Affärsverket Svenska Kraftnät
Box 526
162 15 Vällingby

Datum 2006-02-13
Dnr 32-2005-0714

Löpande granskning av Affärsverket Svenska Kraftnät 2005

Riksrevisionen har som ett led i den årliga revisionen av Affärsverket Svenska Kraftnät (SvK) granskat ledningssystemet för informationssäkerhet (LIS), projektredovisning och redovisningen av effekt- och energiavgifter.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa SvK:s uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2006-03-08 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

Avsaknad av dokumenterad riskanalys på aggregerad nivå gör att det för Riksrevisionen är oklart hur SvK kontinuerligt bedömer och tar om hand de risker och hot som finns i verksamheten. Sannolikt påverkar detta SvK:s möjlighet att göra en realistisk bedömning om systemen i dagsläget har ett relevant skydd. Detta intryck förstärks ytterligare av att resultaten av faktiskt genomförd granskning i enstaka system inte dokumenteras i systemsäkerhetsplaner. SvK har heller inte i kontinuitetsplaner visat att verksamhetskritiska system skyddas på ett sådant sätt att man kan försäkra sig om god säkerhet och tillgänglighet.

Väsentliga dokument saknas i flera av de arkiverade projektakterna samtidigt som det råder osäkerhet inom SvK vad som faktiskt ska diarieföras. För Riksrevisionen är det oklart hur SvK tillförsäkrar sig god översikt och kontroll över de projekt som har bedrivits.

SvK nettoredovisar betalningarna avseende energiavgiften, dvs. i de fall SvK betalar till en kund redovisas detta som en negativ intäkt. Nettobeloppet redovisas under rörelseintäkter i resultaträkningen. Konsekvensen blir att SvK:s rörelseintäkter visar ett för lågt belopp om ca 300 mnkr på årsbasis.

1. Informationssäkerhet

1.1 Inledning

Informationssäkerhet är väsentlig eftersom de flesta myndigheters och affärsverks förvaltning till stor del bedrivs i elektronisk form och allt större krav ställs på att sådana tjänster som tillhandahålls elektroniskt är säkra. Med denna utveckling följer att myndigheter och affärsverk behöver se över och vid behov förstärka sitt informationssäkerhetsarbete.

I granskningen har tyngdpunkten legat på ledningens interna styrning och kontroll för att säkerställa säkerheten/skyddet av SvK:s IT-relaterade informationstillgångar. Denna styrning och kontroll benämns samlat för ledningssystem för informationssäkerhet (LIS). Avgränsningen innebär att faktiskt uppnådd säkerhet i enskilda system inte granskats.

Normkälla vid bedömning och värdering av nedanstående iakttagelser har varit Standarden[1] Ledningssystem för informationssäkerhet.

SvK bedriver verksamhet som har ett stort IT-beroende och den egna uppfattningen är att IT-verksamheten är av stor strategisk betydelse. SvK anser att det är av största vikt att mål och strategier knutna till IT-verksamheten är väl förankrade inom organisationen. Vidare bedöms IT-säkerheten vara en prioriterad fråga och visionen är att den alltid ska hålla en sådan nivå att driftsäkerheten och informationssäkerheten kan garanteras[2].

1.2 Iakttagelser

1.2.1 Ledningens organisation av IT-säkerhetsarbetet

SvK har en policy för IT-säkerhet som beslutats av generaldirektören. Policyn beskriver ledningens intentioner rörande IT-säkerhet. SvK saknar dock tydliga uppföljningsrutiner som visar att ledningens intentioner följs och som säkerställer att organisationen arbetar i enlighet med policyn.

Beslut gällande IT-säkerhetsfrågor har delegerats till IT-chefen. Till sin hjälp har IT-chefen en IT-säkerhetssamordnare och ett IT-säkerhetsråd där IT-chefen sitter som ordförande. Enligt SvK:s egna regler och riktlinjer[3] för IT-säkerheten är IT-säkerhetsrådet rådgivande men ska samtidigt fastställa regler och riktlinjer för IT-säkerheten. Enligt vår bedömning blir rådets roll otydlig i och med att det samtidigt har både en rådgivande och en beslutande funktion.

1.2.2 Riskanalys och informationsklassificering

SvK har en omfattande IT-verksamhet med flera samhällsviktiga och verksamhetskritiska system. Det finns förslag till klassificering av vilka system som ska definieras som samhällsviktiga men vid Riksrevisionens granskning hade ett formellt beslut avseende klassificering inte fattats av SvK. Ett sådant beslut är viktigt eftersom det vid granskningen framkommit olika uppgifter om vilka system som anses samhällsviktiga.

---

[1] SS-ISO/IEC 17799

[2] sid. 3 SvK:s IT-plan 2004-2006

[3] It-säkerhetsregler, allmänna version 1.3 sid.7

Riskanalys finns för enstaka system hos SvK. När det gäller de system som föreslagits vara samhällsviktiga, finns riskanalys för endast ett system. Riskanalyserna förvaras enligt uppgift inlåsta hos varje enskild systemägare men det finns ingen dokumenterad aggregerad analys som kan vara till hjälp vid prioritering och bedömning av vilka system som ska utvecklas, bytas ut etc.

Det är viktigt att systemen förvaltas på ett säkert och effektivt sätt och för att uppnå detta upprättar SvK systemförvaltningsavtal, som bl.a. anger roller, ansvar, säkerhetsklassning och budget. Det har dock inte upprättats systemförvaltningsavtal för samtliga system och vid Riksrevisionens granskning hade SvK inte heller beslutat om vilka system som kräver sådana avtal.

1.2.3 Skyddsåtgärder och uppföljning

SvK genomför granskningar av systemen för att se att de uppfyller ställda säkerhetskrav och fem av ett fyrtiotal system har blivit granskade hos SvK. Efter granskningen upprättar SvK åtgärdslistor i syfte att lista de brister som identifierats. Korrigering av uppdagade brister ska enligt SvK planeras och dokumenteras av systemägarna i så kallade systemsäkerhetsplaner. Systemsäkerhetsplaner saknas helt på SvK. Detta får till konsekvens att de brister i systemen som åtgärdas inte behöver vara inom de områden där störst risker finns. Det finns också risk för att inte alla brister hanteras.

Vid Riksrevisionens granskning kunde SvK inte uppvisa någon aktuell kontinuitetsplan för något av sina system. Konsekvensen av detta är att SvK inte kan visa hur de säkerställer att resurser kan avsättas i det fall en händelse inträffar som leder till allvarliga problem med tillgängligheten till väsentliga system.

Ett penetrationstest gjordes av konsult under hösten 2005 utan IT-säkerhetssamordnarens vetskap. Enligt Riksrevisionens bedömning bör sådan information vara känd för de personer som arbetar med IT-säkerhet på SvK.

1.2.4 Information och utbildning

SvK har ingen regelbundet återkommande utbildning om IT-säkerhet för personalen och detta har enligt Riksrevisionens bedömning försvårat förutsättningarna för att arbeta i enlighet med LIS.

1.3 Sammanfattande bedömning

Avsaknad av dokumenterad riskanalys på aggregerad nivå gör att det för Riksrevisionen är oklart hur SvK kontinuerligt bedömer och tar om hand de risker och hot som finns i verksamheten. Sannolikt påverkar detta SvK:s möjlighet att göra en realistisk bedömning om systemen i dagsläget har ett relevant skydd. Detta intryck förstärks ytterligare av att resultaten av faktiskt genomförd granskning i enstaka system inte dokumenteras i systemsäkerhetsplaner. SvK har heller inte i kontinuitetsplaner visat att verksamhetskritiska system skyddas på ett sådant sätt att man kan försäkra sig om god säkerhet och tillgänglighet.

1.4 Rekommendationer

Vi *rekommenderar* SvK att tillse att de noterade bristerna i LIS blir åtgärdade. Vi anser att arbetet med riskanalys, kontinuitetsplanering och systemsäkerhetsplanering bör genomföras i närtid, framförallt för de samhällsviktiga systemen. Vi anser även att SvK bör ha regelbundet återkommande utbildning om LIS för personalen.

2. Projektredovisning

2.1 Inledning

En väsentlig del av SvK:s arbete är att anpassa stamnätet till samhällets krav på en säker och ekonomisk elförsörjning. Projekten som SvK driver avser bl.a. ny- och ombyggnationer av ledningsnät och stationer. Bokfört värde på immateriella och materiella anläggningstillgångar uppgick 2004 till ca 8,9 mdkr[4].

Urvalet har omfattat tio stycken projekt som avslutats och aktiverats under 2004. Projekten avser såväl materiella som immateriella tillgångar. Totalt bokfört värde på de utvalda projekten uppgår till ca 92 mnkr vilket beloppsmässigt motsvarar en tredjedel av de avslutade projekten under 2004.

Vid granskningen har vi utgått från SvK:s upprättade projekthandbok och sökt i diariet efter några av de dokument[5] som enligt handboken ska finnas i varje avslutad projektakt. Kontakt med respektive projektledare har inte förekommit då dokumenten enligt arkivansvarig på SvK ska finnas arkiverade för varje avslutat projekt.

2.2 Iakttagelser

Det finns ingen koppling mellan projektredovisningen och diariet. Eftersom projektnumret inte alltid är inlagt i diariet är det svårt att identifiera de dokument som tillhör ett projekt. I anläggningsregistret används endast projektnumret vilket gör kopplingen mellan ekonomisystemet och projektredovisningen oklar.

Av de tio projektakter som granskades i diariet saknade tre projekt investeringsbeslut, fem projekt saknade genomförandebeslut, projektplan saknades för åtta projekt. Slutrapport saknades för nio projekt. Riskanalys, lägesrapport, och besiktningsprotokoll/drifttagningsbeslut saknades för samtliga projekt. Enligt uppgift upprättas inte alltid samtliga dokument för mindre projekt, men det finns inga beslut eller riktlinjer som meddelar när undantag kan göras.

Riksrevisionen finner det anmärkningsvärt att väsentliga dokument som ska finnas enligt projekthandboken saknas i diariet för ett stort antal avslutade projekt. Vidare anser Riksrevisionen att det hos SvK råder oklarhet om vilka

[4] SvK:s årsredovisning 2004

[5] Investeringsbeslut, genomförandebeslut, projektplan, riskanalys, lägesrapportering, tilläggsbeslut, uppföljningslistor, slutrapport och besiktningsprotokoll

dokument som ska upprättas för ett projekt, vilket i sig ökar risken för att projekten hanteras olika. Enligt Riksrevisionens uppfattning råder även osäkerhet om vilka dokument som ska diarieföras när ett projekt har avslutats.

Dokument där datum för slutbesiktning/driftssättning framgår saknas i arkivet vilket gör det omöjligt att kontrollera att anskaffningsdag enligt anläggningsregistret är riktigt. Anskaffningsdagen styr när avskrivningarna ska påbörjas. För tidigt eller för sent påbörjade avskrivningar kan ge ett felaktigt ekonomiskt resultat.

Vid granskning och intervjuer framkom att en person hanterar stora delar av projektredovisningen. Riksrevisionen bedömer att SvK:s nyckelpersonberoende inom detta område är mycket stort vilket inte är tillfredsställande ur ett internkontrollperspektiv.

2.3 Sammanfattande bedömning

Väsentliga dokument saknas i flera av de arkiverade projektakterna samtidigt som det råder osäkerhet inom SvK vad som faktiskt ska diarieföras. För Riksrevisionen är det oklart hur SvK tillförsäkrar sig god översikt och kontroll över de projekt som har bedrivits.

2.4 Rekommendationer

Riksrevisionen är medveten om att SVK håller på med en översyn av sin projektredovisning. Riksrevisionen *rekommenderar* att ovanstående iakttagelser beaktas i detta arbete.

3. Stamnätsavgifter

3.1 Inledning

De regionala nätägarna och producenterna betalar stamnätsavgifter till SvK för att vara anslutna till stamnätet. Stamnätsavgiften består av tre delar:

- Effektavgift
- Energiavgift
- Investeringsbidrag

För att stamnätsavgiften ska vara kostnadsriktig följer den det geografiska läget. I norra Sverige är avgifterna för inmatning av el till stamnätet höga, eftersom detta ökar belastningen på stamnätet, medan avgifterna för uttag är låga. Motsatsen gäller för södra Sverige.

Granskningen har omfattat dels effektavgiften, som baseras på årsvisa abonnemang för inmatning respektive uttag, och dels energiavgiften som baseras på verklig inmatad eller uttagen energi.

Effekt- och energiavgiften utgör ca 50%[6] av SvK:s totala rörelseintäkter.

[6] SvK:s årsredovisning 2004

3.2 Iakttagelser

Energiavgiften ska återspegla stamnätets överföringsförluster och är baserad på en serie förlustkoefficienter för varje anslutningspunkt. Förlustkoefficienterna är beroende av anslutningspunktens läge i nätet. Negativa koefficienter innebär att kunden får betalt av SvK vid inmatning. Det beror på att en inmatning till stamnätet i söder kan ge reducerade stamnätsförluster för SvK. På samma sätt kan ett uttag av energi i norr reducera stamnätets överföringsförluster. Kunderna gör i dessa fall stamnätet en ”tjänst” vilket avgiften speglar[7].

Varje månad gör SvK en avräkning där kunderna antingen får betalt eller får betala till SvK. Vissa kunder som t.ex. kärnkraftverken får i stort sett alltid betalt av SvK eftersom de alltid matar in el i söder och därmed reducerar stamnätets överföringsförluster. Det vanligaste är dock att kunderna betalar till SvK.

SvK nettoredovisar betalningarna avseende energiavgiften, dvs. i de fall SvK betalar till en kund redovisas detta som en negativ intäkt. Nettobeloppet redovisas under rörelseintäkter i resultaträkningen. Konsekvensen blir att SvK:s rörelseintäkter visar ett för lågt belopp om ca 300 mnkr på årsbasis.

Riksrevisionen är medveten om att SvK har för avsikt att ändra redovisningsprincip under innevarande räkenskapsår.

Revisionsdirektör Göran Selander har beslutat i detta ärende. Revisionsledare Anne Bryne har varit föredragande. Revisionsledare Carina Franzén har deltagit i den slutliga handläggningen.

Göran Selander Anne Bryne

Kopia för kännedom:

Miljö- och Samhällsbyggnadsdepartementet

Finansdepartementet/budgetavdelningen

[7] Ur SvK:s broschyr ”Den svenska elmarknaden och Svenska Kraftnäts roll”