

# Svenska Bankföreningen

REMISSYTTRANDE

2006-12-13

Näringsdepartementet

103 33 STOCKHOLM

## **Utveckling av Sitic**

N2006/6947/ITFoU

Bankföreningen vill med anledning av rubricerade remiss lämna följande synpunkter.

Sammanfattningsvis är föreningen positiv till de förslag till utveckling av Sitics verksamhet som presenteras i redovisningen av regeringsuppdrag 14 i PTS regleringsbrev 2006.

Informationsteknologi och infrastrukturen för elektronisk kommunikation har en avgörande betydelse för att distributionen av finansiella tjänster ska kunna fungera på ett säkert sätt och motsvara de krav som ägare, kunder, myndigheter m.fl. intressenter idag ställer på finansiell verksamhet. Mot denna bakgrund anser föreningen att ett kvalificerat nationellt centrum för IT-incidenthantering fyller en viktig funktion. Föreningen konstaterar att Sitic idag fungerar som en CERT-organisation med hög kompetens och utvecklat nätverk som omfattar även kontakter med motsvarande organisationer i andra länder. Då de IT-relaterade hoten idag i stor utsträckning är globala är det nödvändigt att det finns en nationell CERT-organisation som kan bedriva omvärldsanalys och som kan bistå myndigheter, företag m.fl. organisationer med partsneutral information om dessa gränsöverskridande hot och risker i form av analyser, varningar, råd mm. Det är önskvärt att Sitics förmåga att leverera dessa tjänster förstärks enligt de förslag som redovisats i rubricerade rapport.

När det gäller de olika förslag som redovisas i rapporten vill föreningen särskilt framhålla Sitics betydelse som koordinerande aktör. Ett exempel på en aktuell företeelse som finansiella institutioner på senare tid utsatts för kallas nätfiske (phishing). Sitic har, bl.a. genom sitt nätverk med CERT-organisationer i andra länder, i vissa fall fyllt en viktig funktion i samarbetet med polis m.fl. myndigheter för att förhindra spridningen av sådana IT-relaterade kriminella aktiviteter. Föreningen är av den uppfattningen att Sitic framöver kommer att få en ännu större betydelse när det gäller koordinering av incidentåtgärdande och sårbarhetsåtgärdande. För att klara dessa uppgifter är det nödvändigt att verksamheten utökas till att omfatta någon form av jour eller dygnet-runt beredskap. Därutöver finns det anledning att förstärka resurserna när det gäller proaktiva åtgärder som syftar till att hjälpa organisationer att skydda sin verksamhet mot de IT-relaterade hoten.

SVENSKA BANKFÖRENINGEN

Ullas Lundquist

Pär Karlsson