FÖRDJUPNING – Cyberrisker och finansiell stabilitet

Digitaliseringen i den finansiella sektorn innebär att sektorns aktörer exponeras mot cyberrisker. Aktörerna är dessutom tätt sammanlänkade både ekonomiskt och tekniskt. Därmed finns det en risk att en cyberincident hos en enskild aktör kan få konsekvenser för det finansiella systemets förmåga att upprätthålla sina grundläggande funktioner. Således kan cyberrisker också hota den finansiella stabiliteten. De enskilda aktörerna i den finansiella sektorn måste därför ha en hög cybersäkerhet, men det är också viktigt att de stabilitetsvårdande myndigheterna bidrar genom att säkerställa att systemperspektivet tas i beaktande i den finansiella sektorns arbete med cybersäkerhet. Även på nationell nivå krävs ett systemperspektiv för att öka hela samhällets motståndskraft mot cyberincidenter.

Cyberrisker kan hota stabiliteten i det finansiella systemet

Digitaliseringen medför stora fördelar. Men den medför också att den finansiella sektorn exponeras för cyberrisker, det vill säga risker som kan ha negativ påverkan på de IT-system som används eller på de data som lagras eller överförs i systemen.[129]

Omvärldsutvecklingen under de senaste åren, och då inte minst det förändrade säkerhetsläget i Sveriges närområde, har dessutom bidragit till att cyberhoten har ökat för svensk del, så också för aktörerna i den finansiella sektorn.[130]

Koncentration och sammanlänkning kan påverka stabiliteten i hela det finansiella systemet

Det finansiella systemet består av en mängd aktörer och marknader samt en uppsjö av sammanlänkningar som finns dem emellan. Flera faktorer i systemets uppbyggnad kan bidra till att det blir sårbart när det kommer till cyberrisker. Koncentration av ekonomisk funktionalitet, IT-system och leverantörer är en sådan faktor. Till exempel kan en koncentration av en viktig ekonomisk funktionalitet till ett fåtal aktörer öka sårbarheten. Detta beror på att hela funktionaliteten då kan försvinna från det finansiella systemet redan då få aktörer råkar ut för en IT-incident. På motsvarande sätt kan sår-

[129] För en ofta använd definition av cyberrisk och relaterade begrepp se exempelvis FSB Cyber Lexicon, november 2018, Rådet för finansiell stabilitet.

[130] Hur en cyberattack kan påverka den finansiella stabiliteten i Sverige beskrivs av Elestedt, L., m.fl. ”En cyberattack kan påverka den finansiella stabiliteten”, *Ekonomiska kommentarer* nr 8, 2020, Sveriges riksbank.

barheten öka om olika aktörer i den finansiella sektorn förlitar sig på samma eller väldigt snarlika IT-system, vare sig det handlar om hård- eller mjukvara. Detta beror på att om det finns en svaghet eller sårbarhet i en viss typ av system så riskerar detta att snabbt kunna påverka ansenliga delar av den finansiella sektorn. Det kan dessutom vara så att flera olika aktörer förlitar sig på samma leverantör av en viss typ av IT-tjänst (som en specifik molntjänst eller en specifik leverantör av IT-drift) och att en cyberincident hos denna leverantör kan få återverkningar hos flera aktörer samtidigt.

Förutom koncentration kan även teknisk och ekonomisk sammanlänkning mellan aktörerna i den finansiella sektorn öka sårbarheten. Detta beror på att IT-incidenter kan sprida sig från enskilda aktörer och IT-system till att så småningom påverka den finansiella stabiliteten.

För att systemriskerna ska minska måste aktörerna i finanssektorn ha en hög cybersäkerhet

Hög nivå av cybersäkerhet uppnås genom arbete i flera olika dimensioner

För att minska de cyberrisker som det finansiella systemet exponeras emot är det viktigt att aktörerna i den finansiella sektorn har en hög cybersäkerhet. För att uppnå en hög cybersäkerhet behöver man arbeta i flera olika dimensioner. Det är exempelvis viktigt att IT-systemen har ett högt skydd, att aktörerna i den finansiella sektorn har förmåga att upptäcka och åtgärda IT-incidenter samt att de har beredskap och förmåga att snabbt och säkert återstarta system och återläsa data.

Ett högt skydd mot IT-incidenter i IT-systemen minskar risken att systemen, eller data i systemen, blir otillgängliga eller att data otillbörligen sprids eller ändras. De IT-system som stödjer det finansiella systemets grundläggande funktionalitet behöver ha ett skydd som är dimensionerat för att stå emot cyberattacker i paritet med sådana som kan utföras av statsaktörer eller statsunderstödda aktörer. Det höga skyddet behöver finnas oavsett om det finansiella företaget som tillhandahåller den grundläggande funktionaliteten själv står för driften av IT-systemet eller om det finns en extern driftsleverantör.

För att undersöka sina system och få en bild av hur skyddet kan bli bättre är det viktigt att aktörerna kontinuerligt genomför olika typer av tester, till exempel penetrationstester, både i enskilda system och i hela IT-miljön.

Oavsett hur hög skyddsnivå som uppnås i IT-systemen är det så gott som omöjligt att helt undvika IT-incidenter. Det kan emellertid vara möjligt att begränsa skadorna om man har god förmåga att upptäcka och åtgärda IT-incidenter. Det kan exempelvis innebära att man har en funktion som dygnet runt, årets alla dagar, bevakar det som händer i IT-systemen och tydligt och tidigt larmar om en incident upptäcks eller om det finns tecken som skulle kunna tyda på att en incident är förestående. En sådan funktion behöver både ha tillgång till information från IT-systemen, såsom säkerhetsloggar, och ha tillgång till system som analyserar informationen och omedelbart signalerar om tecken på en IT-incident upptäcks. Aktörer som tillhandahåller IT-system som

har en direkt betydelse för det finansiella systemets grundläggande funktionalitet kan även undersöka möjligheten att få tillgång till avancerade tekniska detekterings- och varningssystem.[131]

Att ha god förmåga att åtgärda IT-incidenter kan exempelvis innebära att aktörer har tillgång till resurser som kontinuerligt, oavsett tid på dygnet eller dag på året, kan motverka cyberincidenter samt att de har tillgång till personalresurser som med kort varsel kan utreda hur incidenten har uppstått och vilka konsekvenser den har haft eller kan få.

Precis som när det kommer till tester av skyddet i IT-system är det viktigt att kontinuerligt testa och öva förmågan att upptäcka och åtgärda cyberincidenter. Aktörer som är systemviktiga för det svenska finansiella systemet kan exempelvis, som en del av sådana tester för att undersöka såväl skydd som förmågan att upptäcka och åtgärda cyberincidenter, genomföra hotbildsbaserade penetrationstester, så kallade TIBER-tester.[132]

I händelse av en allvarlig IT-incident behöver det finnas en hög beredskap och förmåga att snabbt och säkert återstarta system och återläsa data som med rimlig säkerhet är riktiga.[133] Detta kan exempelvis innebära att man har 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 kan också handla om rutinbeskrivningar för hur IT-system ska återstartas efter en allvarlig IT-incident samt att det finns rutinbeskrivningar för hur data ska återläsas, även i ett allvarligt scenario där den ordinarie IT-miljön inte är tillgänglig.

Precis som det är möjligt att göra olika typer av tester för att bedöma såväl säkerheten som förmågan att upptäcka och åtgärda problem i IT-system så kan det vara bra att göra tester och övningar när det kommer till återstart av system och återläsning av data från backup-kopior.

De aktörer som bedriver verksamhet inom den finansiella sektorn behöver se till att cybersäkerhetsarbetet ständigt beaktar dessa dimensioner och att motståndskraften mot cyberrisker kontinuerligt ökas.

[131] Finansinspektionen har tidigare indikerat att det tekniska detekterings- och varningssystem (TDV) som Försvarets radioanstalt har skulle kunna öka cybermotståndskraften hos de systemviktiga aktörerna i den finansiella sektorn (se rapporten ”Förstärkt digital motståndskraft hos företag i den finansiella sektorn”, 6 maj 2022, Finansinspektionen).

[132] TIBER är ett ramverk inom vilket man kan genomföra hotbildsbaserade penetrationstester och det finns implementeringar såväl på EU-nivå (se t.ex. TIBER-EU Framework, maj 2018, Europeiska centralbanken) som i Sverige (se *TIBER-SE Implementation Guide*, december 2019, Sveriges riksbank) och andra länder. Det är Riksbanken som har tagit fram den svenska implementeringen av TIBER-ramverket och samordnar TIBER-testerna i Sverige.

[133] Det finns olika riktlinjer för hur långa avbrottstider som kan tolereras (se till exempel sammanställningen i *Advancing macroprudential tools for cyber resilience*, februari 2023, Rådet för finansiell stabilitet).

Det krävs också ett systemperspektiv för att värna den finansiella stabiliteten

Insatser av enskilda aktörer är inte tillräckliga

Det är av stor vikt att alla aktörer i den finansiella sektorn långsiktigt och kontinuerligt arbetar för att minska cyberriskerna och öka motståndskraften. Men detta är inte tillräckligt för att motståndskraften i det finansiella systemet som helhet ska bli tillräckligt stor. Som ett komplement behöver det också finnas ett systemövergripande perspektiv i arbetet. En anledning till detta är att cybersäkerhet kan ses som en gemensam nyttighet i det finansiella systemet. Det betyder att en ansträngning som gynnar den enskilda aktören dessutom kan ha positiva effekter på hela det finansiella systemets motståndskraft mot cyberincidenter. Utan ett systemperspektiv på cybersäkerhet finns det bara incitament för aktörerna att agera utifrån sitt egna perspektiv vilket kan resultera i en alltför låg nivå på motståndskraften i systemet som helhet.

Systemperspektiv inom finansiell sektor

En första åtgärd för att värna systemperspektivet i den finansiella sektorn är att kartlägga hur systemets olika centrala ekonomiska funktioner hänger ihop och hur de i sin tur är beroende av olika typer av aktörer och IT-system. En andra åtgärd, som bidrar till hanteringen av en uppkommen IT-incident, är att stabilitetsvårande myndigheterna, utifrån kartläggningen, bildar sig en uppfattning om när en incident kan gå från att vara en angelägenhet för en enskild aktör till att bli en angelägenhet också för dem. Genom att i god tid identifiera när en händelse riskerar att påverka hela det finansiella systemet kan myndigheterna träda in och motverka de systemövergripande konsekvenserna.[134]

Samverkan inom den finansiella sektorn ökar möjligheterna att etablera ett systemperspektiv på cybermotståndskraft. För myndigheterna med ansvar inom finansiell stabilitet (Finansinspektionen, Riksbanken och Riksgälden) finns det flera samarbetsforum som kan bidra till systemperspektivet. Till exempel samarbetar man kring cyberfrågor inom ramen för det finansiella stabilitetsrådet. Men även samverkan mellan myndigheter och privata aktörer är av vikt för att stärka motståndskraften mot cyberincidenter i det finansiella systemet. Redan idag finns det etablerade samarbetsforum, exempelvis inom ramen för Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS).I detta forum behandlas frågor relaterade till cybersäkerhet. Denna typ av samarbete behöver fortsätta även framöver för att öka det finansiella systemets motståndskraft mot cyberrisker och cyberincidenter.

Samverkan mellan samhällsviktiga sektorer

Det är inte bara den finansiella sektorn som i hög grad exponeras mot cyberrisker. Detsamma gäller många andra samhällsviktiga sektorer, varav flera dessutom indirekt

[134] Se mer om verktygen som kallas Systemic Impact Tolerance Objective (SITO) och Cyber Resilience Scenario Testing (CyRST) i *Advancing macroprudential tools for cyber resilience*, februari 2023, Europeiska systemrisknämnden.

kan påverka det finansiella systemets stabilitet. Cybersäkerhet är således en angelägenhet som kräver samordning också på nationell nivå.

Ett initiativ som kan stärka motståndskraften mot cyberincidenter i samhället i stort, och därmed också i det finansiella systemet, är etablerandet av Nationellt cybersäkerhetscenter (NCSC).[135] För närvarande har NCSC:s arbete formen av en samverkan mellan fyra myndigheter inom ramen för deras respektive mandat. Det har nyligen aviserats ett förslag om att ge en av myndigheterna, Försvarets radioanstalt, ansvar för NCSC:s framtida verksamhet.[136] En positiv aspekt av ett sådant förslag är att detta ger förutsättningar för ett tydligare ansvar och ett tydligare mandat när det gäller centrets verksamhet. Att den finansiella sektorn inkluderas även i NCSC:s kommande arbete är viktigt för att värna såväl det finansiella systemets som hela samhällets motståndskraft mot cyberincidenter.

[135] NCSC är 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 samarbete med Försvarets materielverk, Polismyndigheten samt Post- och telestyrelsen.

[136] Se debattartikel av U. Kristersson mfl. (2023), 27 april, DN Debatt. "FRA får ta över ansvaret för Sveriges cybersäkerhet".