Region Gävleborg
REVISORERNA

2019-05-16

Till
Regionfullmäktige

För kännedom
Styrelse/nämnder

Samlad bedömning av informations- och cybersäkerhet

På uppdrag av Region Gävleborgs revisorer har PwC genomfört en granskning av arbetet med informations- och cybersäkerhet i regionen.

Granskningsresultatet har bedömts utifrån skalan "ej uppfyllt", "i begränsad utsträckning", "till övervägande del" eller "helt uppfyllt" och den sammanfattade bedömningen är:

- **att regionstyrelsen i begränsad utsträckning har säkerställt att Region Gävleborg har ett ändamålsenligt arbete med att identifiera, prioritera och hantera säkerhetshot och incidenter som kan påverka regionens informations- och cybersäkerhet.**

Den sammanfattande bedömningen baseras på en sammanvägning av bedömningarna för ett antal kontrollmål i granskningen. Utifrån genomförd granskning kan vi konstatera att de personer som har det övergripande ansvaret för informations- och it-säkerhet är nya på sina roller och har inlett ett förbättringsarbete men det finns fortfarande mycket kvar att göra.

Övergripande kan det sägas att regionen till stor del har en ansvarsfördelning där det är tydligt vem det är som ansvarar för olika områden inom informations- och cybersäkerhet. Det som brister är dock ofta dokumenterade processer för hur arbetet ska genomföras. Detta riskerar att skapa ett personberoende.

Det saknas även övergripande styrande dokumentation för arbetet med informations- och cybersäkerhet. Inom it-säkerhet finns stora brister kring styrande dokumentation. Inom informationssäkerhet finns dokumentation men stora delar är utkast och ännu inte antagna. Det är särskilt arbetet med informationssäkerhetsrisker som saknar styrning. Vidare finns det brister kring uppföljning av den styrande dokumentation som finns och det finns idag inget sätt att mäta eller följa upp arbetet med informationssäkerhet i regionen.

Det finns brister relaterat till mandat och resurser för informationssäkerhetsansvarig. Informationssäkerhetsansvarig rapporterar inte direkt till ledningen och har inte en egen budget. Detta riskerar att hindra ett effektivt och systematiskt arbete med informationssäkerhet i regionen.

Inom it-säkerhet finns det brister gällande säkerställande av kunskap och kompetens. Det finns ingen utbildning i it-säkerhet och det kan inte säkerställas att personal som arbetar inom området har tillräcklig kompetens. Området utbildning behöver även förbättras inom informationsäkerhetsområdet. Det genomförs utbildningar sporadiskt men det finns ingen övergripande plan för när och hur utbildningar ska genomföras.

Det finns även ett behov av att öka samordningen mellan it- och informationssäkerhetsavdelningarna, främst gällande identifiering och hantering av incidenter. I nuläget finns en risk att incidenter inte rapporteras och hanteras på ett korrekt sätt.

Utifrån granskningens resultat är våra rekommendationer till regionstyrelsen:

- Fastställ styrande dokument inom både informationssäkerhet och cybersäkerhet
- Fastställ dokumenterade processer för arbetet med informationssäkerhet och cybersäkerhet
- Formaliseras och systematiseras arbetet med informationssäkerhetsrisker
- Samordna processer avseende hantering av incidenter genom samverkan mellan informationssäkerhetsavdelningen och it-avdelningen.
- Säkerställ att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag samt förvaltar sin egen budget
- Säkerställ att det genomförs utbildningar och kompetenshöjande aktiviteter inom området cybersäkerhet.

Gävle 2019-05-16

För Region Gävleborgs revisorer

Olof Bengtsson
Ordförande

Sture Sandberg
Vice ordförande