Anförande

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Datum	2023-05-04	FI dnr	23-2722
Talare	Andreas Heed		
Möte	Nationell konferens om informations- och cybersäkerhet inom finanssektorn 2023		

Operativ motståndskraft i finanssektorn

Digitalisering skapar utan tvekan stora möjligheter, såsom ökad variation och tillgänglighet till finansiella tjänster, snabbare betalningstransaktioner och effektivare produktionsprocesser. Men med ökad digitalisering kommer också risker för det finansiella systemet.

Jag vill ta det här tillfället i akt och dela med mig av några centrala risker som vi som myndighet ser med digitaliseringen av den finansiella sektorn och hur vi arbetar med dessa risker. Dessutom vill jag presentera några förslag och åtgärder som vi tror kan stärka den digitala motståndskraften i sektorn.

Den finansiella sektorn är sårbar

Tjänsterna i den finansiella sektorn är idag nästan uteslutande digitala. Det gör den finansiella sektorn särskilt sårbar för såväl destruktiva cyberangrepp som andra tekniska störningar, oavsett om de är avsiktliga eller inte.

Samtidigt är tjänsterna av stor betydelse för enskilda företag och hushåll och i flera fall samhällskritiska.

Att inte kunna utföra grundläggande finansiella tjänster till följd av en IT-incident är allvarligt i sig och kan orsaka stor skada för de som drabbas. Men under ogynnsamma förutsättningar kan skadan spridas och drabba samhället i stort. Det finns flera olika kanaler genom vilka skadorna kan spridas, men i grunden handlar det om att finansiella företag är beroende av allmänhetens och de finansiella marknadernas *förtroende*, och att dessa företag är tätt *sammanlänkade* på olika sätt.

När det gäller förtroende skulle det till exempel kunna handla om att kunder inte kan utföra grundläggande finansiella tjänster till följd av tekniska störningar eller om tillförlitligheten i data rörande kontobehållningar, skulder, fondandelar eller liknande börjar ifrågasätts hos ett institut. Om en sådan incident skulle ha en längre varaktighet eller inträffa i ett särskilt känsligt läge finns det en risk för att incidenten kan undergräva allmänhetens förtroende för andra finansinstitut. I förlängningen – om förtroendeförlusten blir tillräckligt stor – kan det skada det finansiella systemet som helhet och därmed utgöra ett hot mot den finansiella stabiliteten.

Sammanlänkningen kommer dels av olika typer av finansiella exponeringar, såsom lån eller derivatkontrakt som direkt knyter samman finansiella aktörer. Men hela det finansiella tjänsteutbudet är också beroende av tekniska system som är sammankopplade globalt, ofta med hög grad av komplexitet och bristande transparens.

Eftersom teknik och finansiella flöden är sammankopplade kan IT-relaterade störningar och incidenter – och bristande kapacitet att hantera sådana – skada hela systemets funktionsförmåga, vilket kan innebära stora samhällsekonomiska kostnader. I värsta fall kan det leda till att centrala funktioner i det finansiella systemet slås ut. Tekniken gör alltså ett redan tidigare starkt sammanlänkat system ännu mer sammanlänkat.

Min inledande poäng här idag är att den finansiella sektorn är sårbar för både avsiktliga och oavsiktliga tekniska störningar och en aktörs problem lätt kan bli allas problem. Dessa omständigheten har en stor betydelse för hur vi som myndighet ser på och angriper riskerna vi ser i sektorn, något jag återkommer till.

Vilka risker ser FI?

Vad gäller de finansiella företagens digitala motståndskraft är det tydligt att riskerna har ökat kraftigt de senaste åren. Vi ser flera drivkrafter bakom dessa ökade risker och jag tänkte ta upp några delar som vi ser som centrala.

För det första kan vi se ökade externa hot i form av cyberhot. Vi kan konstatera att finansiella företag ständigt är utsatta för intrångsförsök och olika typer av attacker. Risken har ökat för både överbelastningsangrepp och direkt destruktiva angrepp. Ökande spänningarna i omvärlden och den pågående ryska invasionen av Ukraina har också kraftigt försämrat det

säkerhetspolitiska läget, vilket ökar risken för att svenska intressen utsätts för angrepp i form av cyberattacker. Ser vi till själva utfallet det senaste året kan vi se att det framför allt är överbelastningsattacker som periodvis har varit intensiva.

Vår bild av cybersäkerheten i den svenska finansiella sektorn generellt sett är att den är god och att många företag arbetar aktivt med att bygga motståndskraft. Det är däremot tydligt att vissa aktörer kommit längre i sitt arbete än andra.

Ett konkret exempel är att flera finansiella företag behöver bli bättre på att i sin kontinuitetsplanering beakta de förändringar som sker både i den interna och externa miljön. Företagen behöver göra tillräckliga investeringar i processer och verktyg för att upprätthålla tillräckliga förmågor för att hantera inneboende kända risker på området, men även tänkbara framtida risker. Här är Covidpandemin ett bra exempel som visade på vikten för de finansiella företagen att ha effektiva och ändamålsenliga kontinuitetsplaner.

Med tanke på den ökade risken för attacker av olika slag är det också viktigt att företag inte bara fokuserar på kontinuitetsplanering, utan också prioriterar förebyggande åtgärder och bygger väldimensionerade skydd mot externa hot.

En annan faktor som driver risk kopplat till digital motståndskraft är det faktum att finansiella företag att i allt högre grad lägger ut kritisk verksamhet till tredjepartsleverantörer. Vissa tjänster levereras endast av en eller ett fåtal leverantörer, vilket skapar ett stort beroende till dessa leverantörer och de får en avgörande roll för en stor andel av finansmarknadens aktörer.

Tredjepartsleverantörerna lägger i sin tur ut verksamhet till andra leverantörer, vilket medför brist på transparens i hela leverantörskedjan. Med många aktörer i leveranskedjan är det också svårt för de finansiella företagen att utöva tillräckligt god styrning och kontroll över den verksamhet de bedriver och är ansvariga för. Koncentrationen av leverantörer till ett färre antal innebär också att ett intrång hos dessa riskerar att få en betydligt bredare påverkan än vad som annars skulle vara fallet.

Vilken är FI:s roll?

De risker vi pekar på är uppenbart sådana risker som det ligger i de finansiella företagens eget intresse att ta höjd för och hantera. Det finns förstås starka incitament att säkerställa att den egna verksamheten kan bedrivas utan avbrott.

Men som vi vet ställer även samhället höga krav på företagen genom gällande reglering om IT-och informationssäkerhet. Det är här FI kommer in i bilden. Det är vår uppgift att genom tillsyn se till att de finansiella företagen följer sådana regleringskrav.

Däremot har de enskilda företagen vare sig tillräcklig överblick eller tillräckliga incitament för att ta höjd för de risker som uppstår genom interaktionen mellan olika delar och aktörer i systemet och som kan leda till problem för hela det finansiella systemet.

Även här har FI en viktig uppgift. Utöver att granska det enskilda institutet är FI:s roll att bidra med ett system- eller samhällsperspektiv – att se till helheten på finansmarknaden – för att säkra den finansiella stabiliteten.

Det kan till exempel handla om att kartlägga beroendet av tredjeparts- och molntjänstleverantörer, och på så sätt kunna identifiera koncentrationsrisker där många finansiella institut är beroende av en och samma leverantör.

Men det kan även handla om att identifiera aktiviteter som behövs på ett övergripande plan för att främja hela det finansiella systemets stabilitet.

Vi har ett flertal förslag på sådana aktiviteter och åtgärder som vi bedömer kommer att stärka den digitala motståndskraften hos företagen i den finansiella sektorn och därmed systemets stabilitet.

Jag tänkte komma in på några av dessa förslag idag. Sammanfattningsvis kan man säga att det rör sig om en bred palett av olika åtgärder som involverar FI, men också flera andra myndigheter och inte minst de finansiella företagen själva.

Hur arbetar vi?

Jag tänkte först berätta något mer om hur vi arbetar och våra huvudsakliga uppdrag kopplade till operativ motståndskraft och IT- och informationssäkerhet.

Man kan säga att vårt arbete kopplat till operativ motståndskraft står på tre ben. Men gemensamt för dessa ben är att tyngdpunkten ligger på det förebyggande arbetet – dvs. så långt som möjligt förebygga problem som kan som kan hota det enskilda företagets och i förlängningen det finansiella systemets stabilitet.

Vi ska givetvis också ha beredskap för att kunna hantera en krissituation om den ändå inträffar, men tillsynsåtgärder inom ramen för de finansiella regelverken, såsom sanktioner och ingripanden, är sällan lämpliga redskap för att hantera akuta krissituationer.

Tillsyn enligt näringsrättslig reglering

Ett grundläggande verktyg för att åstadkomma en hög IT- och informationssäkerhet hos företagen i den finansiella sektorn är som jag nämnde tillsyn. FI har sedan länge bedrivit IT- och informationssäkerhetsrelaterad tillsyn enligt de regler som gäller för hantering av operativa risker inom de olika delsektorerna av finansmarknaden.

Det kan handla om breda kartläggningar av hur flera institut hanterar specifika risker. Det kan även handla om riktade undersökningar mot enskilda institut eller regelbundna bilaterala möten i den löpande tillsynen där fokus ligger på hur instituten hanterar risker, brister och hot, liksom hur de planerar och följer upp incidenter.

Ett exempel på denna tillsyn är en undersökning som vi nyligen genomförde mot en större bank som resulterade i att banken fick en anmärkning och en sanktionsavgift om 850 Mkr.

Bakgrunden var en IT-incident som drabbade ett mycket stort antal personer och ledde till felaktiga saldon på de berörda kundernas konton och att vissa kunder inte kunde göra betalningar.

Vi kunde konstatera att banken hade gjort en ändring i ett verksamhetskritiskt IT-system utan att bankens interna rutiner och processer följdes och att banken saknade ändamålsenliga kontrollmekanismer som kunde fånga upp avvikelsen och säkerställa att de interna rutinerna och processerna följdes. Det innebär att banken inte hade haft en tillfredställande intern kontroll vid ändringen i bankens IT-system.

Det som är viktigt att komma ihåg är att banken inte fick en sanktion för att de hade en IT-incident. Det kan man ha. Banken fick inte heller en sanktion för att den saknade i sammanhanget relevanta rutiner och processer för ändringar i IT-miljön. Banken fick en sanktion för att den inte haft tillräckliga kontrollmekanismer på plats som säkerställde att dessa rutiner och processer efterlevdes.

Det finns ett par pågående initiativ som är av betydelse för vårt tillsynsuppdrag. Inte minst Dora-förordningen som syftar till att stärka finansmarknadens operativa motståndskraft kopplat till cyberrisker och andra IT-relaterade risker.

Mats Malmberg från Sentor kommer att prata mer om Dora-förordningen senare idag. Från FI:s perspektiv är det tydligt att Dora-förordningen kommer bli en viktig del vårt tillsynsuppdrag och kommer innebära en större enhetlighet och skärpning av kraven på finansiella företags kontroll över IT- och informationssäkerhetsrisker, inte minst när det gäller utkontrakterad verksamhet. Det som idag är riktlinjer blir rättsligt bindande och flera oreglerade områden kommer att regleras. Det innebär att vi får bättre verktyg i vår tillsyn och kan ställa tydligare krav.

Säkerhetsskyddstillsyn

Sedan december 2021 utövar FI dessutom tillsyn enligt säkerhetsskyddslagstiftningen över finansiella företag samt för motsvarande utländska företag som är etablerade i Sverige. Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spioneri, sabotage, terroristbrott och vissa andra hot.

Säkerhetsskyddsregelverket är omfattande och ställer höga krav på hur en verksamhetsutövare som anser sig bedriva säkerhetskänslig verksamhet ska skydda sina säkerhetsskyddsklassificerade uppgifter och sin säkerhetskänsliga verksamhet. Till exempel innefattar tillsynen att säkerställa att verksamhetsutövaren har gjort en säkerhetsskyddsanalys som beskriver vad som ska skyddas och mot vad det ska skyddas samt hur det ska skyddas.

Man kan också notera att ordningen för tillsyn av säkerhetsskydd i viss mån avviker från hur offentlig tillsyn normalt är strukturerad. I tillägg till att övervaka efterlevnaden av befintliga regler, utför FI ett antal andra uppgifter.

En av dessa uppgifter innebär att genomföra systematiska kartläggningar av företag och andra objekt som faller inom vår sektor och som har relevans för Sveriges säkerhet. Detta innebär en aktiv insats från FI:s sida som syftar till att skydda Sveriges intressen, inte bara genom att upprätthålla gällande regler på finansmarknaden.

Tillsynen inom säkerhetsskydd inkluderar också en stor andel vägledning och stöd till verksamhetsutövarna. FI har tagit fram information och vägledning som finns tillgänglig på hemsidan, samt blanketter som visar vilken information som behöver förmedlas till myndigheten.

Ett annat exempel på uppgifter som ingår i säkerhetsskyddstillsynen är samråd mellan FI och verksamhetsutövare i vissa fall, exempelvis vid ingående av säkerhetsskyddsavtal eller vid överlåtelse av säkerhetskänslig verksamhet. Inom ramen för dessa samråd är det FI:s ansvar att säkerställa att företagen har utfört en särskild säkerhetsskyddsbedömning och lämplighetsprövning.

Sektorsansvar beredskapssektorn Finansiella tjänster

FI har också blivit utsedd till sektorsansvarig myndighet för beredskapssektorn finansiella tjänster inom det civila försvaret. Det uppdraget fick vi hösten 2022.

FI:s ansvar som sektorsansvarig myndighet handlar inte om tillsyn utan om att utveckla arbetet inom beredskapssektorn med målet att upprätthålla samhällsviktiga funktioner under fredstida krissituationer och höjd beredskap (ytterst krig).

En av de viktigaste uppgifterna är att – i samverkan med Riksbanken – arbeta för att betalningssystemet fortsätter att fungera, även under kris eller krig. Ett fungerande betalningssystem är avgörande för att upprätthålla en fungerande ekonomi under sådana omständigheter. Andra samhällsviktiga funktioner är sparande och finansiering, försäkring och finansiell stabilitet.

FI:s roll som sektorsansvarig myndighet innebär att vi ska stödja andra aktörer inom den finansiella sektorn i deras beredskapsplanering, oavsett om det är myndigheter eller privata företag. Eftersom det handlar om samhällsviktig verksamhet och inte tillsyn kan även företag som inte står under FI:s tillsyn påverkas av vårt arbete inom sektorsansvaret.

Vårt arbete med sektorn är påbörjat och vi tycker vi har god framfart i arbetet och en god dialog med branschen. Vi bedömer utgångsläget som gott eftersom branschen självt arbetat aktivt med sin egen beredskap under flera års tid.

En viktig fråga att reda ut är just företagens tillgång till prioriterad el och omfattningen av egna reservlösningar för el och elektronisk kommunikation. En annan viktig fråga är att i samverkan med aktörerna i sektorn – inklusive privata aktörer – skapa en gemensam bild av vad som är samhällsviktig verksamhet och då även vad som ska klassificeras som samhällsviktig tjänst.

Det finns givetvis fler viktiga frågor.

En potentiell utmaning vi ser är att vi, i rollen som sektorsansvarig myndighet, har begränsade legala verktyg och saknar rätt att föreskriva vissa beredskapsinsatser i företagen. Det här kan bli en liten utmaning eller en stor utmaning beroende på hur arbetet utvecklas.

Viktiga åtgärder

Jag tänkte nu gå över till vad vi anser behöver göras. Vår bedömning är att det behövs ett flertal olika åtgärder för att höja den digitala motståndskraften i den svenska finansiella sektorn. Dessa åtgärder är breda och involverar inte bara FI, utan flera andra myndigheter och inte minst de finansiella företagen själva.

Förväntningar på de finansiella företagen

Jag vill först understryka vikten av att de finansiella företagen själva tar ansvar för att öka sin digitala motståndskraft. Det finns flera områden där företagen kan göra förbättringar, och vårt fokus ligger på att adressera dessa områden. Det är viktigt att ingen lutar sig tillbaka och att banker, infrastrukturbolag och andra finansiella företag arbetar för att säkra sin egen beredskap och motståndskraft. Detta är en pågående process som kräver ständig uppmärksamhet och ansträngning från företagen.

Det är också viktigt att notera att det regulatoriska landskapet förändras och att nya omfattande krav kommer att införas, som till exempel Dora-förordningen. Detta kommer att kräva investeringar, tid och förberedelser från företagen.

Det är inte tillräckligt att luta sig tillbaka på gamla meriter och erfarenheter.

Ett utvecklat samspel mellan det offentliga och det privata

Vi har under en längre tid betonat vikten av en gemensam styrning av all verksamhet som rör samhällets cybersäkerhet. Anledningen till det är frågorna berör många olika samhällssektorer och det behövs en övergripande bild av samhällets samlade behov så att en genomtänkt prioritering mellan de olika sektorernas behov kan göras.

Vi kan konstatera att regeringen har inrättat ett nationellt cybersäkerhetscenter (NCSC) som bland annat ska utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet. Det är positivt och ett steg i rätt riktning, men NCSC är inte en egen myndighet utan en så kallad fördjupad myndighetssamverkan mellan de myndigheter som fått i uppdrag att bedriva verksamheten. Även om denna organisationsform kan medföra vissa fördelar finns det ett flertal utmaningar, inte minst gällande verksamhetens styrning.

Vi har föreslagit att regeringen ser över formen för NCSC för att hitta den mest ändamålsenliga organisationsmodellen på längre sikt. När NCSC:s verksamhet har en mer konkret struktur kan det finnas anledning att överväga om centret bör övergå i myndighetsform.

Vi har också föreslagit en ny struktur för krishantering i Sverige. I dag finns det inget gemensamt forum i Sverige för att hantera operativa kriser för finansiella företag. Vår uppfattning är att det behövs en centralt placerad aktör som kan samordna agerandet vid allvarliga cyberattacker som drabbar ett eller flera finansiella företag och som riskerar att utvecklas till en allvarlig kris för den finansiella sektorn. Ett sådant forum bör omfatta både privata finansiella aktörer och relevanta myndigheter och vi har föreslagit att regeringen utreder hur ett sådant krishanteringsorgan lämpligen kan utformas och vilken myndighet som bör ha huvudansvaret.

Slutligen vill jag också nämna att vi anser att regeringen bör överväga att inrätta ett särskilt cybersäkerhetsråd i Statsrådsberedningen som utifrån en gemensam och samlad hotbild över cyberhoten mot det svenska samhället fastställer en gemensam styrning för cybersäkerhetsfrågor, inbegripet prioriteringar av behov mellan de olika sektorerna. Detta skulle bidra till en ökad samordning och styrning av cybersäkerhetsfrågor på nationell nivå.

Det återstår att se vad som händer med våra förslag, men vi kan redan nu se att vissa delar går i rätt riktning.

Dels kan vi konstatera att regeringen har inrättat ett nationellt säkerhetsråd med en nationell säkerhetsrådgivare som ska utveckla samordningen, inriktningen och analysen av frågor som rör nationell säkerhet. Även om detta inte är särskilt inriktat på IT- och cyberfrågor är det ett steg i rätt riktning.

Förra veckan meddelade också regeringen att man organiserar om NCSC och att FRA blir huvudman för centret. Det tycker vi är positivt – vi har tidigare lyft fram att FRA med sin särskilda kompetens inom informationssäkerhetsområdet bör får en större roll när det gäller stöd till såväl offentliga som privata aktörer.

Relaterat till samspelet mellan det offentliga och det privata vill jag också nämna två andra mer specifika förslag.

För det första anser vi att privata e-legitimationer, såsom Bank-ID, bör stå under full tillsyn. Bank-ID är en central tjänst som används i stor omfattning av svenska konsumenter för att till exempel söka vård eller komma åt känslig information. År 2022 hade 99,2 procent av alla folkbokförda svenskar i åldrarna 18–65 år ett Bank-ID och tjänsten användes 6,7 miljarder gånger. En cyberattack som slår ut Bank-ID kan få allvarliga konsekvenser för flera delar av det svenska samhället. Därför bör statens tillsyn av Bank-ID och liknande verksamheter stärkas kraftigt, och på sikt stödjer vi förslag om att ta fram en statlig motsvarighet.

För det andra anser vi att Finansinspektionen (FI) bör få utökade befogenheter när det gäller utkontraktering av ett finansiellt företags kritiska IT-verksamhet. FI:s befogenheter inom flera sektorer av finansmarknaden är idag inskränkta till att ta emot en anmälan om ett sådant avtal. Här tycker vi att myndigheten bör få utökade befogenheter i syfte att motverka för stora koncentrationsrisker eller inlåsningseffekter där företagets möjlighet att byta leverantör är starkt begränsad. Det skulle ge FI en större möjlighet att hantera de risker som kan uppstå genom en ökad utkontraktering inom finansiell sektor. Ett område där vi har sådana tydliga befogenheter är inom säkerhetsskydd där FI under vissa förutsättningar kan motsätta sig ett avtal om utkontraktering, men endast om företaget och verksamheten omfattas av säkerhetsskyddslagstiftningen.

Som vi har konstaterat kommer Dora-förordningen introducera skärpta krav på detta område och ge tillsynsmyndigheter bättre verktyg, men vi kan samtidigt konstatera att Dora inte går lika långt som säkerhetsskydds-lagstiftningen. Vi kommer därför löpande utvärdera om mandaten i Dora-förordningen är tillräckliga för att möta de risker vi ser. Just nu handlar det för vår del om att aktivt delta i utformningen av framtagandet av tekniska standarder under Dora-förordningen som kommer att specificera kraven relaterade till tredjepartsrisker.

Vad gör FI?

Några avslutande ord om vad vi gör. Jag har redan nämnt vad FI har för roll kopplat till digital motståndskraft i finansiell sektor och hur vi tar oss an den rollen. Återigen, vi ser ett antal centrala risker och det finns det flera områden där vi tycker att företagen kan bli bättre och det är där vi kommer inrikta vår tillsyn och vårt arbete med det civila försvaret.

Jag kan inte gå in på några detaljer när det gäller exakt vad vi gör inom ramen för vår tillsyn, men jag kan säga att vi just nu har ett särskilt fokus på att säkerställa att vissa finansiella institut följer upp och åtgärdar potentiella sårbarheter kopplat till sin digitala motståndskraft. Dessutom genomför vi analyser av förändringshanteringsprocesser inom finansiella företag och fortsätter att prioritera frågor som tredjepartsrisker i vår tillsyn.

…

Sammanfattningsvis är det tydligt att IT- och cyberrisker utgör en stor utmaning för den finansiella sektorn. För att hantera dessa risker krävs en ökad uppmärksamhet och åtgärder från både myndigheter, lagstiftaren och finansiella företag. FI har en viktig roll att spela i detta sammanhang och vi kommer att fortsätta att prioritera vårt arbete på området. Omvärldsläget är en avgörande faktor för hur vi på FI prioriterar vårt tillsynsarbete, och med den ökande hotbilden kommer vi vara extra uppmärksamma och fokusera på att förebygga hoten innan de realiseras.