Västerbottens läns landsting

MISSIV 1 (3)

2017-11-09 REV 26:3–2017

Landstingsstyrelsen och
Hälso- och sjukvårdsnämnden

Granskning av IT-systemens robusthet

Landstingets revisorer har i flera granskningar uppmärksammat brister i kontrollen av landstingets IT- och informationssäkerhet (nr 23/2010, 17/2014, 22/2014 och 18/2015). En uppföljande granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har vidtagit tillräckliga åtgärder med anledning av revisorernas rekommendationer. Endast fyra av 20 lämnade rekommendationer har blivit helt genomförda.

En slutsats från den uppföljande granskningen är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en tillräcklig styrning, uppföljning och kontroll av IT- och informationssäkerheten inom deras ansvarsområden:

- Fullmäktige har inte givits möjlighet att ta ställning till en policy för arbetet med informationssäkerhet i landstinget. I landstinget saknas en sådan policy.
- Det finns inga landstings- och nämndsövergripande riskanalyser inom området för informationssäkerhet.
- Riktlinjer och regler för informationssäkerhet har inte kommuniceras till berörda medarbetare i landstinget.
- Det saknas en tillräcklig uppföljning och kontroll av att verksamheterna följer riktlinjer och regler för informationssäkerhetsarbetet.

Nedan återger vi några konkreta brister som granskningsrapporten identifierat:

- Det saknas en komplett förteckning över landstingets informationssystem.
- För samtliga av landstingets verksamhetskritiska system finns det inte informationsklassning och beslut om längsta acceptabla tid som systemen kan få vara ur funktion. Det saknas också beslut om vilken prioriteringsordning som ska gälla vid återstart i händelse av IT-avbrott.
- Det saknas systematik som säkerställer att det görs regelbundna kontroller över anställdas behörigheter till IT-system.

Västerbottens läns landsting
Landstingshuset, Köksvägen 11, 901 89 Umeå
Telefon: 090-785 00 00, telefax: 090-13 68 82
E-post: landstinget@vll.se Org.nr: 232100-0222
VAT-nr: SE232100022201 Bankgiro 5728-3061

- Det saknas beslut om vilka kriterier som ska gälla för serverhallarnas fysiska säkerhet. Det saknas också periodiska kontroller av tillträde till serverhallar och servrar och inloggningar i databaser.
- Det har under en lång tid inte genomförts några penetrationstester av landstingets IT-system.
- Landstingets personuppgiftsombud och informationssäkerhetsstrateg saknar dokumenterade uppdragsbeskrivningar.

Rekommendationer

Med anledning av granskningens iakttagelser rekommenderar vi landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa:

- Att fullmäktige får ta ställning till ett förslag på informationssäkerhetspolicy för landstinget. Förslaget till policyn bör bland annat inkludera styrelser och nämnders ansvar för informationssäkerhet, inriktning och övergripande mål för informationssäkerhet samt struktur för riskbedömning och riskhantering.
- Att det på landstings- och nämndsövergripande nivå och bland verksamheterna finns riskanalyser för informationssäkerhetsområdet.
- Att riktlinjer och regler för informationssäkerhet är väl kända bland berörda medarbetare i landstinget.
- En tillräcklig uppföljning av informationssäkerhetsarbetet inom sina ansvarsområden.
- Att tidigare lämnade rekommendationer blir genomförda. Exempelvis:
    - Att det genomförs regelbundna kontroller av anställdas behörigheter.
    - Att det fattas beslut om vilken prioritetsordning som ska gälla vid återstart i händelse av avbrott i IT-systemen.
    - Att det finns en förteckning över landstingets samtliga informationssystem där det framgår vilka av dessa som är att betrakta som kritiska för verksamheten.
    - Att det finns beslut om vilka kriterier landstingets serverhallar ska uppfylla avseende fysisk säkerhet men även att säkerheten i de befintliga hallarna höjs till dess att andra lokaler finns tillgängliga.

- Att övriga i granskningen uppmärksammade brister blir åtgärdade. Exempelvis:
    - Att beslut om längsta acceptabla tid som informationssystem kan vara ur funktion fattas för alla verksamhetskritiska system.
    - Att kontroller av programförändringar i IT-systemen genomförs.
    - Att periodiska kontroller av användare med access till servrar och databaser genomförs.

- Att det görs kontroller av inloggning till och aktivitet i servrar och databaser.
- Att det genomförs penetrationstester.
- Att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar.

Vid revisorernas överläggning den 9 november 2017 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 3/2017) lämnar revisorerna för yttrande till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 2 mars 2018.

För landstingets revisorer

Christer Fessé
Ordförande

Bert Öhlund
Vice Ordförande