Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	28. april 2023

Sak 035-2023

Status og regional handlingsplan for arbeidet med informasjonssikkerhet

Forslag til vedtak:

1. Styret tar status for arbeidet med informasjonssikkerhet til orientering.
2. Styret slutter seg til regional handlingsplan for arbeidet med informasjonssikkerhet.
3. Styret ber om å holdes orientert om arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst.

Hamar, 21. april 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 069-2022. I tillegg ba Helse- og omsorgsdepartementet i foretaksmøtet den 17. januar 2023 de regionale helseforetakene om å oppdatere de regionale handlingsplanene for det systematiske arbeidet med å styrke informasjonssikkerheten. Oppdateringen skal skje innen 1. mai hvert år, og det skal rapporteres fra forbedringsarbeidet.

Denne styresaken gir en orientering om status for arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst. Vedlagt saken er forslag til oppdatert handlingsplan for arbeidet med informasjonssikkerhet og en uttalelse fra brukerutvalget i Helse Sør-Øst RHF.

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 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 125-2022. Etter denne rapporteringen har det ikke inntruffet noen hendelser i foretaksgruppen innen informasjonssikkerhet som Helse Sør-Øst RHF har måttet håndtere.

2.1. Bedre oversikt over trusselbildet

Oversikt over og forståelse for trusselbildet har blitt bedre de senere år. I 2021 utarbeidet Sykehuspartner HF en trusselvurdering for digital sikkerhet i samarbeid med Helse Nord IKT. I foretaksmøtet den 10. januar 2022 ble de regionale helseforetakene bedt om å utarbeide en felles årlig rapport om trusler og trender i samarbeid med Norsk helsenett SF. Krav til innhold i rapporten fikk noen mindre justeringer i foretaksmøtet 17. januar 2023, som skal utarbeides innen 1. juni hvert år.

Den forrige trusselvurdering innen digital sikkerhet for spesialisthelsetjenesten ble behandlet i styresak 095-2022. Trusselbildet er i konstant endring som følge av trusselaktørenes tilpasningsevne og kontinuerlige utvikling av verktøy og metoder. Dette medfører at sikkerhetsmekanismene løpende må justeres for å holde risikonivået stabilt.

Rapporten tar for seg statlige aktører, organiserte kriminelle, hacktivister og selvmotiverte innsidere. Den største trusselen mot spesialisthelsetjenesten vurderes å være organiserte kriminelle aktører som er spesialisert på digital utpressing. Konsekvensene av en vellykket inntrengning og digital utpressing vil typisk handle om langvarig nedetid på systemene som er rammet, og helseopplysninger og annen sensitiv informasjon på avveie.

Destruktive angrep mot spesialisthelsetjenesten fra hactivister var en av truslene som var vurdert i rapporten. Den 27. januar 2023 publiserte den russisk-vennlige gruppen KillNet en melding på meldingstjenesten Telegram om at de som hevn for det de kaller «support for the Nazis in Ukraine» ville gjennomføre destruktive cyberangrep mot datanettverk tilhørende sykehus i en rekke vestlige land, inkludert ti forskjellige helseforetak i Norge. Saken fikk medieoppmerksomhet, hvor det ble laget saker om at russiske hackere truet norske sykehus.

Angrepene medførte at helseforetakenes nettsider i svært korte perioder den 28. og 29. januar ikke var tilgjengelige, uten skade eller påvirkning for pasienter eller sykehusenes drift.

Årets trusselvurdering er under utarbeidelse, og forslag til rapport er planlagt behandlet i Sykehuspartner HFs styre den 24. mai 2023.

2.2. Systematisk arbeid for å håndtere trusler og farer

Digitalisering vil redusere og fjerne noen risikoområder, mens nye risikoer kommer til. Risiko handler om avvik fra mål, og det er mange farer og trusler som kan svekke 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, med det resultat at kvaliteten i pasientbehandlingen reduseres. God informasjonssikkerhet er en forutsetning for god pasientbehandling.

Trusselvurderingen for digital sikkerhet har som formål å gi en bedre situasjonsforståelse, og dermed bidra som beslutningsstøtte for å redusere risiko for vellykkede digitale angrep mot våre verdier. Å forstå trusselbildet og –aktørenes motivasjon, evne og vilje setter spesialisthelsetjenesten bedre i stand til å ta gode beslutninger før, under og etter et digitalt angrep.

Det er mange maskiner og servere som skal passes på i Helse Sør-Øst. Sykehuspartner HF har sikring som gir god deteksjons- og responskapabilitet på over 68 000 klienter, 12 000 servere og 13 000 tjenestemobiler.

Digitale verdikjeder er et område som omtales i trusselvurderingen. Dette har oppmerksomhet, og kan inngå som en av flere risikoer i mange av løsningene våre.

For å kunne motstå stadig mer avanserte digitale løsepengeutpressere, er det digitale fotavtrykket på internett vesentlig redusert i senere tid og kontrollert i et eget område av nettverket (DMZ). Av applikasjonene som ikke er eksponert på internett, er også mange applikasjoner faset ut. Helse Sør-Øst har nå omkring 1250 applikasjoner i bruk. Det er etablert en sikker sone med høyt sikkerhetsnivå, og det er innført avansert sikkerhetskopi for opplysninger som trenger særlig beskyttelse mot tap, hvor det kun kan skrives én gang, mens det kan leses mange ganger.

For tilgang til systemer er det innført tofaktorautentisering gjennom ID-porten for all fjernpålogging til Helse Sør-Øst.

Helse Sør-Øst har god evne til å avdekke og håndtere hendelser med et døgnbemannet sikkerhetssenter (CERT) i Sykehuspartner HF. Det arbeides tett sammen med HelseCERT som er helsesektorens nasjonale koordinerings- og responsmiljø.

Styret i Helse Sør-Øst RHF besluttet 28. juni 2017, jf. styresak 77-2017, at sikkerhets-plattformen, en avansert sikkerhetsovervåkningsløsning, skulle dekke alle helseforetak i regionen og regional infrastruktur. Det var denne plattformen som kunne spore dataangrepet i 2018, og dokumentere at ingen helseopplysninger kom på avveie. Sikkerhetsplattformen oppdaget også Riksrevisjonens simulerte dataangrep i en tidlig fase. Sykehuspartner HF hadde mulighet til å stanse det simulerte angrepet, men valgte i samråd med Riksrevisjonen å la angrepet fortsette for å kunne avdekke svakheter dypere i infrastrukturen. Datainnbruddet i 2020 ved Sykehuset Innlandet HF ble også oppdaget av sikkerhetsplattformen, og den ga dokumentasjon om hvilke opplysninger som kom på avveie.

Sikkerhetsplattformen har stadig blitt forbedret. Infrastrukturen er koblet til Nasjonal sikkerhetsmyndighets varslingssystem for digital infrastruktur (VDI) og den er koblet til HelseCERT. Sykehuspartner HF har i en periode leid inn sikkerhetseksperter til å gjennomføre simulerte angrep («Red team») på linje med det Riksrevisjonen gjorde. HelseCERT har testet sikkerheten i regionen, og Sykehuspartner HF kom godt ut i rapporten. Sykehuspartner HF har i tillegg inngått en avtale med en kommersiell tredjepart om kontinuerlig sårbarhetskartlegging av internett-eksponert infrastruktur.

Fra 2016 har foretaksgruppen hatt et felles ledelsessystem for informasjonssikkerhet. Overordnet mål og strategi for informasjonssikkerhet er tilsluttet i foretaksgruppen og vedtatt av styret i Helse Sør-Øst RHF (sak 046-2021).

I oppdragsdokumentet for 2023 er helseforetakene bedt om å ha bedre oversikt over de viktigste verdiene og risikoen, slik at IKT-systemer og tjenester bestilles med egnet sikkerhetsnivå.

Sykehuspartner HF har oversikt over sentrale anbefalinger innen digital sikkerhet og følger opp disse, herunder NSMs grunnprinsipper for IKT-sikkerhet.

I arbeidet med å vurdere trusler og farer er det lagt opp en systematikk for vurdering av risiko, tiltak og håndtering av restrisiko. Risiko vurderes, håndteres og rapporteres på ulike nivåer. Helse Sør-Øst RHF har jevnlig overordnet rapportering av risiko innen informasjons-sikkerhet og personvern til styret. Helseforetakene rapporterer tertialvis risiko innen informasjonssikkerhet til Helse Sør-Øst RHF. I tillegg utarbeides det mer detaljerte sårbarhets og risikovurdering for ulike IKT-løsninger.

Helhetlige beslutninger i ledelseslinjene er tydeliggjort i styrende dokument med kriterier for vurdering og aksept av risiko, tilsluttet av de administrerende direktørene i helseforetakene. Sykehuspartner HF er bedt om å legge bedre til rette for at beslutninger tas i ledelseslinjene. Det er sentralt å benytte ressursene på en hensiktsmessig måte, slik at det settes inn størst innsats der risikoen er størst. Dette er et område med forbedringspotensial som vil prioriteres.

Alle helseforetakene har informasjonssikkerhetskompetanse, og i tillegg er Sykehuspartner HF et kompetansemiljø innen informasjonssikkerhet for hele regionen. Imidlertid er informasjonssikkerhet viktig i det daglige arbeidet på alle nivåer i foretaksgruppen. Det er derfor viktig med systematisk arbeid både med kunnskap og kultur. Informasjonssikker-hetskulturen måles årlig, og hvert enkelt helseforetak er ansvarlig for å følge opp med

egnete tiltak for forbedring av kulturen. Felles digital opplæring for alle ansatte innen informasjonssikkerhet og personvern er under utarbeidelse for foretaksgruppen.

Beredskapsplaner er en forberedelse for å kunne håndtere hendelser på en egnet måte. Beredskapsplanene har vært gjennomgått, og vil oppdateres, jamfør krav fra Helse og omsorgsdepartementet[1].

2.3. Identifiserte sårbarheter og risikoer

For å unngå å havne i en beredskapssituasjon er det viktig å identifisere sårbarheter og risikoer, og håndtere disse.

Riksrevisjonen offentliggjorde i 2020 en undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. Undersøkelsens funn og anbefalinger er fulgt opp i Helse Sør-Øst. Enkelte funn er av en slik karakter at det alltid vil være risiko forbundet med dem. Disse risikoene er innenfor det som er akseptabelt, og Helse Sør-Øst RHF anser oppfølging av undersøkelsen som avsluttet. Noen av funnene vil fortsatt ha oppmerksomhet i ordinær virksomhetsstyring.

Riksrevisjonen har gjennomført en undersøkelse av styring og kontroll av tilganger i elektroniske pasientjournaler i fire helseforetak. Undersøkelsen ble offentliggjort i 2014. I Riksrevisjonens undersøkelse fra 2020 om IKT-angrep ble det påpekt at det fortsatt er funn fra tidligere revisjoner som ikke er håndtert. Funnen er i all hovedsak håndtert, men det arbeids med ytterligere forbedring, jamfør vedlagt handlingsplan.

I de nasjonale trusselvurderingene har oppmerksomheten om sårbarheter i kritisk infrastruktur blitt mer sentral. Det er gjennomført arbeid med å kartlegge hvilke virksomheter og systemer som har avgjørende betydning for grunnleggende nasjonale funksjoner. I denne forbindelse er det pekt ut noen skjermingsverdige verdier i Helse Sør-Øst. Sårbarheter og risiko forbundet med disse må gjennomgås på nytt i lys av betydningen for nasjonal sikkerhet.

Helse Sør-Øst har mange applikasjoner, systemer og en kompleks infrastruktur som inkluderer utdatert maskinvare og gamle domener med ulikt oppsett. Dette hindrer samhandling og flyt av opplysninger mellom systemer, og det gjør at Helse Sør-Øst er mer utsatt for dataangrep.

Det pågår arbeid med sanering av utdaterte applikasjoner og modernisering av infrastrukturen. Infrastrukturen og applikasjoner i Helse Sør-Øst driftes i hovedsak av Sykehuspartner HF. 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 er imidlertid en juridisk usikkerhet

[1] Protokoll fra foretaksmøte i Helse Sør-Øst RHF 17. januar 2023 (regjeringen.no)

omkring rettslige forhold, dels knyttet til hvordan regelverket skal forstås, og dels knyttet til vurderingen av om konkrete løsninger tilfredsstiller rettslige krav. Dette gjelder både tjenester hvor personopplysninger behandles utenfor EØS-området, og for tjenester hvor behandlingen skjer innenfor EU/EØS og hos en europeisk aktør, men hvor tjenestetilbyderen er amerikanskeid.

Regjeringen har en politikk om at skytjenester skal vurderes på linje med andre løsninger,[2] men ingen av de ledende leverandørene innen sky er fullt ut europeiske virksomheter, de har alle hovedsete utenfor Europa[3]. Det er imidlertid typisk disse leverandørene som best kan stå imot avanserte angrep. I melding til Stortinget (meld. St. 9 (2022-2023)) er det påpekt at «Mange norske virksomheter velger å kjøpe skytjenester fra store kommersielle, multinasjonale selskaper. Dette bidrar som oftest til å øke sikkerheten for virksomhetene siden de kan utfase utdaterte IT-løsninger, og få tilgang til sikker infrastruktur og profesjonelle sikkerhetsmiljøer. […] Alternativet er at virksomhetene må velge lokale løsninger, noe som kan føre til høyere kostnader og begrenset tilgang til nye teknologiske verktøy.»[4]

Muligheten for å følge opp arbeidet med sanering og standardisering, jamfør styrevedtak 107-2019, begrenses dersom de mest modne og sikre leverandørene ikke kan benyttes. En avtale mellom EU og USA for behandling av personopplysninger vil forenkle dette arbeidet.

I helselogistikkløsningen for innsjekk og oppgjør er det valgt en norsk leverandør. Leverandøren har utviklet en programvare som leveres som en skytjeneste til Helse Sør-Øst. Programvaren kjører på infrastruktur hos en europeisk underleverandør med et amerikansk morselskap. For denne løsningen er det utarbeidet omfattende informasjonssikkerhetsmessige og juridiske vurderinger. Informasjonssikkerhetsmessig kan risiko i løsningen aksepteres. Det har også vært dialog med Datatilsynet, som nå har avsluttet saken. Det arbeides med noen ytterligere vurderinger i henhold til Datatilsynets oppsummering av siste veiledningsmøte.

2.4. Oppfølging av tiltak

Tiltak knyttet til skjermingsverdige verdier i henhold til sikkerhetsloven vil ha oppmerksomhet i 2023. Disse omtales kun overordnet i regional handlingsplan.

Arbeid med å holde et sikkerhetsnivå som er egnet i forhold til risiko er et kontinuerlig arbeid. I den regionale handlingsplanen for arbeidet med informasjonssikkerhet vises de mest sentrale tiltakene det arbeides med i 2023. Risikoer identifisert i revisjoner har tiltak i handlingsplanen, mens mange av de tiltak som er foreslått i risiko- og sårbarhetsvurderinger for den enkelte løsning følges opp i hver enkelt løsning, og er ikke tatt med i handlingsplanen.

---

[2] Digitaliseringsrundskrivet - regjeringen.no – 1.13 Velg skytjenester.
[3] Magic Quadrant for Cloud Infrastructure and Platform Services - gartner.com
[4] Meld. St. 9 (2022–2023) (regjeringen.no) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet*

3 Administrerende direktørs anbefaling

Digitaliseringen av helsevesenet skaper nye muligheter og gir økt tilgjengelighet av tjenester. For trygg og sikker pasientbehandling, er det er forutsetning at informasjonssikkerheten er god.

Trusselbildet er i konstant endring som følge av trusselaktørenes tilpasningsevne og kontinuerlige utvikling av verktøy og metoder. Dette medfører at sikkerhetsmekanismene løpende må justeres for å holde risikonivået stabilt. Det er derfor avgjørende med en fortsatt prioritering av arbeidet med informasjonssikkerhet i Helse Sør-Øst. Administrerende direktør er tilfreds med det kontinuerlige og systematiske arbeidet som utføres for å holde risikoene under kontroll. I dette er også arbeidet med blant annet modernisering av IKT-infrastrukturen og reduksjon av antall applikasjoner viktige faktorer.

Administrerende direktør anbefaler at styret slutter seg til forslaget til handlingsplan. Administrerende direktør vil holde styret løpende orientert om arbeidet med å styrke informasjonssikkerheten i Helse Sør-Øst.

Trykte vedlegg:

- Regional handlingsplan for arbeidet med informasjonssikkerhet
- Uttalelse fra brukerutvalget

Utrykte vedlegg:

- Ingen