

Landstingsrevisionen

Landstingets revisorer

Landstingsstyrelsen

Granskning av IT-säkerheten inom Landstinget i Jönköpings län

Landstingets revisorer har under 2005 granskat IT-säkerheten inom Landstinget i Jönköpings län. Motivet är att landstinget hanterar många känsliga uppgifter och brister i IT-säkerheten kan ge allvarliga konsekvenser såväl för landstinget som för enskilda personer.

Det övergripande syftet med granskningen har varit att översiktligt granska landstingets IT-säkerhet samt att följa upp tidigare genomförda granskningar inom detta område.

I granskningen ingår bl a att kontrollera regler och stöddokument, ansvarsförhållanden, behörighetshantering, backuptagning och förvaring samt driftsäkerhet. Inom ramen för granskningen har också intrångstester genomförts både externt och internt. Säkerheten i enskilda system har däremot inte granskats.

Granskningen har, med undantag av intrångstesterna, gjorts som en intervju- och dokumentstudie kompletterad med fysisk besiktning av datorrum.

Intervjuer har genomförts med ansvarig personal inom IT-Centrum och de tre sjukvårdsområdena. Frågor har även ställts till användare och ansvariga via webbaserade formulär.

Resultatet av granskningen, som genomförts av Öhrlings PriceWaterhouseCoopers/Komrev, framgår av bifogad revisionsrapport. Resultatet från genomförda intrångstester har muntligen redovisats för revisorerna och landstingsdirektören.

Nedan lämnas revisorernas kommentarer med anledning av rapporten.

Pågående åtgärder måste tidplaneras och slutföras

Landstingets revisorer konstaterar att resultatet av flertalet utförda kontroller bedöms som tillfredsställande, men att vissa brister konstaterats inom områden där förbättringsåtgärder samtidigt pågår. Inom dessa områden, som redovisas i rapporten, anser revisorerna att tidplaner med tydliga sluttidpunkter för åtgärderna måste utarbetas.

Ansvarsfördelning, roller, samordning m m tydligt dokumenterade men efterlevs inte

Revisorerna noterar i granskningen att landstinget på ett föredömligt sätt dokumenterat ansvarsfördelning, befogenheter och arbetsinnehåll för övervakning och utveckling av landstingets IT-säkerhet i en PM dat 2000-06-08. En PM som fastställts av landstingsstyrelsen 2000-12-12.

I granskningen framkommer bl a att samordningen av IT-säkerhetsarbetet inte fungerar optimalt och att rollen som övergripande IT-säkerhetsansvarig är otydlig.

Till den redovisade otydligheten bidrar både IT-säkerhetsansvarigs dubbelfunktion/-roll som IT-säkerhetshandläggare för IT-Centrum och i granskningen redovisad aktuell arbetsfördelning mellan landstingsdirektör, IT-direktör och IT-säkerhetsansvarig. Denna arbetsfördelning skiljer sig i nuläget på vissa punkter från av landstingsstyrelsen fastställd PM.

Landstingets revisorer anser det viktigt att landstingsstyrelsen ser till att fastställda policydokument och riktlinjer efterlevs och att rollen som landstingets IT-säkerhetsansvarig tydliggörs.

Revisorerna har i tidigare granskningar framfört att funktionen/rollen som landstingets övergripande IT-säkerhetsansvarig bör ha en tydligare och mer oberoende utformning. Denna rekommendation kvarstår och förstärks genom iakttagelserna i denna granskning.

Stort antal dokument och riktlinjer men svåröverskådligt

I granskningen redovisas att landstinget både centralt och på förvaltningsnivå har många bra styrande och stödjande dokument. Exempel på detta är säkerhetspolicy, Internetpolicy samt olika riktlinjer och rutinbeskrivningar inom IT-säkerhetsområdet.

Revisorernas iakttagelse är att denna samling dokument är svåröverskådlig och därmed finns en risk att dokumenten inte fyller sitt syfte. Ett exempel på detta i genomförd granskning är landstingets Internetpolicy som inte är tillräckligt känd inom organisationen. Av 81 tillfrågade chefer på olika nivåer uppger över 30 % att man inte tagit del av denna policy.

Landstingets revisorer rekommenderar landstinget att se över både de dokument som finns och hur de ska kommuniceras till ansvariga och användare. Det är också viktigt att en uppföljning sker av att gällande policydokument efterlevs (t ex Internetpolicyen).

Skydd för obehörigt tillträde till datorer och information kan förbättras

Landstingets revisorer konstaterar att granskningen även visar på flera åtgärder som kan vidtas för att förbättra skyddet för obehörigt tillträde till datorer och information. Några av dessa fanns också med i revisorernas tidigare granskning.

Bland de åtgärder som fanns med i tidigare granskning kan nämnas rekommendationer, dels att mer rutinmässigt via intrångstester säkerställa att landstingets brandväggar och andra resurser fungerar på ett tillfredsställande sätt, dels att anskaffa system för att enklare kunna upptäcka försök till obehörigt tillträde till datorer och information från både externt och internt håll.

Revisorerna vill understryka vikten av att föreslagna förbättringsåtgärder beaktas och ges en hög prioritet i arbetet med att förbättra skyddet för obehörigt tillträde till både datorer och information.

2005-11-15

LK05-0359

Övrigt

Överläggningar har ägt rum med landstingsdirektören som inhämtat synpunkter från IT-direktören. Från överläggningarna noteras att både rekommendationerna i granskningsrapporten och från genomförda intrångstester uppfattas som värdefulla och kommer att beaktas i pågående översyn och utvecklingsarbete vad gäller IT-säkerheten i landstinget.

Landstingets revisorer översänder rapporten med hemställan om landstingsstyrelsens yttrande och kommentarer med anledning av de förtroendevalda revisorernas synpunkter.

Yttrandet bör lämnas till revisorerna **senast 2006-02-03**.

För landstingets revisorer

Arnold Carlzon
Ordförande

Stig Andersson
Vice ordförande