Saksframlegg

Saksgang:

Styre	**Møtedato**
Styret Helse Sør-Øst RHF	26. oktober 2023

Sak 123-2023

Status for arbeidet med informasjonssikkerhet

Forslag til vedtak:

1. Styret tar status for arbeidet med informasjonssikkerhet til orientering.

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

Hamar, 19. oktober 2023

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Styret har bedt om å bli holdt orientert om arbeidet med å styrke informasjonssikkerheten, jamfør styresak 035-2023.

Denne styresaken gir en orientering om status for arbeidet med å styrke informasjons-sikkerheten i Helse Sør-Øst.

2 Hovedpunkter og vurdering av handlingsalternativer

Behandling av pasientjournaler, kvalitetsregistre, forskningsdata og andre opplysninger er en vesentlig del av det å yte gode likeverdige helsetjenester. Informasjonssikkerhet handler om konfidensialitet, integritet og tilgjengelighet. Dette inngår i større eller mindre grad i alle ansattes arbeid, og handler om å kunne levere helsetjenester selv om for eksempel flom, brann eller angrep påvirker IKT-systemene. I dette inngår blant annet å håndtere digitale angrep, bygge en kultur der ansatte behandler opplysninger fortrolig, og at digitale systemer gjengir opplysninger uforandret. Ikke minst handler informasjonssikkerhet om at opplysninger om pasienter skal være tilgjengelig for helsepersonell når de trenger dem.

Helse Sør-Øst RHF orienterte om status for arbeidet med informasjonssikkerhet i administrerende direktørs driftsorientering, styresak 035-2023. Trusselbildet for spesialist-helsetjenesten ble lagt frem i driftsorienteringer fra administrerende direktør, styresak 082-2023. Etter denne rapporteringen har det ikke inntruffet noen uønskede hendelser i foretaksgruppen innen informasjonssikkerhet som Helse Sør-Øst RHF har måttet håndtere.

2.1. Avanserte trusselaktører

Nasjonal sikkerhetsmyndighet (NSM) fremhever viktigheten av at norske myndigheter har en omforent situasjonsforståelse av trussel- og risikobildet. Gjennom en omforent forståelse av trusselaktørers evne og vilje til negativt å påvirke spesialisthelsetjenestens verdier, primært gjennom digitale operasjoner og verktøy, kan helseregionene bedre samarbeide og legge til rette for en felles innsats innen informasjonssikkerhetsområdet.

Det er viktig å erkjenne at det eksisterer trusselaktører med både evne og vilje til å påføre betydelig skade på spesialisthelsetjenestens IKT-systemer. Kunnskap om dette er nødvendig for å kunne håndtere truslene vi står ovenfor.

Trusselaktørene er avanserte, motiverte og dyktige. De vil søke å utnytte sårbarheter, svakheter, feil eller mangler til sin fordel. Trusselvurderingen har som formål å gi en bedre situasjonsforståelse, og dermed bidra som beslutningsstøtte på strategisk nivå for å redusere risiko for vellykkede angrep. Å forstå trusselbildet og aktørenes motivasjon, evne og vilje setter oss i bedre stand til å ta gode beslutninger både før, under og etter et digitalt angrep

Trusselvurderingen er publisert på internett under Sykehuspartner HFs ledelsessystem og bruksvilkår: Ledelsessystem og bruksvilkår - Sykehuspartner HF

2.2. Systematisk arbeid for å håndtere trusler og farer

Digitalisering vil redusere og fjerne noen risikoområder, mens nye risikoer kommer til. Det er viktig å arbeide systematisk med risikostyring og ha et bevisst forhold til utvikling i trussel- og sårbarhetsbilde. Både tilsiktede og utilsiktede handlinger kan utløse hendelser som svekker måloppnåelsen i Helse Sør-Øst. Som eksempler kan blant annet menneskelige feil, tekniske feil, naturkatastrofer og tilsiktede angrep føre til at informasjon ikke er tilgjengelighet eller at krav om integritet og konfidensialitet ikke oppfylles. Resultatet kan være at kvaliteten i pasientbehandlingen reduseres. God informasjonssikkerhet er en forutsetning for god pasientbehandling.

I 2023 har det vært et særskilt arbeid med kartlegging og sikring av grunnleggende nasjonale funksjoner (GNF), samt annet arbeid opp mot nasjonale sikkerhetsinteresser. Blant annet gjøres nasjonalt begrenset nett tilgjengelig i helseforetakene, det planlegges øvelse for håndtering av kritiske hendelser og ulike områder risikovurderes.

Utviklingen av kunstig intelligens-baserte verktøy gir muligheter og trusler på informasjons-sikkerhetsområdet. Trusselaktører vil i større grad kunne lage automatiserte og tilpasnings-dyktige angrep, både mot mennesker (feilfri tekst, tale og video som etterligner andre personer) og maskiner. Kunstig intelligens benyttes i sikkerhetsverktøy i Sykehuspartner, og det benyttes blant annet i røntgenavdelingen i Vestre Viken. Det pågår lovgivningsarbeid i EU knyttet til kunstig intelligens, blant annet AI Act og AI Liability Act, som kan påvirke tilgangen til slike verktøy for lovlige formål.

2.3. Identifiserte sårbarheter og risikoer

Det er viktig å arbeide med sårbarheter og risikoer og å håndtere disse, både for å unngå alvorlige enkelthendelser, og for å unngå mange mindre uønskede hendelser som samlet gir vesentlig skade. Det kan for eksempel være tid som brukes på unødvendige steg for å hente informasjon en har tjenstlig behov for.

Helseforetakene har i sin rapportering omtalt de største risikoene. Et utvalg av disse er knyttet til løsepengevirus, usikkerhet rundt bruk av skytjenester, gamle domener og utdatert programvare, medisinsk-teknisk utstyr, manglende tilgjengelighet til IKT-systemer og monitorer som viser pasientinformasjon i sykehusene. Det arbeides med å øke kvaliteten i rapporteringen, slik at Helse Sør-Øst RHF får et bedre helhetlig risikobilde.

Vurderingen fra Helse Sør-Øst RHF er at vi innen informasjonssikkerhet ikke har høye risikoer, på en skala med lav, moderat og høy risiko. Det vil si at det ikke er høy sannsyn-lighet for at alvorlige hendelser inntreffer. Vi har derimot noen moderate risikoer. Som illustrasjon beskriver vi to utvalgte risikoscenarier, med beskrivelse av konsekvens og tilhørende årlig sannsynlighet for at scenariet skal inntreffe med angitt konsekvens:

- I henhold til pasientjournalloven skal behandlingsrettede helseregistre understøtte pasientforløp i klinisk praksis og være lett å bruke og å finne frem i. I henhold til helsepersonelloven skal helsepersonell gis nødvendig og relevante helseopplysninger når det er nødvendig for å gi forsvarlig helsehjelp. Dette gjelder også på tvers av helseforetak og mellom helsetjenestenivåene. Svikt vil typisk være i forbindelse med samhandling og ansvarsoverganger. Et scenario kan være pasienter som får redusert kvalitet i behandlingen, med lettere forbigående reduksjon i helse, fordi relevante

opplysninger ikke var tilgjengelige. Kjernejournal skal ivareta behov for kritisk informasjon på tvers. Vi er imidlertid kjent med at det er et høyere antall registreringer med kritisk informasjon i lokalt pasientjournalsystem enn antall registreringer i kjernejournal for samme periode. Helseforetak er involvert i en rekke samhandlinger om pasientforløp eller ansvarsoverganger i pasientforløp. Helseforetakene rapporterer om manglende tilgjengelighet til IKT-systemer. I tillegg kan det kan være krevende å hente opplysninger fra andre helseforetak og fra primærhelsetjenesten. Hendelser knyttet til informasjonssikkerhetsbrudd med liten konsekvens er meget sannsynlig og skjer flere ganger hvert år. Det utgjør en moderat risiko.

- Et annet scenario er der organiserte kriminelle løsepengeutpressere får tilgang til infrastrukturen og bruker tilgangen til å kryptere deler av opplysningene våre og gjøre systemer utilgjengelig. Konsekvensen vil være alvorlig, både for pasientenes personvern og for pasientbehandlingen. Helse Sør-Øst har en stor portefølje av applikasjoner og en kompleks infrastruktur, hvorav flere applikasjoner er utdatert. Helse Sør-Øst har hatt noen dataangrep med alvorlig konsekvens. Vi vurderer det som lite sannsynlig at scenarioet vil inntreffe, men på grunn av alvorlighetsgraden vil det likevel gi en moderat risiko.

Risiko for uønskede hendelser reduseres blant annet gjennom systematiske sårbarhetsoppgraderinger, sanering eller oppgradering av utdaterte applikasjoner og modernisering av infrastrukturen, i tillegg til systematisk sikkerhetsovervåking. Infrastruktur og applikasjoner i Helse Sør-Øst driftes i hovedsak av Sykehuspartner HF. Sikker infrastruktur og moderne applikasjoner er viktig for å kunne stå imot digitale angrep. Sykehuspartner HF har over lengere tid hatt et systematisk arbeid, sammen med helseforetakene, med sanering av applikasjoner og oppgradering av infrastruktur.

Tilgang til nødvendig kompetanse og mulighet for effektiv og sikker drift er krevende i et marked med rask teknologisk utvikling. Den teknologiske utviklingen er slik at mange tjenester, inkludert fagapplikasjoner, i økende grad kun tilbys som skytjenester.

Ved å bruke store internasjonale leverandører kan Helse Sør-Øst utnytte kompetanse og stordriftsfordeler som regionen selv ikke vil kunne oppnå. Tjenestekjøp av flere applikasjoner og deler av infrastrukturen kan gi bedre motstandskraft mot ressurssterke trusselaktører. En vesentlig utfordring ved tjenestekjøp har vært en juridisk usikkerhet knyttet til bruk av amerikanske skytjenester og europeiske skytjenester med amerikanske morselskaper. Endringer i amerikansk regelverk ledet fram til EU-kommisjonens beslutning 10. juli 2023 hvor USA ble oppført på lista over stater som gir et tilstrekkelig personvernnivå. Avgjørelsen gjelder direkte kun for leverandører som er selvdeklarerte under Data Privacy Framework, men forbedringene av amerikansk regelverk gjelder for alle, inkludert aktører som ikke er sertifisert. Beslutningen gjør det mulig å ta i bruk amerikanske tjenester på lik linje med europeiske. Leverandørenes evne til å ivareta sikkerhetskrav må fortsatt vurderes.

En kvantedatamaskin er en type avansert datamaskin som bruker kvantemekaniske fenomener for å utføre operasjoner på data. For visse typer beregninger er kvantedatamaskin raskere enn tradisjonelle datamaskiner. Det pågår en utvikling av kvantedatamaskiner som også er relevant for kryptoanalyse. Det eksisterer algoritmer for kvantedata

maskiner som kan bryte den krypteringen som benyttes i dag, selv om dagens kvantedata-maskiner ikke er tilstrekkelig store til å kjøre algoritmene. En ondsinnet aktør kan lagre krypterte helsedata i dag, og bryte krypteringen når/hvis en egnet kvantedatamaskin utvikles. Nasjonal sikkerhetsmyndighet presenterte[1] at en egnet kvantedatamaskin kan være utviklet i 2030-2040.

Nye kvanteresistente algoritmer for kryptering og signering har vært under utvikling i flere år. National institute of standards and technology (NIST) valgte algoritmer i 2022, og det er forventet at disse blir standardisert i løpet av 2024[2]. Det vil da være et løp over flere år for å bytte ut kryptoalgoritmene som Helse Sør-Øst benytter til kvanteresistente kryptoalgoritmer.

2.4. Oppfølging av tiltak

Regional handlingsplan for arbeidet med informasjonssikkerhet[3] skal oppdateres innen 1. mai hvert år. Planen ble behandlet den 28. april 2023 i styresak 035-2023. Beskrivelse av tiltakene er gitt i handlingsplanen. Nedenfor følger oppdatert status for tiltakene:

Tiltak	**Status**
Forbedret risikostyring	Sykehuspartner har tilpasset egne prosesser: • NO-52 veileder til NO-05 – Kriterier for vurdering og aksept av risiko, • NO-53 Informasjonsklassifisering og verdimodell, og • NO-54 ROS-prosess informasjonssikkerhet. Helseforetakene ble orientert om prosessen i juni 2023. Bruk av prosessene er nå under operasjonalisering, inkludert kursing av risikoeiere og ledere for å styrke kompetansen i linjen.
Oversikt over verdier	Oppdrag gitt i oppdrags- og bestillingsdokumenter for 2023 til helseforetakene. Fristen er ut året.
Etablere nasjonalt begrenset nett (NBN) i helseforetakene	For Helse Sør-Øst inkludert Pasientreiser HF og Helsetjenestenes driftsorganisasjon HF er seks helseforetak koblet til NBN. De resterende helseforetakene er i prosess med å få etablert NBN.
Forebyggende sikkerhets-tiltak for å beskytte skjermingsverdige verdier	Gitt som oppdrag til Sykehuspartner HF i oppdrags- og bestillingsdokumentet for 2023. Arbeidet går i henhold til Sykehuspartner HFs plan.

[1] Foredrag under sikkerhetsfestivalen på Lillehammer 2023.
[2] NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST
[3] Regional handlingsplan for arbeidet med informasjonssikkerhet (helse-sorost.no)

Tiltak	Status
Måling av informasjons-sikkerhets-kultur	Måling ble gjennomført i august/september. Resultatet vil legges frem for foretaksgruppen i oktober 2023. Helseforetakene vil deretter følge opp funn og resultater i egen virksomhet.
Utarbeide opplæring for styrket digital kompetanse innen informasjonssikkerhet	Pågår
Trusselvurdering	Levert og orientert om i styresak 082-2023.
Øve på håndteringen av uønskede kritiske hendelser	En øvelse er planlagt å finne sted fjerde kvartal 2023.
Forvaltning og oppfølging av leverandører	Det pågår et arbeid, ledet av regionenes ikt-direktører, med å lage en plan for hvordan forvaltning av ulike områder kan fordeles mellom regionene.
Sanering av applikasjoner, systemer og infrastruktur	Sanering av applikasjoner har god fremdrift. Sykehuspartner HF har fått som mål i oppdrags- og bestillingsdokument for 2023 å nå 50 prosent i løpet av 2023. Per september er det oppnådd 47 prosent.
Forbedret tilgangsstyring i journalsystemer	Det pågår et arbeid med innføring av DIPS Arena.
Statistisk logganalyse	Prosjektet er satt på pause ut 2023, blant annet grunnet utfordringer med å etablere drift av løsningen.
Innføre automatisert kvalitetskontroll i offentlig journal	Innført og tatt i bruk i de fleste helseforetakene. To helseforetak gjenstår.
Oversikt over tiltak fra risikovurderinger	Sykehuspartner har under innføring en løsning for utarbeidelse av ROS-vurderinger inklusive anbefalte risikoreduserende tiltak. Løsningen er under pilotering og vil tas bredere i bruk etter neste oppgradering i oktober.
Gjennomgå beredskaps-planverk innen IKT	Beredskapsplanverket er gjennomgått. Planverket er oppdatert for IKT-sikkerhetshendelser, og det er utviklet et gjenopprettingsplanverk.

3 Administrerende direktørs anbefaling

Den teknologiske utviklingen skaper nye muligheter for helsevesenet og gir økt tilgjengelighet av tjenester. For trygg og sikker pasientbehandling er det er forutsetning at informasjonssikkerheten er god.

Det er viktig å erkjenne at det eksisterer trusselaktører med både evne og vilje til å påføre betydelig skade i spesialisthelsetjenestens IKT-systemer. Kunnskap om dette er nødvendig for å kunne håndtere truslene vi står ovenfor. Trusselaktørene er avanserte, motiverte og dyktige, og kan gjøre stor skade. En annen informasjonssikkerhetsutfordring er at nødvendige og relevante helseopplysninger ikke alltid er tilgjengelige for helsepersonell i andre helseforetak og primærhelsetjenesten. Dette er et område som krever oppmerksomhet.

Administrerende direktør er tilfreds med det systematiske arbeidet innen informasjons-sikkerhet, selv om det fortsatt er forbedringspunkter. For å kunne innrette innsats og sikkerhetstiltak på en trygg og effektiv måte som støtter pasientbehandlingen er administrerende direktør opptatt av at helseforetakene arbeider systematisk med oversikt over sikkerhetstilstanden og risikobildet, og ivaretar en god balanse mellom de tre målene for informasjonssikkerhetsarbeidet konfidensialitet, integritet og tilgjengelighet.

Trykte vedlegg:

- Ingen

Utrykte vedlegg:

- Ingen