Revisionsrapport

RIKSREVISIONEN

Affärsverket Svenska Kraftnät
Box 526
162 15 Vällingby

Datum 2009-01-20
Dnr 32-2008-0607

Löpande granskning av Affärsverket Svenska Kraftnät 2008

Riksrevisionen har som ett led i den årliga revisionen av Affärsverket Svenska Kraftnät granskat hanteringen av vissa samhällsviktiga system och övergripande styrning av IT- verksamheten, investeringar, systemintäkter samt den nya förordningen om intern styrning och kontroll.

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

Riksrevisionen önskar information senast 2009-03-16 med anledning av våra iakttagelser.

Sammanfattning

Riksrevisionen granskade under 2005 och 2006 Svenska Kraftnäts styrning av informationssäkerhetsarbetet (revisionsrapport 32-2005-0714, daterad 2006-02-13 samt revisionsrapport 32-2006-0700, daterad 2007-02-15). I rapporterna framförde Riksrevisionen ett antal iakttagelser som berörde informationssäkerhetsområdet, bl.a. avseende riskhantering, upprättande av systemsäkerhetsplaner samt kontinuitetsplanering.

Den granskning som genomförts under hösten 2008 visar att Svenska Kraftnät behöver vidta ytterligare åtgärder inom ovan nämnda områden. Vidare anser Riksrevisionen att Svenska Kraftnät bör tydliggöra kopplingen mellan verksamhetsstyrning och styrning av IT-verksamheten samt genom beslutade inriktningsdokument tydliggöra målen för IT-verksamheten. Detta är en förutsättning för att kunna utvärdera om IT-verksamheten lever upp till verksamhetens mål. En sådan utvärdering försvåras dock i dagsläget ytterligare av de iakttagelser som framförs nedan:

- ansvar för att åtgärda väsentliga risker enligt riskanalys är inte dokumenterat
- strukturerad process för utvärdering och test av kontinuitetsplaner är inte fastställd
- dokumenterad uppföljning av serviceöverenskommelser mellan verksamhet och IT-avdelning saknas

Styrning av IT-verksamheten

Riksrevisionen har vid granskningen inte kunnat identifiera några av ledningen (styrelsen) fastställda och dokumenterade mål och styrdokument för IT- avdelningen. Det går inte heller att tydligt utläsa vilka Svenska Kraftnäts övergripande prioriteringar inom området är. Svenska Kraftnät upprättar ingen årlig verksamhetsplan, utan det inriktningsdokument som gäller för IT-verksamheten är en intern IT-plan som upprättats av IT-avdelningen, men som alltså inte beslutats av ledningen.

Riksrevisionen *rekommenderar* att Svenska Kraftnäts ledning på ett tydligare sätt dokumenterar de kortsiktiga och långsiktiga mål som ska gälla för IT-verksamheten, samt hur ledningen avser att följa upp dessa mål.

Riskanalyser

Riksrevisionen har vid granskningen tagit del av riskanalyser för samtliga system som Svenska Kraftnät bedömt som samhällsviktiga. Beslutet om vilka system som är samhällsviktiga fattades av dåvarande generaldirektör 2005. Enligt de uppgifter Riksrevisionen fått har någon formell förnyad prövning av vilka system som ska bedömas som samhällsviktiga därefter inte gjorts. Enligt uppgift från Svenska Kraftnät kommer ny sådan prövning att göras under 2009.

Risker för de aktuella systemen har identifierats och värderats av personal från såväl IT-avdelningen som från verksamhetsansvariga. Riskanalysen är upprättad efter en traditionell metod. Beroende på hur man bedömer sannolikheten för att händelsen skall inträffa samt vilka konsekvenserna blir väljer man att antingen vidta åtgärder för att motverka risken eller att låta risken kvarstå. I det fall man väljer att vidta åtgärder bör det utses en person som ansvarar för detta samt anges vilken tidsram som gäller för detta.

I de riskanalyser Riksrevisionen tagit del av finns ett stort antal identifierade risker beskrivna och värderade. Det framgår dock inte av riskanalyserna vilka åtgärder som ska vidtas, vem/vilka som är ansvariga för att vidta åtgärder och när de ska vara klara. Det framgår inte heller hur uppföljning ska göras som säkerställer att fungerande åtgärder faktiskt har vidtagits. Enligt uppgift har Svenska Kraftnäts IT säkerhetsråd nu begärt att en handlingsplan arbetas fram för respektive system under 2009.

Riksrevisionen *rekommenderar* att Svenska Kraftnät kompletterar den nuvarande riskanalysprocessen med att tydliggöra hur identifierade risker ska åtgärdas och vem som ansvarar för att genomföra åtgärderna, samt vilken tidsplan som gäller.

Kontinuitetsplanering

Kontinuitetsplaner finns enligt uppgift upprättade för de samhällsviktiga systemen vid Svenska Kraftnät. Syftet med kontinuitetsplanen är att säkerställa att verksamheten kan fortgå vid olika typer av driftsstörningar, genom att ange alternativa sätt att driva verksamheten till dess att störningarna har avhjälpts. I syfte att säkerställa att kontinuitetsplanerna verkligen fungerar bör de regelbundet utvärderas, uppdateras och testas med avseende på sin funktionalitet.

Enligt de uppgifter Riksrevisionen fått vid granskningen genomförs det i dagsläget ingen systematisk uppföljning eller test av att planerna fungerar.

Riksrevisionen *rekommenderar* att Svenska Kraftnät tydliggör vilka rutiner och vilken regelbundenhet som ska gälla för utvärdering och test av befintliga kontinuitetsplaner. Detta för att ledningen med rimlig grund ska kunna bedöma verksamhetens möjlighet att hantera driftsstopp eller andra störningar i verksamheten.

Fastställande av servicenivåer

Som nämnts ovan redovisade Riksrevisionen vid granskningar 2005 och 2006 synpunkter på att det saknades systemsäkerhetsplaner för ett antal system vid Svenska Kraftnät. Den information som tidigare avsågs hanteras i systemsäkerhetsplanerna, hanteras numera i SLA (Service Level Agreements). Syftet med SLA är att beställare (verksamheten) och utförare (t.ex. IT-avdelningen) dokumenterar en överenskommelse om vilka tjänster som ska levereras, vilka krav på service och support som kan ställas etc.

Riksrevisionen har tagit del av samtliga SLA som upprättats för de samhällsviktiga systemen, utom ett system för vilket SLA ännu inte upprättats. I de SLA Riksrevisionen tagit del av anges dels ett antal mål för den tjänst IT-avdelningen ska leverera, dels anges i flera SLA även att vissa säkerhetsaspekter ska specificeras och mätas i särskild ordning. I IT-planen för 2008 framhålls särskilt vikten av mätning och rapportering av uppfyllanden av SLA.

Riksrevisionen har vid genomförd granskning inte erhållit någon dokumenterad uppföljning från 2008 av att det som avtalats i SLA:erna har genomförts. Enligt uppgift har dock återredovisning från IT-avdelningen gjorts muntligen vid s.k. förvaltningsmöten. Avseende säkerhetsmätning har Svenska Kraftnät muntligen angett att sådan kommer att genomföras under 2009.

Riksrevisionen *rekommenderar* att Svenska Kraftnät tydliggör vilka rutiner och vilken regelbundenhet som ska gälla för dokumenterad uppföljning av

SLA:erna. En tydlig dokumenterad uppföljning möjliggör för ledningen att erhålla en samlad analys av den servicenivå som IT avdelningen tillhandahåller gentemot verksamheten.

Ansvarig revisor Göran Selander har beslutat i detta ärende. Uppdragsledare Anne Bryne har varit föredragande. IT revisor Frank Lantz har medverkat i den slutliga handläggningen.

Göran Selander Anne Bryne

Kopia för kännedom:
Regeringen