Staff memo

Cyberrisker och finansiell stabilitet

Joacim Häggmark, Kristian Jönsson, Ulrika Nilsson och Johanna Stenkula von Rosen

Juni 2023

SVERIGES RIKSBANK

Innehållsförteckning

Staff memo

I ett staff memo kan medarbetare på Riksbanken offentliggöra kvalificerade analyser i relevanta frågor. Det är en tjänstemannapublikation som är fri från policyslutsatser och individuella ställningstaganden i aktuella policyfrågor. Publikationen godkänns av berörd avdelningschef. De åsikter som uttrycks i staff memos är författarnas egna och ska inte uppfattas som Riksbankens ståndpunkt.

Sammanfattning/förord/inledning

Riksbankens arbete med finansiell stabilitet har som syfte att värna det finansiella systemets grundläggande funktioner. Detta gör Riksbanken genom att kartlägga och analysera de sårbarheter och risker som hotar dessa funktioner. Dessutom arbetar Riksbanken för att det finansiella systemet ska kunna stå emot störningar. Den allt högre digitaliseringen av samhället, och inte minst den tekniska utvecklingen inom finanssektorn, innebär att cyberrisker kan bli systemrisker och därmed hota den finansiella stabiliteten. I detta staff memo illustrerar vi hur cyberrelaterade sårbarheter och risker kan hänga ihop med Riksbankens arbete med finansiell stabilitet. Dessutom ger vi övergripande exempel på hur cyberrisker kan inkorporeras i en centralbanks arbete med finansiell stabilitet för att det finansiella systemet ska kunna bli mer motståndskraftigt mot cyberrelaterade störningar. Hur samverkan mellan aktörerna i finanssektorn, och samverkan mellan olika samhällsviktiga sektorer, kan öka motståndskraften mot cyberincidenter tas också upp.

Författare: Joacim Häggmark, Kristian Jönsson, Ulrika Nilsson och Johanna Stenkula von Rosen, verksamma vid Riksbankens avdelning för finansiell stabilitet[1]

[1]Vi tackar Karl Blom, Mattias Hector, Olof Sandstedt, Marianne Sterner och Annika Svensson för värdefulla kommentarer.

1 I Riksbankens arbete med finansiell stabilitet har cyberrisker en naturlig plats

För att samhällsekonomin ska fungera på ett bra sätt, och för att ekonomin på sikt ska få utrymme att växa, krävs ett väl fungerande och stabilt finansiellt system. Flera myndigheter, däribland Riksbanken, har i uppdrag att verka för finansiell stabilitet. I detta arbete kartlägger och analyserar Riksbanken sårbarheter och risker som kan hota stabiliteten. Riksbanken verkar också för att det finansiella systemet ska ha motståndskraft mot störningar. Till detta kommer att Riksbanken genom sitt stabilitetsuppdrag också har ett specifikt uppdrag att övervaka finansiella infrastrukturföretag så att dessa lever upp till internationellt överenskomna standarder.

Att det finansiella systemet är stabilt innebär att dess grundläggande funktioner upprätthålls, så att det är möjligt att betala, spara, investera och hantera risk. Risker som hotar dessa funktioner hotar därmed också den finansiella stabiliteten.

I det finansiella systemet finns det en mängd olika aktörer som var och en kan påverka i vilken utsträckning de grundläggande funktionerna upprätthålls. Till exempel tillhandahåller infrastrukturföretagen grundläggande tjänster som exempelvis möjliggör betalningar, andra finansiella överföringar samt registrering av värdepapper. Ytterligare exempel är banker och andra finansiella företag som bland annat tillhandahåller olika typer av betalnings-, sparande- och finansieringstjänster till sina kunder, det vill säga till hushåll och företag som därmed också är viktiga aktörer i det finansiella systemet.

Aktörerna i det finansiella systemet är aktiva både på olika finansiella marknader, där handel med olika finansiella instrument äger rum, och i realekonomin, där handel med varor och tjänster sker.[2]

Det finns vissa typer av risker som kan hota det finansiella sektorns aktörer eller marknader i sådan utsträckning att hela det finansiella systemets grundläggande funktioner också hotas. Sådana risker brukar benämnas systemrisker.

Den allmänna digitaliseringen av samhället har pågått under lång tid och inom den finansiella sektorn går teknikutvecklingen fort. Digitaliseringen av samhället medför stor nytta och stora fördelar, exempelvis genom att vi får nya varor och tjänster samt effektivare och säkrare processer. Men med digitaliseringen följer också en exponering mot risker som hotar de IT-komponenter och de IT-system som digitaliseringen vilar på. Digitaliseringen medför per automatik en exponering mot cyberrisker.

Eftersom aktörerna i det finansiella systemet är direkt beroende av IT-komponenter och IT-system för sin verksamhet blir cyberrisker en viktig faktor att beakta när det kommer till det finansiella systemets grundläggande funktioner.[3] Cyberrisker kan med

[2] Elestedt et al (2021) beskriver mer i detalj olika aktörers roll i det finansiella systemet.

[3] Se även Kashyap och Wetherilt (2019) som utifrån ett makrotillsynsperspektiv, med det finansiella systemets kritiska ekonomiska funktioner i åtanke, kopplar ihop cyberrisker och finansiell stabilitet.

andra ord vara systemrisker.[4] Därmed får de också en naturlig plats i Riksbankens arbete med finansiell stabilitet.[5]

2 Cyberrisker kan utgöra ett direkt hot mot finansiell stabilitet

2.1 Tillgänglighet, riktighet och konfidentialitet viktigt för att bevara stabiliteten

När det gäller cyberrisker generellt lyfts ofta tre aspekter fram i analysen. Dessa är tillgänglighet, riktighet och konfidentialitet för IT-system och för data som finns i systemen. De tre aspekterna är relevanta också när det kommer till cyberrisker och finansiell stabilitet.

Tillgängligheten är en viktig aspekt när det kommer till IT-system. Om en viktig IT-komponent inte längre skulle fungera eller ett viktigt IT-system inte längre skulle vara tillgängligt skulle grundläggande funktioner i det finansiella systemet kunna falla bort. Brister i tillgängligheten kan därmed få en direkt effekt på den finansiella stabiliteten.

Men även om alla komponenter och system fungerar som de ska så finns det cyberrisker som kan hota stabiliteten. Mycket av den aktivitet som sker i det finansiella systemet är nämligen direkt beroende av korrekt information till exempel om priser och saldon. Om sådan information inte längre skulle vara riktig kan det få en direkt påverkan på olika aktörer och marknader. Därmed skulle även det finansiella systemet och dess förmåga att leverera grundläggande funktioner påverkas.

Den tredje aspekten av cyberrisker, konfidentialitet, rör huruvida information i ett system är tillgänglig för obehöriga. I detta fall är det inte lika uppenbart hur den direkta kopplingen till finansiell stabilitet ser ut. Men konfidentialiteten kan likväl ha bäring på finansiell stabilitet, men då snarare genom sådana indirekta kopplingar som tas upp nedan.

2.2 En hög koncentration av ekonomisk funktionalitet eller av IT-system kan öka sårbarheten

En IT-incident, eller en störning som det skulle kunna benämnas i arbetet med finansiell stabilitet, som har direkt påverkan på det finansiella systemets grundläggande funktioner kan se ut på flera olika sätt. Till exempel kan ett visst centralt IT-system drabbas av en störning samtidigt som det saknas alternativ i det finansiella systemet

[4] Synen att cyberrisker kan vara systemrisker för det finansiella systemet förs fram av exempelvis Adelmann et al (2020), ESRB (2020), ESRB (2022), Fell et al (2022) och Koo et al (2022). Elestedt et al (2021) fokuserar på cyberattacker och framhåller att de kan utgöra en systemrisk. Maurer och Nelson (2021) ger dessutom uttryck för synen att det snarast är en tidsfråga innan en cyberattack kommer att ha återverkningar på finansiell stabilitet.

[5] Utifrån det analytiska ramverket som presenteras av ESRB (2020) diskuterar t.ex. Elestedt et al (2021) ingående hur en cyberattack direkt och indirekt kan påverka den finansiella stabiliteten.

som kan leverera samma ekonomiska funktion. Men en störning kan också påverka genom att den på en och samma gång påverkar flera olika system som i ett normalläge skulle kunna utgöra alternativ till varandra för uppnå en viss ekonomisk funktion. Det går också att tänka sig en störning i ett IT-system där funktionen initialt kan uppnås i ett annat system men där störningen gradvis sprider sig till de andra systemen och därmed också gradvis urholkar den finansiella stabiliteten.

De olika aspekterna av cyberrisk och typerna av störning illustrerar att olika typer av arrangemang och åtgärder kan behövas för att stärka den finansiella stabiliteten. Om det inom det finansiella systemet inte finns någon utbytbarhet när det kommer till en viss IT-komponent eller ett visst IT-system, och samma ekonomiska funktion inte går att uppnå på annat håll i det ekonomiska systemet, blir det av yttersta vikt att komponenten eller systemet har en hög IT-säkerhet. Detta innebär mycket god förmåga att skydda sig mot incidenter. Men detta är inte tillräckligt. Det är också viktigt att det tidigt går att upptäcka och hantera eventuella IT-incidenter. Dessutom är det viktigt att det går snabbt att återställa eller ersätta de komponenter eller system som drabbats av en incident som har påverkat eller riskerar att påverka stabiliteten i det finansiella systemet.

När det är svårt att ersätta en komponent eller ett system för att uppnå en viss funktion behöver man satsa på att utveckla alternativ som kan ta över de grundläggande ekonomiska funktioner som riskerar att falla bort vid en IT-incident. Sett från ett systemperspektiv behöver ett sådant arbete inte enbart ta sikte på att ta fram alternativ till en enskild IT-komponent eller ett enskilt IT-system hos en specifik aktör. En central utgångspunkt kan i stället vara hur det på bästa sätt går att hitta alternativ som främjar hela det finansiella systemets stabilitet.

I de fall där olika IT-system och aktörer är utbytbara kan det behövas en annan typ av arrangemang och åtgärder för att värna den finansiella stabiliteten. Det är såklart alltjämt viktigt att upprätthålla IT-skyddet för de olika IT-systemen som bidrar till de grundläggande ekonomiska funktionerna, men det kan dessutom bli viktigt att uppmärksamma vilka faktorer det är som gör att flera datorsystem samtidigt kan drabbas av problem. Det kan till exempel handla om att flera system drivs på samma ställe, med samma mjukvara eller hårdvara eller är beroende av samma tjänsteleverantörer och därför skulle kunna löpa större risk att drabbas av en störning samtidigt. Genom att känna till vilka faktorer som bidrar till att flera system kan drabbas av en störning samtidigt finns det bättre förutsättningar att minska det finansiella systemets sårbarhet för cyberrisker.

Ibland kan det finnas risk att en initial störning i en IT-komponent eller ett IT-system sprids vidare till andra komponenter och system. I sådana fall blir det viktigt att, förutom de två nyss nämnda aspekterna, vara medveten om vilka spridningsvägar som kan finnas mellan komponenter och system som är viktiga i den finansiella sektorn samt att ha planer för man kan stänga ner sådana spridningsvägar om det skulle behövas.

Sammantaget är det av viktigt att i arbetet med finansiell stabilitet uppmärksamma sårbarheter som uppkommer till följd av olika typer av koncentration av ekonomiska

funktioner och IT-resurser i det finansiella systemet samt hur störningar kan spridas mellan olika IT-system och aktörer.

3 Cyberrisker kan också utgöra ett indirekt hot mot finansiell stabilitet

Den finansiella sektorns aktörer är inte bara mycket beroende av sina egna IT-resurser. De är dessutom beroende av grundläggande samhälleliga funktioner som i sin tur vilar på andra IT-resurser. Det kan till exempel handla om elförsörjning eller data- och telekommunikationer. Störningar som slår mot sådana funktioner kan således, utan att direkt påverka IT-resurser inom finanssektorn, få följder som leder till negativa konsekvenser för det finansiella systemets grundläggande funktioner och därmed påverkar den finansiella stabiliteten.

De indirekta effekter som cyberrisker kan föra med sig behöver emellertid inte enbart verka genom tekniska kanaler. Det kan även finnas ett samspel med andra välbekanta ekonomiska spridningskanaler. Exempelvis skulle en IT-incident hos en tillsynes icke systemviktig aktör, eller hos en aktör utanför den finansiella sektorn, kunna få konsekvenser för stabiliteten om den mindre incidenten samtidigt påverkar det allmänna förtroendet för det finansiella systemet. Eftersom förtroende är en stöttepelare för finansiella system kan alla störningar som påverkar förtroendet negativt också hota den finansiella stabiliteten. Tillgänglighet, riktighet och konfidentialitet, som ovan beskrevs i termer av direkta effekter på finansiell stabilitet, är i högsta grad aktuella även när det kommer till indirekta kanaler och aspekter som rör förtroendet för det finansiella systemet.

I detta sammanhang kan man notera att förtroendet för det finansiella systemet inte endast är kopplat till förtroendet för privata aktörer. Myndigheter kan också spela en viktig roll när det gäller att upprätthålla det samlade förtroendet för det finansiella systemet. Det är således viktigt att också stabilitetsvårdande myndigheter upprätthåller ett högt skydd mot cyberrisker så att stabilitetsstörningar inte kan spridas in i det finansiella systemet genom en förtroendekanal som går via myndigheterna.

Det finns, förutom förtroendeaspekterna, minst två andra typer av spridningskanaler där tekniska och ekonomiska aspekter samverkar. För det första kan en IT-incident hos en mindre aktör leda till kaskadeffekter i hela det finansiella systemet. Detta betyder att om en aktör, som initialt ter sig mindre betydelsefull, inte kan fullfölja sina åtaganden så kan det uppkomma konsekvenser hos andra aktörer vilket i sin tur leder till vidare spridning av problemen så att hela systemet till sist riskerar att påverkas. Sådana kaskadeffekter skulle exempelvis kunna uppkomma när det gäller betalningar[6] eller avveckling av värdepapper[7]. Det som kan ske i en sådan situation är att det finansiella systemets inneboende sårbarheter, kopplade till exempelvis likviditet eller belåning av värdepapper, har träffats av en cyberstörning som utlöser problem.

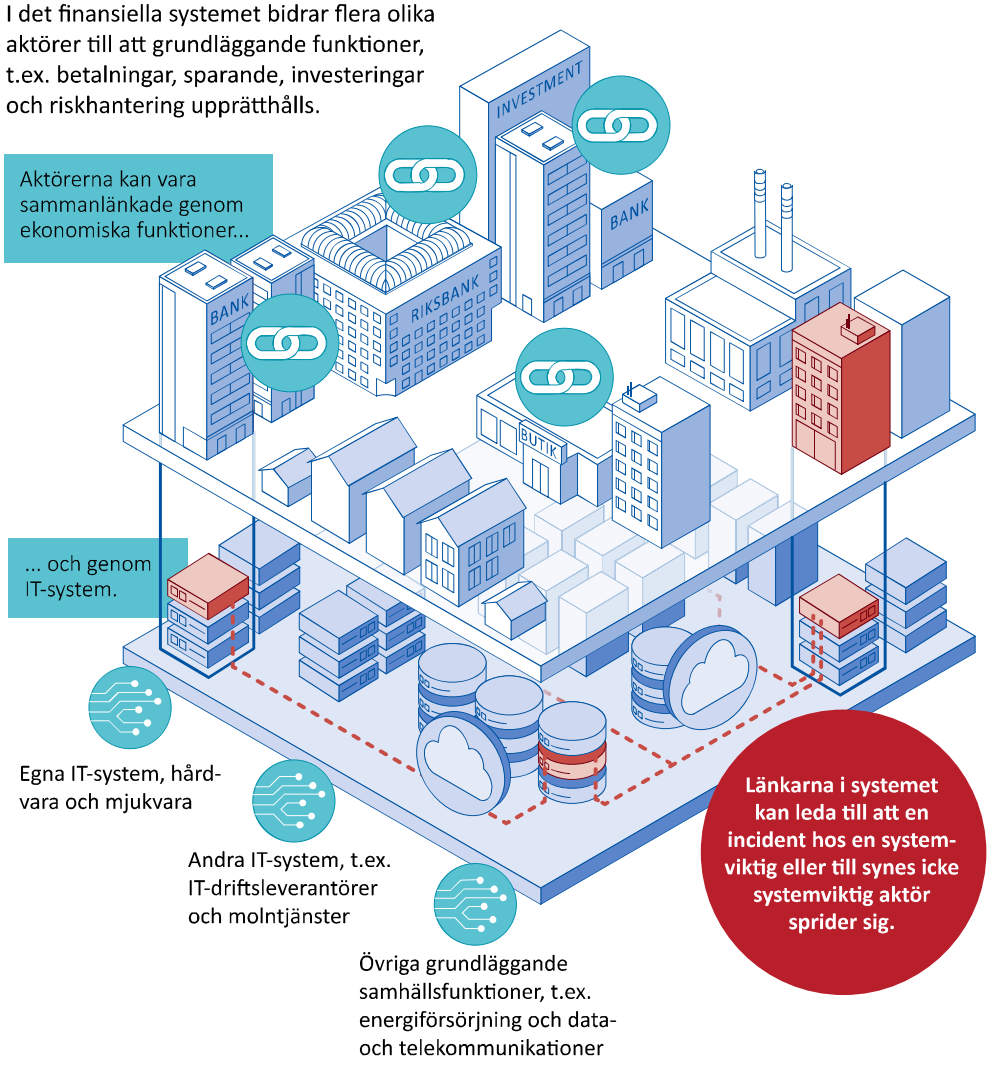
[6] Till exempel Brando et al (2022) och Eisenbach et al (2022) diskuterar cyberrisker och kaskadeffekter kopplade till betalningar.

[7] Kopp et al (2017) nämner kaskadeffekter relaterade till avveckling av värdepapper.

För det andra skulle en cyberincident i realekonomin, genom det finansiella systemets exponering mot kredit- och likviditetsrisker, kunna få effekter på den finansiella stabiliteten.[8] Detta skulle kunna inträffa om IT-resurser på något håll i realekonomin påverkas och det därför uppstår tveksamheter kring de inblandade aktörernas förmåga att fullgöra sina ekonomiska åtaganden. Exempelvis skulle en störning kunna få effekter på den ekonomiska situationen i många eller särskilt viktiga företag, vilket i sin tur skulle kunna påverka aktörer i det finansiella systemet och därmed den finansiella stabiliteten.

Cyberrisker kan alltså påverka den finansiella stabiliteten även indirekt genom både tekniska och ekonomiska spridningskanaler. De olika kanalerna kan dessutom i vissa lägen samverka med varandra (se figur 1). Detta gör att den samlade bilden av cyberriskerna är komplex och att det finns en mängd samspel som är viktiga att uppmärksamma när man ska bedöma potentiella effekter på den finansiella stabiliteten.

Figur 1. Cyberincidenter kan sprida sig genom sammanlänkningar.
I det finansiella systemet bidrar flera olika aktörer till att grundläggande funktioner, t.ex. betalningar, sparande, investeringar och riskhantering upprätthålls.



[8] Se till exempel Fell et al (2022).

4 Komplexiteten kräver ett brett anslag i arbetet med cyberrelaterade systemrisker

4.1 Cybersäkerheten hos enskilda aktörer viktig för finansiella systemets motståndskraft[9]

Viktigt med starkt skydd hos aktörerna

För att motståndskraften i det finansiella systemet ska bli tillräckligt stark behöver de enskilda aktörerna i den finansiella sektorn ha ett starkt skydd mot IT-incidenter i sina IT-system. Det ska alltså inte med lätthet kunna inträffa händelser som ger omfattande eller långtgående konsekvenser. Ett starkt skydd innebär exempelvis att det blir väldigt svårt och oproportionerligt resurskrävande för obehöriga parter att påverka eller bereda sig tillgång till IT-systemen i fråga.

Ett starkt skydd innebär dels att köpa in säkra produkter och tjänster och sedan använda dem på rätt sätt för att uppnå en hög cybersäkerhet. Men IT-system är till sin natur svåra att överblicka och i väldigt många system upptäcks det efter hand olika typer av svagheter och sårbarheter. Så ett starkt skydd i IT-systemen innebär också att aktörerna behöver ha en fullständig överblick över vilka system som är i drift, vilka versioner av systemen som används samt se till att systemen kontinuerligt uppdateras allteftersom svagheter och sårbarheter upptäcks. Det är också viktigt att regelbundet se över behörigheter i systemen och att inte ge högre behörighet än nödvändigt i systemen.

Systemets motståndskraft kan också stärkas om aktörerna sinsemellan kan dela information om sårbarheter som de upptäcker i systemen och information om på vilket sätt sårbarheterna kan komma att leda till IT-incidenter. Sådan informationsdelning behövs både mellan aktörerna i en viss sektor och mellan olika sektorer (mer om detta i avsnitt 4.2 och 4.3 nedan).

En viktig del av de cyberrisker som det finansiella systemet är exponerade mot har sitt ursprung hos aktörer som har avsikt och förmåga att åstadkomma skada, så kallade antagonistiska aktörer. En viktig del i arbetet med en hög IT-säkerhet inom finanssektorn är således att kartlägga vilka antagonistiska hot som finns mot såväl system som aktörer inom finanssektorn. För att få fram en nyanserad hotbild behöver såväl myndigheter som privata aktörer samverka och dela information, kunskap och erfarenheter. Att känna till hotbilden, och därmed få förutsättningar att motverka hoten, stärker hela systemets motståndskraft mot cyberrisker.[10]

[9] För en generell diskussion om åtgärder för en hög cybermotståndskraft se också NCSC (2022).

[10] Ett exempel på hur sådan samverkan kan se ut är den pilotverksamhet som Nationellt Cybersäkerhetscenter har startat med finanssektorn.

För att få en bild av hur skyddet kan förbättras kan aktörerna kontinuerligt genomföra olika typer av tester av sina system. På så sätt kan de få indikationer om hur starkt skyddet i IT-systemen är samtidigt som det går att upptäcka vad som kan förbättra skyddet utan att en IT-incident först har inträffat. Denna typ av tester kan se ut på många olika sätt. En typ är de så kallade TIBER-testerna. Där tar man först fram en bild av hot mot och möjliga sårbarheter i en aktörs IT-system och försöker sedan utnyttja dessa för att ta sig in i systemen. På så sätt får man veta vilka åtgärder som kan höja motståndskraften hos aktören.[11]

Viktigt med god förmåga att upptäcka och åtgärda IT-incidenter

Oavsett hur hög skyddsnivå som uppnås i IT-systemen så är det så gott som omöjligt att helt undvika IT-incidenter. Det är därför viktigt att aktörer som skulle kunna spela en systemviktig roll i det finansiella systemet också kan upptäcka och åtgärda incidenter. Det betyder exempelvis att en aktör med onda avsikter som tagit sig förbi IT-systemens skydd inte ska kunna röra sig fritt i systemen under någon längre tid utan att bli upptäckt och utkastad.

En bra förutsättning för en hög förmåga att kunna upptäcka IT-incidenter är att aktörerna har tillgång till en verksamhetsfunktion som dygnet runt, årets alla dagar, bevakar det som händer i IT-systemen och tydligt och tidigt signalerar om en incident skulle upptäckas eller om det finns tecken som tyder på att en incident är förestående. En sådan funktion behöver ha tillgång till information från IT-systemen, exempelvis säkerhetsloggar, och behöver dessutom ha redskap som analyserar denna information och omedelbart signalerar om tecken på en incident upptäcks. Aktörer som tillhandahåller IT-system som har en direkt betydelse för det finansiella systemets grundläggande funktioner kan även överväga möjligheten att dessutom använda sig av befintliga avancerade detekterings- och varningssystem.

Om en IT-incident skulle upptäckas är det viktigt att den kan åtgärdas. Aktörer som bidrar till att upprätthålla systemviktiga ekonomiska funktioner behöver därför ha kapacitet att snabbt åtgärda IT-incidenter. Det är också en fördel om de kan utreda hur incidenterna uppstått och vilka konsekvenser har blivit.

Viktigt med snabb återstart om viktiga funktioner drabbas av allvarliga incidenter

Om det skulle gå så långt att det blir driftavbrott i IT-systemen så är det viktigt att det finns en beredskap att återstarta systemen. Liknande gäller om data i systemen inte längre går att lita på eller om data i ordinarie system förstörs och försvinner. Det är viktigt att då kunna läsa tillbaka data som med rimlig säkerhet är riktiga.

Detta kan exempelvis innebära att det behövs flera uppdaterade säkerhetskopior av data och ibland hela IT-system där minst en av kopiorna har ett sådant skydd att den inte kan påverkas av samma IT-incident som ordinarie system och andra kopior. Det

[11] ECB:s ramverk för hotbildsbaserade penetrationstester, TIBER-EU, och Riksbankens arbete med en svensk anpassning av detta ramverk, TIBER-SE, är exempel på hur centralbanker kan bidra till att öka det finansiella systemets motståndskraft mot vissa typer av cyberrisker.

kan också innebära att det finns rutinbeskrivningar för hur IT-system ska återstartas efter en allvarlig IT-incident samt att det behövs rutinbeskrivningar för hur data ska återläsas, även i ett allvarligt scenario där den ordinarie IT-miljön inte är tillgänglig.

Precis som det går att göra olika typer av tester för att bedöma såväl säkerhet som förmåga att upptäcka och åtgärda problem i IT-system så går det att göra olika tester och övningar när det kommer till återstart av system och återläsning av data från backup-kopior. Om aktörerna regelbundet genomför sådana tester och övningar ökar förutsättningarna för att IT-incidenter ska bli så korta som möjligt och därmed minskar stabilitetsriskerna i det finansiella systemet.

Hur lång tid viktiga IT-system kan vara oanvändbara utan att det blir ett problem för stabiliteten är såklart svårt att säga och beror i väldigt stor utsträckning på hur situationen ser ut. Men det är viktigt att alla systemviktiga verksamheter i den finansiella sektorn snabbt och säkert kan återstarta sina system och återläsa data. I detta sammanhang kan det också vara viktigt att det, redan det inträffar en incident, finns en ungefärlig uppfattning om hur lång tid det kan ta att återstarta system eller återläsa data under olika scenarier.

Även myndigheterna i finansiella sektorn behöver upprätthålla en hög cybersäkerhet

Det är viktigt att notera att det inte bara är de privata aktörerna inom den finansiella sektorn som behöver ha en hög cybersäkerhet med ett starkt skydd, en god förmåga att upptäcka och åtgärda IT-incidenter och beredskap att snabbt återstarta viktiga system. De stabilitetsvårdande myndigheterna, det vill säga Finansinspektionen, Riksbanken och Riksgälden, har alla en central roll i det finansiella systemet och behöver även de se till att verksamheten har en hög motståndskraft mot cyberrisker.

Det finns minst två anledningar till att det är viktigt att även de stabilitetsvårdande myndigheterna upprätthåller en god motståndskraft mot cyberincidenter. För det första skulle IT-incidenter hos myndigheterna kunna ha direkta effekter på myndigheternas förmåga att fullgöra sina uppdrag inom finansiell stabilitet. För det andra så skulle incidenter också kunna komma att påverka förtroendet för det finansiella systemet, vilket i sig skulle kunna få konsekvenser för stabiliteten.

4.2 Det krävs också ett systemperspektiv för att värna finansiell stabilitet

Insatser av enskilda aktörer är inte tillräckliga för att göra det finansiella systemet motståndskraftigt

Även om det är av stor vikt att alla aktörer i den finansiella sektorn har god motståndskraft mot cyberincidenter så räcker det sannolikt inte för att motståndskraften ska bli tillräckligt stor i det finansiella systemet som helhet. Som ett komplement behöver det således finnas ett systemövergripande perspektiv som återspeglas i arbetet med att motverka cyberrisker.

Det finns åtminstone två konkreta situationer då det är viktigt att ta systemperspektivet i beaktande. Den första situationen är när en enskild aktör sätter in alla de åtgärder som utifrån den egna verksamheten är välavvägda men där aktörens vikt i systemet innebär att åtgärderna inte är tillräckliga från ett systemperspektiv. Denna situation kan uppkomma i ett läge där kostnaderna för en IT-incident sett från systemets perspektiv överstiger den kostnad som är aktuell när en enskild aktör överväger att skydda sig mot IT-incidenten. Liknande mekanismer, dvs. där enskilda aktörer inte till fullo internaliserar de risker som kan uppkomma på systemnivå, finns i det finansiella systemet även när det kommer till andra typer av risker än cyberrisker. Ett sätt att hantera denna typ av risker är att använda olika typer av systemövergripande verktyg, till exempel makrotillsynsverktyg. Sådana verktyg skulle kunna användas också på cyberområdet för att öka den samlade motståndskraften i det finansiella systemet.

Det går också att tänka sig en andra situation där det inte är tillräckligt att enskilda aktörer agerar var för sig utan där det istället krävs ett systemperspektiv för att systemet ska bli motståndskraftigt. Detta skulle kunna vara i en situation när de inblandade aktörerna i och för sig gör tillräckligt stora ansträngningar men där det krävs en samordning mellan dem för att ansträngningarna ska bära frukt och stärka systemets motståndskraft.

Ett exempel på en sådan situation skulle kunna vara om flera aktörer samtidigt inser att det behövs extern hjälp för att klara en snabb återhämtning vid en cyberincident. Var för sig kan aktörerna innan incidenten inträffar ha klarat att binda till sig tillräckligt med sådan extern hjälp. Men om det skulle visa sig att flera aktörer samtidigt skulle drabbas av en cyberincident så finns det utan samordningen en risk att aktörerna har knutit till sig samma externa hjälp och att denna då blir en knapp resurs. I ett sådant läge skulle en koordinering mellan aktörerna kunna bidra till att öka systemets samlade motståndskraft.

Analys av beroenden inom det finansiella systemet kan vara ett första steg mot att öka motståndskraften

Ett av de första stegen för att stärka det finansiella systemets motståndskraft mot cyberincidenter är att kartlägga hur systemets olika centrala ekonomiska funktioner hänger ihop och vilka olika typer av IT-system som de i sin tur är beroende av. Men det räcker inte att kartlägga vilka system som används av en viss aktör. Man behöver också veta hur olika ekonomiska och tekniska funktioner hos olika aktörer i sektorn är sinsemellan beroende av varandra.

En sådan systemövergripande kartläggning kan göras på flera olika sätt, men ett sätt är att använda sig av så kallade cyberstresstester.[12] I ett sådant tar man fram ett scenario med en hypotetisk cyberincident. Sedan undersöker en utvald skara av aktörer i finanssektorn vilka effekter den hypotetiska cyberincidenten får på de egna systemen

[12] Se mer om verktyget som kallas Cyber Resilience Scenario Testing (CyRST) i ESRB (2023).

och på kopplingar till andra aktörer. På detta sätt går det att få en indikation om hur stora de systemövergripande effekterna kan bli av en viss IT-incident.[13]

Den finansiella stabiliteten kan gynnas av kunskap om när en cyberincident riskerar att påverka systemet

Cyberincidenter inträffar kontinuerligt och det är rimligt att förvänta sig att de allra flesta incidenter tas om hand av den eller de aktörer som drabbas utan att det får konsekvenser som drabbar hela det finansiella systemet. Men om det finns en risk att en incident närmar sig en sådan omfattning att hela det finansiella systemets stabilitet kan påverkas är det viktigt att de stabilitetsvårdande myndigheterna träder in och i möjligaste mån motverkar en sådan utveckling. För att kunna göra detta på ett fullgott sätt är det viktigt att det går att avgöra när en incident går från att vara en angelägenhet för en enskild aktör till att bli en händelse som behöver involvera myndigheter med ansvar för finansiell stabilitet. Som ett redskap för att få en sådan bild, och för att kunna vidta åtgärder för att motverka att incidenten får systemövergripande effekter, kan det vara till hjälp att definiera konkreta nivåer som utlöser olika typer av åtgärder hos de stabilitetsvårdande myndigheterna.[14] Åtgärderna skulle till exempel kunna handla om att öka informationsinhämtningen, sprida information mellan myndigheter, förbereda för olika typer av mildrande eller motverkande åtgärder eller allmänna krisförberedande åtgärder. Det övergripande syftet med att definiera nivåerna är att i förväg ha en klar bild av vilka incidenter som riskerar att få systemövergripande effekter och av vad som kan komma att behöva göras för att förhindra sådana effekter.

Samverkan och sektorsövergripande riktlinjer kan bidra ytterligare till motståndskraften[15]

Samverkan inom den finansiella sektorn gör det lättare att värna systemperspektivet och stärka motståndskraften mot cyberincidenter. För de stabilitetsbevarande myndigheterna, Finansinspektionen, Riksbanken och Riksgälden, finns det flera olika samarbeten som kan säkerställa systemperspektivet, till exempel arbetet med cyberfrågor inom ramen för Finansiella stabilitetsrådet och övningar av olika slag. Ett samarbete av särskilt vikt skulle dessutom kunna vara att etablera en strategi för det mer långsiktiga arbetet med att stärka motståndskraften mot cyberincidenter i den finansiella sektorn. En sådan strategi skulle exempelvis kunna specificera hur myndigheterna anser att de enskilda aktörerna kan bidra till det finansiella systemets stabilitet genom att öka sin motståndskraft. Den skulle också kunna beskriva vilka systemövergripande

[13] Cyberstresstester för aktörer i den finansiella sektorn används eller övervägs av institutioner som Bank of England, Europeiska centralbanken samt den danska tillsynsmyndigheten Finanstilsynet.

[14] Se mer om verktyget som kallas Systemic Impact Tolerance Objective (SITO) i ESRB (2023).

[15] Även lagstiftning, såsom säkerhetsskyddslagen, kan återspegla samhällets behov av att ta systemövergripande hänsyn. Vissa risker kan ha en så pass liten sannolikhet för att inträffa att det för en enskild verksamhet kan vara rimligt att acceptera den. Om risken skulle realiseras skulle det emellertid kunna ha stora konsekvenser för samhället, vilket innebär att risken ändå behöver hanteras. Säkerhetsskyddslagen reglerar hanteringen av skydd av säkerhetskänslig verksamhet och aktörer inom den finansiella sektorn kan komma att behöva göra säkerhetsskyddsanalyser för att utreda om man har verksamhet som kan vara av betydelse för Sveriges säkerhet.

överväganden som behövs inom sektorn. Även en inriktning för sektorns arbete med krisberedskapsfrågor skulle kunna få plats i en sådan strategi.

Men även samverkan mellan myndigheter och privata aktörer är av vikt för att stärka motståndskraften i det finansiella systemet. Redan idag finns det etablerade samarbetsforum, exempelvis inom ramen för Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS) och en pilotverksamhet för finansiell sektor med ett samverkansforum inom ramen för Nationellt cybersäkerhetscenter (NCSC)[16]. I båda dessa behandlas frågor relaterade till cybersäkerhet. Att sådant arbete fortsätter också framöver är centralt för att öka det finansiella systemets motståndskraft mot cyberrisker och cyberincidenter.

4.3 Det finansiella systemets stabilitet nära kopplad till andra grundläggande samhällsfunktioner

Det är inte bara den finansiella sektorn och det finansiella systemet som i högre grad exponeras mot cyberrisker som en följd av den ökade digitaliseringen. Detsamma gäller många olika sektorer i samhället, varav flera dessutom kan ha en indirekt påverkan på det finansiella systemets stabilitet.[17] Till exempel är det finansiella systemets funktionalitet beroende av att grundläggande samhälleliga funktioner, som elförsörjning och data- och telekommunikation, upprätthålls. Om sådana funktioner skulle drabbas av omfattande cyberincidenter skulle det med stor sannolikhet också kunna påverka den finansiella stabiliteten. Cybersäkerhet är alltså inte en aspekt som behöver uppmärksammas bara när det kommer till det finansiella systemet utan det bör vara en nationell angelägenhet som rör såväl den finansiella sektorn som andra samhällsviktiga sektorer.

Det faktum att cybersäkerhet är en angelägenhet på nationell nivå talar för att det också krävs samordning och åtgärder på nationell nivå för att möta cyberriskerna i samhället. Argumenten för att beakta flera sektorer på nationell nivå är desamma som argumenten för att samtidigt beakta flera aktörer inom finanssektorn. Det vill säga, det finns problem som på nationell nivå är så pass övergripande att enskilda aktörer eller enskilda sektorer sannolikt inte kan genomföra tillräckliga åtgärder för att komma till rätta med problemen. Således blir samordning på nationell nivå lika nödvändig för samhällets samlade motståndskraft mot cyberincidenter som samordningen inom finanssektorn blir för det finansiella systemets motståndskraft.

Ett initiativ som kan stärka cybermotståndskraften i samhället i stort, och därmed också i det finansiella systemet, är skapandet av Nationellt Cybersäkerhetscenter. NCSC är ett samarbete mellan fyra myndigheter: Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt Säkerhetspolisen. Dessa

[16] NCSC utgörs av ett samarbete mellan fyra myndigheter: Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt Säkerhetspolisen. Det arbete som dessa fyra myndigheter gör i cybersäkerhetscentret ska ske i nära samverkan med Försvarets materielverk, Polismyndigheten samt Post- och telestyrelsen.

[17] Se till exempel Forscey et al (2022) för en diskussion.

ska, inom ramen för sina respektive uppdrag, fördjupa sitt samarbete på cybersäkerhetsområdet och på så sätt kunna koordinera arbetet med att förebygga och åtgärda cyberincidenter. NCSC:s myndigheter ska dessutom förmedla råd och stöd när det gäller cyberrisker och utgöra en nationell plattform för samverkan och informationsutbyte med andra aktörer, såväl privata som offentliga, inom cybersäkerhetsområdet.

Ett samverkansforum för finansiell sektor har skapats som ett pilotprojekt i NCSC. Här deltar både privata aktörer och myndigheter. Bland myndigheterna återfinns dels de som har nära koppling till NCSC, dels de myndigheter som har ansvar för finansiell stabilitet, det vill säga Finansinspektionen, Riksbanken och Riksgälden. Bland de privata aktörerna återfinns branschorganisationer och företag inom finanssektorn.

Nyligen aviserades att Försvarets radioanstalt ska ta över ansvaret för det nationella cybersäkerhetscentret.[18] Att en myndighet får ansvaret för cybersäkerhetscentret kan medföra att det finns större möjligheter att ge centret uppdrag som går längre än det uppdrag som finns idag. Centret skulle bland annat aktivt kunna bidra till det systematiska cybersäkerhetsarbetet hos myndigheter, till exempel genom att tydligt belysa vilka krav som behöver ställas på IT-system i vissa typer av upphandlingar. Centret skulle också kunna få uppdraget att systematiskt dela information som kommer fram i olika myndigheters säkerhetsgranskningar av IT-system. Idag finns ingen samordning på detta område, vilket kan leda till ineffektivitet och ökad riskexponering eftersom varje myndighet behöver göra sina egna säkerhetsgranskningar och inte på ett enkelt sätt kan förmedla resultaten till andra myndigheter. En enda central cybersäkerhetsmyndighet skulle också kunna vara till hjälp när information om sårbarheter i IT-system behöver förmedlas till såväl privata som offentliga aktörer. Som ett ytterligare exempel skulle det kunna bli lättare att tilldela cybersäkerhetscentret resurser, så att det aktivt kan bistå olika aktörer och sektorer med cyberkompetens i händelse av allvarliga cyberincidenter som är av sådan karaktär att de riskerar att få omfattande påverkan på viktiga samhällsfunktioner eller på Sveriges säkerhet.

5 Sammanfattning

Digitaliseringen av finanssektorn medför att såväl enskilda aktörer som hela det finansiella systemet exponeras mot cyberrisker. För att öka motståndskraften i systemet behövs insatser, såväl från enskilda aktörer som på systemövergripande nivå.

För en hög motståndskraft i systemet är det viktigt att aktörerna har ett starkt skydd, en hög förmåga att kunna upptäcka och åtgärda cyberincidenter samt en hög beredskap för att kunna återstarta system och återläsa data.

På systemnivå är det viktigt att kartlägga centrala funktioner i det finansiella systemet och deras beroende på olika IT-system. Det är också viktigt att bedöma vilken nivå av motståndskraft systemet som helhet har och hur olika åtgärder kan bidra till att stärka systemet.

[18] Se Kristersson et al (2023).

Att ta systemperspektivet är viktigt såväl inom den finansiella sektorn som på nationell nivå, exempelvis genom att beakta det ömsesidiga beroendet mellan den finansiella sektorn och andra samhällsviktiga sektorer. På så sätt kan det finnas förutsättningar för att öka hela samhällets motståndskraft mot cyberincidenter.

Referenser

Adelmann, Frank, Elliott, Jennifer, Ergen, Ibrahim, Gaidosch, Tamas, Jenkinson, Nigel, Khiaonarong, Tanai, Morozova, Anastasiia, Schwarz, Nadine och Wilson, Christopher (2020) Cyber Risk and Financial Stability: It's a Small World After All, IMF Staff Discussion Note, SDN/20/07, 7 december 2020, International Monetary Fund.

Brando, Danny, Kotidis, Antonis, Kovner, Anna, Lee, Michael och Schreft, Stacey L. (2022) Implications of Cyber Risk for Financial Stability, FEDS Notes, 12 maj 2022, Board of Governors of the Federal Reserve System.

Eisenbach, Thomas M, Kovner, Anna och Lee, Michael Junho (2022) Cyber Risk and the U.S. Financial System: A pre-mortem Analysis, Journal of Financial Economics, 145, sid. 802-826.

Elestedt, Lukas, Nilsson, Ulrika och Rosenvinge, Carl-Johan (2021) En cyberattack kan påverka den finansiella stabiliteten, Ekonomisk kommentar nr 8, 19 maj, Sveriges riksbank.

ESRB (2020) Systemic Cyber Risk, februari 2020, European Systemic Risk Board.

ESRB (2022) Mitigating Systemic Cyber Risk, januari 2022, European Systemic Risk Board.

ESRB (2023) Advancing macroprudential tools for cyber resilience, februari 2023, European Systemic Risk Board.

Fell, John, de Vette, Nander, Gardó, Sándor, Klaus, Benjamin och Wendelborn, Jonas (2022) Towards a Framework for Assessing Systemic Cyber Risk, Financial Stability Review, November 2022, European Central Bank.

Forscey, David, Bateman, Jon, Beecroft, Nick och Woods, Beau (2022) Systemic Cyber Risk: A Primer, 7 mars 2022, Carnegie Endowment for International Peace och Aspen Institute.

IVA (2022) Cybersäkerhet för ökad konkurrenskraft, Kungliga Ingenjörsvetenskapsakademin.

Kashyap, Anil K. och Wetherilt, Anne (2019) Some Principles for Regulating Cyber Risk, AEA Papers and Proceedings 2019, Vol 109, sid. 482-487.

Koo, Helga, van der Molen, Remco, Vermeulen, Robert, Verhoeks, Ralph och Pollastri, Alessandro (2022) A Macroprudential Perspective on Cyber Risk, Occasional Studies, Volume 20-1, 8 juni 2022, De Nederlandsche Bank.

Kopp, Emanuel, Kaffenberger, Lincoln och Wilson, Christopher (2017) Cyber Risk, Market Failures, and Financial Stability, IMF Working Paper WP/17/185, 7 augusti 2017, International Monetary Fund.

Kristersson, Ulf, Bohlin, Carl-Oskar, Jonson, Pål, Persson, Mats, Slottner, Erik och Strömmer, Gunnar (2023) FRA får ta över ansvaret för Sveriges cybersäkerhet, DN Debatt, 27 april 2023.

Maurer, Tim och Nelson, Arthur (2021) The Global Cyber Threat, Finance & Development, mars 2021, International Monetary Fund.

NCSC (2022) Cybersäkerhet i Sverige 2022 – Del 2: Rekommenderade säkerhetsåtgärder, Nationellt cybersäkerhetscenter.

SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK)