Enheten för operativ analys & säkerhet (OA-AN)
Karl Bruno
010-240 43 19
Karl.Bruno@msb.se

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Remissvar - Promemoria En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur

Sammanfattning

Givet rådande organisatoriska förutsättningar för beredskapssektorn Finansiella tjänster, där Riksbanken (formellt utanför sektorn) ansvarar för krissamverkan med företag inom betalningsområdet, stödjer Myndigheten för samhällsskydd och beredskap (MSB) förslaget om att vid Riksbanken inrätta en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur. MSB vill dock framhålla att förslaget i vissa avseenden kan innebära försvårande omständigheter för det civila beredskapssystemets förutsättningar att agera med önskvärt resultat vid en fredstida kris eller höjd beredskap och krig.

För att motverka att icke sammanhängande strukturer i det civila beredskapssystemet skapas genom förslaget föreslår MSB att Riksbanken, med stöd av artikel 9 punkt 1 i NIS2-direktivet, samtidigt pekas ut som sektorsvis cyberkrishanteringsmyndighet för den finansiella sektorn. Vidare stödjer MSB förslaget om att Riksbanken ska ha en författningsreglerad skyldighet att hålla Finansinspektionen underrättad om viktigare frågor under fredstida krissituationer och vid höjd beredskap. MSB bedömer även att Riksbanken bör ha en reglerad informationsskyldighet gentemot MSB, i linje med den skyldighet myndigheter under regeringen har enligt 12§ förordning (2022:524) om statliga myndigheters beredskap samt den skyldighet myndigheter har i egenskap av sektorsvis cyberkrishanteringsmyndighet.

MSB vill understryka vikten av att det tydligt framgår och kommuniceras att den föreslagna funktionen ska kunna verka i hela hotskalan och att den dimensioneras för höjd beredskap och krig.

6.2 En ny operativ krishanteringsfunktion och 6.3 Ansvarig myndighet

Givet rådande organisatoriska förutsättningar för beredskapssektorn Finansiella tjänster, där Riksbanken (formellt utanför sektorn) ansvarar för krissamverkan med företag inom betalningsområdet, stödjer MSB förslaget att en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur inrättas och att Riksbanken blir ansvarig myndighet för den nya funktionen. MSB förslår dock kompletterande åtgärder i syfte att så långt som möjligt säkerställa att parallella och icke sammanhängande strukturer i krisberedskapssystemet inte skapas genom detta.

Riksbanken bör pekas ut som sektorsvis cyberkrishanteringsmyndighet för den finansiella sektorn

I enlighet med artikel 9.1 i NIS2-direktivet (EU) 2022/2555 skall varje medlemsstat *utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter)*. Om en medlemsstat utser eller inrättar mer än en cyberkrishanteringsmyndighet enligt punkt 1 i NIS2-direktivets artikel 9, ska den tydligt ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser. MSB föreslås i delbetänkande SOU 2024:14 Nya regler om cybersäkerhet bli svensk cyberkrishanteringsmyndighet.[1]

Den nationella cyberkrishanteringsmyndigheten enligt art. 9 i NIS2-direktivet ska agera på operativ nivå. Huvuduppgiften är att ansvara för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, något som ska ske integrerat i det nationella systemet för krishantering. Den nationella cyberkrishanteringsmyndigheten ska koordinera, eskalera och, tillsammans med relevanta myndigheter, samla och stödja hanteringen av särskilt allvarliga incidenter (ett begrepp MSB definierar i utkastet till nationell cyberkrishanteringsplan), samt störningar, följdverkningar av störningar och ytterst kriser som sådana incidenter medför, både nationellt och internationellt. För att utföra dessa uppgifter behöver en nära samverkan ske med det nationella cybersäkerhetscentret, den nationella kontaktpunkten enligt NIS2- och CER-direktiven, CSIRT-enheten, eventuella andra sektorsvisa cyberkrishanteringsmyndigheter, beredskapsmyndigheter och särskilt sektorsansvariga myndigheter samt privata aktörer. Cyberkrishanteringsmyndigheten ska även utgöra en länk mellan den operativa hanteringen i cybersäkerhetscentret och det civila krishanterings- och beredskapssystemet genom att bistå berörda beredskapsmyndigheter i hanteringen av störningen, dess följdverkningar och kriser som särskilt allvarliga incidenter orsakar. Sammanfattningsvis ska den nationella cyberkrishanteringsmyndigheten ansvara för själva hanteringen i sig, inte endast samordningen av hanteringen, när det inträffar storskaliga cybersäkerhetsincidenter. I den nationella cyberkrishanteringsplanen föreslås det att myndigheten ska även samordna av särskilt allvarliga incidenter samt de störningar och följdverkningar av störningar som sådana incidenter orsakar.

[1] Notera att FRA föreslås bli cyberkrishanteringsmyndighet i NCSC-utredningens delbetänkande (Fö2024/00785). MSB har ett regeringsuppdrag om att ta fram förslag till en nationell cyberkrishanteringsplan i vilken, per kraven i NIS2-direktivet, den nationella cyberkrishanteringsmyndighetens roll och uppgifter närmare ska beskrivas – och av vilken det kommer att följa att MSB är den myndighet som är bäst lämpad att ha rollen som nationell cyberkrishanteringsmyndighet.

Om den föreslagna funktionen för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur etableras byggs en ytterligare struktur för organisation och hantering av cyberrelaterade incidenter upp. Med hänsyn till finanssektorns centrala betydelse för samhällets funktionalitet och de många beroenden som finns mellan finanssektorn och andra NIS2-sektorer är det dock enligt MSB:s mening centralt att undvika etablerandet av parallella och icke sammanhängande strukturer. Sådana riskerar att bidra till otydlighet vad gäller ansvarsförhållande och försvåra arbetet med att bygga heltäckande lägesbilder och nyttja synergier vid cyberrelaterade kriser som påverkar flera sektorer. MSB föreslår därför följande:

Förslag: För att tillgodose behovet av koordinering och samverkan mellan den nya krishanterande funktionen och den utsedda nationella cyberkrishanteringsmyndigheten föreslår MSB att Riksbanken, med stöd av artikel 9 punkt 1 i NIS2-direktivet, pekas ut som sektorsvis cyberkrishanteringsmyndighet för den finansiella sektorn. Riksbankens uppgifter som cyberkrishanteringsmyndighet utförs inom ramen för krishantering i finansiell sektor. Detta innebär att den nya funktionen kopplas samman med den kommande nationella cyberkrishanteringsmyndighetens verksamhet på ett tydligt och formaliserat sätt.

En sådan lösning innebär att Riksbankens arbete med krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur skulle utgöra en integrerad del i den struktur för arbete med särskilt allvarliga incidenter som etableras genom den kommande planen för hantering av cybersäkerhetsincidenter och kriser.[2] Det skulle inkludera Riksbanken i en struktur för arbete med lägesbilder, hantering av incidenter, privat-offentlig samverkan, beredskapshöjande åtgärder med mera samt ge Riksbanken en naturlig plattform för nära samverkan avseende krishantering med:

- den nationella cyberkrishanteringsmyndigheten
- det nationella cybersäkerhetscentret (NCSC)
- beredskapsmyndigheter med koppling till beredskapssektorerna Ekonomisk säkerhet och Finansiella tjänster
- myndigheter med sektorsansvar för andra beredskapssektorer
- andra berörda aktörer inom EU
- andra privata och offentliga aktörer.

MSB blir därmed den samordnande cyberkrishanteringsmyndigheten gentemot EU med uppgift att hantera storskaliga cybersäkerhetsincidenter och kriser. Inträffar cybersäkerhetsincidenter och kriser med bäring på den finansiella sektorn kommer ett redan i förväg väl etablerat samarbete mellan de båda cyberkrishanteringsmyndigheterna underlätta hanteringen av både samhällsstörningen och dess orsak.

Den föreslagna funktionen behöver samverka med EU-SCICF, NCSC, och den samordnande cyberkrishanteringsmyndigheten

I syfte att kunna fullgöra sitt uppdrag behöver den krishanterande funktionen enligt MSB:s bedömning ha ett nära samarbete med flera olika myndigheter och funktioner, inte minst

[2] Fö2023/01219 Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram underlag och ge förslag till nationell plan för hantering av cybersäkerhetsincidenter och kriser

inom ramen för EU-samverkan. Roller och ansvarsfördelning behöver vara tydliga, särskilt i fråga om informationsutbyte och incidentrapportering.

DORA-förordningen innehåller inga bestämmelser eller krav på en ny funktion eller krishanteringsplan, men stödjer inrättandet av krishanteringsfunktioner för den finansiella sektorn. Däremot har Europeiska systemrisknämnden (ESRB) utfärdat en rekommendation rörande ett ”pan-European systemic cyber incident coordination framework for relevant authorities” (EU-SCICF) inom finanssektorn. Målsättningen är att skapa ett ramverk för en effektiv samordnad reaktion på EU-nivå i händelse av en cyberincident som hotar den finansiella stabiliteten samt till att stödja myndigheternas uppgifter enligt artikel 49 i DORA-förordningen. Syftet med EU-SCICF är att kunna hantera möjliga negativa konsekvenser av cyberincidenter som kan påverka den finansiella stabiliteten. Regeringen har ännu inte tagit slutlig ställning till vilka eller vilken myndighet som ska vara del av detta ramverk. Enligt MSB:s bedömning bör en nära samverkan etableras mellan EU-SCICF, den finansiella sektorns nationella krishanteringsfunktion på Riksbanken[3], det nationella cybersäkerhetscentret och den samordnande nationella cyberkrishanteringsmyndigheten. MSB anser att myndighetens remissvar på Promemorian Digital operativ motståndskraft för finanssektorn (Fi2024/00073) gällande cyberkrishantering även bör beaktas här.

Det finns kvarstående risker med att placera funktionen utanför beredskapsförordningens ramar

Om Riksbanken pekas ut som sektorsvis cyberkrishanteringsmyndighet för den finansiella sektorn förbättras förutsättningarna för krishantering kopplad till allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur. Samtidigt kvarstår vissa risker för överlappande ansvar och arbetsuppgifter gentemot Finansinspektionen som sektorsansvarig myndighet för beredskapssektor Finansiella tjänster.

I promemorian framgår att det är nödvändigt att den krishanterande funktionen som föreslås även bedriver ett visst krisförberedande arbete för att skapa förutsättningar för effektiv hantering av en allvarlig driftstörning. MSB menar att detta riskerar att leda till ytterligare otydligheter i ansvar mellan myndigheterna då det förberedande arbetet idag samordnas i sektorn genom den sektorsansvariga myndighetens samordnande roll. Detta kan även få följdeffekter för fortsatt beredskapsplanering avseende samordning, övningar och prioritering av åtgärder där Finansinspektionen och Riksbanken behöver samordnas.

6.5 Funktionens styrning och ledning

MSB rekommenderar att Riksbanken samverkar specifikt med den utsedda nationella cyberkrishanteringsmyndigheten samt den gemensamma kontaktpunkten enligt NIS2-direktivet vid framtagande av instruktionen. Att få möjlighet att framföra sina synpunkter innan en ny instruktion antas eller ändras är väsentligt för att få en harmoniserad och heltäckande krishantering som både gynnar finanssektorn och övriga NIS2-sektorer.

[3] Som MSB i detta remissvar föreslår ska utpekas som sektorsvis cyberkrishanteringsmyndighet.

6.6 Deltagare och samverkan

MSB ser positivt på skrivelsen gällande nära samverkan med NCSC samt att funktionen ska samverka med MSB i syfte att delge de lägesbilder som funktionen har tagit fram. Det är även viktigt att funktionen bidrar med informationsutbyte och informationsdelning till MSB och NCSC med anledning av det uppdrag som finns att ta fram och dela lägesbilder och lägesuppfattningar på cybersäkerhetsområdet.

6.10 Utvidgad informationsplikt

MSB anser att funktionens relation till den övriga beredskapsstrukturen måste göras så tydlig som möjligt. Myndigheten stödjer därför förslaget om att Riksbanken även ska hålla Finansinspektionen underrättad om viktigare frågor under fredstida krissituationer och vid höjd beredskap, för att på så sätt säkerställa att det finns tydliga kopplingar till sektorsansvaret, inklusive rapporteringsansvar.

Givet funktionens centrala roll och det faktum att en kris inom den finansiella sektorns digitala infrastruktur kan få stora tvärsektoriella konsekvenser bedömer MSB, till skillnad från promemorian, att Riksbanken också bör få ett särskilt författningsreglerat ansvar att på förfrågan hålla MSB informerat, på samma sätt som myndigheter under regeringen har enligt 12§ förordning (2022:524) om statliga myndigheters beredskap.[4]

I övrigt anser MSB även att funktionens arbetssätt och struktur bör anpassas efter etablerade arbetssätt och arbetssätt som utvecklas inom beredskapsstrukturen. Det är viktigt att den nya funktionen tar hänsyn till Gemensamma grunder – ramverk för samverkan och ledning i utvecklingen av arbetssätt. Ett 60-tal aktörer har tillsammans arbetat fram innehållet i ramverket för att tydliggöra och ge stöd i hur vi arbetar tillsammans vid fredstida kriser och under höjd beredskap.

8 Konsekvenser

MSB menar att det inte i tillräckligt hög grad framgår vilka konsekvenser förslaget kan få för det fortsatta arbetet inom beredskapssektorn Finansiella tjänster. Förslaget kan exempelvis innebära tillkommande överlappande ansvar med parallella funktioner inom den finansiella sektorn. En annan möjlig konsekvens av föreslagen åtgärd är att överlapp och glapp i såväl planering som operativ krishantering kan bli alltför stora för att ge tillräckliga förutsättningar att hantera en kris eller krigssituation. För att hantera verkningarna av en fredstida kris eller ett krig finns, utöver vad som framgår av promemorian, också andra ansvarsområden inom sektor Finansiella tjänster som behöver beaktas och inarbetas i den operativa hanteringen. Det kan till exempel avse försäkring, kapitalmarknad, inlåning och utlåning med mera.

MSB saknar också en övergripande konsekvensbeskrivning av vad förslaget kan innebära för det civila beredskapssystemet i sin helhet. Genom att skapa en funktion med ansvar både för operativ hantering och krisförberedande arbete utanför den struktur som upprätthålls av förordning (2022:524) om statliga myndigheters beredskap, påverkas den

[4] ”Varje myndighet ska även på förfrågan från Myndigheten för samhällsskydd och beredskap lämna den information som behövs för att Myndigheten för samhällsskydd och beredskap ska kunna fullgöra sina uppgifter enligt 7 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.”

principiella grunden för det system som nu byggs upp med utgångspunkt i förslagen i SOU 2021:25 Struktur för ökad motståndskraft. Om en eller flera sektorer hänskjuter ansvar till en myndighet som varken är sektorsansvarig myndighet eller lyder under beredskapsförordningen problematiseras ambitionen att skapa tydliga lednings- och ansvarsförhållanden för samordning inom det civila försvaret. MSB menar sammantaget att den instans som är satt att leda samordning inom respektive beredskapssektor i regel bör vara den som svarar för att leda helheten, såväl det beredskapsuppbyggande och förberedande arbetet likväl som den operativa krishanteringsfunktionaliteten. Det är därför viktigt att noggrant beakta möjliga konsekvenser för det civila beredskapssystemet och de sektorsansvariga myndigheternas uppdrag i de fall särregleringar övervägs.

Övriga synpunkter

Funktionen behöver planera och dimensioneras för höjd beredskap och krig

Det framgår att funktionen ska kunna användas under höjd beredskap, men i stora delar av promemorian används främst ordet kris och fredstida krissituationer samt allvarliga driftstörningar. Om den föreslagna funktionen etableras anser MSB att det är viktigt att det särskilt tydligt kommuniceras att det är en funktion som ska kunna verka i hela hotskalan och att funktionen dimensioneras för höjd beredskap och ytterst krig.

I detta ärende har generaldirektör Charlotte Petri Gornitzka beslutat. Karl Bruno har varit föredragande. I den slutliga handläggningen har också avdelningschefen Robert Wallén och enhetschefen Alexandra Nordlander deltagit.

Charlotte Petri Gornitzka Karl Bruno

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984