Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	22. juni 2022

Sak 069-2022

Status for arbeidet med informasjonssikkerhet og vurdering av trusselbildet

Forslag til vedtak:

1. Styret tar sak om status for arbeidet med informasjonssikkerhet og vurdering av trusselbildet til orientering.

2. Styret ber om å bli holdt orientert om arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst.

Hamar, 15. juni 2022

Terje Rootwelt
administrerende direktør

1. Hva saken gjelder

Status for arbeidet med informasjonssikkerhet og regional handlingsplan for informasjonssikkerhet ble behandlet i styret 23. september 2021 i styresak 104-2021. Styret sluttet seg til handlingsplanen og ba om å bli holdt orientert om arbeidet med å forbedre informasjonssikkerheten i Helse Sør-Øst. Styret merket seg at Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer adresserer viktige problemstillinger. Videre fremhevet styret at Sykehuspartner HF har en sentral rolle i arbeidet med informasjonssikkerhet i regionen. Styret viste videre til at det er viktig å se på hele verdikjeden i arbeidet med informasjonssikkerhet, herunder oppfølging av underleverandører.

Denne styresaken gir en orientering om status for arbeidet med å forbedre informasjonssikkerheten i regionen, oppdatert status for tiltakene i regional handlingsplan for arbeidet med informasjonssikkerhet og en vurdering av trusselbildet.

2. Hovedpunkter og vurdering av handlingsalternativer

Behandling av pasientjournaler, kvalitetsregistre, forskningsdata og andre opplysninger er en vesentlig del av det å yte gode helsetjenester. Informasjonssikkerhet handler om å sikre informasjonsbehandlingen og inngår i større eller mindre grad i alle systemer og alle ansattes arbeid. Informasjonssikkerhet handler om å kunne levere helsetjenester selv om flom, brann eller digitale angrep påvirker IKT-systemene, det handler om å hindre avansert datainnbrudd, om en kultur der ansatte behandler opplysninger fortrolig, om at digitale systemer gjengir opplysninger uforandret, og ikke minst handler informasjonssikkerhet om at opplysninger om pasienter skal være tilgjengelig for helsepersonell når de trenger dem.

Vurdering av trusselbildet

Bruk av IKT og digitalisering vil redusere og fjerne noen risikoområder, mens nye risikoer kommer til. Risiko handler om avvik fra mål, og det er mange trusler som kan svekke måloppnåelsen i Helse Sør-Øst. Tilsiktede angrep, menneskelige feil, uhell, utro tjenere og naturkatastrofer kan føre til brudd på tilgjengelighet, integritet og konfidensialitet, med det resultat at kvaliteten i pasientbehandlingen reduseres.

Regionalt beredskapsutvalg har blant annet behandlet naturkatastrofer i regionalt beredskapsseminar i 2021, og på grunnlag av denne gjennomført en risikoanalyse hvor konsekvenser for kliniske, tekniske og forsyningsfunksjoner er vurdert.

Sykehuspartner HF presenterer oversikt over tjenestekvaliteten i ordinær rapportering til eget styre og Helse Sør-Øst RHF. Oppgraderinger som feiler, uhell og andre hendelser kan påvirke tjenestekvaliteten.

Sykehuspartner HF har i samarbeid med Helse Nord IKT utarbeidet en trusselvurdering for regionene. I rapporten beskrives statlige aktører, organiserte kriminelle, hacktivister og selvmotiverte innsidere. I samarbeid mellom helseregionene og Norsk helsenett SF vil det utarbeides en årlig trusselrapport.

Helse Sør-Øst behandler opplysninger om en stor andel av befolkningen, inkludert personer som er sentrale i norske beslutningsprosesser og personer som noen stater kan ønske å hindre at uttaler seg fritt. Politiets sikkerhetstjeneste skriver i nasjonal trusselvurdering for 2022 at flere land søker informasjon om norske beslutningsprosesser og at enkelte land er villige til å gå langt for å tie i hjel politiske motstandere som oppholder seg i Norge. Nasjonal sikkerhetsmyndighet skriver i Risiko 2022 at risiko for alvorlige cyberoperasjoner er høy og øker blant annet for virksomheter som driver forskning og utvikling innenfor helse.

Helse Sør-Øst angripes digitalt hele tiden, og noen ganger vil angriperen lykkes. Angriperne er internasjonale ressurssterke aktører som kan angripe hvem som helst. Det betyr at både små og store helseforetak må spille i samme internasjonale toppliga for å kunne stå imot digitale angrep.

Digitale angripere utvikler stadig sine verktøykasser, det forventes mer ekstremvær og den geopolitiske situasjonen er uklar. Kjennskap til trusler som kan påvirke måloppnåelsen er et grunnlag for å vurdere risiko og iverksette tiltak innen informasjonssikkerhet.

Sikkerhetstilstand

Helse Sør-Øst har en stor og kompleks portefølje av applikasjoner som også inneholder gamle og utdaterte systemer. Riksrevisjonen har påpekt at gjennomsnittsalderen til medisinsk-teknisk utstyr har økt fra 2015 til 2020 og skriver at gammelt utstyr svekker forutsetningene for å støtte opp om helseforetakenes mål om et likeverdig og forsvarlig pasienttilbud og god ressursbruk. Gamle domener, utdaterte operativsystemer og gammelt utstyr kombinert med uønsket variasjon mellom helseforetakene i regionen gir høy kompleksitet.

Mange applikasjoner og høy kompleksitet fører til sårbarheter. Leverandører melder ifra når de blir kjent med nye sårbarheter, og Sykehuspartner HF oppdager sårbarheter gjennom verktøy for sårbarhetsskanning og penetrasjonstesting. I tillegg har Sykehuspartner HF leid inn sikkerhetseksperter til å gjennomføre simulerte angrep («Red team») på linje med det Riksrevisjonen gjennomførte. Sårbarheter kan føre til sikkerhetshendelser, enten de utnyttes av en angriper eller om det er planlagte endringer som feiler.

HelseCERT har testet sikkerheten i regionen, og Sykehuspartner HF kommer godt ut i rapporten. Helse Sør-Øst har god evne til å avdekke og håndtere hendelser med et døgn-bemannet sikkerhetssenter i Sykehuspartner HF, som også arbeider tett med HelseCERT.

Det er ikke bare de digitale løsningene som gir sårbarheter, også den menneskelige faktoren er viktig. Holdningen til digital sikkerhet er jevnt over ganske god i Helse Sør-Øst, selv om kartleggingen av digital sikkerhetskultur i foretaksgruppen viser at det er enkelte forbedringspunkter. Det vil gjennomføres måling av sikkerhetskulturen årlig, gjennom oppdrag gitt til Sykehuspartner HF. Felles måling vil bidra til en felles sikkerhetskultur.

God informasjonssikkerhet gir oversikt og kontroll med risikoen, og har vært en forutsetning for å kunne bruke IKT-løsninger og levere god pasientbehandling. Det arbeides med å redusere risikoen innen informasjonssikkerhet, samtidig som endringer i trusselbildet og teknologi medfører behov for mer arbeid for å hindre risikoen i å øke.

Risikobasert arbeid med informasjonssikkerhet

Det arbeides systematisk med å identifisere og håndtere informasjonssikkerhetsrisiko, slik at informasjonsbehandlingen har et egnet sikkerhetsnivå som møter trusselbildet.

Helsetilsynet har understreket viktigheten av at risikovurderinger balanserer kravene til forsvarlig helsehjelp, brukervennlighet, pasientsikkerhet, personvern og informasjons-sikkerhet[1]. Helhetlige beslutninger er et lederansvar. Organisering av arbeidet med informasjonssikkerhet, inkludert roller og ansvar er revidert. De administrerende direktørene har behandlet i felleskap og hver for seg tilsluttet seg en overordnet lik praksis i regionen[2]. Praksisen er i henhold til overordnet mål og strategi for informasjonssikkerhet[3] hvor ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret. I tillegg har Sykehuspartner HF et helhetlig ansvar for infrastrukturen, og har fått myndighet til å sette bruksvilkår (styresak 107-2019) som helseforetakene må forholde seg til.

Kompleksitet og antall applikasjoner tas ned ved å sanere gamle applikasjoner og i større grad å etablere regionale løsninger. Dette gir bedre kontroll med angrepsflaten. Sikkerhets-brudd i regionale løsninger kan gi større konsekvenser, men risikoen vil trolig bli mindre om ressursene samles til sikring av en felles løsning fremfor for mange lokale løsninger.

Kvaliteten og skalerbarheten som skytjenester tilbyr kan gi redusert kompleksitet og økt kvalitet i pasientbehandlingen. Flere internasjonale leverandører, spesielt innen digital hjemmeoppfølging, tilbyr ikke alternativer til skybaserte løsninger. Det er imidlertid usikkerhet knyttet til bruk av skytjenester, spesielt knyttet til tredjelands myndigheters mulighet til å innhente opplysninger, samlet avhengighet av noen få internasjonale leverandører og fragmentering av journalen når den lagres i ulike løsninger. Helse Sør-Øst RHF arbeider med å vurdere handlingsrommet for bruk av skytjenester.

Tillit til leverandører og deres underleverandører er en utfordring ved kjøp av tjenester og løsninger. Tilpasset innsats for å oppnå tilstrekkelig kontroll med leverandører er krevende, særlig i lange verdikjeder; hvordan kan en etablere tilstrekkelig tillit til at leverandøren etterlever det som er avtalt? Dette gjelder både skytjenester og andre leveranser.

Oppfølging av regional handlingsplan for arbeidet med informasjonssikkerhet

Handlingsplanen (styresak 104-2021) omfatter tiltak basert på mål og strategi for informasjonssikkerhet i Helse Sør-Øst, revisjoner, øvelser, angrepssimuleringer, avvik og faktiske hendelser. Det utføres i tillegg mange risikovurderinger i Helse Sør-Øst hvor risikoreduserende tiltak identifiseres.

Regional handlingsplan for arbeidet med informasjonssikkerhet har sytten tiltak. Ni av tiltakene er gjennomført. Status for øvrige tiltak gjengis nedenfor. To av de øvrige tiltakene, merket med stjerne nedenfor, er knyttet til funn i Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer.

[1] Rapport fra Helsetilsynet 7/2021
[2] Organisering av personvern- og informasjonssikkerhetsarbeidet (helse-sorost.no)
[3] Mål og strategi for informasjonssikkerhet i Helse Sør-Øst – overordnet styrende dokument (helse-sorost.no)

- **Informasjonssikkerhet som del av ordinær virksomhetsstyring**: Utarbeidelse av kriterier for å akseptere risiko gjenstår. Dette er et krav i overordnet mål og strategi for informasjonssikkerhet. Et forslag til kriterier for å vurdere og akseptere risiko er under utprøving i en pilotperiode.

- **Forvaltning og oppfølging av leverandører**: En interregional forvaltningsmodell for å ivareta informasjonssikkerhet i anskaffelser er besluttet. Helseregionenes IKT-direktører skal beslutte hvilken region som har et overordnet ansvar for et område med bakgrunn i underlag som vil bli utarbeidet av Sykehusinnkjøp HF.

- **Revisjon av Sykehuspartner HF***: Konsernrevisjonen har fått i oppgave å revidere Sykehuspartner HF innen informasjonssikkerhetsområdet. Ekstern leverandør vil bistå i revisjonen. Planlegging i mai/juni og gjennomføring i september/oktober.

- **Tekniske sikkerhetstiltak i infrastrukturen***: For Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer er 43 av 47 identifiserte tekniske tiltak gjennomført per 1. mars 2022. Noen av funnene er av en slik karakter at det alltid vil være en problemstilling omkring dem. Tiltakene avsluttes når behovet for ekstraordinær oppfølging er borte og videre oppfølging håndteres som en normal linjeaktivitet.

- **Forbedret tilgangsstyring i journalsystemer**: Neste versjon av DIPS (Arena) har forbedret tilgangsstyring. Tiltaket følger derfor innføringsplanen for oppgradering til Arena som vil skje i perioden 2022-2025. Gjennomføring av prosjektet EPJ-modernisering ble behandlet i styret 10. mars 2022 i styresak 035-2022.

- **Statistisk logganalyse**: Prosjektet statistisk logganalyse skal innføre automatisk overvåking av oppslag i pasientjournalen med den hensikt å avdekke uvanlige oppslag som deretter vil være utgangspunktet for manuell vurdering. Tiltaket følger prosjektets plan og vil være gjennomført når løsningen er innført i 2023.

- **Innføre automatisert kvalitetskontroll i offentlig journal**: Støtte for å oppdage helse- og personopplysninger i journalpostene som skal publiseres i helseforetakenes offentlige postjournal er under utvikling. Planlagt innført i løpet av 2022.

- **Videreutvikling av ledelsessystemet for informasjonssikkerhet**: Den styrkede videreutviklingen av ledelsessystemet som ble iverksatt i 2020, er forventet å kunne avsluttes innen utgangen av 2022. Når endringene i mål og strategi for informasjons-sikkerhet i Helse Sør-Øst er reflektert i underliggende dokumenter, kan den kontinuerlige videreutvikling av ledelsessystemet fortsette som normalt.

3. Administrerende direktørs anbefaling

Digitaliseringen av helsevesenet skaper nye muligheter og økt tilgjengelighet av tjenester og viktig informasjon. Samtidig er det både tilsiktede og utilsiktede hendelser som kan påvirke de digitale tjenestene. God informasjonssikkerhet gir kontroll med risikoen og er en forutsetning for trygg og sikker pasientbehandling.

Riksrevisjonens undersøkelse avdekket viktige problemstillinger og administrerende direktør er opptatt av å følge opp arbeidet med handlingsplanen, slik at funnene er håndtert innen utgangen av 2022. Videre er administrerende direktør opptatt av at trusselbildet vurderes og at det arbeides systematisk med informasjonssikkerhet for å vedlikeholde en sikkerhetstilstand som er tilpasset trusselbildet og gir et håndterbart risikobilde.

Administrerende direktør anbefaler at styret tar redegjørelsen til orientering og vil holde styret orientert om arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst.

Trykte vedlegg:

- Ingen

Utrykte vedlegg:

- Trusselvurdering for Helse Sør-Øst og Helse Nord 2021 (unntatt offentlighet)