HELSE NORD | DAVVIDEARVVAŠVUOHTA VARRESVUOHTA NUORTTA HEALSOE NOERHTE

Møtedato: 14. mars 2024

Vår ref.:	Saksbehandler:	Dato:
2021/1553-19	Rolandsen/Martinussen	7.3.2024

Styresak 37–2024 Informasjonssikkerhet – status for arbeidet

Vedlegg 3 til saksdokumentene er unntatt offentlighet, jf. offl. §24, 3. ledd, da det gjelder opplysninger som kan lette straffbare handlinger.

Forslag til vedtak
Styret i Helse Nord RHF inviteres til å fatte følgende vedtak:

1. Styret i Helse Nord RHF tar status for arbeidet med informasjonssikkerhet til orientering.

2. Styret ber adm. direktør legge frem en styresak med oppdatert handlingsplan for informasjonssikkerhet for perioden 2024- 2027 innen 1. mai 2024.

Bodø, 7. mars 2024

Marit Lind
administrerende direktør

Postadresse:
Helse Nord RHF
Postboks 1445
8038 Bodø

Besøksadresse:
Helse Nord RHF
Moloveien 16, 6. et.
8003 Bodø

Telefon sentralbord: 75 51 29 00

postmottak@helse-nord.no
www.helse-nord.no

Org.nr: MVA 883 658 752

Formål
Styret blir i denne saken orientert om status for *Regional handlingsplan for informasjonssikkerhet.*

Sammenheng med strategi og grunnleggende verdier
God informasjonssikkerhet er en forutsetning for god virksomhetsstyring og vellykket digitalisering. Arbeidet med informasjonssikkerhet skjer gjennom samspillet mellom dimensjonene organisasjon (arbeidsprosesser), menneske (kompetanse og kultur), og en større målrettet satsning på et teknologisk løft. Arbeidet krever høy grad av *kvalitet* i planlegging og gjennomføring, *trygghet*, *respekt* og godt *lagspill* mellom alle aktører.

Bakgrunn
Styret behandlet styre*sak 119-2021 Regional handlingsplan for informasjonssikkerhet* i styremøte 29. september 2021. Vedtak er vedlegg 1 til denne sak. Handlingsplanen er oppdatert fire ganger etter at styret behandlet saken.

Status for det systematiske arbeidet med å styrke informasjonssikkerheten er rapportert til Helse- og omsorgsdepartementet (HOD) innen 1. mai hvert år[1]. Innholdet i denne saken bygger på oppfølgingsmøte hos HOD 19. oktober 2023 (vedlegg 3).

Beslutningsgrunnlag
Beskrivelse av nåsituasjon deles inn i kommentar om trusselbildet, og ut fra dimensjonene organisasjon, menneske og teknologi.

Beskrivelse av trusselbildet
Trusselvurderingen for spesialisthelsetjenesten 2023 var en viktig milepæl for det nasjonale sikkerhetssamarbeidet i spesialisthelsetjenesten. Trusselvurderingen ble redegjort for i styret i styremøte 31. mai 2023 (jf. *styresak 64-2023/4 Orienteringssak ad. Trusselvurdering – det digitale trusselbildet mot spesialisthelsetjenesten 2023*), og til alle styrene i helseforetakene i regionalt styreseminar 24. oktober 2023.

I 2023 var trusselvurderingen for første gang utarbeidet for å kunne være offentlig tilgjengelig. Dette ble ansett som viktig for å enklere kunne nå ut til flest mulig ansatte i regionen. Offentliggjøringen kommer som følge av en utvikling av sikkerhetssamarbeidet og prosessen de siste årene, men kan i seg selv også si noe om utviklingen i trusselbildet.

Pågående kriger og hendelser i verden har gjort den storpolitiske sikkerhetssituasjon mer tilspisset, og viktigheten av å bygge forståelse om hvilke trusler som kan påvirke våre tjenester har blitt mer aktualisert.

Trusselvurderingen tilsier at norske forsknings- og utdanningsinstitusjoner må påregne å bli utnyttet til ulovlig kunnskapsoverføring og at aktører knyttet til Russland, Kina, Iran og Pakistan vil representere en særskilt utfordring. Fremmede staters etterretningstjenester benytter et bredt spekter av metoder og virkemidler i Norge, som rekruttering av kilder, fordekt anskaffelsesvirksomhet og ulovlig kunnskapsoverføring. Person- og helseopplysninger har historisk sett vært attraktive mål globalt, og kan være interessant for statlige aktører fordi det kan brukes som et virkemiddel innenfor bl.a. spionasje.

[1] I tråd med krav foretaksprotokoller 2020-2023

Organisasjon – prosess
Helseforetakene har fått i oppdrag å følge opp de lokale handlingsplanene (jf. Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet) for det systematiske arbeidet med å styrke informasjonssikkerheten og med å lukke de sårbarhetene som Riksrevisjonens undersøkelse avdekket. Helseforetakene rapporter status til eget styre og overordet til regional styringsgruppe for informasjonssikkerhet.

"Rammeverk for styring av IKT"[2] er utarbeidet, parallelt med evaluering av regional sikkerhetsorganisering. Styringsdokument for Regional sikkerhetsorganisering er under oppdatering i henhold til anbefalinger fra arbeidet med regional sikkerhetsorganisering og i tråd med "Rammeverk for styring av IKT".

Regionalt nettverk for risikostyring er etablert. Integrert og helhetlig risikostyring på strategisk nivå ledes av Helse Nord RHF. På sikt er det et behov for at det utarbeides felles metodikk, der også informasjonssikkerhet inngår. Regionale initiativer er under utarbeidelse.

Helse Nord RHF har gjennomført sikkerhetsrevisjon (2-linje revisjon) av Helse Nord IKTs nettverk. Rapport fra revisjonen viser til at Helse Nord IKT er en moderne driftsorganisasjon med tilgang på moderne verktøy, nødvendig kompetanse og transparent innsikt i egne driftstall som fremstår meget godt utviklet, men i kontrast til dette ble det avdekket flere grunnleggende problemer som blir stående uløst.

Beredskapsplan IKT er en delplan til regional beredskapsplan. IKT-beredskapen omfatter både regional og lokal IKT-beredskap, og består derfor både av delplan beredskapsplan IKT (regional) og helseforetakenes egne IKT-beredskapsplaner. Det enkelte helseforetak er ansvarlig for å utarbeide og oppdatere egen beredskapsplan IKT. Helseforetakenes arbeid med dette har vært fulgt opp gjennom oppfølgingsmøter våren 2023.

Beredskapsplan IKT er et rammeverk som kontinuerlig må videreutvikles. I samarbeid med helseforetakene er det identifisert flere forbedringspunkter som innarbeides fortløpende. Det har blant annet vært jobbet for å forbedre rutiner for å sikre enhetlig kommunikasjon ved en IKT-beredskapshendelse, og rutine for øyeblikkelig nedkobling av IKT systemer. Videre har foretaksgruppen utviklet metodikk for regional verdivurdering av IKT systemer, skapt felles forståelse for verdivurdering som forutsetning for prioritering, og utarbeidet et første utkast til regional verdivurdering.

Helse Nord RHF har sammen med helseforetakene gjennomført en første modenhetsvurdering. Dette er ikke en nøyaktig beskrivelse av sikkerhetstilstanden, men en egenvurdering fra hvert helseforetak (mai/oktober 2023) gjeldende oppfyllelse av NSM[3] grunnprinsipper (se vedlegg 2) i kategori 1 og 2. For en stor del viser modenhetsvurderingen samsvar mellom helseforetakenes egenvurdering og vurderinger fra de regionale prosjektene. I tillegg viser vurderingene enkeltområder hvor det foreløpig er lav aktivitet/modenhet. Det må derfor fortsatt arbeides strukturert og godt med å få på plass grunnleggende og nødvendige sikkerhetstiltak.

---

[2] *Styresak 133–2023 Rammeverk for styring av IKT, oppfølging av styresak 32-2021 og 119-202*1 (styremøte 29. september 2023)
[3] NSM: Nasjonal Sikkerhetsmyndighet

Menneske (kompetanse og kultur)
Medarbeidernes adferd, både i helseforetakene og særlig hos IKT-leverandørene, kan påvirke en trusselaktørs sannsynlighet for å lykkes med å få fotfeste i infrastrukturen. Tidligere undersøkelser viser at flere ansatte hos IKT leverandøren og helseforetakene har en praksis som kan bidra til å svekke IKT sikkerheten. Det avdekkes fortsatt forsøk på å ta "snarveier", for eksempel ved å omgå sikkerhetsbarrierer bevisst eller ubevisst.

Helseforetakene har i foretaksmøter fått i oppdrag å inkludere informasjonssikkerhet i virksomhetskulturen ved å kartlegge virksomhetens sikkerhetskultur, og identifisere hva som kan forbedres.

Det gjennomføres flere typer opplæringstiltak, f.eks. obligatorisk e-læringskurs for alle ansatte, nano-læring i form av små korte informasjonspakker om relevante sikkerhetstema og kartlegging av digital sikkerhetskultur. Det er utfordrende å nå bredt ut i organisasjonen med generelle opplæringstiltak. Flere av tiltakene har for lav deltakelse.

Resultatene fra kartlegging av digital sikkerhetskultur samt at ansatte forsøker å omgå sikkerhetsbarrierer viser at det fortsatt er behov for å styrke kompetansen. God sikkerhetskultur krever langsiktige og målrettede tiltak slik at alle enkeltindivider utvikler ønsket adferd.

Arbeidet med å oppnå NSMs anbefalte nivå[4] for informasjonssikkerhet er et kontinuerlig forbedringsarbeid. Det må påregnes at trusselbildet fortsetter å utvikle seg i overskuelig fremtid, og at vår avhengighet til IKT og digitale løsninger blir stadig høyere.

Trusselvurderingen for spesialisthelsetjenesten påpeker at norske forsknings- og utdanningsinstitusjoner utnyttes av fremmede stater for å kartlegge potensielle kilder. Et forsøk på å rekruttere en norsk forsker kan for enkeltpersoner fremstå som tilforlatelig og legitimt. En rekruttert kilde kan ha store skadevirkninger for Norge.

Helse Nord arbeider med relevante tiltak for å håndtere innsiderisiko. Dette gjøres ved å identifisere såkalte høyrisikoroller, at håndtering av innsiderisiko inntas i det regionale styringssystemet for informasjonssikkerhet, bruk av sårbarhetssamtaler for medarbeidere i høyrisikoroller og at det utarbeides internopplæring om innsiderisiko med fokus på at medarbeiderne skal være en barriere mot sikkerhetstruende virksomhet.

Informasjonssikkerhet må i større grad integreres i arbeidsprosessene, slik at sikkerhet ikke skal være noe som kommer *i tillegg*. Dette må kombineres med tekniske sikkerhetstiltak slik at muligheten for å gjøre feil, og konsekvensen av menneskelige feil, reduseres. Innføring av tekniske tiltak for sterkere autentisering, utrulling av verktøy og tilpassing av arbeidsprosesser for tilgangsstyring (IAM) samt innføring av tilgangsstyring av privilegerte rettigheter, gir rask effekt slik at ansatte i større grad velger sterkere passord/ sikrere innlogging.

[4] https://nsm.no/getfile.php/133747-1592917276/NSM/Filer/Dokumenter/Veiledere/nsm_grunnprinsipper_for_ikt-2018.pdf

Teknologi – Målrettet satsning «Sikkerhet i dybden»
De siste årene er det gjennomført flere større initiativ, som HIS 1[5], HIS 2[6], MODI[7] og sterk autentisering. Formålet har vært å forbedre oversikten, de tekniske kapabilitetene, evnen til å detektere og å håndtere sikkerhetshendelser, samt sikker tilgangsstyring.

Gjennom modenhetsvurderinger og tester dokumenteres klare forbedringer i sikkerhetstilstanden. Det observeres fortsatt utfordringer tilknyttet sårbare løsninger og konfigurasjoner, og ikke minst teknisk gjeld.

Ett av tiltakene er årlige inntrengingstester fra Norsk Helsenett, tilsvarende det Riksrevisjonen gjennomførte i 2019. Selv om det fremdeles avdekkes svakheter i de årlige testene, viser resultatene en betydelig framgang. Sammenliknet med 2021 og 2019 er sentral infrastruktur bedre sikret, og en kan dokumentere betydelig forbedret evne til å oppdage forsøk på å omgå sikkerhetsbarrierer. I testen fra 2023 oppsummerer Norsk Helsenett med at «*Sikkerhetsarbeidet i Helse Nord har gitt merkbare forbedringer de siste årene*».

Medbestemmelse
Status for arbeidet med informasjonssikkerhet ble behandlet i samarbeidsmøte med de konserntillitsvalgte og konsernverneombud i Helse Nord RHF, den 12. desember 2023.

Brukermedvirkning
Det vil bli orientert om status for arbeidet med informasjonssikkerhet i det Regionale brukerutvalget i Helse Nord RHF.

Administrerende direktørs vurdering
Digitale løsninger utgjør en stadig større del av helse- og omsorgssektoren. Dette er en ønsket utvikling, og den teknologiske utviklingen skaper nye muligheter for trygg og sikker pasientbehandling. Tilfredsstillende informasjonssikkerhet er en forutsetning for de tiltak som skal realiseres innen digitaliseringen.

Den målrettede satsningen rundt sikkerhet og teknologi har gjort regionen betydelig bedre rustet mot regionale trusler som digital utpressing og tilsvarende. Det gjenstår fremdeles betydelige risikoer tilknyttet teknisk gjeld, mangelfull helhetlig oversikt i en kompleks infrastruktur, og robusthet ved bortfall av IKT. Disse utfordringene betyr at regionen fremdeles er sårbar for ondsinnet påvirkning mot enkelttjenester og løsninger, som videre vil kunne få regionale implikasjoner.

Foretaksgruppen må fortsatt ha en god plan og tett oppfølging av forbedringsarbeidet, og hensynet til informasjonssikkerhet må tillegges stor vekt ved prioritering av ressurser.

Administrerende direktør er tilfreds med det systematiske arbeidet som er gjort innen informasjonssikkerhet. For å innrette innsats og sikkerhetstiltak styrt og koordinert, vil administrerende direktør utarbeide ny handlingsplan for informasjonssikkerhet for perioden 2024- 2027, som dekker områdene teknologi, menneske og organisasjon.

[5] Helhetlig informasjonssikkerhet fase 1
[6] Helhetlig informasjonssikkerhet fase 2
[7] Moderne digital arbeidsflate

Vedlegg

1. Sammendrag: Nasjonal sikkerhetsmyndighet grunnprinsipper for IKT sikkerhet
2. Vedtak styresak 119-2021 Regional handlingsplan for informasjonssikkerhet
3. Presentasjon "Systematiske arbeidet med å styrke informasjonssikkerheten – status Helse Nord" - *u. off. jf. offl. §24, 3. ledd*

Vedlegg 1

Vedtak styresak 119-2021 Regional handlingsplan for informasjonssikkerhet

1. Styret slutter seg til adm. direktørs vurdering av at handlingsplan og målbilde for sikkerhetsarkitektur for å lukke hovedfunn, merknader og anbefalinger knyttet til Riksrevisjonens undersøkelse om helseforetakenes forebygging av angrep mot sine IKT-systemer.

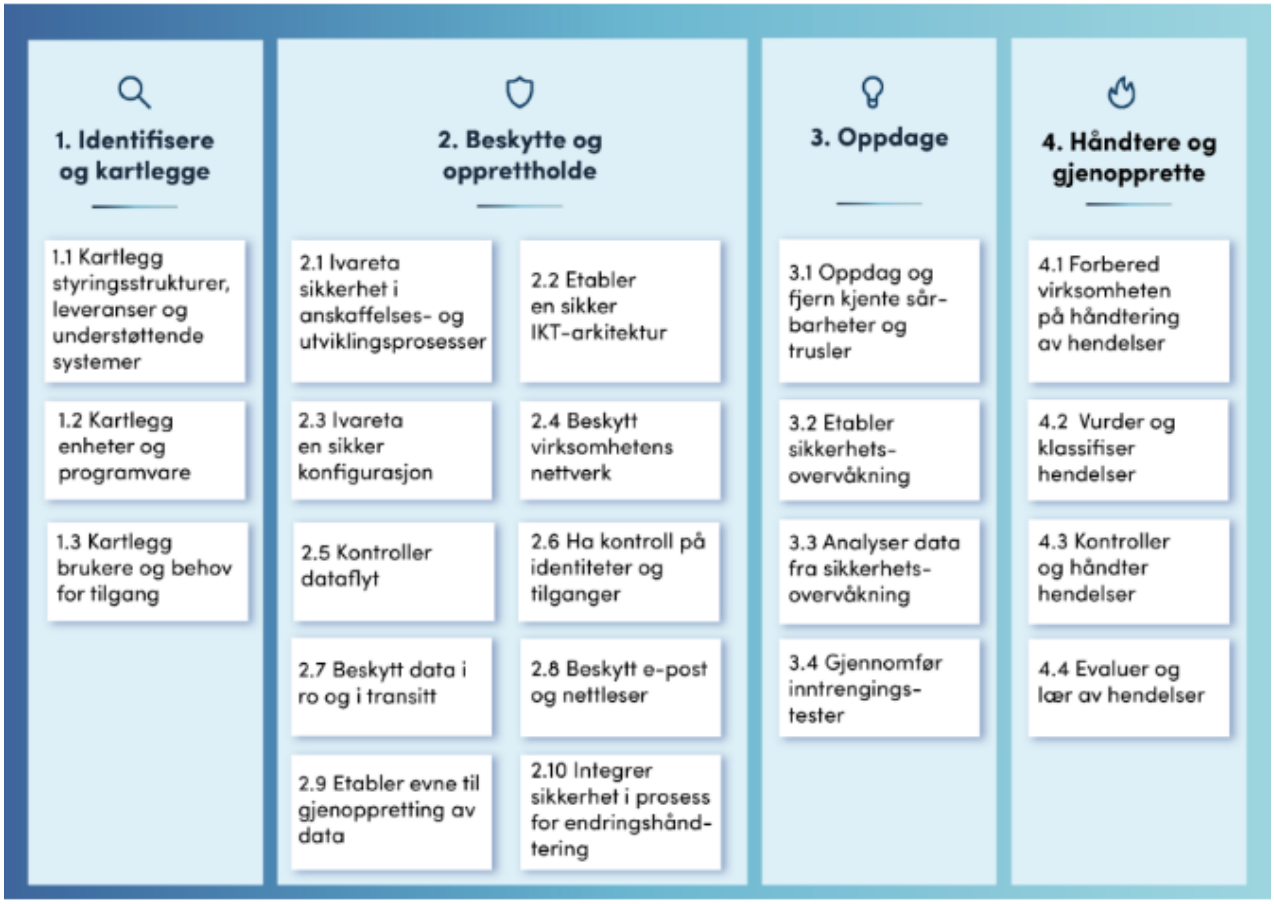
2. Styret godkjenner regional handlingsplan for arbeidet med informasjonssikkerhet i Helse Nord.

3. Styret ber om at det i forbindelse med konsolidert budsjett 2022 legges frem egen orientering om hvordan samlet finansiering knyttet til den regionale handlingsplanen for informasjonssikkerhet blir ivaretatt.

4. Styret ber om å bli orientert om gjennomføring gjennom løpende tertialrapporter. I tilfelle vesentlige avvik fra plan, skal styret informeres gjennom eget saksfremlegg.

Vedlegg 2

Nasjonal Sikkerhetsmyndighet (NSM) grunnprinsipper for IKT – sikkerhet



Figur 2 - Oversikt over NSMs grunnprinsipper for IKT-sikkerhet.