VEDLEGG 4 – STYRKET TILGANGSSTYRING

Innledning

Tilgangsstyring skal sikre at rett person får rett tilgang, til rett ressurs/informasjon, til rett tid og fra rett sted, med tilhørende sporbarhet og kontrollmekanismer. Tilgangsstyring er summen av policyer, prosesser og teknologi som er ment å regulere og etterleve dette området. Det finnes ulike teknologier som benyttes for å ivareta identitet- og tilgangsstyring som område, og Helse Sør-Øst (HSØ) har valgt å ta i bruk flere av disse for å understøtte regionens behov for autentisering og autorisasjon. Videre reguleres tilgang gjennom databehandleravtaler og personlige taushetserklæringer.

Se Appendix A for definisjoner vedrørende Tilgangsstyring/-kontroll.

Bakgrunn

Det henvises til vedlegg 3 «Redegjørelse av dagens driftssituasjon når det gjelder konfidensialitet, integritet og tilgjengelighet».

Kortsiktige tiltak

Det vil være behov for å fortsette arbeidet med organisering, ansvarsfordeling, styring, policy, prosesser og rutiner for tilgangsstyring i perioden fremover. Det er den siste tiden avdekket flere utfordringer ved dagens praksis, som vil måtte adresseres gjennom tiltak den kommende perioden. I tillegg til de overnevnte punktene vil det iverksettes arbeid knyttet til sterkere og bredere tiltak innenfor sporbarhet og kontrollmekanismer.
I og med at området er stort og komplekst anbefales det at kortsiktige tiltak fokuseres mot privilegerte tilganger som benyttes for drift, forvaltning og leverandøraksess.

En rekke kortsiktige tiltak er allerede iverksatt:

- Forsterket rutine for tildeling av priviligerte tilganger
- Forsterket rutine for gjenåpning av eksisterende tilganger
- Gjennomgang av kontroll og rapporteringsbehov
- Full gjennomgang av tilganger for leverandører og eksternt personell
- Påbegynt deaktivering av tilganger for leverandører og eksternt driftspersonell som ikke har tjenestelig behov
- Bedret kontrollrapportering av tilgangsendringer for leverandører og eksternt personell

Det vil også bli gjennomført vurderinger av endringer og/eller bredding av allerede tilgjengelige produkter som f.eks:

- Saksbehandlingsverktøyet (HPSM) er planlagt oppgradert høsten 2017 slik at godkjenningsprosessen styrkes.
- Økt bruk av passordhvelvet (PAM) for priviligerte tilganger. Dette vil innebære økt løpende driftskostnad i året. Ytterligere utvidet bruk av produktet PAM må ses opp mot et langsiktig målbilde før det kan vurderes. Utvidet bruk av passordhvelvet kan iverksettes høsten 2017 dersom finansiering avklares.

- Bredding av analyseplattformen til alle HFene vil gi økt sporbarhet og kontroll/rapporteringsmulighet. Dette er også definert som et regionalt tiltak etter hendelsen med Wannacry. Det er ikke budsjettert med midler til dette i 2017. Bredding kan igangsettes i august 2017 dersom finansiering avklares.

Disse tiltakene vil gi en positiv effekt på tilgangsstyringen, men utelukker ikke muligheten for at driftspersonell med privilegerte rettigheter kan eksponeres for helseopplysninger/sensitive personopplysninger.

Langsiktige tiltak

Et samlet initiativ for forsterking av tilgangsstyring har en betydelig kompleksitet, gitt det store antall brukere i Helse Sør-Øst og volumet av servere og applikasjoner som eksisterer, samt behovet for etablering av styringsmodeller for tilgangsstyring og applikasjonsportefølje i HSØ. Dette initiativet vil også ha en betydelig økonomisk og ressursmessig konsekvens, som gjør at det vil være behov for å gjennomføre en prioritering av tilnærmingen på dette initiativet.
For å sikre en strukturert og samlet tilnærming til tilgangsstyring bør det igangsettes et prosjekt som har som formål å definere og forankre et målbilde for dette område, samt en GAP-analyse og et veikart som grunnlag for en prioritert implementeringsplan. Dette målbildet må også sees opp imot den planlagte infrastrukturmoderniseringen og andre regionale prosjekter, for å sikre at disse er samkjørt og at det ikke gjennomføres overlappende aktiviteter. Prosjektet må sees i sammenheng med IAM og de andre prosjektene som er vurdert for viderføring fra iMod. På det nåværende tidspunkt antas at en foranalyse kan foreligge i starten av kvartal 4 2017.

SYKEHUSPARTNER

Appendix A:

Normen om informasjonssikkerhet i Helse og omsorgstjenesten beskriver kravene til informasjonssikkerhet, herunder tilgangsstyring:

- Med ”tilgang” menes at helse- og personopplysninger om en eller flere bestemte pasienter/brukere er eller gjøres tilgjengelige for autorisert personell. Beslutning om tilgang til behandlingsrettede helseregistre skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til pasienten. Tilgang til fagsystemer i forbindelse med ytelser til pasient/bruker skal iverksettes basert på tjenstlig behov. Tilgang i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra tjenstlig behov (Normen)

- Med ”autorisere/autorisert/autorisasjon” menes at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av helse- og personopplysninger. Autorisasjon kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra tjenstlig behov og er i henhold til bestemmelser om taushetsplikt (Normen)

- Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes. (Normen)

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

Web: www.sykehuspartner.no
E-post: post@sykehuspartner.no
Org.nr.: 991 324 968