilde? Utdyp gjerne i fritekstfeltet.

☐ Ja ☒ Nei ☐ Har ingen kommentar

Under mål 1 står det at virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder. I nasjonal strategi for digital sikkerhet har de skissert tiltak som myndighetene gjennomfører og tiltak som hver virksomhet bør gjennomføre for å ivareta sitt selvstendige ansvar for digital sikkerhet. Burde det være en tilsvarende to-deling her?

Under mål 5 foreslås en tekstendring i nest siste setning til: Å være robust i møte med et risikobilde i endring innebærer at virksomheter må være i stand til å håndtere nye trusler og sårbarheter. Dette fordi det innføres nye måter å jobbe på i tillegg til ny teknologi, og begge deler fører til nye sårbarheter som trusselaktørene kan utnytte. (nevnt i risikorapporter fra NSM og i innsatsområde «Ny teknologi og digitale verdikjeder»).

Videre ønsker vi å påpeke at ny teknologi og digitale verdikjeder ikke alltid trenger å gi større avhengigheter til leverandører med påfølgende lange og komplekse verdikjeder. Verdikjedene kan også være korte slik de er for applikasjoner man utvikler på tynnkode og som driftes lokalt. Dette forutsetter selvfølgelig kapasitet og kompetanse i organisasjonen. Å øke denne kompetansen lokalt kan derfor også inngå som et tiltak i kapittel 5

5) Er de foreslåtte innsatsområdene og de foreslåtte tiltakene (kapittel 5) hensiktsmessige, og er de realistiske å gjennomføre? Utdyp gjerne i fritekstfeltet.

☐ Ja ☒ Nei ☐ Har ingen kommentar

Her savnes større fokus på kommunal sektor og spesielt videreutvikling av nasjonale virkemidler for å støtte opp om informasjonssikkerhetsarbeidet lokalt. Under kapitlet «Aktiviteter i kommunene» står det at målet er å skape løsninger i felleskap og ikke hver for seg. Det bør konkretiseres hva disse tiltakene er slik at dette gjøres kjent.

6) Tilbakemelding på innsatsområde 1: Videreutvikling av eksisterende nasjonale virkemidler
   Vi anbefaler en videreutvikling av Normen (innenfor informasjonssikkerhetsområdet) som i større grad baseres seg på de ulike grunnprinsippene til NSM. Dette for å standardisere kravene og gjøre dem gjenkjennbare. Økt bruk av sertifiseringsordninger og selvdeklarering kan også være mulige virkemidler.

7) Tilbakemelding på innsatsområde 2: Kompetanse og sikkerhetskultur
   Tiltakene kan med fordel være enda mer spisset utover det å skulle gjennomføre kartlegginger. Vi mener videre at kompetanse må besittes på operativt nivå og at sentralisert utøvende kompetanse som regel vil ha en reaktiv rolle som først benyttes når hendelser inntreffer.

8) Tilbakemelding på innsatsområde 3: Planverk og øvelser
   Ingen kommentar

9) Tilbakemelding på innsatsområde 4: Etterlevelse og oppfølging
   Ingen kommentar

10) Tilbakemelding på innsatsområde 5: Ny teknologi og digitale verdikjeder
    For at ulike kommuner som anskaffer samme teknologi og som forholder seg til samme sett med leverandører, kunne man gått enda lenger for å lette arbeidet? Kunne leverandører sertifiseres etter Normen, og teknologien være sertifisert etter relevant sertifiseringsordning? Da hadde hver kommune sluppet og gjøre inngående vurderinger, men heller bruke krefter på vurderinger rundt eget bruk.

11) Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter
    Viser til kommentar under pkt 10 – det samme vil kunne gjelde for mindre virksomheter som for kommuner. I tillegg bør leverandører ta et større ansvar for at små virksomheter får de riktige rutinene og vet hvilke rutiner de bør ha i bruken av deres løsninger for å ivareta informasjonssikkerhet og personvern.

12) Andre innspill og tilbakemeldinger
    Vi mener man i dokumentet har satt opp mange gode tiltak, men det er mye «bør» tekst i tiltakene. De kan virke litt vage og litt lite konkrete. Det pekes i enkelte avsnitt på at ting skal utredes – da er også utredning et tiltak som må konkretiseres. Nasjonal strategi for digital sikkerhet er mer konkret, og vi mener man kunne pekt på noen av tiltakene som er beskrevet der.