Saksframlegg

Saksgang:

Styre	Møtedato
Styret Sykehuspartner HF	12. desember 2018

SAK NR 090-2018

STATUS OG PLAN FOR PROGRAM FOR INFORMASJONSSIKKERHET, PERSONVERN, IDENTITETS- OG TILGANGSSTYRING (ISOP)

Forslag til vedtak

Styret tar status og plan for program for informasjonssikkerhet, personvern, identitets- og tilgangsstyring til etterretning.

Skøyen, 5. desember 2018

Gro Jære
administrerende direktør

1. Administrerende direktørs anbefalinger / konklusjon

I saken gis en redegjørelse for status og plan for program for informasjonssikkerhet, personvern og tilgangsstyring (ISOP) i Sykehuspartner HF.

Det innstilles på at styret tar saken til etterretning.

2. Faktabeskrivelse

2.1 Bakgrunn

ISOP er Sykehuspartner HF sitt program for styrket tilgangsstyring og forbedret informasjonssikkerhet og personvern. I denne saken oppsummeres overordnet status for programmet per november 2018.

Programmet har identifisert tiltak innen følgende områder (strømmer), som fremlagt i sak 035-2018, av 2. mai 2018:

- Styrket tilgangsstyring
- Personvern
- Sikkerhetsplattform
- Forbedret risikostyring

Sykehuspartner HF har i tillegg organisert tiltak som følge av dataangrepet inn under ISOP-programmet, ref. sak 46-2018, av 19. juni 2018.

2.2 Fremdrift

I 2018 har programmet prioritert tiltak innen strømmen sikkerhetsplattform for å styrke Sykehuspartner HF sin evne til å stå imot, oppdage og respondere på dataangrep. Noen av tiltakene har vært innenfor prosess og organisering, blant annet i form av justeringer og presiseringer i beredskapsplanverket og etableringen av Sykehuspartner CERT. Andre tiltak har vært av mer teknisk art, blant annet bredding av analyseplattformen for bedre overvåking av nettverkstrafikk samt anskaffelse av verktøy for endepunktssikring. Det er også gjennomført flere tiltak for å lukke kjente sårbarheter i infrastrukturen.

I tillegg har programmet hatt leveranser innenfor strømmene tilgangsstyring, personvern og forbedret risikostyring. Det er blant annet etablert automatisert tilgangsstyring til DIPS på samtlige helseforetak i regionen. Dette gir økt sikkerhet og reduserer behovet for manuell håndtering, både for Sykehuspartner HF sitt driftspersonell og for kliniske ansatte i helseforetakene som får tilgangene de trenger betydelig raskere enn tidligere. I tillegg vil automatisk tilgangsstyring øke kvaliteten og redusere antall avvik. Programmet har også breddet løsning for bestilling av tilganger til Vestre Viken HF, Sykehuset Innlandet HF og Sunnaas HF i 2018. Denne løsningen muliggjør bestilling av tilganger som ikke er omfattet av den automatiserte tilgangsstyringen.

I løpet av 2019 vil programmet ferdigstille de fleste leveransene som er planlagt innenfor alle de fire strømmene. Programmet vil i 2020 ha fokus på å avslutte de siste prosjektleveransene og sikre kompetanseoverføring og overlevering til linjeorganisasjonen. Det er ikke planlagt oppstart av nye leveranser i 2020.

3 Status og plan

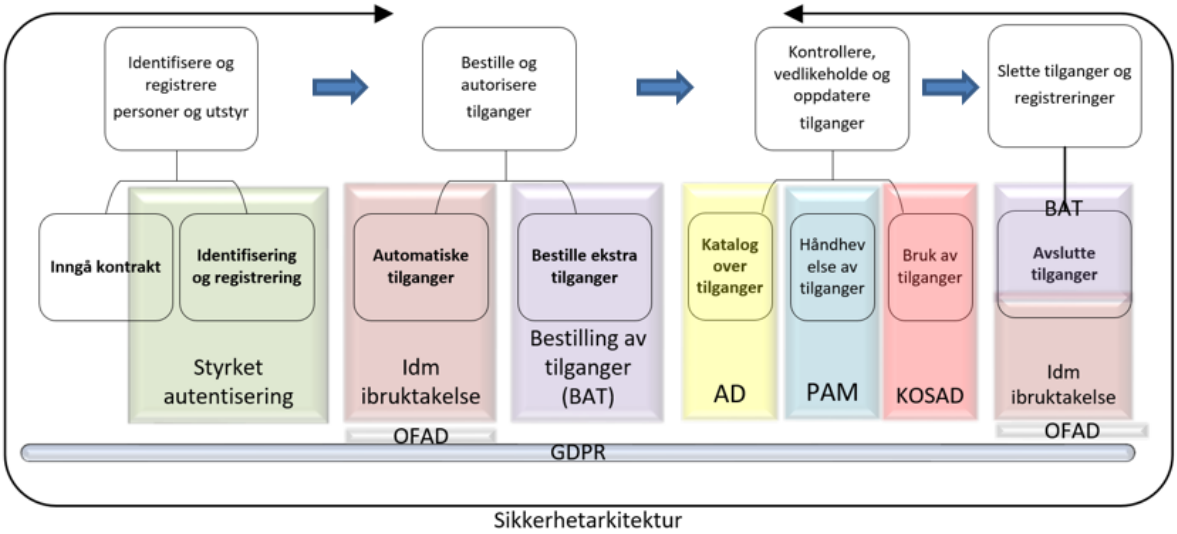
Nedenfor beskrives mål og tiltak, leveranser 2018 og planlagte leveranser i 2019 for prosjektene gruppert i de ulike strømmene.

3.1 Styrket tilgangsstyring

Styrket tilgangsstyring skal sikre at rett person får riktige tilganger til rett tid, at tilgangene fjernes når behovet opphører, og at dette er sporbart og uavviselig i ettertid. For å effektivisere denne prosessen og samtidig redusere risiko for feil, vil det også bli innført automatisert tilgangsstyring og selvbetjeningsløsninger for bestilling av tilganger. Under redegjøres det kort for innhold og status i de ulike prosjektene i denne strømmen.

Figur 1 under illustrerer hvor disse tiltakene i de ulike prosjektene i styrket tilgangsstyring inngår i livssyklusen til den overordnede tilgangsstyringsprosessen.

Figur 1 Overordnet tilgangsstyringsprosess



Prosjektene under arbeidsstrømmen styrket tilgangsstyring vil i sum svare ut målsetningen om styrket kontroll på tilgangsstyringen i alle viktige ledd i tilgangsstyringsprosessen. Det er derfor en viss avhengighet prosjektene imellom i denne arbeidsstrømmen.

3.1.1 Styrket autentisering

Prosjektets skal svare ut behovet for autentisering i Helse Sør-Øst, både i forhold til nye krav fra EU (eIDAS)- og HelseID om elektroniske signaturer og tillitstjenester. Prosjektet skal etablere en autentiseringsplattform med tilhørende forvaltning.

Prosjektet har i 2018 beskrevet nåsituasjonen i Helse Sør-Øst samt etablert målbilde. På bakgrunn av dette skal det i 2019 leveres en autentiseringsplattform for ansatte i Helse Sør-Øst samt leverandører. Det kan være aktuelt å tjenesteutsette noen funksjoner knyttet til autentisering, prosjektet vil gjennomføre vurderinger knyttet til dette.

3.1.2 Automatisk tilgangsstyring

Ved innføring av automatisk tilgangsstyring vil tilgang til en applikasjon tildeles automatisk basert på stillingskategori og rolle, uten behov for manuell opprettelse av tilganger i applikasjonen. Tilganger fjernes automatisk når arbeidsforholdets sluttdato inntreffer. Dette gir både økt sikkerhet rundt tilgangsstyringen og redusert behov for manuelt arbeid.

Prosjektet er en underleverandør av automatisk tilgangsstyring til programmet for Regional Klinisk Løsning (RKL) og følger deres implementeringsplaner.

Prosjektet har i 2018 etablert automatisk tilgangsstyring for elektronisk pasientjournal (DIPS) for samtlige helseforetak i regionen. I 2019 planlegges videre bistand og tilrettelegging i forbindelse med EPJ-journalinnsyn mellom helseforetak og tilpasninger til DIPS Arena.

I tillegg vil prosjektet innføre og bredde automatisert tilgangsstyring for applikasjonene Kurve (Metavision) til Oslo Universitetssykehus, Sykehuset Østfold og Akershus Universitetssykehus, laboratoriesystemer (LVMS) til Sykehuset Østfold, Sykehuset i Vestfold og Akershus Universitetssykehus, Medikamentell kreftbehandling (MKB/CMS) til Sykehuset Telemark og Akershus Universitetssykehus og prosjekt- og porteføljestyringsverktøy (Clarity) til hele Helse Sør-Øst.

3.1.3 Selvbetjeningsløsning for bestilling av tilganger (BAT)

Prosjektet leverer en løsning som skal forenkle tilgangsbestillinger og gi en bedre oversikt over tilganger som er gitt. Tjenesten skal erstatte funksjonene som i dag ligger i «Tilganger» i Min Sykehuspartner HF. Dersom en bruker skal ha tilganger utover det man har fått via automatisert tilgangsstyring kan dette bestilles via denne løsningen.

I 2018 vil løsningen være implementert på Vestre Viken HF, Sunnaas sykehus HF og Sykehuset Innlandet HF. I 2019 er det planlagt videre bredding av løsningen til øvrige helseforetak i Helse Sør-Øst.

3.1.4 Opprydning i Active Directory (AD)

Det er delegeringsgruppene i Active Directory som en bruker er medlem i som bestemmer hvilke tilganger man har.

I 2018 har prosjektet utarbeidet ny felles navnestandard som gir entydighet og bedre kontroll over hvilke tilganger en bruker får gjennom medlemskap i en gruppe. I tillegg skal prosjektet rydde i sikkerhetsgrupper med utvidete tilganger.

I 2019 skal prosjektet fortsette opprydding i AD-struktur for privilegerte tilganger i SIKT, Akershus universitetssykehus HF og Oslo universitetssykehus HF, samt etablere rollekatalog for privilegerte tilganger.

3.1.5 Privilegert tilgangskontroll

Privileged Access Management-prosjektet (PAM) arbeider med løsningsdesign og kravspesifikasjon for å kunne gjøre avrop på PAM-verktøy i IAM rammeavtalen.

I 2018 er det avklart behov for nytt verktøy og utarbeidet kravspesifikasjon.

I 2019 skal verktøy anskaffes og pilot etableres. Prosjektet prioriterer å gjennomføre noen utvalgte strakstiltak for å oppnå bedret kontroll i påvente av etablering av fullskala PAM-verktøy. I hovedsak innebærer dette en nettverksmessig nedlåsning av tilgangene til driftsarbeidsflater, og stenging for datatrafikk mellom ulike driftsarbeidsflater ved å innføre en felles portal.

3.1.6 Konsolidering av driftsarbeidsflater (KOSAD)

Bredding av standardisert driftsplattform i Helse Sør-Øst er en del av Helse Sør-Øst RHF sin strategi for en helhetlig og strømlinjeformet infrastruktur i regionen, på tvers av helseforetak. Prosjektet skal bredde eksisterende driftsarbeidsflater som i dag benyttes på Oslo universitetssykehus HF. Prosjektet er delt inn i to faser.

I fase en vil man bredde driftsarbeidsflatene Admin desktop og Ekstern desktop til Akershus universitetssykehus HF, samt migrere brukere over til ny løsning. Dette er planlagt gjennomført i første kvartal 2019.

I fase to vil man fortsette bredding av felles driftsarbeidsflater og migrering av brukere til de resterende helseforetakene som er på SIKT plattformen. Fase to planlegges ferdigstilt i løpet av første kvartal 2020.

3.1.7 Organisasjons- og fullmaktsadministrasjon (OFAD)

Prosjekt for organisasjons- og fullmaktsadministrasjon skal levere en løsning for forvaltning av masterdata knyttet til organisasjonshierarki i regionen. Dette er sentralt for å sikre automatisk tilgangsstyring av høy kvalitet.

Prosjektet er forsinket, og har måttet re-planlegge fremdriften. De viktigste årsakene til manglende fremdrift har vært ressursmangel (fagkompetanse) og manglende eksterne avklaringer angående rettigheter i forhold til kodeverk som er helt sentralt. Ressursmangel er nå løst, og avklaring det pågår avklaringer knyttet til kodeverk mot Norsk Helsenett SF. Prosjektet har fått ny prosjektleder. Det planlegges for pilotering av versjon 1.0 i første kvartal 2019.

3.1.8 Identitetsbasert sikker samhandling (ISS)

Prosjektet skal etablere IAM rammeavtale og gjennomføre avrop på sikkerhetskomponent (API-GW). Sikkerhetskomponenten skal sikre tekniske grensesnitt og er nødvendig for å kunne tilby digitale samhandlingstjenester som f.eks. innsyn i pasientjournal på en sikker måte.

I Helse Sør-Øst RHF sitt program for å etablere Regionale Kliniske Løsninger (RKL) er det opprettet et prosjekt for å etablere digitale innbyggertjenester (DIT). Dette vil blant annet gi innbyggerne i regionen tilgang til sin egen journal, samt mulighet for å samhandle med spesialisthelsetjenesten på nett. Sikring av tekniske grensesnitt er en forutsetning for at dette skal skje på en trygg og sikker måte. Dette løses ved å implementere en API Gateway. I 2018 har prosjektet etablert IAM rammeavtale og utarbeidet kravspesifikasjon API-GW. Forberedelse på avrop pågår. Det henvises til egen sak 094-2018, *Fullmakt – ny avtale for sikring av tjenester for elektronisk samhandling.*

Forutsatt beslutning om anskaffelse, så vil prosjektet anskaffe og implementere API-GW i løpet av første kvartal 2019. Prosjektet Digitale Innbyggertjenester vil da kunne starte pilotering og testing av sin tjeneste innsyn i pasientjournal med påfølgende lansering.

3.2 Personvern

Prosjektet skal bidra til at Sykehuspartner HF etterlever kravene i personvernlovgivningen, både som databehandler for helseforetakene og som dataansvarlig for opplysninger om egne ansatte.

I 2018 har prosjektet etablert nye maler for databehandleravtaler og mal for protokoll over behandlingsaktiviteter. Prosjektet har også stått for rådgivning og opplæringsaktiviteter i linjeorganisasjonen. Prosjektet har startet arbeidet med å få leverandører over til ny mal, før ansvaret for dette arbeidet ble overført til driftsorganisasjonen. Sykehuspartner HF erfarer at det kan være utfordrende å få leverandører til å akseptere et ubegrenset økonomisk ansvar i DBA med leverandører, og har etter dialog med Helse Sør-Øst RHF fått avklaring knyttet til hvilke risikobaserte kommersielle vurderinger Sykehuspartner HF kan gjøre knyttet til dette.

I første halvår 2019 skal prosjektet ha følgende leveranser:
- Bistand til kontraktforvaltning og leverandørstyring av personvernkrav
- Forvaltning av protokoll over behandlingsaktiviteter
- Roller og ansvar for personvern
- Revisjon av internkontroll knyttet til personvern og forslag til tiltak

- Policyer og prosedyrer for å forvalte dataansvar
- Policyer og prosedyrer for å ivareta innebygd personvern
- Revisjon av etterlevelse / gapanalyse

Prosjektet er planlagt avsluttet første halvår 2019. Status for GDPR vil bli ytterligere belyst i styremøtet.

3.3 Sikkerhetsplattform

Denne arbeidsstrømmen skal sikre forbedring av informasjonssikkerheten, øke deteksjonskapabiliteten, redusere angrepsflaten samt øke responsevnen mot dataangrep. Det er etablert tre prosjekter som skal bidra til dette.

3.3.1 Analyseplattform

Prosjektet skal styrke informasjonssikkerhetsarbeidet, i form av implementering av løsning for sporing og logging av uønsket aktivitet i Helse Sør-Øst sine datanettverk.

I 2018 er analyseplattformen breddet til Akershus universitetssykehus HF og Sykehuset i Østfold Moss samt til lokasjoner uten lokal infrastruktur (46 lokasjoner). I 2019 vil prosjektet fortsette bredding til 22 lokasjoner med lokal infrastruktur før prosjektet avsluttes, etter plan i første kvartal 2019.

3.3.2 Sikkerhetsarkitektur

Prosjektet skal etablere en helhetlig sikkerhetsarkitektur i Helse Sør-Øst. Etablering av en slik regional sikkerhetsarkitektur er tidkrevende. Prosjektet vil derfor prioritere leveranser i dialog med STIM og STIM sine behov.

I 2018 er det tatt frem en metodikk for etablering av sikkerhetsarkitektur. Arbeidet med å etablere sikkerhetsarkitektur med hjelp av denne metodikken er påstartet og vil fortsette i 2019.

3.3.3 Charmander (Unntatt offentlighet. Off.l § 24.3)

Jf. vedlegg.

3.4 Risiko

3.4.1 Virksomhetsbasert risikostyring

Prosjektet skal etablere en forbedret prosess for identifisering, rapportering og håndtering av risiko i organisasjonen. Prosjektets leveranser er:

- Effektivisere metodisk rammeverk
- Styrke prosess for identifisering, rapportering og håndtering av risiko
- Etablere prosessdokumentasjon
- Bistå linjen med å implementere prosess og metodikk
- Utarbeide vurderingsgrunnlag for beslutning om verktøystøtte
- Implementering av støtteverktøy ved beslutning om anskaffelse

I 2018 har prosjektet ferdigstilt rammeverk, prosess og dokumentasjon. I 2019 skal prosjektet bistå driftsorganisasjonen med å styrke prosess og metodikk i Sykehuspartner HF, samt vurdere og eventuelt anskaffe og implementere støtteverktøy.

3.4.2 Forbedret risikostyring

I sak nr. 058-2017 vedtok Helse Sør-Øst RHF sitt styre at metodikk for risiko og sårbarhetsanalyser knyttet til informasjonssikkerhet må gjennomgås, forsterkes og implementeres. Som et av flere tiltak har Sykehuspartner HF utarbeidet forslag til felles risikoakseptansekriterier for regionen innenfor området informasjonssikkerhet.

Utgangspunktet for felles risikoakseptansekriterier er en underliggende felles metodikk for å vurdere sannsynlighet og konsekvens på mulige uønskede hendelser knyttet til informasjonssikkerhet. Metoden forutsetter at databehandler definerer risikoakseptkriterier mht. konfidensialitet, integritet og tilgjengelighet. Ved å beslutte en felles, regional metodikk vil vi oppnå konsistens i vurdering av risiko, og Sykehuspartner HF sine ROS-rådgivere vil ha et faglig forankret grunnlag til å skille akseptabel fra uakseptabel risiko samt til å skape tydelighet i kommunikasjon av risiko. Et sentralt element i oppdraget har vært utarbeidelsen av risikoskalaer for fremme av transparens og målbarhet i fastsettelse av risiko, og for utvikling av en felles plattform for fastsettelse av risikonivå.

Prosjektet har også gjennomført risikovurdering av dagens driftssituasjon i 2018.

I 2019 vil prosjektets resterende leveranser ferdigstilles i løpet av første halvår, med unntak av en eventuell anskaffelse og implementering av støtteverktøy som forventes å pågå ut 2019.

4 Økonomi

4.1 Budsjettbehov for 2019

For 2019 utgjør revidert budsjettinnspill totalt 150 MNOK, fordelt på 55 MNOK i driftskostnader og 95 MNOK i investeringer. Finansielle rammer for program og prosjekt for 2019 inngår i budsjettprosessen for 2019, jf. sak 092-2018 *Revidert budsjettinnspill Sykehuspartner HF 2019*.

5 Administrerende direktørs vurdering

I 2018 har programmet prioritert tiltak for å styrke Sykehuspartner HF sin evne til å stå imot, oppdage og respondere på dataangrep. I tillegg er programmet i gang med leveranser innen styrket personvern, styrket tilgangsstyring og forbedret risikostyring. Dette arbeidet øker informasjonssikkerheten i eksisterende infrastruktur og legger til rette for god sikkerhet i modernisert plattform.

Arbeidet som er gjennomført i 2018 har økt informasjonssikkerheten i Helse Sør-Øst. Samtidig erkjenner administrerende direktør at det gjenstår et omfattende arbeid. Trusselbildet er i stadig utvikling, dette krever et kontinuerlig arbeid med informasjonssikkerhet. Administrerende direktør vil derfor prioritere disse oppgavene høyt også i 2019. Flere store leveranser som kommer i 2019 er basert på forberedende arbeid utført i 2018.

Administrerende direktør anbefaler at styret tar status og plan for program for informasjonssikkerhet, personvern, identitets- og tilgangsstyring til etterretning.

Vedlegg

- Charmander (Unntatt offentlighet. Off.l § 24.3)