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: Nordre Follo kommune

Kontaktperson: Imad Bahson

E-postadresse: **Imad.Bahson@nordrefollo.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

TEKST: «Sikkerhetshendelser kan oppdages på mange ulike måter. HelseCERT har etablert ensensorplattform som kan bidra til å oppdage trusselaktører i den digitale infrastrukturen. Itillegg er HelseCERTs rike nettverk med andre sikkerhetsmiljøer en kilde til å oppdagesikkerhetshendelser hos tilknyttede virksomheter. HelseCERT varsler virksomheterfortløpende når det er tydelige indikasjoner på at de er rammet av en sikkerhetshendelse.» KOMMENTAR: Kommune Norge har ytret et stort behov for sikkerhetsovervåkning og er vel det Pri 1 tiltaket fra NSM Grunnprinsipper for IKT Sikkerhets som kommunene ser størst behov for å forbedre. Både mtp systemer, ressurser og kompetanse. Vi synes derfor evnen til å «Oppdage» sikkerhetshendelser kunne vært beskrevet i litt mer i detalj i dokumenter for å adressere dette behovet til kommunene. HelseCERT overvåker Helsenettet, men hvordan fungerer samarbeidet om sikkerhetsovervåkning/SOC av kommunene ellers? Som dere selv skriver «Teknologi og systemer kan være sårbare for digitale trusler, og det inkluderer ikke bare systemer knyttet direkte til pasientbehandling» og at «Medisinsk utstyr og velferdsteknologi blir stadig tettere integrert i den øvrige IKT-infrastrukturen» noe som vil si at kommunenes generelle sikkerhetsnivå er avgjørende for

sikring av Helse. Har eksempelvis HelseCERT noen planer for å utvide scopet for sikkerhetsovervåkning/SOC for å ivareta sikring av systemer og infrastruktur som ikke er direkte knyttet til systemer for pasientbehandling som kommunene kan dra nytte av? I NPISK starter det opp et prosjekt for å bygge regionale SOCer for sikkerhetsovervåkning av kommunene, DigiViken har satt i gang et prosjekt for å etablere en regional SOC for kommuner i Viken. Er det noen planer for samarbeid med noen av disse prosjektene eller tilsvarende prosjekter for å øke evnen til å oppdage?

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:

Klikk eller trykk her for å skrive inn tekst.

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

☐ Ja ☒ Nei ☐ Har ingen kommentar

Utfordringen med kompleksitet er tatt opp i dokumentet, men ønsker likevel å kommenter hvordan dette påvirker kommunens evne til å følge ansvarsprinsippet. Det er ikke viljen til å ta dette ansvaret som er utfordringen, det er kompetanse og evnen til å navigere kompleksiteten som er hovedutfordringen. Innledningsvis står det at «Helse- og omsorgssektoren kjennetegnes ved et omfattende og komplekst aktørbilde.» Som kommune opplever vi kompleksiteten i sektoren som overveldende, og når man har mange sektorer å forholde seg til forsterkes naturligvis denne utfordringen. Dette høringsnotatet bidrar lite til å oppklare ansvarsforhold og redusere denne kompleksiteten. Vi som kommune ser at det er masse gode initiativer av høy kvalitet og mange aktører som ønsker å øke den digitale sikkerheten i sektoren. Samtidig ser vi som kommune at den aller største utfordringen er hvordan vi skal evne å absorbere disse initiativene og aktørene til at det materialiserer seg i bedre digital sikkerhet i kommunene. Finnes det en helhetlig oversikt som en kommune kan bruke for å navigere seg i hvordan samarbeidet/ansvarsfordelingen er mellom aktørene som nevnt i dette dokumentet, som for eksempel Helsetilsynet, Helse- og omsorgsdepartementet, Kommunal- og distriktdepartementet, Helsedirektoratet, Justis- og beredskapsdepartementet, Kunnskapsdepartementet, Digitaliseringsdirektoratet, Direktoratet for e-helse, Direktoratet for e-helse ved Normsekretariatet …. GNF, interkommunale samarbeid, Kommune-CSIRT, Politiet og hvordan er det tenkt at en kommune skal forholde seg til disse? Finnes det en helhetlig oversikt som en kommune kan bruke for å navigere seg i hvordan prosjektene/tiltakene som nevnt i dette dokumentet, som for eksempel RSB, Rammeverk for Trygg Digitalisering, NPISK, «Bedre bruk av kunstig intelligens», Normen, Nasjonal Beskyttelsesprogram (NBP), …. VDI, ITN prosjektet Privacy Matters, henger sammen og hvordan det er tenkt at en kommune skal benytte seg av dette?

Hvordan henger aktørene og prosjektene/tiltakene beskrevet for Helsesektoren i dette dokumentet sammen med aktører og prosjekter/tiltak i andre sektorer, og hvordan er det tenkt at en kommune skal forholde seg til dette som en helhet?

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**

Tekst:

«Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder.

Alle virksomheter har et ansvar for egen digital sikkerhet og helseberedskap. Gjennom en risikobasert tilnærming må det sørges for nødvendig egenevne til å overvåke, oppdage, håndtere og beskytte seg mot digitale hendelser. Samtidig er det mange likheter mellom virksomhetene i deres oppgaver og utfordringer knyttet til digital sikkerhet. Gode felles tjenester og ressurser kan gi gevinster både i kvalitet, kostnader og tidsbruk. Det totale potensialet er stort, fordi små forbedringer hos mange virksomheter til sammen vil ha stor effekt.»

Kommentar:

Vi tror det er viktig å fremheve her at egenevnen til en kommune er *avhengig* av felles tjenester og ressurser. Ikke bare at «felles tjenester og ressurser kan gi gevinster» men at det er en absolutt nødvendighet for å bygge kommunens egenevne og igjen kommunenes evne til å ivareta ansvarsprinsippet.

Tekst:

«Virksomhetene evner å effektivt ta i bruk nye teknologier på en sikker måte og er robuste i møte med et risikobilde i endring.

Trusler, teknologi og relasjoner som sektorens virksomheter opererer i, endrer seg raskt. Trygg og effektiv innovasjon oppnås ved å sørge for god digital sikkerhet samtidig som en utnytter mulighetene teknologien gir for å utvikle bedre tjenester. Virksomheter må være i stand til å vurdere sikkerhet ved innføring og bruk av ny teknologi, noe som er krevende. Å være robust i møte med et risikobilde i endring innebærer at virksomheter må være i stand til å håndtere nye trusler. Dette innebærer blant annet innføring av nye og utfasing av gamle løsninger i henhold til egne behov og risikovurderinger.»

Kommentar:

Er det tenkt av enkeltvirksomheter skal vurdere sikkerheten individuelt i dette punktet? Vi forsto punktet om «Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder» som at disse vurderingen burde løftes på sektor-nivå?

Tekst:

«Virksomhetene i sektoren har høy bevissthet om sårbarheter og trusler, og er forberedt og øvet på å avdekke og effektivt håndtere ekstraordinære IKT-hendelser.

Virksomhetene i sektoren må være i stand til å forebygge, avdekke, varsle og håndtere enhver form for IKT-hendelse som truer evnen til å levere helse- og omsorgstjenester, pasientsikkerheten og skjerming av sensitiv helseinformasjon. Det er nødvendig med gode risikovurderinger, tiltak for å avdekke, begrense og stanse alvorlige IKT-sikkerhetshendelser, samt evne til å gjenopprette sikker tilstand for berørte systemer etter hendelser. Egnede beredskapsplaner, velutviklet kompetanse, god kapasitet, forberedte tiltak, trening samt systematisk gjennomføring og læring fra øvelser, er sentrale virkemidler.»

Kommentar:

Henviser igjen til spørsmålet om hva dere legger i «avdekke» i dette punktet. Vi mener «oppdage» bør være mer operasjonelt en deling av sårbahetsinformasjon og hendelser, og bredere en overvåkning av Helsenettet.

Klikk eller trykk her for å skrive inn tekst.

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

De foreslåtte innsatsområdene er gode, men vi kan ikke se helt hvem som står ansvarlig for disse og hvordan det praktisk skal gjennomføres. Blir dette bare mer av kompleksiteten som beskrevet over?Vi kan heller ikke se at dette med å «redusere kompleksitet» eller i hvert fall gi bedre oversikt over aktører, prosjekter og tiltak, som er tatt opp i utfordringsbilde, kommer inn her som et innsatsområde?Normen er et veldig godt utarbeidet og detaljert dokument. Spørsmålet vårt er om hvorfor det er hensiktsmessig at Helsesektoren har egne råd/veiledning for Digital Sikkerhet når NSM som dere beskriver som «Norges ekspertorgan for informasjons- og objektsikkerhet, og er det nasjonale fagmiljøet for IKT-sikkerhet» har utviklet NSM Grunnprinsipper for IKT Sikkerhet? Vi kan ikke se at det er referanse til NSM Grunnprinsipper for IKT Sikkerhet i Normen, eller visa versa. Er det tenkt at en kommune skal forholde seg til Normen innenfor Helse og NSM Grunnprinsipper for IKT Sikkerhet i andre sektorer? Andre sektorer kan ha sine versjoner av «beste praksis». Vi er bekymret for at det blir for komplisert å forholde seg til flere sett med «beste praksiser». Er de like, overlapper de delvis, eller er det viktig forskjeller i rammeverkene som en kommune må forholde seg til? Spørsmålet om kompleksitet og hvordan tiltak/aktører henger sammen er tatt opp i spørsmål 3, men noen konkret spørsmål i kontekst av Normen. Hva er relasjonen mellom Normen og andre rammeverk for sikkerhet? Hva er knytningen til NSM Grunnprinsipper? Hvorfor skal Normen brukes som grunnlag for sikkerhetskrav i anskaffelser, når KS har utviklet egne sikkerhetskrav til anskaffelser, og NSM har sine krav til anskaffelser? Dekker kravene til KS Normen sine krav til sikkerhet? Er de like, overlapper de delvis, eller er det viktig forskjeller en kommune må forholde seg til?

6) Tilbakemelding på innsatsområde 1: Videreutvikling av eksisterende nasjonale virkemidler

Tekst:«Videreutvikling av HelseCERTRegjeringen styrker HelseCERT, helsetjenestenes kompetansemiljø for operativinformasjonssikkerhet, i Norsk helsenett SF. HelseCERT skal sikre økt kapasitet til å gjennomføresikkerhetstesting av aktørene i sektoren, overvåke sikkerhetssituasjonen og drive aktivkommunikasjon og bistand til aktørene i helse- og omsorgssektoren. Samtidig vil HelseCERTskapasitet til å inngå i nasjonalt IKT-beredskapsarbeid styrkes. Den internesikkerhetsmonitoreringen i helseregionene og Norsk helsenett SF forsterkes, og arbeidet gjøres isamarbeid med de regionale helseforetakene, slik at HelseCERT bygger monitoreringstjenestersom treffer de regionale helseforetakenes behov. Trusselbildet og sårbarhetene for digitaleangrep er i endring og styrking av arbeidet med informasjonssikkerhet er viktig for å sikre atsensitive opplysninger ikke kommer på avveie.»Kommentar:Ref kommentar i punkt 1 om HelseCERT evne til oppdage/overvåke

sikkerhetshendelser utenfor Helsenett opp mot kommunens behov for sikkerhetsovervåkning/SOC

7) **Tilbakemelding på innsatsområde 2: Kompetanse og sikkerhetskultur**
Klikk eller trykk her for å skrive inn tekst.

8) **Tilbakemelding på innsatsområde 3: Planverk og øvelser**
Klikk eller trykk her for å skrive inn tekst.

9) **Tilbakemelding på innsatsområde 4: Etterlevelse og oppfølging**
Tekst: Etterlevelse og oppfølging. Økt kontroll med digital risiko vil styrke den forebyggende sikkerheten og øke virksomhetenes evne til å motstå uønskede digitale hendelser. En forutsetning for å oppnå dette er etterlevelse avgrunnleggende sikkerhetskrav og anbefalinger. Økt kontroll med digital risiko vil også gi fleksibilitet til raskere å ta i bruk nye løsninger på en trygg måte. Kommentar: En forutsetning etterlevelse er også redusert kompleksitet i hva «grunnleggende sikkerhetskrav og anbefalinger» faktisk betyr. Er det Normen, råd fra Digidir/KS/DFØ/DSB, NSM Grunnprinsipper for IKT Sikkerhet etc? I dag er aktørene og initiativene så fragmentert at virksomhetene ikke helt veit hva de skal etterleve hvor? Etterlevelse krever standardisering på aktør/tiltakssiden slik at «grunnleggende sikkerhetskrav og anbefalinger» betyr det samme, overalt, alltid.

10) **Tilbakemelding på innsatsområde 5: Ny teknologi og digitale verdikjeder**
Klikk eller trykk her for å skrive inn tekst.

11) **Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter**
Klikk eller trykk her for å skrive inn tekst.

12) **Andre innspill og tilbakemeldinger**
Klikk eller trykk her for å skrive inn tekst.