Tjänsteställe, handläggare
Nämndadministration, Sofia Öhrman

Sammanträdesdatum
2024-12-17

Beteckning
Dnr: 24RS9817

Er beteckning:

Regionens revisorer, c/o PWC
Box 885
721 23 Västerås

# Svar på revisionsrapport ”Nulägesanalys NIS2-direktivet”

Under 2024 genomförde regionfullmäktiges revisorer (revisorerna) en granskning för att bedöma om regionstyrelsen har säkerställt ett ändamålsenligt förberedelsearbete inför NIS2- direktivet. Revisorernas samlade bedömning är att Region Örebro län inte helt har säkerställt ett ändamålsenligt förberedelsearbete inför NIS2 och lämnar kommentarer och förslag vilka framgår av deras rapport.

Region Örebro län ber att få svara revisorerna på följande sätt.

Region Örebro län anser att informationssäkerhetsfrågorna är viktiga och lägger ett stort fokus på arbetet med dessa frågor. Det sker dels i direkt anslutning till de olika verksamheterna, dels från centralt håll och även via arbete som sker inom ramen för ett förvaltningsövergripande informationssäkerhetsråd.

Informationssäkerhetsrådet är ett rådgivande organ till regionens ledningsgrupp med minst en deltagare från varje förvaltning samt ett antal nyckelpersoner såsom IT-chef, IT-säkerhetsansvarig, chefläkare och dataskyddsombud. Rådets främsta uppgift är att på olika sätt arbeta med informationssäkerhetsfrågor och att vara ett forum för diskussion och arbete med att främja informationssäkerheten i regionen. I hälso- och sjukvårdsförvaltningen finns sedan ett par år tillbaka en informationssäkerhetshandläggare som har en operativ roll genom att stötta hälso- och sjukvårdsförvaltningen i informationssäkerhetsarbetet.

Omfattningen av de resurser som ställs till förfogande för informationssäkerhetsarbetet måste dock ställas i relation till de resurser som behövs för att bedriva den huvudsakliga verksamhet som regionen ansvarar för. Målet är att genom ett fortsatt skapande av för verksamheterna användbara rutiner, mallar och olika verktyg hela tiden såväl förbättra som förenkla regionens informationssäkerhetsarbete inom ramen för de resurser som kan anslås.

Allt sedan NIS1- direktivet trädde i kraft och sedan implementerades genom den nu gällande lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster har ett arbete pågått med att intensifiera det systematiska och riskbaserade informationssäkerhetsarbetet i hela regionen och i synnerhet i hälso- och sjukvården och folktandvården som är de verksamheter som idag omfattas av lagen. Genom NIS2- direktivet kommer flera sektorer att omfattas och för regionens del, då hela regionorganisationen. NIS2-direktivet har ännu inte implementerats i svensk lag men lagstiftningsarbetet bevakas. Det viktiga är att nu fortsätta med och utveckla det systematiska och riskbaserade informationssäkerhetsarbetet i enlighet med ISO-27000 då detta är grundläggande för NIS-lagstiftningen.

NIS2 direktivet och den kommande nya svenska lagstiftningen har varit föremål för diskussion i informationssäkerhetsrådet och i de regiongemensamma NIS-frågorna såsom exempelvis incidenthanteringen behöver en samverkan ske mellan förvaltningarna. Ett samarbete sker också med andra regioner, exempelvis genom hälso- och sjukvårdsregionens informationssäkerhetsnätverk. Detta för att skapa en samsyn i frågor och exempelvis skapa likalydande dokument i den mån det är möjligt.

Inom en snar framtid kommer regionen att införa SKR:s informationsklassningsverktyg KLASSA. Avsikten är att KLASSA kommer att underlätta det riskbaserade och systematiska informationssäkerhetsarbetet. Dels kommer det att bli enklare för verksamheterna och informationsägarna att genomföra klassningar och riskanalyser, dels får informationsägarna en bättre överblick över sina informationsmängder och identifierade risker. Detta kommer också att kunna underlätta det uppföljande riskarbetet i stort.

Vidare pågår ett arbete med att etablera ett ”årshjul” för informationssäkerhetsarbetet (inklusive dataskydd). Detta ska bland annat stötta informationsägarna i det systematiska och riskbaserade informationssäkerhetsarbetet, där uppföljningen är en naturlig och viktig del gällande incidenter, risker samt uppföljning av leverantörer. Behovet av

stödjande och styrande dokument och uppdateringar av befintliga dokument ses löpande över och ingår också i ”årshjulet”.

Under hösten har ett arbete startats med att skapa digitala regionövergripande och regiongemensamma utbildningar inom informationssäkerhetsområdet. Tanken är att dessa ska vara obligatoriska med möjlighet att även följa upp deltagandet. Även Myndigheten för samhällsskydd och beredskap och Sveriges kommuner och regioner arbetar med att ta fram fler utbildningar och mer stödjande informationsmaterial inom informationssäkerhetsområdet som regionerna kommer att kunna använda sig utav.

Sammanfattningsvis pågår således flera viktiga övergripande aktiviteter som sammantaget kommer att bidra till att regionen kan fortsätta att utveckla det systematiska och riskbaserade informationssäkerhetsarbete som blir ännu viktigare med den kommande NIS2- lagstiftningen.

För Region Örebro län