Landstinget i Värmland

Landstings-IT
Handläggare och telefon
Mikael Borén, 054-61 91 01

Datum
2016-10-10
Ert datum
2016-04-12

Vår beteckning
LK/161169
Er beteckning
REV/15041

Landstingets revisorer

Svar på revisionsrapport om IT-säkerhet

Landstingsstyrelsen vill avge följande svar på rubricerad revisionsrapport. Den övergripande revisionsfrågan är att bedöma om det finns ett behov av och förutsättningar för att genomföra en fördjupad granskning avseende landstingets arbete med att tillskapa och upprätthålla en tillräcklig IT-säkerhet.

Revisorernas samlade bedömning är att:

- Landstingsstyrelsen uppvisar medvetenhet om vad de i sina styrdokument benämner som IT-säkerhet. Det gör de genom att framför allt säkerställa att en informationssäkerhetspolicy finns antagen och beslutad av landstingsfullmäktige.

I rapporten lämnar revisorerna följande rekommendationer:

1. *Styrdokumenten (policydokument och därtill hörande tillämpningsföreskrifter) behöver förtydligas, uppdateras och kompletteras för att fortsatt bilda verkningsfull grund för bland annat vad som kan kallas IT-säkerhet. Det arbetet noterar revisorerna har återupptagits mer aktivt än tidigare i och med att en informationssäkerhetsansvarig anställdes i september 2015.*

Som revisorerna noterar så pågår ett arbete i samverkan mellan Informationssäkerhetsansvarig och IT-säkerhetsansvarig med att uppdatera styrdokument. Den kommande Dataskyddsförordningen kommer utöver detta att medföra en större översyn av styrdokument inom området.

Sammantaget noterar styrelsen att det påbörjats flera aktiviteter inom området för att höja kvalitén på styrdokument.

Postadress
Landstinget i Värmland
651 82 Karlstad

Besöksadress
Rosenborgsgatan 50

Telefon (växel)
054-61 50 00
Telefax

E-postadress
johanna.orre@liv.se
Organisationsnummer
232100-0156

2. *En väsentlig aktivitet i uppdateringen av styrdokumenten är att utföra analyser (verksamhetsanalys, riskanalys och en GAP-analys), få informationen klassad och tydliggöra för verksamhetenschefer att de har det yttersta praktiska ansvaret för informationssäkerheten. Landstingsstyrelsen bör tillse att detta även innebär återkommande utbildning av och/eller information till alla delar av verksamheten.*

Landstinget arbetar aktivt inom området IT- och informationssäkerhet och har inom området riskanalys och riskbedömning i många fall kommit längre än övriga landsting. Styrelsen noterar att det finns en välfungerande process där IT- och informationssäkerhet samverkar i riskanalys och riskbedömning i samband med att nya system och tjänster införs.

Ett arbete med att klassificera system utifrån informationsinnehåll och hur kritiskt systemet är för att verksamheten skall fungera har initierats inom PM3-förvaltningen.

3. *Landstingsstyrelsen bör förbättra och tydlig ange hur de vill få arbetet med informationssäkerheten rapporterad till sig. I samband med detta kommer det att underlätta för praktiskt ansvariga om styrelsen också anger på vilket sätt detta kommer att nå medborgarna.*

I den årliga informationssäkerhetsrapporten sammanställs både informations-säkerhetsincidenter och IT-säkerhetsincidenter.

4. *Det finns motiv för revisorerna att fortsättningsvis på olika sätt innefatta informationssäkerhet i kommande granskningar.*

Som framkommit ovan så har ett antal aktiviteter påbörjats för att ytterligare höja kvalitén inom området. Detta i kombination med den kommande Dataskyddsförordningen gör att styrelsen bedömer att en revison av området informationssäkerhet som helhet bör genomföras inom 18-24 månader.

I rapporten nämns även införandet av ett loggverktyg och styrelsen ger i uppdrag till objektägare verksamhet och IT inom patientjournal att utvärdera införandet inom 6-12 månader.

Sammantaget anser styrelsen att rapporten ger en rättvis och sammanfattande bild av områdets nuläge.

En utmaning i rapporten är att de frågor den adresserar är inom IT-säkerhet medans resultatet i rapporten till större delen rör informationssäkerhet. Styrelsen tycker dock att revisionen hanterat detta bra.

Övrigt:

I rapportens avsnitt 6 nämns att landstingets organisation där IT-säkerhet är underordnad Informationssäkerhet och att detta skulle vara unik för Landstinget i Värmland.

Styrelsens omvärldsanalys visar på att detta är en vedertagen praxis och inget unikt jämfört med övriga Landsting.

I kapitel 6.1.2 så tolkar styrelsen som att en övergripande riskanalys för Landstinget i Värmlands hela IT-miljö bör genomföras. Någon sådan finns inte idag. Och styrelsen är frågande till hur denna skulle användas för styrning inom området?

Den incident i Cosmic som nämns i rapporten har det genomförts en omfattande händelseanalys för och lämnat förslag på åtgärder. Och händelse-analysen visar på att orsaken var beroende av dels konfiguration och dels på beslut om arbetssätt i verksamheten.

Det kan även nämnas att i samband med incidenter/avvikelser genomförs händelseanalys och resultatet från dessa tas om hand om och förbättringsåtgärder genomförs.

Landstingsstyrelsen

Fredrik Larsson
Ordförande

Gunilla Andersson
Landstingsdirektör