regionernes sundheds-it

Statusbilag til regionsrådets drøftelse 2016

Regionernes politiske linje for informationssikkerhed

Hver eneste dag behandles fortrolige oplysninger af medarbejdere i de 5 regioner. Medarbejdernes adgang til relevante data er helt afgørende for en god og sammenhængende behandling af den enkelte borger, ligesom data er vigtige for at vi kan have et moderne og effektivt sundhedsvæsen.

Borgerne skal kunne være trygge ved at deres personfølsomme oplysninger behandles sikkert og med den nødvendige fortrolighed.

Danske Regioners bestyrelse har derfor den 22. januar 2015 vedtaget "Regionernes politiske linje for informationssikkerhed".

Den politiske linje for informationssikkerhed indebærer at regionerne fremover skal have en risikobaseret tilgang til informationssikkerhed inden for sikkerhedsstandarden ISO 27001. Sikkerhedsstandarden hviler på to principper.

Det ene er at indsatsen for informationssikkerhed er baseret på en konkret vurdering og afvejning af risici. Det indebærer en prioritering af indsatsen for at forebygge sikkerhedsbrister. Heri indgår en analyse af, hvad der er organisationens mest kritiske systemer. Endvidere skal der være en handlingsplan for håndtering af risici.

Det andet princip er, at informationssikkerhed er forankret i topledelsen for at sikre den nødvendige ledelsesmæssige bevågenhed. Derfor er det en del af den politiske linje at der skal foregå en årlig drøftelse af den enkelte regions informationssikkerhed i regionsrådet.

RSI pejlemærke om informationssikkerhed

For at kunne realisere implementeringen af den politiske linje for informationssikkerhed er det vigtigt at regionerne har en fælles tilgang til området. Regionernes Sundheds-IT (RSI) har derfor igangsat et pejlemærke, som skal understøtte implementeringen af regionernes politiske linje for informationssikkerhed.

Pejlemærket skal være med til at sikre, at regionerne opretholder et højt fælles niveau af informationssikkerhed samt overholder gældende lovgivning. Dette har afgørende betydning for borgernes tillid til at regionerne forvalter borgernes data sikkert og forsvarligt. Pejlemærkets initiativer vil derfor typisk være tiltag, som under alle omstændigheder skal iværksættes i den enkelte region.

Pejlemærkets leverancer er blandt andet en række værktøjer, skabeloner og modeller, som den enkelte region kan bruge i sit eget arbejde med informationssikkerhed. Den fælles tilgang

og indsats på området skal være med til at lette den enkelte regions arbejde med at styrke informationssikkerheden og bidrage til den enkelte regions compliance på området.

Pejlemærkets indsatser i 2016
Pejlemærket har to forskellige former for indsatser. Den ene er områder, hvor der udvikles fællesregionale løsninger. Her er det pejlemærkets opgave at sikre videndeling og værktøjer, som skal understøtte regionernes egen indsats hen mod de fælles mål i regionernes politiske linje for informationssikkerhed. Det andet indsatsområde i pejlemærket er rettet mod den enkelte region, hvilket indebærer at initiativerne skal gennemføres i hver region og ikke nødvendigvis på samme tid i alle regioner.

Fællesregionale indsatser
Følgende fællesregionale indsatser vil blandt andet blive gennemført i 2016:

- En fællesregional politik for informationssikkerhed
- Idébank og forslag til en fælles ramme for awareness-kampagner for medarbejderne i de enkelte regioner
- Fælles ramme for risikovurdering af it-systemer og medico-teknisk udstyr
- Fælles retningslinjer for bruger/rollestyring i de enkelte regioner
- Fælles skabelon for databehandleraftaler
- Fælles ramme for kortlægning af datastrømme, som er et krav i forhold til EU-forordningen
- Kortlægning af behovet for at modernisere lovgivningen
- Vurdering af de regionale konsekvenser af EU-forordningen om persondatabeskyttelse.

Regionale indsatser
Følgende regionale indsatser vil blive gennemført i 2016:

- Awareness-kampagner, der sætter fokus på medarbejdernes viden om informationssikkerhed. Flere regioner er allerede i gang med konkrete initiativer på området
- Konkret risikovurdering af egne systemer, der skal danne baggrund for et overblik over risici og handlingsmuligheder i den enkelte region
- Indgåelse af databehandleraftaler
- Begyndende implementering af sikkerhedsstandarden ISO 27001, herunder forankring i ledelsen og risikobaseret tilgang til informationssikkerhed.

Status på arbejdet i pejlemærket
Det tværregionale arbejde med RSI pejlemærket om informationssikkerhed er kommet godt i gang. Regionerne har på mange områder et forskelligt udgangspunkt. Styregruppens ambitioner med pejlemærket er blandt andet, at regionerne har en fælles tilgang til området og er med til at sikre, at regionerne dels overholder gældende lovgivning og dels opretholder et højt fælles niveau af informationssikkerhed. Samtidig er det vigtigt at der i pejlemærkets leverancer tilstræbes en balance mellem ønsket om at skabe en fælles standard i regionerne og det faktum at regionerne er organiseret forskelligt og at produktet derfor skal kunne tilpasses den enkelte region.

Pejlemærkets leverancer forudsætter en lokal forankring hos den enkelte region. Det er derfor afgørende for pejlemærkets succes, at regionerne har forpligtet sig til at sikre den lokale forankring af pejlemærkets initiativer i deres egne organisationer.

En række af pejlemærkets leverancer for 2016 er leveret og godkendt af styregruppen. Dette gælder blandt andet udarbejdelsen af en fællesregional informationssikkerhedspolitik samt en fælles skabelon for databehandleraftaler.

Trusselsvurdering fra Center for Cybersikkerhed
Behovet for en indsats for informationssikkerhed er blevet yderligere aktualiseret af, at Center for Cybersikkerhed har offentliggjort en trusselsvurdering den 6. januar 2016. Heri peges på, at truslen fra cyberspionage mod offentlige myndigheder og private virksomheder er meget høj. Gennem de seneste år er der et stigende antal af cyberangreb mod Danmark, og metoderne er blevet mere avancerede. Derfor anbefales det, at myndighederne kender deres egen infrastruktur og gennemfører løbende risikoanalyser for at kunne identificere de mulige konsekvenser af de forskellige typer angreb.

EU-forordning om persondatabeskyttelse
EU har vedtaget en persondataforordning, der får retsvirkning i medlemslandene den 25. maj 2018. Forordningen kommer til at erstatte persondataloven. Efter forordningen bliver det blandt andet et krav, at regionerne som dataansvarlige kan dokumentere, at behandlingen af personoplysninger sker i overensstemmelse med forordningens bestemmelser. Dette indebærer blandt andet, at der i højere grad vil være krav til dokumentation af datastrømme, databehandleraftaler og hjemmelsgrundlag samt til dokumentation af, at sikkerheden opfylder gældende regler. Et centralt tiltag i forordningen er desuden et krav om, at alle offentlige myndigheder skal have en særlig dataansvarlig, en såkaldt DPO. DPO'en har en særlig ansættelsesretlig beskyttelse og får en række centrale opgaver med bl.a. at kontrollere om reglerne bliver overholdt i den enkelte region.