



Finansdepartementet

Operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur

Sammanfattning av uppdraget

En sakkunnig person (i det följande utredaren) ges i uppdrag att utreda och lämna förslag på en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur. Syftet med uppdraget är att skapa förutsättningar att vid en sådan driftstörning i möjligaste mån kunna upprätthålla nödvändiga finansiella tjänster, i synnerhet betalningssystemet, och därmed värna den finansiella stabiliteten.

En krisledning av det aktuella slaget ska inte aktiveras vid varje tillfälle då det förekommer en allvarlig driftstörning i den finansiella sektorns digitala infrastruktur. En allvarlig driftstörning i den finansiella sektorns digitala infrastruktur som slår ut nödvändiga finansiella tjänster kan dock snabbt leda till att en allvarlig kris inträffar i samhället. I förlängningen kan en allvarlig driftstörning även hota den finansiella stabiliteten. Det är privata företag som tillhandahåller samtliga finansiella tjänster i den finansiella sektorn. De finansiella företagen ska ha en sådan motståndskraft att de själva, i linje med ansvarsprincipen, kan hantera allvarliga driftstörningar – även i krissituationer. I en situation där driftstörningen riskerar att leda till att samhället slutar fungera ställs dock andra krav på att även det offentliga kan behöva agera för att nödvändiga finansiella tjänster i möjligaste mån ska kunna upprätthållas för att värna den finansiella stabiliteten.

Mot denna bakgrund ska utredaren

- föreslå en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur,

- föreslå vilken myndighet som ska ansvara för funktionen och hur samverkan med andra berörda myndigheter bör regleras,
- föreslå hur samarbetet mellan privat och offentlig sektor ska utformas,
- föreslå när och hur en sådan krisledningsfunktion ska kunna aktiveras,
- kartlägga vilka behov av stödinsatser till finansiella företag som kan bli aktuella vid en allvarlig driftstörning och göra en analys avseende vem som ska tillhandahålla dessa,
- föreslå hur krisledningsfunktionen bör verka och vilka åtgärder som funktionen bör vidta under perioder när den inte är att betrakta som aktiverad,
- föreslå vilka åtgärder som krisledningsfunktionen ska kunna vidta vid en allvarlig driftstörning, och
- lämna nödvändiga författningsförslag.

Utredaren, som ska biträdas av en sekreterare, ska påbörja uppdraget den 1 juni 2023. Uppdraget ska redovisas senast den 31 december 2023.

Uppdraget att föreslå en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorn

Bakgrund

De senaste årens snabbt ökande digitalisering innebär att finansiella tjänster är beroende av fungerande nätverks- och informationssystem. Den digitala utvecklingen medför stora möjligheter, såsom bättre utbud av tjänster och ökad effektivitet, men också ökade risker. I takt med den betydande försämringen av säkerhetsläget ökar risken för olika former av allvarliga driftstörningar som kan få omfattande negativa effekter för den finansiella sektorn. Behovet av säkerhet är särskilt stort när det gäller nödvändiga finansiella tjänster, som behöver upprätthållas för att samhället ska fungera. En finansiell tjänst är nödvändig om ett bortfall av, eller en svår störning i verksamheten, på kort tid kan leda till att en allvarlig kris inträffar i samhället eller att samhällets förtroende för hela eller delar av det finansiella systemet rubbas och vars driftstörning i förlängningen hotar den finansiella stabiliteten.

I den finansiella sektorn tillhandahålls samtliga finansiella tjänster av privata företag, även sådana tjänster som betraktas som nödvändiga för att samhället ska fungera. Det finns omfattande regelverk som ställer krav på att finansiella företag har tillräckligt hög säkerhet i sina system för att kunna stå emot driftstörningar och kunna hantera konsekvenserna av dessa. De rättsakter

som nyligen har antagits på EU-nivå ställer ytterligare krav på företagens digitala och fysiska motståndskraft oavsett vad störningen beror på (NIS2- och CER-direktiven¹ och Dora-förordningen²). Det ingår i både Finansinspektionens och Riksbankens verksamheter att genom tillsyn och systemtester säkerställa att företagen lever upp till kraven och har tillräckligt motståndskraftiga system. I Riksgäldskontorets arbete ingår att säkra kontinuitet för de svenska myndigheternas betaltjänster och myndigheten kan därför ställa krav på bankerna i den statliga betalningsmodellen.

En grundprincip i svensk krisberedskap är den så kallade ansvarsprincipen. Den innebär att alla som har ansvar för en viss verksamhet under normala förhållanden också har ett ansvar för att verksamheten fungerar under en krissituation. De finansiella företagen har därför ett ansvar att själva ta höjd för operativa risker och ha säkra och motståndskraftiga system för att på egen hand kunna hantera en driftstörning. Ansvarsprincipen innebär ett ansvar för varje aktör att samverka med andra aktörer, ofta i andra sektorer än den egna. Ansvaret innebär också att under en kris kunna bedriva verksamhet och hantera situationer.

En allvarlig driftstörning i den finansiella sektorns digitala infrastruktur där nödvändiga finansiella tjänster slås ut kan snabbt leda till att en allvarlig kris inträffar i samhället. I förlängningen kan en sådan driftstörning även hota den finansiella stabiliteten. Vid en sådan allvarlig driftstörning som i förlängningen hotar den finansiella stabiliteten kan driftstörningens omfattning, komplexitet och konsekvenser innebära att det krävs insatser utöver företagens egen förmåga att hantera krisen. Sådana driftstörningar behöver dessutom ofta hanteras skyndsamt. Därmed ställs andra krav på att även det offentliga kan behöva agera för att nödvändiga finansiella tjänster i möjligaste mån ska kunna upprätthållas för att värna den finansiella stabiliteten.

I dagsläget finns inte någon organisation eller funktion som kan ta ett sådant operativt ansvar. Detta har i flera olika sammanhang lyfts fram som en brist som behöver åtgärdas. Se till exempel Finansinspektionens rapport den 6 maj 2022 ”Förstärkt digital motståndskraft hos företag i den finansiella sektorn”, Finansinspektionens, Riksbankens och Riksgäldskontorets gemen-

¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen samt Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft

² Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn

samma rapport i december 2022 till Finansiella stabilitetsrådet ”Ansvarsfördelning och samverkansformer rörande cybersäkerhet i den svenska finansiella sektorn” samt Internationella valutafondens slutsatser i 2022 års granskning av den svenska finansmarknaden inom ramen för fondens Financial sector assessment program.

Riksgäldskontoret och Finansinspektionen är sedan den 1 oktober 2022 beredskapsmyndigheter i beredskapssektorn Finansiella tjänster enligt förordningen (2022:524) om statliga myndigheters beredskap (beredskapsförordningen). Riksgäldskontoret är dessutom beredskapsmyndighet i beredskapssektorn Ekonomisk säkerhet. Enligt förordningen ska beredskapsmyndigheterna ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. De ska även verka för att övriga statliga myndigheter, kommuner, regioner, sammanslutningar och näringsidkare som är berörda utvecklar sin förmåga i dessa avseenden. Beredskapsmyndigheterna ska vid höjd beredskap i första hand inrikta sin verksamhet på uppgifter som har betydelse för totalförsvaret. Beredskapsmyndigheterna har ett brett uppdrag att samverka både med varandra och övriga statliga myndigheter, berörda länsstyrelser och civilområdesansvariga länsstyrelser, kommuner och regioner, näringsidkare, sammanslutningar samt med Försvarmakten avseende behovet av stöd till det militära försvaret.

Finansinspektionen är dessutom sektorsansvarig myndighet för beredskapssektorn Finansiella tjänster. Den sektorsansvariga myndigheten ska inom sin beredskapssektor leda arbetet med att samordna åtgärder inför och vid fredstida krissituationer och höjd beredskap. Den ska också driva på arbetet inom beredskapssektorn, stödja beredskapsmyndigheterna samt verka för att uppgifter och roller inom beredskapssektorn tydliggörs. I uppdraget ingår också att samverka med andra berörda myndigheter och med näringslivet. Försäkringskassan är sektorsansvarig myndighet för beredskapssektorn Ekonomisk säkerhet.

Beredskapsförordningen reglerar statliga myndigheters beredskapsuppgifter inför och under fredstida krissituationer och höjd beredskap. Förordningen reglerar även de särskilda uppgifter som de myndigheter som är utpekade som beredskapsmyndigheter och sektorsansvariga myndigheter har. Förordningen reglerar dock inte myndighets- och sektorsspecifika uppgifter. Vid en fredstida krissituation som berör den finansiella sektorn har även Riksbanken

en roll. Riksbanken omfattas inte av beredskapsförordningen, men i 5 kap. lagen (2022:1568) om Sveriges riksbank (riksbankslagen) finns det krav på Riksbankens agerande under fredstida krissituationer och höjd beredskap, inbegripet att allmänheten ska kunna göra betalningar även under sådana omständigheter.

Sammanfattningsvis kan det konstateras att den finansiella sektorn är uppbyggd på så sätt att privata företag tillhandahåller de finansiella tjänsterna och myndigheternas uppdrag är av övervakande eller tillsynande karaktär. Detta innebär att den offentliga sektorn i nuläget har mycket begränsade möjligheter att agera vid en allvarlig driftstörning i den finansiella sektorns digitala infrastruktur och att bistå i arbetet med att upprätthålla nödvändiga finansiella tjänster för att värna den finansiella stabiliteten. Den nya beredskapslagstiftningen ändrar inte myndigheternas uppdrag i detta hänseende och skapar inga utökade möjligheter för dem att agera för att aktivt motverka den allvarliga driftstörningen och dess effekter.

En ny operativ krisledningsfunktion

Beredskapsarbetet inom den finansiella sektorn kan behöva kompletteras med en funktion inom offentlig sektor som kan säkerställa att det finns en operativ krisledning som kan aktiveras med kort varsel för att kunna hantera en allvarlig driftstörning som slår ut nödvändiga finansiella tjänster och i förlängningen hotar den finansiella stabiliteten. Med allvarlig driftstörning avses inte nödvändigtvis enbart cyberattacker av viss omfattning, vilka riskerar att leda till allvarliga störningar i den finansiella sektorns digitala infrastruktur som i förlängningen hotar den finansiella stabiliteten. Även andra allvarliga driftstörningar kan uppstå som får liknande konsekvenser som en cyberattack. Till exempel skulle ett omfattande avbrott i elförsörjningen eller i telekommunikationen kunna få likartade konsekvenser för den finansiella sektorns digitala infrastruktur som en direkt riktad, omfattande cyberattack. På samma sätt kan en allvarlig driftstörning i den finansiella sektorns digitala infrastruktur medföra allvarliga störningar i beredskapssektorn Ekonomisk säkerhet, till exempel om statliga utbetalningar inte kan genomföras. Den operativa krisledningsfunktionens roll bör dock inte vara att upprätthålla verksamhet i andra samhällsviktiga sektorer, utan att bistå finansiella företag i syfte att upprätthålla nödvändiga finansiella tjänster för att värna den finansiella stabiliteten.

En operativ krisledningsfunktion bör vara utformad så att den kan arbeta snabbt och effektivt i syfte att så fort som möjligt vidta de åtgärder och i förekommande fall fatta de beslut som behövs för att

- skapa en korrekt lägesbild av driftstörningen och dess möjliga konsekvenser,
- motverka allvarliga konsekvenser av driftstörningen,
- hantera de konsekvenser som uppstår av driftstörningen, och
- (om möjligt) hantera den aktuella driftstörningen.

Funktionen behöver även snabbt kunna involvera och få till stånd ett samarbete med andra berörda aktörer, både inom privat och offentlig verksamhet.

Utredaren ska därför

- föreslå en funktion för operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur,
- föreslå vilken myndighet som ska ansvara för funktionen och hur samverkan med andra berörda myndigheter bör regleras,
- föreslå hur samarbetet mellan privat och offentlig sektor ska utformas, och
- lämna nödvändiga författningsförslag.

Utredaren ska beakta de befintliga strukturer, funktioner och regler som finns för att undvika en dubblering av dessa.

Förutsättningar för att aktivera den operativa krisledningen

En krisledning av det aktuella slaget ska inte aktiveras vid varje tillfälle då det förekommer en allvarlig driftstörning i den finansiella sektorns digitala infrastruktur. De finansiella företagen ska ha en sådan motståndskraft att de själva, i linje med ansvarsprincipen, kan hantera driftstörningen. I ett läge där en driftstörning i finansiella företag slår ut nödvändiga finansiella tjänster med följden att en allvarlig kris inträffar i samhället som i förlängningen hotar den finansiella stabiliteten kan dock den operativa krisledningen behöva aktiveras.

En potentiell kris i den finansiella sektorns digitala infrastruktur behöver skyndsamt hantering. För att undvika osäkerhet i en pressad situation och åstadkomma en effektiv aktivering av krisledningsfunktionen behöver det därför på ett transparent och förutsebart sätt framgå under vilka förut-

sättningar som en sådan funktion ska aktiveras. Det behöver även finnas tydliga rutiner och tillvägagångssätt för hur funktionen ska aktiveras samt anges vem som har ansvar för att sammankalla krisfunktionen.

Utredaren ska därför

- föreslå när och hur en sådan krisledningsfunktion ska kunna aktiveras, och
- lämna nödvändiga författningsförslag.

Krisledningsorganisationens uppdrag och mandat

För att en krisledningsfunktion ska kunna agera vid en allvarlig driftstörning, som slår ut nödvändiga finansiella tjänster eller hotar den finansiella stabiliteten, behöver den ha ett tydligt mandat och rätt verktyg för att kunna hantera krisen. I dagsläget saknas dock en genomlysning av vilka stödinsatser till finansiella företag som kan bli aktuella vid en sådan allvarlig driftstörning och vilka som ska tillhandahålla dessa. Det handlar här om insatser både för att komma till rätta med själva störningen och för att hantera konsekvenserna av denna. En kartläggning av behovet av stödinsatser behöver därför göras i syfte att kunna identifiera vilket mandat som den operativa krisledningen ska ha. Utredaren ska utgå från att de åtgärder och verktyg som kan bli aktuella kan behöva tas i bruk omgående samt att de endast ska användas under en begränsad tid.

En operativ krisledning ska aktiveras först när en allvarlig driftstörning inträffar. Utöver ett tydligt mandat förutsätter en väl fungerande krishantering att krisledningsfunktionen är väletablerad, att de aktörer som ingår i funktionen har tydliga roller att agera utifrån och en upparbetad nära dialog mellan privat och offentlig sektor. Detta förutsätter i sin tur att det upprätthålls någon form av beredskapsarbete knutet till krisledningsfunktionens uppdrag även när denna är ”vilande”.

Utredaren ska därför

- kartlägga vilka behov av stödinsatser till finansiella företag som kan bli aktuella vid en allvarlig driftstörning och göra en analys avseende vem som ska tillhandahålla dessa,

- föreslå hur krisledningsfunktionen bör verka och vilka åtgärder som funktionen bör vidta under perioder när den inte är att betrakta som aktiverad, och
- föreslå vilka åtgärder som krisledningsfunktionen ska kunna vidta vid en allvarlig driftstörning.

Konsekvensbeskrivningar

Utredaren ska beräkna förslagets ekonomiska konsekvenser och analysera konsekvenser i övrigt för företag och det allmänna. Om förslag som lämnas innebär offentligfinansiella kostnader ska förslag till finansiering lämnas. Utredaren ska även i övrigt tillämpa riktlinjerna i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Kontakter och redovisning av uppdraget

Utredaren, som ska biträdas av en sekreterare, ska påbörja uppdraget den 1 juni 2023. Uppdraget ska redovisas senast den 31 december 2023. Till utredaren ska knytas en referensgrupp med representanter från berörd offentlig och privat sektor.

Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämpligt, ha dialog med och inhämta upplysningar inom Regeringskansliet (däribland Enheten för försäkring, pension och myndighetsstyrning i Finansdepartementet, Enheten för samordning av samhällets krisberedskap i Försvarsdepartementet samt Nationella säkerhetsrådgivaren i Statsrådsberedningen), Finansinspektionen, Riksbanken, Riksgäldskontoret, Försäkringskassan, Nationellt cybersäkerhetscenter och de myndigheter som detta består av, samt med andra myndigheter, självreglerande organ och intresseorganisationer som berörs.

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, utredningsväsendet och EU. Av särskilt betydelse är att beakta arbetet i utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, NIS2, och EU:s direktiv om kritiska entiteters motståndskraft, CER (dir. 2023:30) samt arbetet med vidareutveckling av Nationellt cybersäkerhetscenter. Även eventuella konsekvenser i förhållande till bestämmelserna i Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av

förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, DORA, behöver beaktas.