Saksframlegg

Saksgang:

Styre	Møtedato
Styret Sykehuspartner HF	8. mars 2023

SAK NR 018-2023

KONSERNREVISJONSRAPPORT *STYRING AV INFORMASJONSSIKKERHET I SYKEHUSPARTNER HF*

Forslag til vedtak

Styret tar saken til etterretning.

Skøyen, 1. mars 2023

Hanne Tangen Nilsen
administrerende direktør

Vedlegg:
Konsernrevisjonen Helse Sør-Øst RHF: Rapport 7/2022

1. Hva saken gjelder

I saken presenteres konsernrevisjonen i Helse Sør-Øst RHF sin rapport om styring av informasjonssikkerhet i Sykehuspartner HF.

2. Hovedpunkter

Etter Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer[1], besluttet Helse Sør-Øst RHF å gjennomføre flere tiltak, hvorav ett var å gjennomføre en revisjon av informasjonssikkerheten i Sykehuspartner HF.

Gjennomføringen i regi av Konsernrevisjonen ville ivareta både revisjonsfaglige hensyn, samt å sikre at det ble gjennomført én felles revisjon av Sykehuspartner.

Revisjonen ble gjennomført fra og med medio juni 2022, og ferdigstilt rapport ble oversendt Sykehuspartner HF ultimo desember. Sykehuspartner HF har blitt involvert på en god måte av Konsernrevisjon, særlig i sluttføringen av rapporten har dialogen vært svært god. Konsernrevisjonen har også hatt dialog med foretaksgruppen før og under revisjonen, og har inkludert representanter fra RSR[2] på en egnet og hensiktsmessig måte. Foretaksgruppen ved informasjonssikkerhetsledere har hatt mulighet til å gi sine innspill til områder som Konsernrevisjonen burde se på.

Om rapporten

I all hovedsak har Konsernrevisjonen sett på to områder:

- **I hvilken grad har Sykehuspartner HF etablert et ledelsessystem for informasjonssikkerhet? (del 1)**
- **I hvilken grad skaper Sykehuspartner HFs system for styring av informasjonssikkerhet et godt grunnlag for at de øvrige helseforetakene kan ivareta sitt selvstendige ansvar for informasjonssikkerhet? (del 2)**

I all hovedsak konkluderer Konsernrevisjonen i del 1 med at:

> *Sykehuspartner har etablert og innført et ledelsessystem for IS og jobber kontinuerlig med forbedring og vedlikehold av systemet,*

og at

> *Sykehuspartners ledelse viser engasjement og har stor oppmerksomhet rettet mot styringssystemet», og at «videre oppfattes Sykehuspartner å ha en kultur for å oppdage, rapportere og dokumentere avvik i systemet.*

Rapporten identifiserer 5 – fem – bevarings- og forbedringspunkter. Disse utløser ikke noen nye behov i form av investeringer, prioriteringer eller kompetanse, og er områder som det allerede er fokus på å utbedre. Dette fremkommer også i Konsernrevisjonens anbefalte tiltak, hvor det fremkommer formuleringer som «*Sykehuspartner HF bør fortsette […]*»

[1] Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer (riksrevisjonen.no)
[2] Regionalt Sikkerhetsfaglig Råd

For del 2 legges det til grunn at;

> *Sykehuspartners ledelsessystem for informasjonssikkerhet tar hensyn til interne og eksterne interessenter gjennom de etablerte faste møtearenaene hvor Sykehuspartner normalt deltar,*

og at

> *Sykehuspartner har innført tiltak for å heve kompetanse og bevissthet innen informasjonssikkerhet i helseforetakene.*

Rapporten identifiserer 2 – to – bevarings- og forbedringspunkter. Som med del 1 utløser heller ikke disse noen nye behov i form av investeringer, prioriteringer eller kompetanse. Det er verdt å merke seg at Konsernrevisjonens del 2 også påpeker noen forhold som ikke utleder anbefaling om tiltak, men som styret likevel bør være kjent med. Dette gjelder:

- Prosessen for å utarbeide risiko- og sårbarhetsvurderinger (ROS) omtales, uten at Konsernrevisjonen konkluderer i saken. Det fremheves «*gjennomføringstiden for ROS-analyser blir altfor lang*», samt også at Sykehuspartner HF opplyser om at det er «*uklart i hvilken grad tiltakene fra ROS-analysene blir fulgt opp av helseforetakene*».

- Konsernrevisjonens intervjuer med informasjonssikkerhetslederne ved helseforetakene har også avstedkommet synspunkter og meninger som Konsernrevisjonen gjør kjent i rapporten, dog uten å vurdere dem eller konkludere på dem. Som innspill til Konsernrevisjonen fremmer informasjonssikkerhetslederne et ønske om at Sykehuspartner «*kan være mer aktiv for å tilby flere kompetansehevende og bevisstgjørende tjenester til helseforetakene*». Informasjonssikkerhetslederne har likevel ikke gitt noen eksempler på hvilke kompetansehevende og bevisstgjørende tjenester de etterlyser, og Konsernrevisjonen håndterer dette klokt ved å oppsummere at «*dette vil forutsette at helseforetakene for sin del blir tydeligere på hvilke behov de faktisk har innen dette området*», og at «*helseforetakene bør benytte de etablerte bestillingskanalene til dette*».

Konsernrevisjonens anbefalte tiltak fremkommer i tabellen, under:

	Delområder	**Anbefaling**
Del 1	Virksomhets-kontekst	Sykehuspartner HF bør etablere rutiner for risikobasert gjennomgang og oppfølging av avtaler med helseforetakene.
	Ledelse	Sykehuspartner HF bør systematisk revidere og oppdatere sine styrende dokumenter i sitt ledelsessystem for informasjonssikkerhet.
	Risikostyring	Sykehuspartner HF bør fortsette forbedring av prosessene som ledelsen bruker for å følge opp og ha oversikt over helseforetakets egne risikoreduserende tiltak.
	Gjennomføring	Sykehuspartner HF bør fortsette med å styrke prosesser og praksis som gir en helhetlig tilnærming ved ledelsens gjennomgang av styringen av informasjons-sikkerhet.
	Ytelse og evaluering	Sykehuspartner HF bør vurdere tiltak som bidrar til en helhetlig intern rapportering av sikkerhetstilstanden.
Del 2	Virksomhets-kontekst	Sykehuspartner HF og de øvrige helseforetakene bør utvikle en målrettet og risikobasert rapportering til helseforetakene som bidrar til nødvendig trygghet for helseforetakenes egen styring.

	Ytelse og evaluering	Sykehuspartner HF bør vurdere å dele sentrale funn og erfaringer fra rapporter og CERT med de øvrige helseforetakene, forutsatt at helseforetakene håndterer fortrolig informasjon på en forsvarlig måte.

3. Administrerende direktørs anbefaling

Konsernrevisjonen har utarbeidet en rapport som i stor grad bekrefter at Sykehuspartner HF jobber godt med informasjonssikkerhet, og anbefalingene fra Konsernrevisjonen er i tråd med dette arbeidet. Konsernrevisjonen peker også på noen områder som ikke avstedkommer direkte anbefalinger, men disse vil det også jobbes med videre.

Administrerende direktør anbefaler at styret tar rapporten til etterretning.