Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	24. september 2026

Sak 113-2026

Status for sikkerhetsarbeidet i Sykehuspartner HF

Forslag til vedtak:

Styret tar saken til orientering og ber om ny status for arbeidet i løpet av 2027.

Hamar, 17. september 2026

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Styret i Sykehuspartner HF behandlet i mai 2025 modenhetsvurdering av cybersikkerhet. Sykehuspartner HF etablerte samtidig slik modenhetsvurdering som en regelmessig aktivitet.

Denne saken presenterer den oppdaterte vurderingen og status for sikkerhetsarbeidet i Sykehuspartner HF.

2 Hovedpunkter og vurdering av handlingsalternativer

2.1 Oppdatert modenhetsvurdering

I 2024 gjennomførte *mnemonic* AS på vegne av Sykehuspartner HF en modenhetsvurdering av Sykehuspartner HFs arbeid med cybersikkerhet basert på anbefalingene i *NIST*[1] *Cybersecurity Framework 2.0* (NIST CSF). Resultatet ble videre koblet til og presentert opp mot Nasjonal sikkerhetsmyndighets *grunnprinsipper for IKT-sikkerhet*, som Sykehuspartner HF skal etterleve, jf. tidligere års oppdrags- og bestillingsdokument. Resultatet ved kobling til grunnprinsippene for IKT-sikkerhet vil være avvikende, da det ikke foreligger et direkte en-til-en-forhold mellom rammeverkene og tilhørende anbefalinger.

Med utgangspunkt i funn og anbefalinger fra vurderingen i 2024 har *mnemonic* i perioden mars til mai 2026 gjennomført en ny vurdering med den samme metodiske tilnærmingen.

Resultater

Den oppdaterte vurderingen av arbeidet med cybersikkerhet i Sykehuspartner HF viser en svak forbedring siden vurderingen i 2024. Sykehuspartner er vurdert over bransjesnittet for både teknologi- og helsesektoren. Bransjesnitt er gitt ut fra NIST CSF. Helsesektoren har en betydelig forbedring siden 2024 – fra 1,81 til 2,51. Årsakene er todelte; et bredere grunnlag for *mnemonic* sitt bransjegjennomsnitt, samt en generell modenhetsøkning i helsesektoren.

Samlet vurderer *mnemonic* modenheten i Sykehuspartner HF som akseptabel, hovedsakelig som følge av at Sykehuspartner HF har etablert de mest sentrale elementene som inngår i et ledelsessystem for informasjonssikkerhet. Av de seks hovedkategoriene i NIST CSF (govern,

[1] National Institute of Standards and Technology

identify, protect, detect, respond og recover) er likevel *govern* den som totalt sett er vurdert som svakest, mens *protect* er vurdert som den sterkeste.

Utviklingen siden 2024 er sammensatt. Det er fremgang innen områder som plattform- og datasikkerhet, operativ sikkerhetsevne og håndtering av sikkerhetshendelser. Samtidig vurderte *mnemonic* at flere grunnleggende utfordringer vedvarer, særlig for risikostyring på tjenestenivå (applikasjonsnivå), styring og ansvar i sky og helhetlig livsløpsstyring av IT-eiendeler (systemer, maskinvare, programvare, lisenser med mer).

Rapporten peker også på at den operative utviklingen ikke fullt ut understøttes av helhetlige styringsmekanismer. Økt bruk av skytjenester, større avhengighet av leverandører og et mer komplekst tjenestelandskap stiller økte krav til tydelige ansvarsforhold og systematisk oppfølging av både leverandører og tjenester, samt forbedret deteksjons- og overvåkningskapasitet.

2.2 Status for sikkerhetsarbeidet

Veikartet for sikkerhet i inneværende strategiperiode ble første gang lagt frem for styret i Sykehuspartner HF i august 2024 og omfatter om lag 40 forbedringsinitiativ. Initiativene spenner på tvers av hele virksomheten og omfatter tiltak innen organisering, prosess, teknologi og personell. Veikartet ble etablert i 2024 for å samle pågående og planlagte sikkerhetsinitiativ for å understøtte Sykehuspartner HFs strategi for 2024–2028.

I desember 2025 vedtok Sykehuspartner HF en sikkerhetskapabilitetsmodell, som nå erstatter veikartet. Modellen består av fem kapabiliteter som Sykehuspartner HF må ha for å sikre og opprettholde tilstrekkelig motstandsevne mot uønskede sikkerhetshendelser: (1) sikkerhetsstyring, (2) identifisere og kartlegge, (3) beskytte og opprettholde, (4) oppdage og (5) håndtere og gjenopprette.

I april 2025 ble sikkerhetsområdet reorganisert og samlet i et virksomhetsområde som omfatter sikkerhetsstyring, helhetlig risikostyring, sårbarhetsvurdering- og håndtering, beredskap og operativ sikkerhet som responsmiljø for hendelser (CERT), senter for sikkerhetsovervåking (SOC)og tilgangsstyring. Dette har resultert i bedre forståelse av det samlede risikobildet for sikkerhet, samt lagt grunnlaget for et sikkerhetsveikart som møter behovet fremover.

Sykehuspartner HF arbeider systematisk for å beskytte virksomheten mot trusler og tilpasser beskyttelsestiltak deretter. Ansattes bruk av kunstig intelligens utenfor arbeidsgivers kontroll er en ny trussel som det er behov for å jobbe strukturert med. Tiltakene omfatter styring av hvilke KI-tjenester som kan brukes, og bedre kontroll med hvor sensitive opplysninger behandles. Videre er det initiert prosjekter knyttet til tilgangsstyring av KI agenter og overvåking av hvilke KI-tjenester som benyttes. KI-relatert risiko behandles som del av ordinær risikostyring.

3 Administrerende direktørs anbefaling

Administrerende direktør anser at å samle sikkerhetsressursene har gitt et viktig løft for sikkerhetsarbeidet i Sykehuspartner HF, og at det har lagt til rette for en mer helhetlig og samlet forståelse av sikkerhetssituasjonen i virksomheten. Det jobbes systematisk og målrettet, og det er positiv fremgang på flere områder hvor utvikling av overvåkningsfunksjonen og sårbarhetshåndteringen kan fremheves.

Arbeidet med sikkerhet vil fortsette å ha høy prioritet fremover. Det forventes ytterligere forbedringer gjennom fortsatt oppmerksomhet på styring, kompetanseheving og risikoreduserende tiltak.

Det anbefales at styret tar saken til orientering, og at det bes om ny status for arbeidet i løpet av 2027.

Trykte vedlegg:

- Ingen

Utrykte vedlegg:

- Ingen