REGION JÄMTLAND HÄRJEDALEN

IT- och eHälsoavdelningen
Marit Nilsson
Tfn: 063-147677
E-post: marit.nilsson@regionjh.se

2021-08-25

RS/338/2021

Svar på granskning av IT-säkerhet

Granskningsrapporten

KPMG under 2020 på uppdrag av de förtroendevalda revisorerna i Region Jämtland Härjedalen genomfört en granskning av regionens arbete med IT-säkerhet, , se dnr RS/338/2021. Granskningen har syftat till att svara på om regionens organisation och interna kontroll är ändamålsenlig gällande IT-säkerhet. Granskningen har utgått från följande frågeställningar;

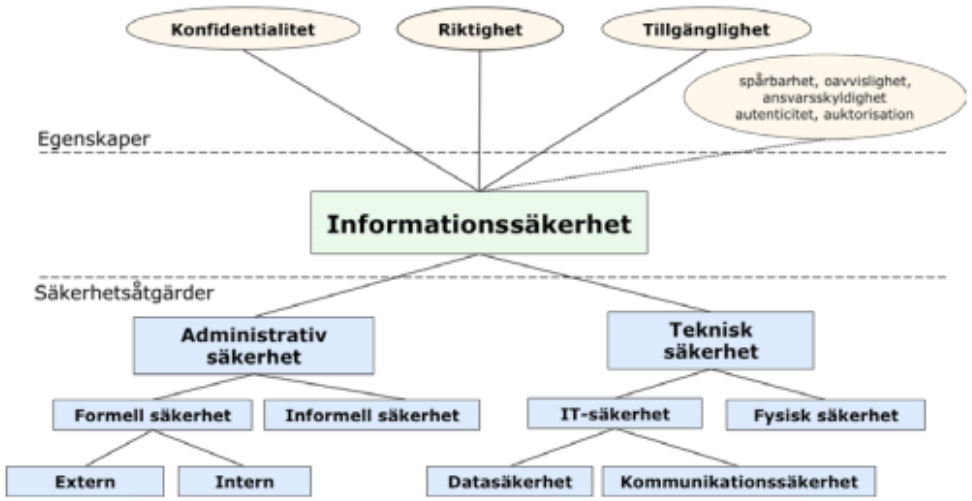
- Finns det en övergripande styrning av informations-och IT-säkerhet inklusive styrande dokument?
- Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?
- Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?
- Sker säkerhetsklassning av funktioner och tjänster?
- Finns ändamålsenliga rutiner för behörigheter och lösenord? Inkluderar även leverantörer av enskilda system.
- Har regionen en ändamålsenlig incidenthanteringsprocess?
  - Upptäcks och hanteras icke önskvärda incidenter både internt och externt?
  - Finns det rutiner för att säkerställa att nya risker och hot identifieras och hanteras?
- Är medborgarnas integritet säkerställd (patientdatalagen) och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?
- Är känsliga patientdata lagrade på ett säkert sätt, till exempel genom kryptering?
- Är det säkerställt att personal som hanterar lagring och hantering av känsliga uppgifter om enskilda patienter har den utbildning i informationssäkerhet som behövs utifrån tilldelade arbetsuppgifter?
- Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Granskningen har genomförts genom dokumentgranskning, intervjuer samt kartläggning av arbetsprocesser och rutiner för ett systematiskt informations-och IT-säkerhetsarbete.

Regionstyrelsens svar

Titeln på rapporten är Granskning av IT-säkerhet, vilket inte helt speglar rapportens innehåll. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk och IT-säkerhet ingår i den tekniska säkerheten.

Bilden nedan från Teknisk rapport SIS-TR 50:2015 Terminologi för informationssäkerhet, illustrerar vad som omfattas av begreppet informationssäkerhet.



Figur 1 – Informationssäkerhetsmodell

Informationssäkerhet handlar om att förhindra att information läcker ut, förvanskas eller förstörs. Det handlar också om att göra information lättillgänglig när den behövs och för rätt person. Begreppet omfattar information tryckt på papper, lagrad elektroniskt, som överförs per mejl eller post, visas på film eller yttras i en konversation.

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, men även tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd.

IT-säkerhet handlar om skydd av IT-system och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation. En viktig del av arbetet med IT-säkerhet handlar om att förstå olika hotbilder, hantera sannolikheter för att utsättas för skada samt att balansera kostnader för motmedel för skydd mot värdet av det man skyddar.

Huvuddelen av rapportens bedömningar och rekommendationer utgörs av informationssäkerhetens administrativa delar.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att avdelningar och områden tillsätter resurser och tar sitt ansvar för det systematiska informationssäkerhets-arbetet i enlighet med ledningssystemet för informationssäkerhet.

Regionstyrelsens svar: Uppdraget att tillsätta resurser för detta arbete är fördelat enligt verksamhetsplaneringen. Ansvaret har placerats på nivån förvaltningsområdeschefer och aktiviteter har fördelats till områdeschefsnivån.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att informations-klassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.

Regionstyrelsens svar: Regionen behöver arbeta aktivt med att peka ut informationsägarskap som följer informationen inom samtliga verksamhetskritiska processer samt inom de processer där känsliga uppgifter hanteras. Detta tydliggör ansvaret för att planera, genomföra och följa upp att informationsklassningar och tillhörande riskbedömningar utförs. Enligt övergripande handlingsplan för informationssäkerhet 2021-22 ska en prioritering utarbetas för att styra vilka verksamheter som ska utse informationsägare och etablera arbetssätten för denna roll.

Detta följer inriktningsmål 1 i ovan nämnda plan: ”Regionen har ett tydligt utpekat och utövat informationsägarskap för sina viktigaste informationstillgångar”.

Ansvaret för att informationsklassningar genomförs har placerats på nivån förvaltningsområdeschefer. Ansvaret för att kontinuitetsplaner (avbrottsplaner) har placerats på områdeschefsnivån.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.

Regionstyrelsens svar: För att uppnå en adekvat behörighetshantering, såväl i verksamhetsapplikationer som i IT-infrastrukturen, krävs att behörighetsrutiner upprättas och införs. För ändamålet har en mall som underlättar dokumentationen av dessa rutiner tagits fram under 2020 och testats för att dokumentera rutiner till några system. Ambitionen är att successivt införa en enhetlig och styrd hantering av behörigheter där samhällsviktiga IT-system/resurser kommer att prioriteras. Det kommer också att krävas att merparten av regionens behörigheter kan styras från en central behörighetskälla, något som ännu inte har införts. Denna centrala källa bedöms också kunna förenkla uppföljningen av behörigheter i hög grad.

Det pågår dock utveckling och tester av en portal för hantering av behörigheter. Portalen ska förenkla behörighetstilldelning för chefer och behörighetsbeställare samtidigt som krav baserat på bl a GDPR tillgodoses. Ytterligare automatisering ska ske av behörighets-tilldelning och verksamheten ska få möjlighet till snabbare leveranser av behörigheter så att nyanställda och inhyrda personer kommer i arbete utan väntetider och med liten administrativ insats. Säkerheten ska höjas genom att få bättre kontroll av befintliga behörigheter och säkrare/godkänd tilldelning av nya behörigheter.

Det pågår även en översyn av behörighetshanteringen i regionens journalsystem COSMIC. I december 2020 övergick det från en lokal behörighetstilldelning med administratörer på enhetsnivå till central behörighetstilldelning som utförs av Servicecenter. En majoritet av alla behörigheter sker nu centralt och arbete fortgår för att lyfta över kvarvarande behörigheter. I slutet av 2020 gick Integritetsskyddsmyndigheten ut med en granskning av hur åtta vårdgivare styr sin behörighetstilldelning till vårdinformationssystem, vilket lett till sanktionsavgifter för berörda parter. Det har lett till att processen kring behörighets-tilldelning har setts över och just nu pågår ett arbete med att utveckla processen för att säkerställa att lagar efterlevs. Ett steg i den processen är att säkerställa att behovs- och riskanalys utförs i samband med behörighetstilldelning.

Revisorerna rekommenderar Regionstyrelsen att: Riskanalyser upprättas regelbundet för IT-infrastruktur och drift.

Regionstyrelsens svar: IT-enheten har förstärkts med 1,0 tjänst som IT-säkerhetsspecialist, via statlig finansiering. Tjänsten blir en del av regionens funktion för IT-säkerhet med uppgift att:

- Stödja verksamheterna med specialistkompetens avseende IT-säkerhet (tekniska risk-analyser, granskningar, kravställning, säker IT-arkitektur etc)
- Identifiera risker och sårbarheter i IT-miljö samt bistå med åtgärdsförslag
- Förvalta införda IT-säkerhetssystem
- Inhämta och delge relevanta underrättelser
- Ta fram utbildningsmateriel och utbilda

Regionen har även förstärkt med 2, 0 Tjänsteansvariga för server och IT-arbetsplats samt för datornätverk. Ansvaret att genomföra riskanalyser ligger på Tjänsteansvariga/ systemansvariga. IT-säkerhetsspecialister är en av flera resurser som deltar i genomförandet av riskanalyser. Det innebär en förstärkning med två tjänsteansvariga och en IT-säkerhetsspecialist, totalt tre resurspersoner som del av tid kan arbeta med riskanalyser.

Revisorerna rekommenderar Regionstyrelsen att: Upprätta en riskanalys över att privata enheter kan ansluta via fjärraccess till regionens IT-miljö och utifrån dessa risker fatta beslut om relevanta åtgärder för att möta dessa.

Regionstyrelsens svar: IT-enheten har pågående uppdrag att undersöka kostnadseffektiva regionägda alternativ. Uppdraget utökas med att upprätta efterfrågad riskanalys.

Revisorerna rekommenderar Regionstyrelsen att: Uppdatera kontinuitetsplan för IT-driften.

Regionstyrelsens svar: Upphandling av nya leverantörer av IT-drift har avslutats under våren och nu pågår arbetet med övertagande och etablering. Revidering av kontinuitets-planer startar i samverkan med de nya leverantörerna efter att övertagandeprojekten slutförts.

Revisorerna rekommenderar Regionstyrelsen att: Besluta om regionövergripande rutin för incidenthantering och rapportering för informationssäkerhetsincidenter samt

kommunicera denna till verksamheterna.Det behöver även säkerställas att en uppföljning sker av samtliga inträffade incidenter så att dessa kan beaktas i förbättringsarbetet.

Regionstyrelsens svar: Rapportering av informationssäkerhetsincidenter ska ske inom ramen för den ordinarie avvikelsehantering som regionen har. I den obligatoriska e-utbildningen för medarbetare gällande informationssäkerhet lärs ut vad som ska identifieras och rapporteras som en informationssäkerhetsincident. Ett förtydligande ska tas fram gällande rutinen för hur uppföljning ska ske av rapporterade incidenter/avvikelser inom informations- och IT-säkerhet och vem som ansvarar för vad. Något ytterligare arbete är inte planerat inom detta område.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.

Regionstyrelsens svar: Under 2021 införs internkontrollpunkter gällande riskarbetet inom informationssäkerhet och dataskydd. Dessa är riktade mot områdeschefer. För 2022 kommer ytterligare internkontrollpunkter att införas till förvaltningsområdeschefer samt divisionschefer.

REGIONSTYRELSEN

Eva Hellstrand (C)
Regionstyrelsens ordförande

Hans Svensson
Regiondirektör