Sak 36 2026 – Trusselvurdering spesialisthelsetjenesten

Saksbehandler	Suzanne Nyborg og Anders Lein
Ansvarlig leder	Trond Utne
Saksmappe	2026/192
Dato for styremøte	19.06.2026

Forslag til vedtak:

1. Styret tar orientering om trusselvurdering for spesialisthelsetjenesten 2026 til etterretning
2. Styret ber om at trusselvurderingen legges til grunn for sikkerhetsstyring i Hemit.

Trondheim, 12.06.2026

Trond Utne
Administrerende direktør

NUMMERERTE VEDLEGG SOM FØLGER SAKEN

1. *Sak 36-2026 vedlegg 1 – Trusselvurderingen for spesialisthelsetjenesten*

SAKENS HENSIKT

Saken har til hensikt å orientere styret om utviklingen i trusselen mot informasjonssikkerheten til spesialisthelsetjenesten. Trusselvurderingen skal være et grunnlag i arbeidet med sikkerhets- og risikostyring i regionen. Dette inkluderer sikring av infrastruktur og tjenester, samt etablering av grunnleggende sikkerhetsbarrierer som beskytter mot digitale angrep.

BAKGRUNN

Helsevesenet er avhengig av informasjonsteknologi for å yte effektive helsetjenester. Et vellykket cyberangrep mot spesialisthelsetjenesten kan få store konsekvenser for evnen til å yte helsetjenester og ivareta helseberedskapen. De fire IKT-leverandørene i helseregionene, sammen med Norsk Helsenett, har utarbeidet trusselvurderingen for 2026. Vurderingen beskriver det digitale trusselbilde mot spesialisthelsetjenesten og gjelder for ett år. Trusselvurderingen er viktig for å forstå det digitale trusselbildet spesialisthelsetjenesten står overfor. Den gir oss innsikt i hvem som ønsker å ramme våre IKT-system og digitale løsninger, og hvordan de kan gjøre det.

HOVEDPUNKTER OG VURDERING AV HANDLINGSALTERNATIVER

Nedenfor gis en kort oppsummering av de viktigste vurderingene i trusselvurderingen for spesialisthelsetjenesten 2026, med vekt på forhold som er særlig relevante for styrets forståelse av risiko og prioriteringer i Hemit.

Trusselvurderingen viser at det digitale trusselbildet for spesialisthelsetjenesten er ytterligere skjerpet i 2026. Økt geopolitisk uro, større bruk av sammensatte virkemidler og en mer kompleks digital infrastruktur gjør sektoren mer sårbar for både målrettede og opportunistiske angrep. For styret er det særlig viktig å merke seg at utviklingen ikke bare

påvirker informasjonssikkerheten isolert sett, men også Hemits evne til å understøtte stabil drift, helseberedskap og tillit til de digitale tjenestene som leveres til helseforetakene.

Rapporten vurderer organisert cyberkriminalitet som den mest alvorlige trusselen mot spesialisthelsetjenesten. Dette skyldes særlig risikoen for utpressingsangrep, kompromittering av brukerkontoer og utnyttelse av sårbarheter i systemer og leverandørkjeder. I tillegg vurderes cyberspionasje og innsidevirksomhet som høye trusler. Dette reflekterer at helsesektoren både forvalter store mengder sensitive data og inngår i samfunnets kritiske infrastruktur og totalberedskap.

Et sentralt budskap i rapporten er at trusselaktørene i økende grad utnytter de samme utviklingstrekkene som gir sektoren gevinster: skytjenester, integrerte verdikjeder, mobile arbeidsflater og økt bruk av kunstig intelligens. Rapporten peker samtidig på at KI bidrar til å gjøre etablerte angrepsformer raskere, mer skalerbare og mer treffsikre, blant annet innen phishing, sosial manipulering, skadevareutvikling og utnyttelse av sårbarheter.

For Hemit innebærer dette at sikkerhetsarbeidet må videreutvikles i takt med et mer sammensatt og hurtigskiftende trusselbilde. Styret bør særlig merke seg behovet for fortsatt oppmerksomhet på grunnleggende sikkerhetstiltak, beredskap, identitets- og tilgangsstyring, leverandøroppfølging, robusthet i skytjenester og evne til rask oppdagelse og håndtering av hendelser. Trusselvurderingen gir dermed et viktig grunnlag for å prioritere og forankre det videre arbeidet med sikkerhetsstyring i Hemit.

Rapporten understreker også at skillet mellom samfunnssikkerhet, beredskap og informasjonssikkerhet blir mindre tydelig. For spesialisthelsetjenesten betyr dette at digitale hendelser i større grad må forstås som virksomhetskritiske hendelser med potensielle konsekvenser for pasientbehandling, prioritering av ressurser og evne til å opprettholde tjenester i krise og krig. Styret bør derfor se trusselvurderingen som et bidrag til

virksomhetens samlede styrings- og beredskapsgrunnlag, og ikke kun som et sikkerhetsfaglig dokument.

Et viktig funn i rapporten er den økende betydningen av avhengigheter og konsentrasjonsrisiko. Spesialisthelsetjenesten er i økende grad avhengig av et begrenset antall teknologileverandører, skytjenester og eksterne verdikjeder. Dette gir effektivitetsgevinster, men innebærer også en strategisk sårbarhet dersom leveranser svikter, sikkerhetsmekanismer hos leverandører ikke er tilstrekkelige, eller geopolitiske forhold påvirker tilgang til tjenester og teknologi. For styret er dette særlig relevant fordi slike avhengigheter kan få direkte betydning for Hemits evne til å levere stabile og trygge tjenester over tid.

Rapporten peker videre på at tempoet i cyberangrep øker. Tiden fra en sårbarhet blir kjent til den utnyttes blir kortere, og angripere kombinerer i større grad tekniske metoder med sosial manipulering og automatisering. Dette forsterker behovet for raskere oppdateringstakt, bedre oversikt over eksponerte flater, og evne til hurtig deteksjon og respons. For styret understreker dette at robust sikkerhetsstyring ikke bare handler om modenhet over tid, men også om virksomhetens evne til å reagere raskt når trusselbildet endrer seg.

Samlet sett gir trusselvurderingen et tydelig bilde av at den digitale risikoen for spesialisthelsetjenesten må håndteres som en del av virksomhetsstyringen. For styret er hovedbudskapet at Hemit må videreføre og forsterke et langsiktig arbeid med digital motstandsevne, samtidig som virksomheten må være forberedt på å håndtere mer sammensatte og hurtig utviklende hendelser enn tidligere. Dette stiller krav til prioritering, ledelsesforankring og systematisk oppfølging av sikkerhetsarbeidet i hele virksomheten.

Trusselvurderingen for spesialisthelsetjenesten 2026 legges til grunn for Hemit sitt videre arbeid med sikkerhetsstyring, beredskap og prioritering av tiltak. For Hemit innebærer dette at trusselvurderingen må brukes aktivt i virksomhetens risikovurderinger, sikkerhetsfaglige prioriteringer og videre utvikling av tekniske og organisatoriske sikkerhetstiltak. Arbeidet må omfatte både forebyggende, detekterende og hendelseshåndterende tiltak, og sees i sammenheng med Hemit HF sitt ansvar for å understøtte helseforetakenes tjenesteleveranser og regionale helseberedskap. Det er særlig viktig å vurdere risiko knyttet til KI, skytjenester, leverandøravhengigheter, identitets- og tilgangsstyring, sårbarheter i eksponerte systemer og økende bruk av sosial manipulering som angrepsmetode

Hemit vil følge opp vurderingen gjennom ordinære prosesser for sikkerhets- og risikostyring, samt nettverksstrukturen i HMN. Dette omfatter blant annet forankring i ledelsen, kommunikasjon til relevante fag- og driftsmiljøer, oppdatering av risikovurderinger og prioritering av tiltak der trusselbildet tilsier behov for økt beskyttelse eller beredskap. Trusselvurderingen vil også inngå som et viktig grunnlag for videre arbeid med sikkerhetsarkitektur, overvåking, hendelseshåndtering og kontinuitetsplanlegging. Det er samtidig viktig at de øvrige foretakene i HMN gjennomfører tilsvarende forankring i egen organisasjon og prosesser.

Administrerende direktørs anbefaling

Administrerende direktør anbefaler styret i Hemit HF å ta informasjon om trusselvurdering for spesialisthelsetjenesten 2026 til etterretning, og å be om at den oppdaterte trusselvurderingen legges til grunn for sikkerhetsstyring i Hemit.