Försvarsdepartementet
Enheten för det civila försvaret m.m.
103 33 STOCKHOLM

DNR 2005-822-STA

Yttrande över delbetänkandet "Säker information – förslag till informationssäkerhetspolitik" (SOU 2005:42) (Fö2005/1418)

2005-10-04

1 INLEDNING OCH RIKSBANKENS ÖVERGRIPANDE SYNPUNKTER

Sveriges riksbank har beretts tillfälle att yttra sig över rubricerade remiss.

Riksbanken vill inledningsvis instämma i utredningens uppfattning att informationssäkerhet är en angelägenhet för hela samhället. Det är av grundläggande betydelse att se informationssäkerhetsarbete inte bara som viktigt vid extraordinära händelser, utan att det är något som ständigt måste vara i fokus för att säkerställa en god funktion av verksamheter inom samtliga samhällsområden.

Riksbanken har förståelse för att det behövs en målformulering för de statliga insatserna inom detta område, vilket utredningen arbetat med. En sådan målformulering bör vara så konkret och kortfattad som möjligt. I detta avseende anser Riksbanken att utredningen inte har lyckats och att förslagen därför behöver omarbetas.

Riksbankens uppfattning är därtill att åtgärder för att säkerställa en god informationssäkerhet behöver baseras på en syn på samhällets funktion där merparten av informationsbehandlingen och informationsutbytet sker i decentraliserade former av självständiga aktörer i ekonomin som hushåll, företag och kommuner. För att uppnå förbättringar av informationssäkerheten hos dessa aktörer är det med stor sannolikhet mest effektivt att arbeta med att stärka incitamenten för dem att vidta konkreta åtgärder.

Staten kan främst verka genom att föregå med gott exempel i sin egen verksamhet, genom att ge ekonomiska incitament till ett agerande som stärker informationssäkerheten, samt genom att utforma tydliga regelsystem och att verka avskräckande genom effektiva brottsutredande och rättsvårdande myndigheter.

En åtgärd som staten kan vidta är att utforma ett regelsystem för styrningen av de statliga myndigheterna, vilket utredningen ger förslag till. Därtill kan en sammanhållande lagstiftning om informationssäkerhet vara lämplig, vilket utredningen också anser. I huvudsak anser dock Riksbanken att regeringskansliet borde kunna pröva att komplettera och se över de generella regelsystemen, som t.ex. associationsrättsliga regler och straff- och skadeståndsrättsliga regler för att ge

ytterligare incitament till önskvärt agerande hos enskilda aktörer. Det kan t.ex. gälla att peka ut att informationssäkerhet och ändamålsenliga rutiner för att uppnå god nivå inom detta område är en fråga som ligger inom ramen för ansvaret t.ex. hos företagsstyrelser och kommunstyrelser. Sådana initiativ skulle sannolikt öppna vägen för en utveckling av åtgärder av marknadsaktörerna som t.ex. differentierade försäkringspremier med avseende på den nivå informationssäkerheten i en verksamhet har. Riksbanken saknar en sådan syn på statens roll och därpå baserade analyser och förslag till åtgärder från utredningen. När det gäller brottsbekämpning och rättssystemets funktion bör också mer konkreta åtgärdsförslag utarbetas.

Riksbanken har under det senaste året besvarat ett stort antal utredningar och förslag från regeringskansliet, Post- och Telestyrelsen, Krisberedskapsmyndigheten och utredningsväsendet som syftar till att stärka informationssäkerhet, krisberedskap och krishanteringsförmåga. Riksbanken är positiv till att staten på dessa olika sätt försöker stärka samhällets samlade uthållighet och förmåga att hantera hot, störningar och kriser. Riksbanken ser inom sina egna verksamhetsområden flera exempel på att risker för störningar av t.ex. de samhällsviktiga betalningssystemen finns.

Sammanfattningsvis måste dock Riksbanken tyvärr konstatera att de åtgärder som presenterats inte ger uttryck för en samlad syn, delvis överlappar varandra och i många avseenden är alltför centrerade på statens egen organisation och funktionssätt inom området. Detta är också något som den nu aktuella utredningen själv påpekat. Riksbanken anser därför att det finns ett behov av att formulera en mer sammanhållen strategi för kommande åtgärder för ett förbättrat säkerhetsarbete, i staten och i samhället i stort. Riksbanken deltar gärna i en diskussion om olika sådana åtgärder inom detta område, och då främst när det gäller Riksbankens huvudområden finansiell stabilitet, effektiva och säkra betalningssystem och kontanthantering.

2 RIKSBANKENS DETALJSYNPUNKTER

Nedan redovisas Riksbankens syn på utredningens förslag mer i detalj.

Förslaget till nationell strategi

Riksbanken anser att en nationell strategi för informationssäkerhet bör göras kortare och mer konkret än den som presenteras i utredningen.

Förslaget om en handlingsplan för att genomföra den nationella strategin

I detta förslag vill Riksbanken särskilt framhålla:

- Riksbanken behöver få bättre tillgång till information från underrättelsetjänsterna för att kunna vidta relevanta skyddsåtgärder mot aktuella hotbilder.
- Ett säkrare internet är av stor vikt för samtliga aktörer inom finanssektorn och även för betalningssystemen som sådana. Internet är dock ett globalt nätverk, vilket innebär att nationella åtgärder endast kan säkra en liten del

av denna infrastruktur. Det krävs därför internationellt samarbete för att stärka säkerheten för såväl internet som all infrastruktur för kommunikation.

- Utredningen redovisar inte tillräckligt konkreta åtgärder för att stärka rättsväsendets roll inom informationssäkerhetsområdet. Brottsutredande myndigheters förmåga att beivra IT-relaterade brott, samt tilltron till denna förmåga, måste stärkas genom såväl kompetens- som resursförstärkningar. Riksbanken anser att detta är av stor vikt för att, som utredningen vill, stärka förtroendet för IT i allmänhet.
- Utredningen blandar begreppen ISO/IEC 17799, LIS och OffLIS, vilket är olyckligt då LIS och OffLIS är tillämpningar och rekommendationer baserade på standarden ISO/IEC 17799. Riksbanken anser att utredningen bör rekommendera den internationella standarden i sitt ordinarie utförande som en grund för det nationella informationssäkerhetsarbetet. På detta sätt undviks att olika angreppssätt skapas.
- En brist i förslaget till handlingsplan är att planen saknar mätbara mål för de föreslagna åtgärderna, vilket bland annat försvårar effektutvärdering.

Förslaget att säkerhetsmedvetandet bör höjas bland annat inom ramen för utbildningssystemet

Riksbanken anser att en mycket viktig grund i informationssäkerhetsarbetet är att åstadkomma en allmän höjning av säkerhetsmedvetandet. För detta krävs utbildning om hotbilder och framförallt skyddsåtgärder inom såväl offentlig som privat sektor samt för varje medborgare som nyttjar IT.

Krisberedskapsmyndigheten och Post- och Telestyrelsen bör kunna tillhandahålla anpassad utbildning och informationsmateriel till lärare och pedagoger. Detta angreppssätt kan ge goda resultat på kort sikt, utan omfattande resursåtgång, vilket Riksbanken har egna erfarenheter av inom sina egna ansvarsområden. För att på längre sikt tillgodose informationssäkerhetskompetensen hos lärare och pedagoger krävs dock kompletteringar av lärarutbildningar, etc.

Förslaget om forskningsinsatser inom informationssäkerhetsområdet

Utredningen beskriver vilka samhällsinstitutioner som bör ansvara för ökade forskningsinsatser. Därtill anser Riksbanken att det tydligare behöver anges prioriterade forskningsområden för att säkerställa att forskningsmedlen används effektivt.

Förslaget att revision av informationssäkerhet bör utvecklas och att den standard som revision bör tillämpa är Ledningssystem för informationssäkerhet (LIS)

Riksbanken stödjer förslaget men vi vill förtydliga att det i detta fall är standarden ISO/IEC 27001 som är avsedd för certifiering och revidering av informationssäkerhet. (Se även resonemanget ovan kring ISO/IEC 17799.)

Förslaget till en ny förordning

Förordningen bör i större utsträckning än i utredningens förslag, baseras på standarden ISO/IEC 17799 för att täcka samtliga relevanta informationssäkerhetsområden. I utredningens förslag saknas viktiga delar så som riskanalys och kontinuitetsplanering.

Riksbanken vill i detta sammanhang påpeka att banken inte omfattas av regeringens förordningar, men beaktar dessa i bankens verksamhet.

Beslut i detta ärende har fattats av vice riksbankschef Villy Bergström efter föredragning av Martin Bergling, Jan-Olof Andersson, Jan Närling, Urban Örtberg och Björn Hasselgren.

Villy Bergström

Martin Bergling