STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest RHF
DATO:	22.11.2022
SAKSHANDSAMAR:	Inger Cathrine Bryne, Erik M. Hansen, Lars Erik Baugstø-Hartvigsen
SAKA GJELD:	**Status for regional handlingsplan for informasjonssikkerheit**
ARKIVSAK:	2021/1010
STYRESAK:	**117/22**
STYREMØTE:	**07.12.2022**

FORSLAG TIL VEDTAK

1. Styret tar status for arbeidet med gjennomføring av Regional handlingsplan for Informasjonssikkerheit i Helse Vest til etterretning.

2. Styret ber administrasjonen sende kopi av styresak om Status for regional handlingsplan for Informasjonssikkerheit i Helse Vest til Helse- og omsorgsdepartementet i tråd med krav gitt i føretaksprotokollen av 14.01.2022.

Oppsummering
Riksrevisjonen gjennomførte i 2019/2020 ein forvaltingsrevisjon i alle dei 4 regionale helseføretaka for å kartlegge førebygging mot angrep mot sine IKT-system. Riksrevisjonen la fram sin rapport etter revisjonen 15.12.2020.

Helse- og omsorgsdepartementet fylgde opp Riksrevisjonen sin revisjon med krav knytt til dei regionale helseføretaka i føretaksmøtet 14.01.2021, jfr. fylgjande;
«Føretaksmøtet bad dei regionale helseføretaka om å:

- *utvikle ein regional handlingsplan for arbeidet med informasjonstryggleiksikkerheit som og omfattar langsiktige tiltak. Planen skal presenterast på felles tertialoppfølgingsmøte i oktober 2021.*»

Denne saka er gir ein status for gjennomføring av «Regional handlingsplan for informasjonssikkerheit i Helse Vest». Status skal presenterast for departementet i felles oppfølgingsmøte i 24. november 2022, og styresaka skal sendast til HOD etter handsaming i styret i Helse Vest RHF, jfr. fylgjande frå føretaksprotokollen for Helse Vest RHF datert 14.01.2022;
«Føretaksmøtet bad dei regionale helseføretaka om å;

- *rapportere på arbeidet med dei regionale handlingsplanane for det systematiske arbeidet med å styrke informasjonssikkerheita, og med å lukke dei sårbarheitene som Riksrevisjonen si undersøking avdekka innan utgangen av 2022.»*

Fakta
Helse- og omsorgsdepartementet har gjennom oppdragsdokumentet for 2022 framleis lagt stor vekt på å fylgje opp revisjonen utført av Riksrevisjonen. Helse Vest RHF har vidareført dette gjennom styringsdokumenta til helseføretaka og Helse Vest IKT AS.

Tekniske tiltak knytt til IKT-sikkerheit er i all hovudsak delegert til Helse Vest IKT. Tiltaka i regi av Helse Vest IKT vert gjennomført i samarbeid med helseføretaka. Ut frå ein risikobasert tilnærming har dei tekniske tiltaka hatt høg prioritet. Funn gjort av Riksrevisjonen er lukka. Dette gjeld og omfattande tiltak knytt til nettverkssikring. Det vert arbeid kontinuerleg med nye tekniske tiltak for auka IKT-sikkerheit. HelseCERT gjennomfører regelmessig inntrengingstestar frå ulike angrepsvinklar.

Det regionale arbeidet med informasjonssikkerheit[1] er i Helse Vest organisert som ein del av arbeidet med Topp 5 risiko. I det arbeidet er det etablert ei eiga arbeidsgruppe med deltakarar frå alle føretak i føretaksgruppa Helse Vest RHF, samt med representantar frå dei private, ideelle føretaka.

Sentralt i handlingsplanen er å integrere informasjonssikkerheit i den meir overordna og ordinære verksemdstyringa. På dette punktet i handlingsplanen var eitt av tiltaka å tilsette informasjonssikkerheitsleiar i Helse Vest RHF frå 01.09.2022. Stillinga er plassert i E-

[1] *Informasjonssikkerheit* handlar om å sikre at informasjon i alle former; (1) ikkje vert kjent for uvedkommande (*konfidensialitet*), (2) ikkje vert endra utilsikta eller av uvedkommande (*integritet*), (3) er tilgjengelig ved behov (*tilgjengelegheit*). *IKT-sikkerheit* er ei delmengd av informasjonssikkerheit og fokuserer på teknisk sikring av IKT-infrastruktur og IKT-applikasjonar.

helseavdelinga, men informasjonssikkerheitsleiar rapporterer direkte til administrerande direktør i saker som angår informasjonssikkerheit.

Informasjonssikkerheitsleiaren har teke over leiinga av det regionale utvalet for IKT-sikkerheit, samt leiinga av arbeidsgruppa for topp 5-risiko informasjonssikkerheit. Han styrer dei ulike tiltaka (organisert som prosjekt, jfr. nedanfor) som er forankra i den regionale handlingsplanen og arbeidet med topp-5-risiko for informasjonssikkerheit, og rapporterer i dette arbeidet til direktør for e-helse.

Helse Nord IKT HF og Sykehuspartner HF har saman med Helse Vest IKT AS, HEMIT HF og Norsk helsenett SF (HelseCERT) utarbeid ein felles trusselvurdering om IKT- og informasjons-tryggleik for 2022, jfr. styresak 098/22 i styremøtet i Helse Vest RHF 05.10.2022. Dette er ei felles trusselvurdering som dekker heile spekteret av verksemder og verdiar i spesialisthelsetenesta.

Kommentarar
Den regionale handlingsplanen for informasjonssikkerheit i Helse Vest er utarbeidd av arbeidsgruppe for topp 5 risiko – Informasjonssikkerheit. Handlingsplanen tok utgangspunkt i det kunnskapsgrunnlaget som var samla inn, primært gjennom revisjonen utført av Riksrevisjonen, men og basert på andre lokale, regionale og nasjonale kjelder.

Den regionale handlingsplan har fylgjande overordna *tiltak*;

1. *Roller, ansvar og oppgåver.*
2. *Oversikt, rapportering og oppfylging.*
3. *Kultur og kompetanse innanfor informasjonssikkerheit.*
4. *Informasjonssikkerheit i anskaffing og utvikling.*
5. *Applikasjonar, infrastruktur og teknisk sikkerheit.*

Handlingsplanen er operasjonalisert i fylgjande *prosjekt*;

1. *Felles tilnærming til NSM 2.0*
2. *Revisjon av regionalt styringssystem for informasjonssikkerheit og personvern*
3. *Vidareutvikling av sikkerheitskultur*
4. *Tiltak for IKT-sikkerheit i regi av Helse Vest IKT*
5. *Felles tiltak for økt IKT-sikkerheit for MU og TU*
6. *Tiltak for økt IKT-sikkerheit for Lokal IKT*

Dei to fyrste prosjekta er førande, og dels styrande, for dei etterfølgande prosjekta. Det er nedanfor gitt ein kort status for kvart av desse prosjekta.

Prosjekt 1: Felles tilnærming til NSM 2.0

Overordna status
Prosjektet har saman med Prosjekt 5 kartlagt føretaka sitt omfang av medisinteknisk utstyr teknisk utstyr og lokal IKT. På denne måten har ein kunne kartlagt i kva grad føretaka og utvalde IKT-miljø opererer i samsvar med NSM sine grunnprinsipp for IKT-sikkerheit. Kartlegginga gjev ein heilheitsforståing av kvar føretaka står, og gjev faktagrunnlag for å kunne diskutere nødvendige fellestiltak mellom desse.

Det overordna biletet på tvers av føretaka er stort sett likt, men Helse Bergen HF har arbeid med tiltak i ein lengre periode og har meir på plass enn øvrige helseføretak. Erfaringa frå Helse Bergen HF er eit nyttig grunnlag for det andre helseføretaka.

Prosjektet har og oppdatert Helse Vest IKT sin status på NSM-grunnprinsipp. Fleire av tiltaka Helse Vest IKT har iverksett vil kunne understøtte behov identifisert i helseføretaka.

Viktigaste leveransar

Målet har til no vore å kartlegge status og gje grunnlag for å kunne vurdere risiko med dagens situasjon, og vidare kunne peike på behov for fellestiltak og lokale tiltak. Dei viktigaste leveransane til no;

- Felles situasjonsforståing i og mellom helseføretak
- Eit oppdatert bilete for arbeidet med NSM sine grunnprinsipp i Helse Vest IKT
- Eit grunnlag for å prioritere risiko, foreslå løysningar og fellestiltak i regionen
- Innspel til tiltak som bør startast no og løysast i *Tiltak 6 - Lokal IKT*.

Vidare plan

Vidare plan i prosjektet er, gjennom ei risikobasert tilnærming, å finne dei fellestiltaka som bør anbefalast å arbeidast vidare med i 2023. Dette arbeidet vil bli gjort i tett samarbeid med både helseføretak og Helse Vest IKT.

Prosjekt 2 - Revisjon av regionalt styringssystem for informasjonssikkerheit og personvern

Overordna status

Prosjektet starta opp i august 2022 og har gjennomført intervju med tilsette i ulike helseføretak, for å forstå deira behov og deira bruk av dagens styringssystemet. Det er semje om å etablere det nye styringssystemet på strukturen frå "ISO 27001:2022 Administrasjon av informasjonssikkerheit". Endringane i 2022-versjonen av standarden er endra frå 12 kontrolldomene til fire hovudkategoriar (organisatoriske, fysiske, tekniske og personellrelaterte dokument). Dokument i dei tre siste kategoriane er reviderte, og har vore sendt til høyringar i styringsgruppa.

Viktigaste leveransar

Målet med prosjektet er å lage eit styringssystem som er lett å bruke for alle medarbeidar, med så kort, presist og konkret innhald som mogeleg. Dette trur vi vil skape meir forståing for styringssystemet sitt innhald, samt for informasjonssikkerheit i stort, samt betre etterleving. Dette kjem gjennom desse leveransane: Oppdatert struktur for styringssystem og dokumenta i dette. Oppdatert og forenkla innehald i styringssystemet basert på tilbakemeldingar frå styringsgruppe og intervju. Det nye styringssystemet skal og dekke nye område som tidligare ikkje har vore dekka. Informasjonspakke om korleis styringssystemet skal brukast og gjerast operativt, samt kva som har blitt oppdatert.

Vidare plan

I løpet av 4. kvartal 2022 skal prosjektet sluttføre gjennomgang og oppdatering av det eksisterande styringssystemet. I tillegg skal ein første informasjonspakke klargjerast, slik at dokument kan publiserast i løpet av 1. kvartal 2023. I 1. kvartal 2023 skal nye område bli identifisert og innarbeida.

Prosjekt 3 – Vidareutvikling av sikkerheitskultur

Overordna status
Føretaksgruppa Helse Vest gjennomførte hausten 2021 ei kartlegging av den digitale sikkerheitsskulturen blant dei tilsette. Heile 10 236 tilsette svara på undersøkinga. Med bakgrunn i resultata frå undersøkinga, er det arbeidd med tiltak knytt til sikkerheitskultur og kompetanse om informasjonssikkerheit for ulike grupper av medarbeidarar.
Viktigaste leveransar
Det er laga ein regional kommunikasjonsplan for digital sikkerheitskultur, og det er laga ein tiltaksplan for 2022 og 2023. Helse Vest har gjennomført ei storsatsing knytt til nasjonal sikkerheitsmånad i oktober 2022. Her var det mange saker på Intranett, fag-lunsjar kvar fredag med aktuelle tema innan informasjonssikkerheit og personvern, videoar og filmsnuttar på sosiale media/intranett, samt ein kronikk av administrerande direktør i Helse Vest IKT i Dagens Medisin. Det vart også laga eit informasjonsskriv til alle leiarar i Helse Vest, med ei verktøykasse med informasjon for leiarar. Informasjonen nådde ut til mange.
Vidare plan
Målet for prosjektet er betre sikkerheitskultur og meldekultur blant medarbeidarane i Helse Vest. For å få til dette trur vi at deler av kommunikasjonsplanen bør være obligatorisk. Arbeidet med sikkerheitskultur bør i nokon grad være ein kontinuerleg aktivitet og utviklast i takt med trusselbildet. Kommunikasjon og formidling av styringssystem, og særleg IKT-sikkerheitsinstruksen bør inngå i dette arbeidet. Leiarane våre, og då særleg nærmaste leiar er viktige kulturbyggjarer og nøkkelpersonar i dette arbeidet. Ved å utvikle verktøykassa for leiarar, kan vi bruke desse til å nå ut til alle medarbeidarane i Helse Vest. Vi må og revidere det obligatoriske e-læringskurset for informasjonssikkerheit, både for å spegle nytt styringssystem (prosjekt 2) og endringar som skjer når meir data skal handsamast i skytenester. E-læringskurs for melding av avvik bør og oppdaterast.

Prosjekt 4 – Tiltak for IKT-sikkerheit i regi av Helse Vest IKT - Modernisert sikkerheitsarkitektur

Overordna status
Prosjektet har no fokus på autentisering og sikker informasjonsutveksling. Det er bestilt teknologi som skal legge til rette for autentisering ved passordfri pålogging. Konfigurering og oppsett av plattformen pågår. Prosjekt skal utvikle ein modernisert plattform for styring av programmeringsgrensesnitt for god informasjonsutveksling («API-management»).
Viktigaste leveransar
Det er prøvd ut konsept for løysingar som støttar autentisering på applikasjonsnivå med passordfri pålogging. Dette er i hovudsak mobile løysingar som app til mobiltelefon for IMATIS og for desentralisert blodprøvetaking. Det er utarbeid ei konseptvurdering og tilråding for programmeringsgrensesnitt.

Vidare plan
Prosjektet skal prøve ut FIDO2 (Fast Identity Online – version 2) to-faktor autentisering, slik at utprøving heng saman med prosjektleveransane for øvrige delar av modernisert sikkerheitsarkitektur. Ferdigstille målarkitektur for identitets- og tilgangsstyring (Identity and Access Management (IAM)).

Prosjekt 5 og 6 - Felles tiltak for auka IKT–sikkerheit for MU og TU, og for Lokal IKT

Overordna status
Prosjektet har kartlagt ansvarsforhold for IKT-komponentar knytt til Medisinsk utstyr (MU) og Teknisk utstyr (TU). Det har vore tett samarbeid med prosjektleiar i prosjektet *Felles tilnærming til NSM 2.0.* Prosjektet har ei samla lista over system/IKT-komponentar som er aktuelle kandidatar for endra driftsmodell når Helse Vest IKT kan tilby dette. Lista er brukt som faktagrunnlag for å få på plass ein ny utvida leveransemodell for forvaltnings- og driftsmodellar med tilhøyrande ansvarsmatriser. Dagens situasjon er prega av at Helse Vest IKT og MU/TU-avdelingar i helseføretak har oversikt over kvar sin del av systemet/IKT-komponentar, men ingen har ein samla og total oversikt. Det gjenstår arbeid med Lokal IKT.
Viktigaste leveransar
Målet er at mal for forvaltnings- og driftsmodellar skal forankrast som eit eige bilag til Tenesteavtalen (SLA) som Helse Vest IKT inngår årleg med helseføretaka, og at dette bilaget viser til ein mal for ei operasjonell samarbeidsavtale (OLA) mellom Helse Vest IKT og helseføretaket. Kvart system/IKT-komponent som har delt driftsansvar mellom helseføretak og Helse Vest IKT, også i kombinasjon med ekstern leverandør, skal dokumenterast i ei felles systemoversikt med tilhøyrande ansvarsmatrisa.
Vidare plan
Helse Vest IKT og MU/TU-einingane må samarbeide best mogeleg, med direkte kontakt mellom fagfolk på riktig nivå. Prosjektet har oppdaga fleire manglar på oversikt i kartlegginga. Det er behov for hjelpemiddel/verktøy for å få ein betre samla oversikt over system og IKT-komponentar. Dette vil kunne medføra felles regionale investeringar. Behovet vårt må koordinerast med *prosjekt 1.*

Konklusjon

Arbeidet med informasjonssikkerheit er eit kontinuerleg arbeid for å sikre at personell har tilgang til relevant informasjon på rett tid og stad, sikre integriteten i informasjonen og unngå truslar knytt til konfidensialitet. Administrasjonen er av det syn at gjennomføring av «Regional handlingsplan for informasjonssikkerheit» har godt fart og rett retning.

Informasjonstryggleik er på agendaen kvar dag. Sjølv om den regionale handlingsplanen gjev eit løft i 2022 og 2023, er det også viktig å erkjenne at dette er eit arbeid utan tidshorisont og ende. IKT-systema våre blir stadig utsett for angrep – kvar dag, året rundt. Dette viser at informasjonstryggleik krev eit kontinuerleg arbeid, der kvar dag kan gje nye, uventa utfordringar. Då blir det ekstra viktig å skape innhald i tanken om at i Helse Vest er vi over 30.000 som arbeider med informasjonssikkerheit, slik at vi saman kan være på den sikre sida.