

1 Sammanfattning

Utredningens uppdrag

Utredningens uppdrag är att med utgångspunkt i rapporten SKRIB (Fi 2010/1619) och avlämnade remissvar vidareutveckla och ytterligare konkretisera de förslag som där anges avseende grundläggande säkerhetsnivåer och nationellt samordningsansvar för såväl förebyggande krisberedskapsåtgärder som åtgärder vid en akut kris inom det centrala betalningssystemet. Inriktningen på arbetet ska vara att ta fram förslag till grundläggande säkerhetsnivåer för det centrala betalningssystemet av mer kvantitativ karaktär. Vidare ska inriktningen vara att det föreslås en ansvarig myndighet som, utan att överta annans ansvar, ska ha ett nationellt samordningsansvar för såväl förebyggande krisberedskapsåtgärder som åtgärder vid en akut kris i det centrala betalningssystemet.

Bakgrund

I rapporten Krisberedskap i betalningssystemet (RiR 2007:28) konstaterade Riksrevisionen att det fanns ett antal avgörande brister i statens åtgärder för att förebygga och hantera allvarliga störningar i det centrala betalningssystemet.

Riksrevisionen konstaterade i rapporten att ett stort antal myndigheter hade ansvar för den finansiella sektorns krisberedskap och att en privat-offentlig samverkan bedrevs. Ingen myndighet ansåg sig emellertid ha ett övergripande och samlat ansvar för ledning, planering, samverkan och uppföljning av krisberedskapen inom betalningssystemet. Oklarheten i ansvarsförhållanden och uppgifter bidrog till att det saknades en samlad bild av hot, risker, sårbarheter och konsekvenser samt att myndigheterna inte hade samordnat sina förberedande åtgärder tillräckligt.

Riksrevisionen anförde i rapporten att regeringen borde fastställa vilka grundläggande säkerhetskrav som ska gälla för betalningssystemet och dess nödvändiga infrastruktur. Regeringen borde också fastställa hur uthålligt betalningssystemet måste vara.

Regeringen borde enligt Riksrevisionen även fastställa vilken myndighet som har det övergripande krisberedskapsansvaret för betalningssystemet och incidentbevakningen samt föreslå riksdagen i vilka avseenden Riksbanken eller Finansinspektionen ska ha ansvar för krisberedskapen.

Finansinspektionen och Riksgäldskontoret fick av regeringen i uppdrag att redovisa vilka initiativ som hade tagits eller var planerade med anledning av Riksrevisionens rapport. Även Riksbanken sammanställde en liknande redovisning.

Med anledning av Riksrevisionens rapport och de redovisningar som Finansinspektionen, Riksgäldskontoret och Riksbanken lämnade i frågan utarbetades inom Finansdepartementet under 2010 en rapport innehållande förslag på hur statens förmåga att hantera allvarliga kriser i betalningssystemet kunde stärkas, Fi 2010/1619.

I rapporten föreslogs bl.a. att ett nationellt samordningsansvar skulle införas och att Riksbanken var den myndighet som skulle ges detta ansvar. Vidare föreslogs att detta ansvar samt grundläggande säkerhetskrav (mål) skulle regleras genom en ny lag. Rapporten har remitterats.

Utredningens slutsatser

Det centrala betalningssystemet

Någon allmänt vedertagen definition av begreppet det centrala betalningssystemet finns inte. I utredningen definieras det centrala betalningssystemet som de funktioner i det nationella betalningssystemet som har en sådan betydelse att ett bortfall, direkt eller över tid, skulle innebära en risk eller fara för samhällets funktionalitet eller samhällets grundläggande värden.

Viktiga system inom det centrala betalningssystemet är RIX – systemet för stora betalningar, Bankgirocentralens betalningssystem för massbetalningar, Euroclear Swedens VPC-system där transaktioner från aktie- och räntemarknaden clearas och avvecklas samt Nasdaq OMX Derivatives Markets som är central motpart för standardiserade derivatkontrakt. Andra viktiga aktörer inom det

centrala betalningssystemet är Riksgäldskontoret samt de fyra storbankerna.

Den ovan redovisade beskrivningen utgör dock inget försök att exakt definiera det centrala betalningssystemet. I utredningen föreslås att det ska vara en uppgift för Riksbanken att definiera vilka aktörer och verksamheter som ska anses ingå i det centrala betalningssystemet. Det kan förutses att denna definition kommer att bli föremål för en fortlöpande översyn av Riksbanken med hänsyn till den dynamik som präglar utvecklingen inom den finansiella sektorn.

Riksbankens samordningsansvar

Utredningen föreslår att Riksbanken tilldelas det nationella samordningsansvaret för krisberedskap i det centrala betalningssystemet. Samordningsansvaret innefattar inte ett övertagande av ansvar från en annan aktör i det centrala betalningssystemet för det fall en kris uppstår. Däremot får Riksbanken ett ansvar att leda samordningen mellan aktörerna i en sådan situation.

Riksbankens samordningsansvar för krisberedskap ska avse det centrala betalningssystemet. Finansinspektionen ska fortsatt ha krisberedskapsansvaret för den finansiella sektorn i övrigt.

Finansinspektionens tillsynsansvar över de privata aktörerna i det centrala betalningssystemet kvarstår.

Grundläggande säkerhetsnivåer

Utgångspunkten för utredningens förslag till grundläggande säkerhetskrav på det centrala betalningssystemet är att målen bör ha en kvantitativ (mätbar) karaktär för att kunna värderas och vara föremål för revision.

De säkerhetskrav som bör ställas på det centrala betalningssystemet bör utformas som en kombination av funktionskrav på detta system och krav på de tekniska system – externa och interna – som det centrala betalningssystemet är beroende av.

Riksbanken får i den av utredningen föreslagna lagen uppgiften att genomföra en årlig risk- och sårbarhetsanalys i syfte att identifiera de kriser som kan drabba det centrala betalningssystemet. Beredskapsplaneringen bör syfta till att hantera alla de kriser som identifieras i risk- och sårbarhetsanalysen. Även osannolika händelser

med allvarliga konsekvenser bör värderas. Kritiska beroenden som finns mellan det centrala betalningssystemet och andra samhällsverksamheter ska identifieras. Risk- och sårbarhetsanalyser ska vara förankrade på ledningsnivå.

Utredningen formulerar också funktionskrav på det centrala betalningssystemet. Målet är att det centrala betalningssystemet även vid en allvarlig kris kan avveckla alla transaktioner i enlighet med ingångna avtal och gällande lagstiftning, i regel senast under pågående bankdag. Reservsystem och alternativa driftsmiljöer ska genom kontinuitetsplaner vara väl förberedda att klara målet.

Kontinuitetsplaner måste innefatta tider för återställande av system. Målet för tiden till återstart vid ett avbrott i centrala betalningssystemet bör vara högst två timmar. De krav eller mål som utredningen föreslår ansluter sig väl till de rekommendationer som formuleras inom ramen för Bank for International Settlements (BIS) och Internationella organisationen för värdepapperstillsyn (IOSCO).

Det går dock inte helt att bortse från att det kan uppstå situationer då högt ställda mål inte kan tillgodoses. Att utgå ifrån att det centrala betalningssystemet inte under några omständigheter kan drabbas av sådana händelser är knappast tillrådligt. Därför är det nödvändigt att i ett svårt krisläge ha förberett åtgärder som utgår ifrån att endast en del av transaktionerna i det centrala betalningssystemet kan hanteras eller att det kan ta längre tid än en bankdag att avveckla transaktionerna. I sådana lägen måste vissa typer av transaktioner ges företräde under den tid krisen varar. Det bör inte ske slumpmässigt och improviserat utan bör utgå från en uppsättning på förhand fastlagda prioriteringsprinciper.

Aktörerna inom det centrala betalningssystemet föreslås också bli skyldiga att i rimlig utsträckning bistå varandra när något eller några av dem drabbas av allvarliga tekniska störningar eller avbrott.

De grundläggande säkerhetskrav som bör ställas på det centrala betalningssystemet sammanfattas av utredningen på följande sätt:

1. Målet är att det centrala betalningssystemet även vid en allvarlig kris kan avveckla alla transaktioner i enlighet med ingångna avtal och gällande lagstiftning, i regel senast under pågående bankdag.
2. Vid en allvarlig störning eller avbrott i verksamheten hos en aktör i det centrala betalningssystemet ska återgång till ordinarie drift eller övergång till reservsystem ske senast inom två timmar.

3. Om detta inte är möjligt ska en alternativplanering finnas som gör det möjligt att vid en kris prioritera de viktigaste transaktionerna.

4. Principer och metoder för att identifiera och vid en kris prioritera de viktigaste transaktionerna ska utvecklas.

Privat-offentlig samverkan

Aktörerna i det centrala betalningssystemet utgörs av både myndigheter och privata företag. Ett samarbete mellan de berörda parterna avseende krisberedskapsåtgärder inom det centrala betalningssystemet är därför nödvändigt. Den privat-offentliga samverkan som behöver ske bör även i fortsättningen hanteras inom ramen för samarbetet inom den finansiella sektorns privat-offentliga samverkansorgan, FSPOS.

Samordning av krisberedskapsåtgärder

Behovet av att samordna de krisberedskapsåtgärder som vidtas beträffande det centrala betalningssystemet har ytterst att göra med att olika aktörer inom detta system är beroende av varandra och att de krisberedskapsåtgärder som vidtas av dessa aktörer måste ligga på en sådan nivå att de mål som sätts för systemets samlade prestationsförmåga vid en kris kan uppnås.

Behovet av att samordna såväl beredskapsåtgärder som operativa åtgärder under en kris är större inom det centrala betalningssystemet än inom många andra verksamheter. Anledningen är att systemet omfattar ett antal aktörer vars verksamheter är nödvändiga för att systemet ska fungera och där ett bortfall av en aktör kan få långtgående konsekvenser för systemet som helhet. Betydelsen av detta förstärks av att hela det finansiella systemet är beroende av att det centrala betalningssystemet fungerar. Brister i beredskapen hos en aktör kan därför få omfattande spridningseffekter inom hela den finansiella sektorn. Av dessa skäl måste höga krav ställas på samordningen av de krisberedskapsåtgärder som vidtas beträffande det centrala betalningssystemet.

För närvarande saknas ett system som är direkt inriktat mot samordning av de krisberedskapsåtgärder som vidtas beträffande det centrala betalningssystemet.

Vid kriser i det centrala betalningssystemet är det väsentligt att det finns en krisledningsfunktion med befogenhet att samordna de åtgärder som behöver vidtas för att minska skadeverkningarna och att återupprätta systemets funktion så snabbt som möjligt. Det bör även vara en uppgift i det nationella samordningsansvaret att utbilda och öva personal som ska ha uppgifter i krisledningsorganisationen.

Följande uppgifter bör därför ingå i det nationella samordningsansvaret för krisberedskapsåtgärder inom det centrala betalningssystemet:

1. Utforma föreskrifter avseende grundläggande säkerhetskrav på det centrala betalningssystemet vid en kris.
2. Ta fram en risk- och sårbarhetsanalys för det centrala betalningssystemet i enlighet med de anvisningar för risk- och sårbarhetsanalyser som gäller inom krisberedskapen.
3. Leda och samordna beredskapsplaneringen inom det centrala betalningssystemet med inriktning mot de krissituationer som identifieras i risk- och sårbarhetsanalysen.
4. Utbilda och öva personal inom det centrala betalningssystemet för de krisberedskapsuppgifter som behöver utföras.
5. Verka för att en effektiv privat-offentlig samverkan sker mellan det centrala betalningssystemets aktörer.
6. Lämna information om beredskapsläget vad gäller det centrala betalningssystemet efter förfrågan från Regeringskansliet eller Myndigheten för samhällsskydd och beredskap (MSB).

Under en pågående kris bör det nationella samordningsansvaret för det centrala betalningssystemet omfatta följande uppgifter:

1. Leda och samordna de åtgärder som vidtas av det centrala betalningssystemets aktörer för att hantera krisen.
2. Löpande upprätta lägesrapporter som redovisas till riksdag och regering samt till MSB och andra myndigheter.
3. Samordna den information som riktas till allmänheten och media om krisens förlopp.

Behovet av lagreglering

I utredningen föreslås att Riksbanken ges det nationella samordningsansvaret för krisberedskapen i det centrala betalningssystemet.

Av Riksbankens konstitutionella ställning följer att den i utredningen föreslagna ordningen ska regleras i lag. Den föreslagna lagen

innehåller de grundläggande principerna för Riksbankens samordningsansvar samt principerna för de grundläggande krav som är rimliga att sätta upp för krisberedskapen i det centrala betalningssystemet. Förslaget innehåller även bemyndiganden för Riksbanken att meddela närmare föreskrifter för vissa delar av lagens tillämpning.

Den föreslagna ordningen innebär att ett nära samarbete mellan Riksbanken och Finansinspektionen kommer att krävas inom detta område. Redan idag finns ett väl utvecklat samarbete mellan dessa myndigheter i olika frågor. Vad avser finansiella kriser finns också en överenskommelse mellan myndigheterna från 2009 om bl.a. samråd, informationsutbyte och informationsinhämtning. I överenskommelsen anges att myndigheterna ska ha rutiner som möjliggör för den andra parten att på ett enkelt sätt få uppgift om vilken information som myndigheten besitter. Myndigheterna åtar sig att samarbeta för att samordna insamlandet av data av snarlikt innehåll.

Ett liknande samarbete torde kunna förutses även vid icke-finansiella kriser och den nya ordning som föreslås i denna utredning bedöms därför inte innebära något behov av ytterligare lagtiftning i detta avseende. Det ingår i Finansinspektionens tillsyn att följa upp efterlevnaden av de föreskrifter som Riksbanken meddelar.

Myndigheternas krisberedarbete regleras i krisberedskapsförordningen. Förordningen är tillämplig på statliga myndigheter under regeringen och således inte på Riksbanken. För att undvika att den nu föreslagna ordningen medför en splittring av myndigheternas krisberedskapsarbete har vissa centrala delar av innehållet i krisberedskapsförordningen kommit till uttryck i författningsförslaget. Den föreslagna ordningen innebär inte att ansvaret för de myndigheter som omfattas av krisberedskapsförordningen påverkas.

Informationssäkerhet

Enligt MSB och Försvarets radioanstalt (FRA) har det under de senaste åren skett en markant ökning av antalet IT-angrepp gentemot alla nivåer och funktioner i samhället. Den finansiella sektorn är ett naturligt mål för olika typer av angrepp då verksamheten hanterar stora värden.

För att få ett ändamålsenligt skydd krävs inte bara robusthet definierat som tillgänglighet utan även skyddsåtgärder för konfidentialitet, riktighet och spårbarhet.

Krisberedskap förutsätter ett långsiktigt och systematiskt arbete med informationssäkerhet under normala förhållanden. Systematik ger möjlighet att hantera den dynamiska hotbilden och vidta rätt åtgärder vid olika typer av allvarliga störningar eller kriser.

I en kritisk situation för det centrala betalningssystemet krävs ett friktionsfritt samarbete mellan flera, ibland ett stort antal aktörer. Ur denna aspekt skulle gemensamma begrepp och metoder underlätta samordning om allvarliga störningar skulle uppstå. Utredningen bedömer det lämpligt att i föreskrift ange att ett systematiskt informationssäkerhetsarbete ska bedrivas av det centrala betalningssystemets aktörer enligt de nationella och internationella standarderna ISO/IEC 27001 och ISO/IEC 27002. Det innebär bl.a. ledningssystem hos varje aktör, i enlighet med ansvarsprincipen, med klart definierade ansvar och roller för informations-säkerhet, systematiskt arbete med riskanalyser och informationsklassning.

Utredningen föreslår att Riksbanken i egenskap av nationell samordnare bör ges rätten att meddela föreskrifter på området.

Det centrala betalningssystemet kan inte uteslutas som mål för t.ex. antagonistiska IT-angrepp. För att så långt möjligt skydda det centrala betalningssystemet från störningar bör kraven på administrativ och teknisk informationshantering därför ställas högt och IT-incidenter hanteras på ett systematiskt sätt.

Syftet med IT-incidenthantering är att i realtid eller nära realtid medverka till att attacker mot datasystem avstys och upphör. Incidentstödet ska ha överblick och kunskaper om IT-hot och informationssäkerhet i ett helhetsperspektiv samt förmåga att kunna skilja okvalificerade och osystematiska intrångsförsök från kvalificerade och systematiska angrepp. Kvalificerad rådgivning ska kunna lämnas.

Utredningen föreslår en förstärkning av den befintliga funktionen CERT-SE vid MSB med kompetens för incidenthantering rörande det centrala betalningssystemet.

I ett senare skede, om behov finns, bör det vara möjligt att inrätta en separat incidenthanteringsfunktion för det centrala betalningssystemet eller en större del av den finansiella sektorn. Eftersom MSB är en samordnande myndighet utan sektorsansvar för krisberedskap inom den finansiella sektorn, är det logiskt om en sådan funktion för den finansiella sektorn i så fall senare upprättas utanför MSB, exempelvis inom Finansinspektionen.