Saksframlegg

Saksgang:

Møte	Møtedato
Styret i Helse Sør-Øst RHF	23. april 2026

Sak 053-2026

Status og regional handlingsplan for arbeidet med informasjonssikkerhet

Forslag til vedtak:

Styret tar status og regional handlingsplan for arbeidet med informasjonssikkerhet til orientering.

Hamar, 16. april 2026

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Helse Sør-Øst skal øke bruken av helsedata og stå imot trusler mot våre informasjons- og IKT-systemer. God informasjonssikkerhet skal legge til rette for dette.

Denne saken presenterer status for arbeidet med informasjonssikkerhet og en oppdatert handlingsplan med tiltak for å styrke informasjonssikkerheten.

2 Hovedpunkter og vurdering av handlingsalternativer

Helse Sør-Øst RHF har fått i oppdrag å øke bruken av helsedata, blant annet for kunnskaps-utvikling, næringslivssamarbeid, for å følge kvaliteten og redusere uønsket variasjon og for å kunne effektivisere driften. Samtidig må sykehusdriften beskyttes mot både uhell og tilsiktede angrep.

Informasjonssikkerhet handler blant annet om å finne en god balanse mellom økt tilgjengelighet av helsedata, ivaretakelse av personvernet og beskyttelse av informasjon som er nødvendig for drift av sykehusene.

2.1. Trusler og trusselaktører

Informasjonssystemene er avhengige av strøm, vann, personell, diverse leverandører, programvareoppdateringer, nettverk med mer. Disse kan ha sårbarheter som en trusselaktør kan utnytte.

Organiserte kriminelle og enkelte statlige aktører vurderes fremdeles å utgjøre den største trusselen for tilsiktede handlinger mot våre digitale løsninger. Trusselvurderingen for digital sikkerhet i spesialisthelsetjenesten handler om tilsiktede hendelser og vil oppdateres i løpet av første halvår.

Programvarefeil, feilkonfigurasjon og uhell kan også ha betydning for våre IKT-systemer. For eksempel har DIPS arena hatt utfordringer med tilgjengelighet flere ganger det siste året.

2.2. Systematisk arbeid

Digdir, Datatilsynet, NSM, KS, DFØ og Helsedirektoratet har utarbeidet anbefalinger for offentlige virksomheter om hvilke styringsaktiviteter de bør ha innen informasjons-sikkerhet. Målet er at ledelsen skal kunne ivareta ansvaret sitt. Anbefalingene er lagt ut på sikkert.no. De anbefalte styringsaktivitetene er:

- Ledelsens styring og oppfølging
- Ha oversikt og prioritere
- Vurdering av risiko
- Håndtering av risiko
- Måling, evaluering og revisjon
- Overvåking og hendelseshåndtering
- Kompetanse- og kulturutvikling
- Anskaffelser og leverandørstyring
- Kommunikasjon

Helse Sør-Øst har aktiviteter innen alle disse områdene, og vil bruke anbefalingene i det videre forbedringsarbeidet på informasjonssikkerhetsområdet.

2.3. Utvalgte tema

Arbeidet med informasjonssikkerhet dekker en rekke områder. Vi gir nedenfor mer inngående informasjon om noen sentrale risikoområder.

Innsidere
Ansatte har i kraft av arbeidsoppgavene tilganger som de kan utnytte. NSM definerer innsidere som ansatte som misbruker tilgangen for å skade virksomheten til fordel for en annen virksomhet, en fremmed stat eller for egen vinning.

Mange helseforetak har etablert personellsikkerhetsgrupper, med HR, juridisk og sikkerhetskompetanse, for å lede arbeidet lokalt.

Det er laget en veileder for kartlegging av høyrisikoroller. Denne piloteres i Sykehuspartner HF i første kvartal 2026.

Ifølge veilederen må virksomheten avklare hvilke verdier som er beskyttelsesverdige, og kunne identifisere hvilke stillinger/funksjoner som anses å utgjøre en høy risiko.

Prosessen innebærer kartlegging av verdier og roller som kan skade disse verdiene, samt beskrivelser av konsekvenser i verstefallscenarier. Noen eksempler på roller som bør vurderes som en høyrisikorolle, kan være:

- Ansatte med administratorrettigheter til systemer som er kritiske for virksomheten
- Ansatte med tilgang til store datasett brukt i forskning eller tilgang til alle data i regionale systemer
- Ansatte med brede finansielle fullmakter eller fullmakt til å inngå avtaler
- Ansatte som alene godkjenner store avtaler eller prosjekter
- Ansatte i roller med svært høy omdømmerisiko

Interne prosesser av særlig interesse for trusselaktører kan for eksempel være håndteringen av kongefamilien og andre myndighetspersoner, lokaliserende informasjon om trusselutsatte eller logistikk knyttet til A-preparater.

Kvantemigrering
Trusler og sårbarheter forbundet med kryptografisk relevante kvantedatamaskiner ble omtalt i styresak 123-2023. Kryptografiske algoritmer brukes i programvare, nettverks-utstyr, pålogging, signering av dokumenter og mye mer. De algoritmene som benyttes i dag, er sårbare for kryptografisk relevante kvantedatamaskiner og bør byttes ut i god tid før slike maskiner utvikles. I 2016 startet et arbeid for å standardisere algoritmer som er resistente mot kryptografisk relevante kvantedatamaskiner. Disse ble ferdigstilt i 2024, så nå er det klart for arbeidet med å bytte ut de sårbare algoritmene. Nasjonal sikkerhetsmyndighet har publisert en veileder om kvantemigrering som kan følges. Det er lagt inn et tiltak om kvantemigrering i vedlagte handlingsplan.

Konsentrasjonsrisiko og fare for press
Leverandørkjedesårbarheter er svakheter i en virksomhets leverandørkjede – i produkter, tjenester, prosesser eller avhengigheter – som kan utnyttes til å forårsake driftsforstyrrelser, økonomiske tap eller sikkerhetsbrudd. Disse sårbarhetene kan oppstå eller plantes i programvare, maskinvare, tredjepartstjenester eller organisatoriske forhold.

En trusselaktør vil foretrekke det svakeste punktet i en kjede; de hopper over gjerdet der det er lavest, og når store virksomheter som Helse Sør-Øst har god sikkerhet, kan det være lettere å angripe en mindre virksomhet som inngår i våre verdikjeder. Det er pilotert et selvdeklareringsskjema som Sykehuspartner HF sender til utvalgte leverandører for å kartlegge sikkerhetsnivå og etterlevelse av krav stilt til leverandør i forbindelse med anskaffelser. Status på piloten er at kun 45 leverandører svarte opp av de 300 som fikk undersøkelsen. Det arbeides videre med forbedring av undersøkelsen og oppfølging av leverandører.

NSM understreker i årets risikovurdering at lands- og leverandøravhengigheter gir en konsentrasjonsrisiko som kan utnyttes i politisk eller økonomisk press. USA fremstår som mindre politisk stabilt enn tidligere, og amerikanske myndigheter utsetter i økende grad også allierte land for press. Kontinuitetsplaner må derfor ta høyde for scenarioer der tjenester med tilknytning til amerikanske aktører blir utilgjengelige eller får endrede rammevilkår som følge av denne typen press.

Relevante tiltak vil både være exitstrategier og grader av nasjonal kontroll med leverandørkjeden (digital suverenitet). Med et internasjonalt leverandørmarked innen IKT og medisinsk-teknisk utstyr, vil vektlegging av motstandskraft og evne til rask omstilling, både teknologisk og operasjonelt, være viktige strategier for å møte konsentrasjonsrisiko og fare for press.

Kunstig intelligens
Innen sikkerhetsarbeid benyttes kunstig intelligens både i angrep og for beskyttelse. Blant annet har de generelle språkmodellene gjort det mulig å avdekke flere sårbarheter i programvare enn tidligere. Det kan variere om fordelen ved bruk av kunstig intelligens vil være størst for angriper eller den som skal beskytte seg. Det er viktig å utnytte muligheter som kunstig intelligens gir, i sikkerhetsarbeidet.

Digital hjemmeoppfølging
Det er et mål at mer pasientbehandling foregår hjemme hos pasientene. Sikring av medisinsk-teknisk utstyr hjemme hos pasienter kan være krevende. For eksempel kan noe medisinsk-teknisk utstyr være laget for å stå i et beskyttet nettverk på et sykehus, eller det kan være utstyr som fremdeles fungerer godt medisinsk, men som er utdatert med tanke på digital sikkerhet. Brukerutvalget er opptatt av informasjonssikkerhet knyttet til digital behandling og digital oppfølging.

Iran
Vi har sett flere digitale angrep etter at krigen i Iran startet. Det har for eksempel vært en hendelse med et stort antall forsøk på innlogging i våre systemer. Noen brukere fikk sperret sine kontoer etter gjentatte mislykkede forsøk, men det er ikke avdekket noen vellykkede uønskede innlogginger. To av våre leverandører har blitt hacket, hvor konsekvensene for

oss har vært noen avlyste operasjoner, bestillinger av utstyr som måtte håndteres manuelt og noen administrative kontaktopplysninger på avveie. Det har også vært en sak i media om en legestudent som på TikTok truet motstandere av det iranske regimet med å misbruke sine tilganger til journalsystemene og dele informasjon om dem.

2.4. Hendelser, sårbarheter og risikoer

Det har siden forrige rapportering i styresak 123-2025 ikke vært noen hendelser med en alvorlighetsgrad som Helse Sør-Øst RHF har måttet følge opp.

Hver måned oppdages det titalls og opp mot hundretalls sårbarheter i programvare som benyttes i Helse Sør-Øst. Fordelt på våre klienter og servere gir det hundretusenvis av sårbarheter på våre klienter (datamaskiner, telefoner med mer) og titusener av sårbarheter på våre servere. Hver måned lukkes det omtrent like mange sårbarheter gjennom oppdatering av våre systemer. Det vil si at vi til enhver tid har systemer med kjente sårbarheter, og noen av disse vil være kritiske sårbarheter.

Den største trusselen mot spesialisthelsetjenesten er utpressingsangrep fra kriminelle. Det er satt i verk en rekke tiltak for å stå imot slike angrep og dermed redusere risikoen, men samtidig forbedrer trusselaktørene stadig sine angrep. Det er derfor et omfattende arbeid bare å holde risikoen på stedet hvil. Digitale angrep er fremdeles den største tilsiktede risikoen. Et datainnbrudd med svært alvorlig konsekvens, tilsvarende et tap på 62,5 millioner kroner eller mer, er av Sykehuspartner HF anslått til å skje med 50 prosent sannsynlighet i løpet av et år.

Det andre større risikoområdet er manglende tilgjengelighet og integritet som for eksempel kan føre til at pasienter forveksles ved operasjoner eller tildeling av medisiner, i verste fall med fatale følger. Hvor mange pasientskader som kunne vært unngått ved mer tilgjengelig informasjon, er ukjent. Dette risikoområdet følges i hovedsak opp gjennom pasientsikkerhetsarbeidet, og fanges i liten grad opp i informasjonssikkerhetsarbeidet.

2.5. Oppfølging av tiltak

De viktigste tiltakene under arbeid er omtalt i vedlagte handlingsplan for arbeidet med informasjonssikkerhet. Det finnes mange etablerte tiltak. Nylig er arenaer for samarbeid om sikkerhet i anskaffelser og statistisk logganalyse etablert. Kontroll med enheter i nettverket er en type tiltak som aldri kan bli helt ferdig. Det følges opp videre i linjen og er derfor nå tatt ut av regional handlingsplan for arbeidet med informasjonssikkerhet.

3 Anbefaling

Helsetjenesten er berørt av konflikter og usikkerhet globalt. Administrerende direktør erkjenner at det gir flere krevende problemstillinger, blant annet ved valg av leverandører til Helse Sør-Øst.

Endringsevne med mulighet for raskere omstilling kan være viktig i møte med usikkerhet globalt. Handlingsplanen for arbeidet med informasjonssikkerhet beskriver flere av tiltakene som gjennomføres for å bli mer robuste og øke endringsevnen.

Samtidig som vi må beskytte oss mot digitale angrep, så må vi også ha oppmerksomhet på økt tilgjengelighet og en mer datadrevet helsetjeneste for å kunne behandle flere pasienter og øke kvaliteten uten å bruke flere ressurser.

Administrerende direktør anbefaler at styret tar status og regional handlingsplan for arbeidet med informasjonssikkerhet til orientering.

Trykte vedlegg:

- Regional handlingsplan for arbeidet med informasjonssikkerhet

Utrykte vedlegg:

- Ingen