DNR: 3.1.2-2015-0612

LÄNSSTYRELSEN I VÄSTRA GÖTALANDS LÄN BESLUT: 2015-10-20

403 40 GÖTEBORG

Brister i ledning och styrning av informationssäkerhet för länsstyrelserna

Riksrevisionen har som ett led i den årliga revisionen av länsstyrelsen i Västra Götalands län granskat ledning och styrning av informationssäkerhet för länsstyrelserna.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa länsstyrelsens uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2015-11-19 med anledning av våra iakttagelser i denna rapport.

Efter uppdrag i regleringsbrev 2008 har länsstyrelserna etablerat en gemensam IT-enhet, LstIT, med länsstyrelsen i Västra Götaland som värdmyndighet. LstIT ansvarar för drift och IT-säkerhet av den gemensamma IT-miljön i enlighet med de riktlinjer som beslutas för LstIT av länsstyrelserna. Dock är ansvaret för informationssäkerheten varje länsstyrelses ansvar (informationssäkerhet är ett vidare område än IT-säkerhet) [1]. Vi har valt att granska ledning och styrning av informationssäkerhet pga. tidigare observerade brister samt att informationssäkerhet är en viktig del i den övergripande kontrollmiljön för en myndighet. Brister i informationssäkerhet kan också påverka årsredovisningen. Detta visade sig bl.a. för flera länsstyrelser under arbetet med årsredovisningen 2014, då för arbetet viktiga Word-filer inte fanns tillgängliga under ett antal dagar p.g.a. hårdvarufel samt att informationen inte var tillräckligt högt prioriterad i kontinuitetshänseende. Granskningen har genomförts via intervjuer av företrädare för LstIT och länsrådet i Västernorrland, Sten-Olov Altin samt dokumentstudier.

[1] Definition av informationssäkerhet:

Informationssäkerhet omfattar både administrativa och tekniska aspekter med avseende på konfidentialitet, riktighet och tillgänglighet av informationstillgångar. Som komplement till dessa tre aspekter används bland andra även begreppet spårbarhet.

Med informationstillgångar menas både information, elektronisk eller i annan form, och de resurser som används för att hantera informationen. Informationssäkerhet handlar därmed om mer än att säkra informationssystem. Även andra resurser, inte minst människors förmåga, är viktiga komponenter i informationssäkerhetsbegreppet.

403 40 GÖTEBORG

Vi noterar att länsstyrelserna arbetar med frågorna men att ledning och styrning av informationssäkerhet fortfarande är oklar inom länsstyrelserna. Beslut om prioriteringar, medel till utveckling samt uppföljning är tänkt att delas av samtliga länsstyrelser men att formerna för detta, sedan bildandet av LstIT, är oklara. De oklarheter som finns rörande beslut- och uppföljning av IT- och informationssäkerhet inom länsstyrelserna innebär också att det är otydligt vem som ska fatta vilka beslut samt följa upp informationssäkerheten.

För informationssäkerhet gäller ”svagaste-länk-resonemanget”. Länsstyrelserna har ett delat ansvar som kräver att samtliga länkar i kedjan håller – detta för att inte utsätta verksamheten för onödiga risker. I övrigt bör länsstyrelserna stärka medvetandet om vilka risker som finns rörande informationssäkerhet, samt vidta de åtgärder som är möjliga och prioriterade för att informationssäkerheten ska hålla så god kvalitet som möjligt. Detta kräver fortlöpande analys och beslut då riskbilden varierar över tid och nya risker tillkommer. En förutsättning för detta är också att frågorna prioriteras tillräckligt högt av respektive länsledning.

I dagsläget är läget följande:

- Det saknas en klar ordning för vad som ska prioriteras vid utveckling/förvaltning av IT-system. Även prioritering av vilka behov som bör åtgärdas först saknas.

- Uppföljning av informationssäkerhetens status har inte genomförts för länsstyrelserna som kollektiv. Dvs. brister och förbättringsbehov är inte kända vilket gör det svårt att fatta rätt beslut om åtgärder. Terrängen och kartan är till del okänd vad gäller länsstyrelsernas brister rörande informationssäkerhet. LstIT genomför under hösten en ”gapanalys” avseende länsstyrelsen i Västra Götaland för att se vad som behöver åtgärdas för att uppfylla kraven på ett ledningsinformationssystem (LIS) för IT-säkerheten. Men denna analys avser således inte samtliga länsstyrelser och avser inte informationssäkerhet. Då kunskapen om informationssäkerhetens status saknas för länsstyrelserna som helhet, finns brister i beslutsunderlaget som också gör det svårt för länsstyrelserna att kunna prioritera rätt åtgärder för utveckling och förvaltning.

- Ingen heltäckande informationsklassning har genomförts för all information inom länsstyrelserna. Informationsklassning är ett grundkrav för att kunna säkerställa att IT-tillgångar och andra handlingar hanteras på ett tillräckligt säkert och kostnadseffektivt sätt utifrån handlingens eller informationens art och känslighet. I dagsläget hanteras all information som inte avser rikets säkerhet på samma nivå vilket skulle kunna medföra att viss information har för högt eller lågt skydd. Informationsklassning är också viktigt då det hjälper personalen att hantera informationen på lämpligt sätt.

DNR: 3.1.2-2015-0612

LÄNSSTYRELSEN I VÄSTRA GÖTALANDS LÄN BESLUT: 2015-10-20

403 40 GÖTEBORG

- Länsstyrelserna uppfyller därmed inte de krav Myndigheten för samhällsskydd och beredskap (MSB) har ställt upp för informationssäkerhet (MSBFS 2009:10). Dessa krav anger att en myndighet i arbetet med att upprätthålla säkerhet i sin informationshantering ska tillämpa ett LIS. De brister länsstyrelserna har i dagsläget rör främst punkterna om att klassificera information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. Utifrån risk- och sårbarhetsanalyser samt inträffade incidenter bör länsstyrelserna avgöra hur risker lämpligen bör hanteras. Länsstyrelserna bör därefter tydligt besluta om åtgärder för att förbättra informationssäkerheten samt dokumentera de granskningar och säkerhetsåtgärder av större betydelse som genomförs. Myndigheternas ledning bör löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet. Det sistnämnda bör genomföras för respektive länsstyrelse men även för länsstyrelserna som kollektiv, inkl. LstIT, p.g.a. den organisation länsstyrelserna har för IT- och informationssäkerhetsfrågor.

Rekommendation

Styrningen av länsstyrelsernas kollektiva informationssäkerhet, inkl. LstIT, bör förbättras för att åstadkomma en tydligare struktur och ansvar för informationssäkerhetsfrågorna. Beslutsfattandet kring länsstyrelsegemensamma IT- och informationssäkerhetsfrågor bör förtydligas. Vi ser ett starkt behov av att länsstyrelsernas ledning och styrning av informationssäkerheten förtydligas och konkretiseras i praktiken, så att ansvar och befogenhet klart framgår. En informationsklassning bör göras för att säkerställa att all information skyddas på ett tillräckligt säkert och kostnadseffektivt sätt. Länsstyrelserna bör årligen följa upp informationssäkerhetens kvalitet för respektive länsstyrelse men även för kollektivet länsstyrelserna med LstIT. Utifrån detta underlag bör relevanta åtgärder för utveckling och förvaltning av system m.m. fattas.

Ansvarig revisor Arne Månberg har beslutat i detta ärende. Uppdragsledare Annika C. Karlsson har varit föredragande.

Arne Månberg Annika C Karlsson

Kopia för kännedom:

Regeringen
Finansdepartementet
Finansdepartementet, budgetavdelningen