Datum 2011-03-30
Diarienr 2011-765
Ert datum 2011-02-04
Er referens Fi 2010/1619

ROS-ISÄK
Fia Ewald
010-2404493
fia.ewald@msb.se

Regeringskansliet
Finansdepartementet

103 33 Stockholm

En samlad reglering för stärkt krisberedskap mot allvarliga tekniska fel och störningar i det centrala betalningssystemet

Sammanfattning

MSB anser det värdefullt att en utredning gjorts kring stärkt krisberedskap i det centrala betalningssystemet med tanke på systemets betydelse för det svenska samhällets stabilitet. Krisberedskap är dock ett omfattande område som även omfattar aspekter som inte berörts i rapporten.

MSB:s uppfattning är att för att uppnå nödvändig effektivitet och systematik i krisberedskapen bör denna kopplas tydligare till den nationella samordningen av informationssäkerhet generellt samt till den nationella hanterandeplanen för allvarliga IT-incidenter. Likaså bör det tydliggöras om det är krav eller mål som ska föreskrivas aktörerna i betalningssystemet, och hur dessa ska vara utformade. MSB anser det lämpligt att i författning ställa krav på ett systematiskt informationssäkerhetsarbete utformat efter de nationella och internationella standarderna ISO/IEC 27001 och ISO/IEC 27002.

Om Riksbanken ska ha det nationellt samordnande ansvaret bör formerna för samverkan med de myndigheter som omfattas av förordningen (2006:942) om krisberedskap och höjd beredskap (KBF) förtydligas i den föreslagna lagen om krisberedskap i det centrala betalningssystemet.

Behov av fördjupad analys

Koppling till informationssäkerhet

I utredningen definieras det centrala betalningssystemet som en delmängd av det finansiella systemet. Med system avses i detta sammanhang inte ett IT-system utan en avgränsad integration av bl.a. tjänster, funktioner, IT-system och aktörer med syfte att stödja ekonomiska transaktioner. Trots att utredningen behandlar krisberedskap i betalningssystemet handlar den i huvudsak om informationssäkerhet, d.v.s. åtgärder som syftar till att skapa och upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i

informationshanteringen, då betalningssystemets funktion helt bygger på informationshantering. Fokus riktas nästan helt mot tillgänglighetsaspekten. Samtliga kriser som utredaren presenterar som ”typkriser” gäller avbrott i informationshanteringen.

En beredskap för kris förutsätter ett långsiktigt och systematiskt säkerhetsarbete i vardagen. MSB menar att det därför vore lämpligt att använda terminologi och metoder hämtade från informationssäkerhetsområdet i arbetet med krisberedskapen i det centrala betalningssystemet. Stöd kan även hämtas i de internationella standarder som finns för systematiskt informationssäkerhetsarbete[1]. Detta skulle tydliggöra samband och underlätta en samordning i en gemensam nationell krisberedskap för ett område med ett högt beroende av välfungerande informationshantering.

Allvarliga IT-incidenter och dess konsekvenser

MSB har nyligen redovisat sex regeringsuppdrag, bland annat rörande obligatorisk IT-incidentrapportering för statliga myndigheter. Förslaget omfattar även frivillig rapportering av IT-incidenter. Här finns fördelar att vinna både i ett krisläge men också i normalläget då aktörerna i det centrala betalningssystemet exempelvis kan få mer relevanta beslutsunderlag om de kan hämta information ur ett gemensamt IT-incidentrapporteringssystem.

I ett annat uppdrag har MSB tagit fram en *nationell hanterandeplan för allvarliga IT-incidenter*. Syftet med hanterandeplanen är bland annat att säkerställa möjligheterna till att upprätthålla en gemensam, kvalificerad lägesbild, ge samordnade budskap till allmänheten och stödja effektiv teknisk hantering av incidenten. MSB:s uppfattning är att allvarliga IT-incidenter i det centrala betalningssystemet och följderna av sådana händelser kan ställa krav på en nationell samverkan mellan en rad olika aktörer och hanterandeplanen visar hur en sådan samverkan bör ske. Även på grund av samverkansbehoven är det därför lämpligt med en anpassning av terminologi och metoder till det som gäller inom informationssäkerhet. Ett steg i rätt riktning vore att använda begreppet allvarliga IT-incidenter istället för ”allvarliga tekniska fel och störningar”. En allvarlig IT-incident definieras i den nationella hanterandeplanen som en IT-relaterad händelse som avviker från det normala, innebär en allvarlig störning i samhällsviktig verksamhet samt kräver snabba insatser på nationell nivå. Någon begränsning när det gäller orsaken till en allvarlig IT-incident finns inte utan planen utgår från en s.k. all-hazard approach. De typkriser som beskrivs i utredningen omfattas enligt MSB:s mening av hanterandeplanens definition av allvarliga IT-incidenter.

Ur krisberedskapssynpunkt kan det också ses som ett problem att utredaren valt en avgränsning där kriser med ”katastrofala” konsekvenser utesluts ur

[1] I första hand ISO/IEC 27001 och ISO/IEC 27002

resonemanget. I en eskalering från normalläge till en mycket allvarlig kris är det viktigt att centrala moment är kartlagda. MSB skulle därför vilja se en beskrivning av hur övergången från ”händelser som har betydande konsekvenser” till ”händelser med katastrofala konsekvenser” ska ske. I utredarens förslag till utformning av det nationella samordningsansvaret står det att myndigheten som har detta ansvar vid en akut kris ska rapportera till MSB, något som tydligare bör kopplas mot den nationella operativa samordningen.

Mål och krav

Att formulera frågeställningarna som informationssäkerhetsrelaterade är också funktionellt när det kommer till att reglera de grundläggande säkerhetskrav (mål) som utredaren föreslår. Utredaren diskuterar här huruvida de grundläggande säkerhetskraven (målen) bör vara av kvantitativ alternativt kvalitativ karaktär och föreslår att de i huvudsak bör vara kvalitativa. Med kvalitativa avse utredaren att målen ska vara ”mer principinriktade och övergripande” av typen att betalningssystemet ska fungera ”tillfredställande” eller att betalningar ska kunna genomföras inom ”rimlig” tid. Här bör också övervägas om ”krav” och ”mål” verkligen är synonyma begrepp. En synpunkt är att krav är något som ska införas omedelbart medan mål är något som på sikt ska infrias. Innan det regelverk som föreslås i utredningen utformas bör detta vara tydliggjort. Slutligen kan sägas att även de förebyggande uppgifter som föreslås ingå i det nationella samordningsansvaret rimmar väl med ett systematiskt informationssäkerhetsarbete.

Det är positivt att utredaren vill märka ut vissa särskilt viktiga funktioner men i den praktiska tillämpningen kan det vara svårt att hitta en gemensam uppfattning om vad som ska ses som ”rimligt” alternativt ”tillfredställande”. MSB menar att det kan vara nödvändigt att komplettera dessa kvalitativa krav med konkreta funktionella krav. Ett exempel på detta skulle kunna vara krav på att införa viktiga komponenter i ett systematiskt informationssäkerhetsarbete såsom det beskrivs i Ledningssystem för informationssäkerhet, ISO/IEC 27001 och ISO/IEC 27002. Detta har visat sig ha en tydligt säkerhetshöjande effekt hos statliga myndigheter när först Verva och nu MSB ställer krav i föreskrifter[2] på att arbetet med informationssäkerhet ska bedrivas i former enligt nämnda internationella standarder. Inriktningen att följa standarden har sedan spridits till andra samhällsområden som exempelvis hälso- och sjukvård där Socialstyrelsen tagit fram föreskrifter med liknande innehåll.

Systematiken skapar förutsättningar för att hantera den dynamiska risksituationen vilket också gör att man undviker de nackdelar som utredaren pekar på då kvantitativa mål sätts upp. När det gäller denna typ av mål delar MSB utredarens syn att de grundläggande kraven (målen) bör tas in i en ny lag.

---

[2] MSBFS 2009:10

Detta skulle också leda till en större likhet med andra samhällsviktiga områden och möjliggöra en systematik på nationell nivå i de fall då en kris eskalerar så att den inte längre omfattar en enskild sektor. MSB anser det lämpligt att i författning ställa krav på att systematiskt informationssäkerhetsarbete ska bedrivas i former enligt de nationella och internationella standarderna ISO/IEC 27001 och ISO/IEC 27002.

Behov av helhetsbild – krisberedskap

Riksrevisionens rapport som låg till grund för utredningen behandlade främst olika typer av tekniska avbrott som kunde orsaka kriser i betalningssystemet. MSB ser dock fördelar med att anlägga en s k all-hazard approach och analysera även andra typer av kriser som kan ge upphov till allvarliga konsekvenser i betalningssystemet. Utbredd underminering av tilliten till informationshanteringen och därmed till hela det centrala betalningssystemet kan uppstå exempelvis på grund av IT-attacker, skadlig kod eller annan typ av intrång. Denna typ av kriser kan i delar få samma konsekvenser som de ”allvarligare tekniska störningar och avbrott” som utredaren beskriver men kan även leda till andra mycket allvarliga konsekvenser i samhället. Önskas en helhetsbild av krisberedskapen är det nödvändigt att analysera även sådana scenarier. För att skapa tydlighet bör en ändamålsenlig terminologi användas. Den lag som föreslås, lag om krisberedskap i det centrala betalningssystemet, tar i sin nuvarande utformning endast sikte på en begränsad del av krisberedskapen. För att förtydliga den föreslagna lagens tillämpningsområde bör därför lagens namn ses över.

God krisberedskap bygger i stor utsträckning på väl fungerande samverkan mellan olika aktörer, vilket också är en av grundstenarna i förordningen (2006:942) om krisberedskap och höjd beredskap (KBF). Att etablera och utveckla sådan samverkan, exempelvis inom de i bilagan till förordningen utpekade samverkansområdena, är ett långsiktigt och kontinuerligt arbete. Om Riksbanken ska ha det nationellt samordnande ansvaret bör formerna för samverkan med de myndigheter som omfattas av KBF förtydligas i den föreslagna lagen.

I detta ärende har generaldirektören Helena Lindberg beslutat. Fia Ewald har varit föredragande. I den slutliga handläggningen har också chefsjuristen Key

Hedström, avdelningschefen Cecilia Nyström, enhetschefen Richard Oehme, handläggare Helena Andersson, Per-Arne Blad och Wiggo Öberg deltagit.

Helena Lindberg

Fia Ewald

Kopia:Försvarsdepartementet/SSK