Utdrag ur Regionstyrelsens svar 2020-03-18

Svar på revisionsrapport "Granskning av informationssäkerhet"

Regionens revisorer har i skrivelse den 13 december 2019 bett om regionstyrelsens kommentarer och synpunkter på revisionsrapporten "Granskning av informationssäkerhet".

Regionstyrelsen ser positivt på det absoluta flertalet av revisorernas rekommendationer och noterar med tillfredsställelse att de flesta av dem redan är under hantering inom ram för det pågående informationssäkerhetsprojektet "Översyn av ledningssystem för informationssäkerhet (ISO27000)" och att detta uppmärksammats i revisionsrapporten.

En färdplan för införande av ett ledningssystem för informationssäkerhet är under utarbetande inom ram för informationssäkerhetsprojektet. Knutet till denna kommer målsättningar och ansvarsbeskrivningar att tas fram -därtill en uppdaterad tidsram.

En utvecklad arbetsgrupp för informationssäkerhet kommer att tas fram -även detta inom informationssäkerhetsprojektet -varvid en organisation för informationssäkerhet skapas. Grunden kommer att utgöras av den nuvarande dataskyddsorganisationen som sedan sin tillkomst under våren 2019 bedrivit ett omfattande arbete knutet till GDPR-lagstiftningen och därmed utgjort en mycket viktig del av regionens befintliga informationssäkerhetsarbete. Det bör noteras att dataskydds-och informationssäkerhetsarbete till stor del är närbesläktat -men inte fullt överlappande.

Som en del av arbetet med regionens förvaltningsmodell för verksamhetssystem åligger det systemförvaltningarna att genomföra informationsklassning och riskanalys. Regionstyrelsen ser positivt på att dessa riskanalyser aggregeras till ett riskregister som administreras av den kommande organisationen för informationssäkerhet.

Inom ram för informationssäkerhetsprojektet kommer även erforderliga styrdokument att tas fram och revideras. Detta i enlighet med informationssäkerhetspolicyn. Den kommande organisationen för informationssäkerhet kommer att bli den gruppering som svarar för förvaltningen av dessa styrdokument.

Arbete med att utforma grunden till obligatorisk informationssäkerhetsutbildning för samtliga medarbetare inom regionen kommer att tas fram inom ram för informationssäkerhetsprojektet och därefter förvaltas av organisationen för informationssäkerhet. Även här utgörs grunden av dylika insatser inom dataskyddsområdet.

Hanteringen av incidenter inom informationssäkerhetsområdet kommer att utvecklas inom informationssäkerhetsprojektet och även den förvaltas inom den kommande organisationen för informationssäkerhet. Grunden utgörs av motsvarande hantering inom dataskyddsområdet.

Det ligger inom utvecklingsarbetet för säkerhetsskyddsområdet att genomföra en analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

Det inom ram för informationssäkerhetsprojektet pågående arbetet med att ta fram en organisation för informationssäkerhet kommer även att peka på det ansvar knutet till informationssäkerhet som vilar på rollerna inom regionens förvaltningsmodell för verksamhetssystem.

Ett första steg mot en central behörighetshantering kommer att realiseras i och med införandet av Framtidens Vårdinformationssystem (FVIS). Inom FVIS kommer en tjänst för identitets- och åtkomstkontroll att utvecklas vilket är en förutsättning för ett framtida arbete med att automatisera processer för tilldelning, förändring, och borttagning av behörigheter.

Tillgång till fysiska lokaler som serverhallar kommer fortsatt att vara begränsat till de medarbetare som har behov av åtkomst för att kunna utföra sina arbetsuppgifter.

Accessloggar för åtkomst till nätverk och logginformation för brandväggar lagras i två separata system under 90 dagar. Denna lösning fyller behovet gällande uppföljning och kontroll på ett acceptabelt sätt. Vidare är ett införande av en SIEM-lösning med utökad lagringstid till 180 dagar både omfattande och kostnadsdrivande på ett sätt som inte kan motiveras i dagsläget.

Att utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans är ett omfattande arbete som måste vägas mot arbetsmängd och kostnad och i dagsläget anses inte detta vara en prioriterad åtgärd.

REGIONSTYRELSEN

Glenn Nordlund
Ordförande

Anders Sylvan
T.f. Regiondirektör