RAPPORT

Förstärkt digital motståndskraft hos företag i den finansiella sektorn

6 maj 2022

Dnr 22-10015

Innehåll

Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Förord

Finansinspektionen (FI) fick genom ett regeringsbeslut den 31 mars 2022 (Fi2022/01168) i uppdrag att lämna förslag till ytterligare åtgärder som bedöms ändamålsenliga för att stärka den digitala motståndskraften i den finansiella sektorn. FI har inom ramen för det här redovisade uppdraget inhämtat kunskap och erfarenhet från Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten, Riksgäldskontoret, Sveriges riksbank och Säkerhetspolisen.

Vi redovisar resultatet av uppdraget i form av denna rapport.

Stockholm den 6 maj 2022

Erik Thedéen

Generaldirektör

Sammanfattning

Rapporten omfattar ett antal förslag och åtgärder som FI bedömer kommer att stärka den digitala motståndskraften hos företagen i den finansiella sektorn. Vissa av åtgärderna är av mer allmän karaktär, medan andra är mer inriktade på att avhjälpa en mer specifik brist. Förslagen i den här rapporten gäller såväl FI:s egen verksamhet som andra myndigheters.

FI föreslår följande åtgärder:

- En kraftig ambitionshöjning i FI:s tillsyn över finansiella företags cyberrisker, genom att
    - ta fram en tillsynsstrategi för mer genomgripande och frekvent tillsyn samt nya tillsynsmetoder,
    - utveckla en databas för utlagda verksamheter, och
    - ge FI rättsligt mandat för att kunna motsätta sig avtal om utlagd kritisk verksamhet.
- Möjliggöra för Försvarets radioanstalt (FRA) att bistå finansiella företag.
- Stärka den nationella styrningen av cybersäkerhetsfrågorna genom att inrätta ett cybersäkerhetsråd i Statsrådsberedningen.
- Se över det nationella cybersäkerhetscentrets (NCSC) organisation samt extra medel för att påskynda dess etablering.
- Införa en ny struktur för operativ hantering av operationella kriser i finansiella företag till följd av cyberangrepp och liknande.
- Införa en ny struktur för cyberrelaterade övningar.
- Utveckling av en gemensam portal för företags inrapportering av it-incidenter till myndigheterna.
- Bank-id och andra privata e-legitimationer bör bli föremål för tillsyn, alternativt bör en statlig e-legitimation ersätta dagens privata lösningar.

FI bedömer att följande av de ovan nämnda förslag bör prioriteras på kort sikt:

- Kraftigt höja ambitionen i FI:s tillsyn,
- ge FRA möjlighet att bistå enskilda företag,
- inrätta ett nytt cybersäkerhetsråd i Statsrådsberedningen,
- extra medel för att påskynda NCSC:s etablering, samt
- utreda ansvaret för en ny struktur för operativ hantering av operationella kriser i finansiella företag.

Bakgrund

De senaste decenniernas digitala utveckling inom den finansiella sektorn innebär stora möjligheter, men de innebär också risker som rör informationssäkerhet och som behöver hanteras. Riskerna avser it-incidenter av olika slag. Bland uppsåtliga it-incidenter märks dels cyberrelaterad brottslighet, dels statsunderstödda, antagonistiska angrepp.[1] Dessa risker har förstärkts genom den försämrade säkerhetspolitiska situationen i Sveriges närområde, inte minst efter Rysslands invasion av Ukraina.

Cybersäkerhet är en viktig fråga för det finansiella systemet eftersom den finansiella sektorn i väldigt hög grad är digitaliserad. Det faktum att de finansiella företagen och marknaderna är nära sammanlänkade med varandra, och att eventuella problem därför snabbt kan sprida sig, gör att behovet av samverkan här är större än på många andra områden. Givet den finansiella sektorns centrala roll i samhällsekonomin är cybersäkerheten i de finansiella företagen en angelägenhet för hela samhället.

Cyberriskerna i den svenska finansiella sektorn

Ett försämrat säkerhetspolitiskt läge leder till ökade cyberrisker

Det säkerhetspolitiska läget i Sveriges närområde och i Europa har över tid försämrats, inte minst efter den ryska invasionen av Ukraina. Det går därför inte att utesluta ett angrepp mot Sverige.[2] Den som vill angripa Sverige kan göra det bland annat genom en cyberattack av något slag mot en eller flera viktiga samhällssektorer. Det går inte att veta vilken form av angrepp som är mest sannolik. Inte heller går det att med säkerhet förutsäga vilken sektor som löper störst risk att bli utsatt för en cyberattack.

Exempelvis elförsörjning och elektronisk kommunikation är helt centrala för att ett samhälle ska fungera och är därför naturliga måltavlor. Trots detta kan man även tänka sig att andra viktiga sektorer blir angripna. De mest kvalificerade antagonistiska aktörerna kommer alltid att ha intresse av att kunna agera mot de

[1] I denna rapport används begreppet it-incident som en beteckning för en, medveten eller omedveten, händelse som äventyrar cybersäkerheten i ett it-system eller strider mot de säkerhetsföreskrifter som gäller för it-systemet i fråga. Med cyberattack eller cyberangrepp avser vi en it-incident som är ett resultat av en medveten handling av en aktör i syfte att på något vis skada det system som angrips eller någon annan. Den som genomför en cyberattack eller ett cyberangrepp kan därmed ha gjort sig skyldig till brottet dataintrång (4 kap. 9 c § brottsbalken). Financial Stability Board (FSB) har i sitt Cyber Lexicon från 2018 definierat ett flertal olika termer när det gäller cybersäkerhet inom den finansiella sektorn.
[2] Prop. 2020/21:30 Totalförsvaret 2021–2025 (s. 58 f.).

svaga länkarna i de olika sammankopplade försörjningssystem som Sverige är beroende av.[3] Att stärka cybersäkerheten i samhället har därmed betydelse för förmågan att kunna upprätthålla en fungerande krisberedskap och ett motståndskraftigt totalförsvar. Det finns därför goda skäl för varje sektor som driver samhällsviktig verksamhet att göra sitt yttersta för att stärka cybersäkerheten inom den sektorn.

Den finansiella sektorn är en av flera samhällsviktiga sektorer som kan komma att angripas. Motivet för en angripare är uppenbart: betalningar är centrala för ett fungerande samhälle och därmed för samhällets motståndskraft. Hushållens konsumtion, företagens utbetalningar av löner och över huvud taget betalningar mellan privatpersoner och företag respektive mellan företag är avgörande för att samhällsekonomin, och därmed samhället i stort, ska kunna fungera. Ett cyberangrepp mot den finansiella sektorn kan därför vara ett viktigt instrument för den som vill skada Sverige. Detta särskilt om angriparen lyckas med att slå ut eller allvarligt inskränka möjligheten att göra betalningar mellan enskilda, företag och myndigheter.

Den finansiella sektorns motståndskraft mot cyberangrepp bör mot denna bakgrund vara hög. Samtidigt är det även för den finansiella sektorn viktigt att motståndskraften hos andra samhällsviktiga sektorer stärks parallellt. Detta inte minst eftersom flera sektorer är beroende av varandra. Det är exempelvis svårt att bedriva finansiell verksamhet utan fungerande elförsörjning, samtidigt som Försvarsmakten och andra myndigheter behöver kunna göra betalningar för att införskaffa försvarsmateriel.

Hur allvarliga är cyberriskerna för det finansiella systemet?

Cyberangrepp utgör ett växande hot mot finansiella företag. Men i princip kan allvarliga it-incidenter i finansiella företag ha en negativ inverkan på den finansiella stabiliteten oavsett incidentens typ och dess eventuella syfte. Såväl rena driftsstörningar som cyberangrepp, med eller utan kriminellt syfte, och statsstödda cyberangrepp i syfte att spionera eller sabotera kan påverka vitala funktioner i det finansiella systemet, såsom förmågan att göra betalningar. Att inte kunna utföra grundläggande finansiella tjänster ger i sig upphov till en skada för dem som drabbas.

Under ogynnsamma förutsättningar kan skadan få bredare spridning och drabba samhället i stort. Saken förvärras av att incidenten kan undergräva allmänhetens förtroende för drabbade finansinstitut eller det finansiella systemet som helhet. Förtroendet kan dessutom skadas om en incident medför att tillförlitligheten i data

[3] Se MSB och Försvarsmakten, Handlingskraft – en samlad plan för ett starkare totalförsvar, 2021 (s. 14). Cyberattacker kan också utföras av andra statliga eller statsunderstödda aktörer samt av kriminella organisationer.

rörande kontobehållningar, skulder, fondandelar eller liknande ifrågasätts. Om förtroendeförlusten blir tillräckligt stor kan den - oavsett dess orsaker - komma att utgöra ett hot mot den finansiella stabiliteten.

Avgörande för stabilitetsrisken blir därför it-incidentens omfattning, varaktighet och spridning, kombinerat med det läge då den inträffar. Konstaterade statsstödda cyberangrepp är potentiellt särskilt allvarliga men i ett säkerhetspolitiskt spänt läge, torde även incidenter av annat slag utgöra en större risk än vanligt, eftersom spekulationer om avsikter och förövare då kan antas påverka förtroendet mer än i lugnare lägen. Internationella valutafonden (IMF) tar i sin senaste stabilitetsrapport upp risker kopplade till Rysslands krig mot Ukraina.[4] Bland de risker som lyfts är cyberattacker som kan påverka det finansiella systemets motståndskraft. Kriget i Ukraina har ökat risken för cyberattacker, med en potentiell negativ inverkan på finansiell stabilitet. Slutsatsen är att den finansiella stabiliteten bäst värnas om de finansiella företagen har en god motståndskraft mot alla typer av allvarliga it-incidenter.

FI:s bild av cybersäkerheten i den svenska finansiella sektorn är att många företag arbetar aktivt med att bygga motståndskraft. Det är dock tydligt att vissa aktörer kommit längre i sitt arbete än andra. I det följande utvecklar FI ytterligare vår syn kring den finansiella sektorns skyddsvärda företag och processer. Flera olika åtgärder behövs för att stärka den finansiella sektorns motståndskraft mot cyberattacker. Inledningsvis ger vi en bild av redan pågående arbete hos FI och hos andra myndigheter.

Pågående arbete hos FI och andra myndigheter

FI arbetar sedan länge med cyberrisker inom ramen för den löpande tillsynen av de finansiella företagen.[5] FI bedriver cyberrelaterad tillsyn enligt de regler som gäller för hantering av operativa risker inom de olika delsektorerna av finansmarknaden. Sedan december 2021 utövar FI dessutom tillsyn enligt säkerhetsskyddslagstiftningen över finansiella företag samt för motsvarande utländska företag som är etablerade i Sverige.[6] Förra året presenterade en statlig utredning ett förslag på ny struktur för det civila försvaret.[7] Förslaget innebär att FI blir sektorsansvarig myndighet för beredskapssektorn finansiella tjänster. Även inom ramen för detta uppdrag arbetar FI med cybersäkerheten inom den finansiella sektorn.

[4] Global Financial Stability Report, 2022 APR.
[5] FI beskriver sin roll och sitt arbete när det gäller cyberrisker i de finansiella företagen i rapporten Cyberhot och finansiell stabilitet – FI:s roll och uppgifter (dnr 20-3685) som publicerades i mars 2021.
[6] 8 kap. 1 § säkerhetsskyddsförordningen (2021:955).
[7] SOU 2021:25 Struktur för ökad motståndskraft.

Det finns ett par pågående initiativ som är av betydelse för detta uppdrag. Ny lagstiftning som avser att stärka den digitala motståndskraften inom den finansiella sektorn håller på att tas fram inom EU. Ett svenskt nationellt cybersäkerhetscenter har inrättats och är under uppbyggnad.

En cybersäkerhetsstrategi för den finansiella sektorn

FI deltar sedan hösten 2021, tillsammans med Riksbanken och Riksgälden, i Finansiella stabilitetsrådets arbete med att ta fram ett förslag på en cybersäkerhetsstrategi för den svenska finansiella sektorn. Syftet är att stärka samarbetet, förtydliga rollfördelningen och höja kunskapen om cyberhot som riktas mot den svenska finansiella sektorn.

Strategin kommer att innehålla följande förslag:

- en ändamålsenlig roll- och ansvarsfördelning i cybersäkerhetsarbetet,
- en långsiktigt hållbar form för delning av operativ information om cyberrisker mellan finansiella företag och myndigheter med ett särskilt ansvar för cybersäkerheten i samhället, exempelvis Försvarsmakten, FRA, MSB och Säkerhetspolisen, samt
- ett antal mer långsiktiga kunskapsbyggande åtgärder.

Förslaget till strategi beräknas vara färdigt i juni 2022. Vissa av de förslag som presenteras i denna rapport kan därför komma att behöva utvecklas ytterligare inom ramen för strategiarbetet.

Nationellt cybersäkerhetscentrum

Inrättandet av ett nationellt cybersäkerhetscenter (NCSC) med i sammanhanget centrala uppgifter påverkar ovan nämnda strategi och detta uppdrag. MSB ska tillsammans med FRA, Försvarsmakten och Säkerhetspolisen bygga upp och driva NCSC. Centret har i uppgift att koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter. Vidare ska centret förmedla råd och stöd i fråga om hot, sårbarheter och risker. Slutligen ska centret utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet. Centret är inne i en uppbyggnadsperiod och ska, enligt ett tidigare fattat regeringsbeslut, vara fullt verksamt år 2025.

Dora-förordningen

I september 2020 presenterade Europeiska kommissionen ett förslag till en förordning för att stärka finansmarknadens operationella motståndskraft för cyberrisker (Dora-förordningen).[8] Huvudmotivet är dels ett ökat behov av reglering

[8] Förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014.

och tillsyn i ljuset av den växande sårbarheten för cyberrisker, dels ett behov av större enhetlighet i regelverken, både mellan delsektorer av finansmarknaden och mellan länder.[9] Den föreslagna regleringen riktar sig till i princip alla de typer av företag som i dag står under FI:s tillsyn. Förslaget innehåller ett generellt krav på dessa företag att ha kontroll över alla sina it-relaterade risker. Förordningen ställer långtgående krav på de finansiella företagen att ha tillräckliga processer, system och styrdokument på plats för att hantera dessa risker.

Dessutom innehåller förslaget till ny förordning regler som tydliggör företagens ansvar även för den del av it-verksamheten som kan ha lagts ut till en tredje part. Förordningen ställer krav på att tredjepartsrisker ska ingå som en integrerad del av de finansiella företagens riskramverk. Det ställs bland annat krav på dokumentation och att de finansiella företagen ska värdera de risker som kan uppkomma till följd av att en viss verksamhet läggs ut. De europeiska tillsynsmyndigheterna får i uppdrag att övervaka de tredjepartsleverantörer som bedöms som *kritiska*.

Genom denna förordning skapas mer enhetliga regler för aktörerna inom den europeiska finansiella sektorn. Parallellt pågår förhandlingar om ett nytt NIS-direktiv. Dora-förordningen föreslås dock tillämpas före NIS-direktivets regler om ett och samma företag skulle omfattas av såväl NIS-direktivet som Dora-förordningen. Förhandlingarna rörande Dora-förordningen är för närvarande i ett slutskede och den beräknas bli antagen inom de kommande månaderna. Bestämmelserna ska börja tillämpas två år efter det att förordningen har antagits.

[9] I FI:s rapport Cyberhot och finansiell stabilitet – FI:s roll och uppgifter (s. 13 ff.) finns en genomgång av den relativt stora mängd olika regler som gäller finansiella företags hantering av cyberrisker.

Förslag

Det behövs ett flertal olika åtgärder för att höja den digitiala motståndskraften i den svenska finansiella sektorn. Det rör sig om en bred palett av olika åtgärder som involverar FI, men också flera andra myndigheter och de finansiella företagen. I det här avsnittet redovisar FI förslag på åtgärder som vi bedömer kommer att leda till en stärkt digital motståndskraft i den svenska finansiella sektorn.

Inledning

Även om cybersäkerheten i vissa företag i privat sektor är ett samhällsintresse, har företagen själva det primära ansvaret för sin egen digitala motståndskraft. Det finns en nivå av cyberskydd – både att införskaffa information om risker och hot och att vidta olika slags åtgärder för att skapa motståndskraft – som samhället kan begära att privata företag själva ska ombesörja och bekosta på egen hand. De krav som samhället ställer på företagen framgår av gällande reglering om cyber- och informationssäkerhet. När det gäller finansiella företag är det FI:s uppgift att genom tillsyn se till att de följer sådana regleringskrav. Med större resurser kan tillsynen göras mer genomgripande och mer frekvent, vilket bör påverka regelefterlevnaden och därmed motståndskraften hos företagen positivt.

För systemviktiga företag i den finansiella sektorn bör kraven på motståndskraft mot cyberangrepp sättas högt på samma vis som vi exempelvis ställer högre kapitalkrav på de systemviktiga kreditinstituten. Även tillsynen bör vara mer genomgripande för dessa företag. Anledningen är att det inte är självklart att de enskilda företagen på eget initiativ beaktar de systemmässiga konsekvenserna av störningar i samhällskritiska funktioner som kan uppstå genom störningar i företaget.

En väg kan då vara att enligt den modell som nyligen införts i Storbritannien genom lagstiftning föreskriva en maximal tolerans för operationella störningar och därefter i den finansiella tillsynen, till exempel genom cyberstresstester, bedöma om företagen uppfyller denna toleransnivå.[10] Härigenom kan ansvariga myndigheter få underlag för att bedöma hur länge tjänster kan förväntas vara otillgängliga. Det kan ligga till grund för en kontinuerlig diskussion om vad som är en rimlig maximal tolerans för störningar och vilka åtgärder som kan behövas för att säkerställa att toleransgränsen inte överskrids. Det blir möjligt att formulera striktare krav för de tjänster som bedöms vara särskilt samhällsviktiga. Att på så vis

[10] Se Financial Conduct Authority, Building operational resilience: Feedback to CP19/32 and final rules. Reglerna tillämpas från och med den 31 mars 2022. Även i Danmark slår man nu in på en liknande väg genom att Finanstilsynet inleder test av finansiella företags operationella motståndskraft mot konsekvenserna av en definierad allvarlig cyberrelaterad störning.

definiera samhällets toleransnivå för allvarliga driftsstörningar inom den finansiella sektorn kan vara ett bra verktyg för att kommunicera samhällets förväntningar till de finansiella företagen. Inom ramen för tillsynen blir det sedan möjligt att följa upp om det enskilda företaget har vidtagit rätt åtgärder för att kunna hantera ett avbrott i sina system som ligger inom den i förväg definierade toleransnivån.

Samhället har alltså rätt att begära att företagen vidtar långtgående åtgärder för att upprätthålla kritiska funktioner. Men samtidigt måste det också beaktas att det finns cyberhot mot företag som är så destabiliserande för samhället att staten kan behöva bistå hotade företag med informationsdelning, övningsverksamhet och konkreta skyddsåtgärder. En stor del av det pågående arbetet med att ta fram en nationell cybersäkerhetsstrategi för finansiell sektor handlar, som nämns ovan, om lämpliga former och ansvarsfördelning för sådana insatser från statliga myndigheters sida. Vilka möjligheter statliga myndigheter har att bistå finansiella företag när det gäller skydd mot cyberattacker kommer också att utvecklas ytterligare i det följande.

En kraftig ambitionshöjning i tillsynen

FI utövar, som beskrivs ovan, tillsyn över hur de finansiella företagen hanterar cyberrisker med utgångspunkt i tillämpliga regelverk. Syftet med tillsynen är att, så långt det är möjligt, förebygga problem som kan hota det enskilda företagets och i förlängningen det finansiella systemets stabilitet. För en tillsynsmyndighet som FI ligger tyngdpunkten i verksamheten på det *förebyggande* arbetet – tillsynsåtgärder inom ramen för de finansiella regelverken är sällan lämpliga redskap för att hantera akuta krissituationer. Syftet är snarare att se till att företag som inte uppfyller kraven inte får tillstånd att driva finansiell verksamhet samt att de företag som får tillstånd har tillräckliga system, processer och kunskap för att kunna hantera de risker som deras verksamhet innebär.

En effektiv tillsyn av ett finansiellt företags interna styrning, kontroll och beteende kräver att tillsynsmyndigheten har en överblick av möjliga så kallade attackvektorer, det vill säga företagets sårbarhet för olika slags attacker, och hur företagets systemtekniska sammanlänkningar ser ut. Såväl myndigheternas som företagets kunskaper om dessa områden kan och bör förbättras. FI föreslår därför att kraftigt höja ambitionerna i tillsynen av de finansiella företagens hantering av de cyberrisker de är utsatta för. I det följande ges en närmare beskrivning av hur vi ser att denna ambitionshöjning bör genomföras.

Behov av ny tillsynsstrategi

Analys av skyddsvärden

De finansiella marknaderna tillhandahåller tjänster som är nödvändiga för att samhället ska fungera. Dessa tjänster kan närmast liknas vid grundläggande

infrastruktur. Särskilt betalningar är en tjänst som i princip alltid bör fungera och där även mindre driftstörningar kan få relativt stora konsekvenser. Därutöver finns ett flertal andra finansiella tjänster som kan vara kritiska för stora delar av samhället. I detta sammanhang utgår vi dels från FI:s uppdrag att värna den finansiella stabiliteten i Sverige, dels från vårt uppdrag att bedriva tillsyn enligt säkerhetsskyddslagstiftningen, en tillsyn som ytterst syftar till att värna Sveriges säkerhet.[11]

Utgångspunkten för tillsynen är att definiera vilka processer i företagen som är skyddsvärda. De svenska finansiella företagen genomför sedan flera år tillbaka identifiering av väsentliga processer ur företagens eget perspektiv. Denna process har kommit längre än identifieringen av vad som är skyddsvärd verksamhet i företagen, sett ur ett nationellt systemperspektiv. En anledning till att det är svårare att göra analysen ur det nationella perspektivet är att företagen måste bedöma sitt beroendeförhållande till andra företag och deras processer. Ingår det enskilda företaget exempelvis i en sektorövergripande process som är skyddsvärd ur ett nationellt perspektiv blir analysen mer komplex och tar mer tid.

För vissa delar av den finansiella sektorn har analysen kommit längre än andra när det gäller att identifiera vad som är skyddsvärd verksamhet ur ett nationellt perspektiv. FI:s tillsyn av cyberrisker har hittills främst varit fokuserad på de större och de medelstora bankerna. Det är dock inte givet att det är just dessa banker som är mest skyddsvärda ur ett nationellt cybersäkerhetsperspektiv. I alla händelser kan det finnas andra finansiella företag som är lika skyddsvärda. För att uppnå en mer träffsäker tillsyn behövs en bred och omfattande analys i syfte att identifiera vilka företag och processer som är mest skyddsvärda ur ett nationellt perspektiv. Analysen av sektorn bör också förhålla sig till att bedömningen av vad som är väsentliga processer och skyddsvärden ur ett nationellt perspektiv kan ändras över tid. Analysen av skyddsvärdena inom sektorn behöver därmed ses över med jämna mellanrum.

Metod och omfattning av tillsynen

Med stöd av en sådan analys av skyddsvärda företag och processer kan FI utforma en strategi för sin tillsyn över de finansiella företagens hantering av cyberrisker. En möjlig utgångspunkt för en sådan strategi är de fem cybersäkerhetsförmågor som en organisations it-system bör ha: *identifiera, skydda, upptäcka, hantera* och

[11] Se 1 kap. 2 § säkerhetsskyddslagen (2018:585): ”Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter”. I sammanhanget kan det även nämnas att Riksgälden kartlägger kritisk verksamhet och kritiska tjänster som en del av resolutionsplaneringen för systemviktiga institut.

återhämta.[12] En stor del av regleringen på cybersäkerhetsområdet fokuserar på hur pass väl ett företags organisation har dessa förmågor.

Den samlade förmågan att skydda en organisation mot cyberhot kan liknas vid en kedja med flera länkar. Med ett systematisk och holistiskt säkerhetsarbete är länkarna i kedjan ungefär lika starka. En angripare letar initialt efter svagheter i företagets systemskydd, för att inleda ett angrepp via någon av de svagare länkarna. De nämnda fem förmågorna är ett sätt att inrikta en organisations cybersäkerhetsarbete. Genom undersökningar av var och en av förmågorna får tillsynsmyndigheten en god uppfattning om det granskade företagets samlade cybersäkerhetsförmåga och om det finns någon svag länk. FI har sedan något år tillbaka använt detta ramverk som stöd för att granska några banker vad avser förmågan *identifiera* och i ett fall, förmågan *skydda*.

Vid de cybersäkerhetsundersökningar som hittills genomförts har FI uppmärksammat flera brister. Företagen har svarat att de ska åtgärda bristerna. Ingen undersökning har hittills lett till en sanktion. Hur arbetet med åtgärderna fortlöpt skiljer sig åt. Vissa företag har åtgärdat flera av bristerna innan undersökningen avslutades, medan andra företag visserligen har påbörjat insatser men fortfarande arbetar med samma brister efter flera år. Att arbetet med att åtgärda bristerna blir utdraget kan ha flera förklaringar. Det kan vara svårt att styra och koordinera cybersäkerhetsarbetet för att åtgärda vissa typer av brister. Men det kan också bero på att företag utgår från att det kommer dröja innan tillsynsmyndigheten återigen granskar deras cybersäkerhetsarbete, givet de begränsade resurser som FI har.

En utmaning är att FI med nuvarande resursläge enbart kan genomföra i storleksordningen två granskningar årligen. Resultaten från de första granskningarna i ett företag riskerar då att vara förlegade när den andra granskningen om något år har avslutats. Det är därför svårt för FI att med tillgängliga tillsynsresurser få en aktuell helhetsbild av de viktigaste företagens samlade cybersäkerhetsförmåga inom hela finanssektorn.

FI menar att betydligt fler företag årligen bör bli föremål för myndighetens granskningar och att samtliga fem förmågor behöver täckas in. Tillsynen bör breddas så att den, utöver de större och medelstora bankerna, även inkluderar andra typer av finansiella företag, exempelvis finansiella infrastrukturföretag och större

[12] Dessa fem förmågor beskrivs närmare i det internationella ramverket *NIST Cybersecurity Framework*. *Identifiera* omfattar organisationens hantering av cybersäkerhetsrisk och inkluderar system, människor, tillgångar, information och förmågor. *Skydda* omfattar säkerhetskontroller för att skydda IT-miljö för det skyddsvärda, inklusive förmåga att begränsa eller isolera ett cybersäkerhetsangrepp. *Upptäcka* omfattar förmågan att i tid upptäcka ett cybersäkerhetsangrepp. *Hantera* omfattar aktiviteter för att hantera ett cybersäkerhetsangrepp och stoppa skadan av det angreppet. *Återhämta* omfattar aktiviteter för att vara robust och att i tid kunna återställa kapaciteten från ett cybersäkerhetsangrepp.

försäkringsbolag. Åtminstone bör de systemviktiga företagen granskas regelbundet. Med systemviktiga företag avser FI i detta sammanhang samtliga kreditinstitut i de så kallade tillsynskategorierna 1 och 2, särskilt betydande filialer samt större finansiella infrastrukturföretag.[13]

Utöver att fler företag ska omfattas av tillsynen, bör granskningar genomföras med tätare intervall. På så sätt kan FI hålla en kontinuerligt aktuell helhetsbild av sårbarheterna i sektorn och driva på företagens arbete med cybersäkerhet. Tillsynen på cyberområdet ska, liksom på FI:s övriga tillsynsområden, vara riskbaserad. Den ska därför ta sin utgångspunkt i den ovan nämnda analysen av skyddsvärda företag och processer. Exakt vilka företag som ska granskas och med vilken intervall måste därför vara ett resultat av en sammanvägning av hur skyddsvärt företaget och dess processer är samt vilket skyddsbehov företaget har givet dess egen förmåga.

En svårighet när det gäller att höja ambitionsnivån i tillsynen är den generella bristen på personer med cybersäkerhetskompetens. FI vill fortsätta med sitt långsiktiga arbete med att rekrytera och behålla personer med denna kompetens. Därutöver kan FI använda sig av externa konsulter som ett stöd där det finns behov av särskild fackkunskap.[14] FI har även möjlighet att, inom ramen för vår tillsyn, tillsätta en revisor för att delta i revisionen av ett finansiellt företag.[15]

Även om granskningarna genomförs med tätare intervall och med en bättre uppfattning om företagens säkerhetsförmåga kommer arbetet ta tid. Eftersom det är fem förmågor som granskas kommer det vara något år mellan granskningen av den första och den sista förmågan hos ett företag. Ett sätt att överbrygga denna tidsrymd är att vid varje granskning av en förmåga identifiera nyckelindikatorer hos företaget, som i någon utsträckning beskriver den delen av cybersäkerhetsförmågan. Nyckelindikatorerna skulle därefter kunna följas upp i löpande tillsyn, till exempel på FI:s återkommande mer generella riskgenomgångar med företag under tillsyn. Sådana riskgenomgångar äger regelbundet rum flera gånger per år. På så vis går det att i viss utsträckning löpande följa upp ändringar i ett företags förmåga inom cybersäkerhetsområdet.

Ytterligare ett sätt att utveckla metoden och kvaliteten i tillsynen är att i vissa tillsynsaktiviteter även inkludera så kallade *penetrationstester* (tekniska säkerhetsgranskningar). Om det vid vissa tillsynsaktiviteter tillkommer en säkerhetsgranskning, skulle ytterligare brister kunna uppmärksammas. Säkerhetsgranskning kan utföras i samarbete med andra kompetenta myndigheter.

---

[13] FI tillsynskategorier framgår av Tillsynskategorisering av svenska kreditinstitut och utländska kreditinstituts svenska filialer för 2022 (FI dnr 21-19788).
[14] Att FI har en sådan möjlighet framgår av bland annat 23 kap. 14 § lagen (2007:528) om värdepappersmarknaden och 9 kap. 1 § 3 st. lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag. Kostnaden belastar i sådant fall det företag som tillsynen avser.
[15] Se exempelvis 13 kap. 9 § lagen (2004:297) om bank- och finansieringsrörelse.

Inom ramen för sin tillsyn skulle FI sedan kunna följa upp hur väl ett företag har åtgärdat de brister som har identifierats vid säkerhetsgranskningen.

Slutligen kan vi konstatera att regleringen av cybersäkerhet inom finanssektorn är under omvandling. Dels ändrades säkerhetsskyddsregelverket i slutet av 2021, dels kommer Dora-förordningen sannolikt att träda i kraft omkring halvårsskiftet 2024. I likhet med annan reglering är det de finansiella företagens ansvar att känna till de regler som gäller för deras verksamhet och anpassa sig därefter. Mot bakgrund av vad som sagts ovan bör även FI under den närmaste tiden lägga tid på att beskriva och förklara regleringen för företagen i sektorn. Det kan göras i flera former, från att ta fram vägledningar till presentationer och dialoger i olika former. Samtidigt ska den granskande tillsynen fortsätta och successivt utvecklas och utökas.

Utlagd verksamhet – tillsyn, verktyg och anmälningsplikt

Finansiella företag väljer att i allt högre grad utkontraktera en del av sin kritiska verksamhet, inte minst inom it-området (outsourcing). Detta kan vara positivt i de fall företaget inte på egen hand kan skaffa sig tillräcklig kompetens att hantera en viss verksamhet. Företaget måste dock alltid själv ha tillräcklig kompetens för att kunna styra över den verksamhet som utkontrakterats till en tredjepartsleverantör. Ett viktigt verktyg i tillsynen över de finansiella företagens cyberrisker är därför tillsynen över utlagda verksamheter hos så kallade tredjepartsleverantörer. En tredjepartsleverantör är ett – ofta icke-finansiellt – företag som utför olika it-relaterade tjänster åt ett finansiellt företag.[16]

De finansiella företag som väljer att lägga ut verksamhet behöver ha tillräcklig kunskap och utöva god styrning och kontroll över den utlagda verksamheten. De bör inte heller samla alltför många kritiska tjänster hos en och samma leverantör för att undvika oönskade beroenden och koncentrationsrisker.[17] Vidare är utläggning av verksamhet en stor risk för ett företag ur ett säkerhetsskydds-perspektiv. Utöver att fler finansiella företag bör granskas i mer frekventa tillsynsundersökningar enligt vad som beskrivits ovan, finns det således starka skäl för FI att utöva en betydligt mer omfattande tillsyn över de finansiella företagens utlagda verksamhet.[18]

Det följer av Europeiska bankmyndighetens (EBA) riktlinjer att finansiella företag – bland andra kreditinstitut och betaltjänstförmedlare – ska föra register över

[16] I EBA:s riktlinjer för utkontraktering (EBA/GL/2019/02) benämns tredjeparts-leverantörer som tjänsteleverantör vilket definieras som ”en tredje part som tar på sig en utkontrakterad process, tjänst eller verksamhet, eller delar därav, enligt ett arrangemang för utkontraktering”.
[17] Dora-förordningen innehåller förslag till regler som tydliggör de finansiella företagens ansvar även för den del av it-verksamheten som har delegerats till tredje part.
[18] I Dora-förordningen får de europeiska tillsynsmyndigheterna i uppdrag att övervaka de tredjepartsleverantörer som bedöms som ”kritiska”.

samtliga uppdragsavtal som avser utkontraktering.[19] FI ska i sin tur föra ett register över dessa avtal för att kunna identifiera koncentrationsrisker på sektornivå. FI bör utveckla en sökbar databas för de uppdragsavtal som anmälts till myndigheten, för att uppfylla de krav som ställs i EBA:s riktlinje, minimera risken för dubbelarbete och manuella fel samt möjliggöra hanteringen av en stor mängd information på ett effektivt sätt. En sådan databas skulle även stärka arbetet med att identifiera de skyddsvärda processerna inom sektorn eftersom även leverantörer till de finansiella företagen identifieras. För att effektivisera hanteringen bör databasen ha ett digitalt gränssnitt gentemot dem som anmäler ny information eller ändringar av befintlig information.

FI bedömer dessutom att den nuvarande rättsliga regleringen om de finansiella företagens anmälan av nya uppdragsavtal bör ses över. I dagsläget har FI vissa möjligheter att motsätta sig att ett finansiellt företag ingår ett uppdragsavtal med stöd av säkerhetsskyddslagstiftningen. Detta förutsätter dock att såväl företaget som den aktuella verksamheten omfattas av denna lagstiftning. I övrigt är FI:s befogenhet inom flera sektorer av finansmarknaden inskränkt till att ta emot en anmälan om att ett finansiellt företag avser ingå ett sådant avtal.[20]

Vi anser att FI bör ha möjlighet att motsätta sig att ett avtal om utkontraktering av ett finansiellt företags kritiska it-verksamhet ingås. Anledningen kan exempelvis vara att FI bedömer att det aktuella företaget inte har tillräcklig kunskap om den utlagda verksamheten, att FI bedömer att koncentrationsrisken är för hög eller kan anses olämplig för att den skapar en inlåsningseffekt, dvs att företagets möjlighet att byta leverantör är starkt begränsad. En utkontraktering kan också försvåra en effektiv tillsyn.[21] För att möjliggöra uppföljning av företagens utkontraktering anser FI att företagen ska vara skyldiga att upplysa myndigheten om de väljer att ändra eller avsluta ett avtal om utkontraktering.

Behov av reglering utöver Dora-förordningen

Starka samhällsintressen talar för att finansiella företag bör omfattas av tydliga regler i fråga om vilka krav de har att uppfylla när det gäller deras motståndskraft mot cyberattacker. Som framgår ovan träder en ny omfattande reglering av finansiella företags hantering av cyberrisker inom kort i kraft inom EU, Dora-

[19] EBA/GL/2019/02.

[20] Se 6 kap. 7 § lagen (2004:297) om bank- och finansieringsrörelse, 8 kap. 22 § lagen (2007:528) om värdepappersmarknaden samt 10 kap. 19-22 §§ försäkringsrörelselagen (2010:2043). När det gäller kreditinstitut gäller lagkravet om att anmäla utlagd verksamhet till FI enbart de verksamheter som räknas upp i 7 kap. 1 § samma lag. För övrig utlagd verksamhet regleras anmälan till FI i ett allmänt råd till 10 kap. 2 § Finansinspektionens föreskrifter och allmänna råd (2014:1) om styrning, riskhantering och kontroll i kreditinstitut.

[21] Jfr 4 kap. 7 § lagen (2004:46) om värdepappersfonder som medger en möjlighet för FI att förelägga ett fondbolag att hos motparten begära de ändringar som behövs för att avtalet ska uppfylla lagens krav.

förordningen. Förordningen är när detta skrivs fortfarande föremål för förhandlingar mellan det Europeiska rådet och Europaparlamentet. Ett beslut väntas dock före halvårsskiftet 2022. Så snart ett beslut har fattats behöver FI analysera vilka effekter den nya förordningen kommer att få för företagen under tillsyn.

FI bedömer att Dora-förordningen kommer att innebära såväl en höjning som en harmonisering när det gäller de krav som ställs på de finansiella företagens hantering av cyberrisker. Inte minst när det gäller företagens kontroll över utlagd verksamhet ställs ökade krav. I dagsläget skiljer sig regelverken om cyberrisker sig åt mellan olika delar av den svenska finansiella sektorn, vilket kan leda till otydligheter och till en ojämn skyddsnivå. Den nya förordningen kommer även att harmonisera de olika, till viss del parallella, kraven på incidentrapportering, vilket är positivt. FI kan också konstatera att förslaget innebär att medlemsstaterna ska se till att den behöriga tillsynsmyndigheten har möjlighet att utfärda sanktioner som är effektiva, proportionella och avskräckande. Vi vill här betona vikten av att FI ges möjlighet att utfärda tillräckligt kraftfulla sanktioner mot de företag som överträder förordningens bestämmelser om cyberskydd.

I likhet med övrig tillsyn som FI utövar behöver tillsynen enligt Dora-förordningen vara riskbaserad. Det innebär att FI:s tillsyn är mer genomgripande avseende de företag som driver systemviktig verksamhet. Systemviktigheten är nära kopplad till hur stor betydelse företagets verksamhet har för Sveriges säkerhet. Den tillsyn som ska bedrivas enligt förordningens regler behöver därför kompletteras med FI:s tillsyn enligt säkerhetsskyddslagstiftningen.

Givet att Dora-förordningen sannolikt inom kort kommer att vara direkt tillämplig i Sverige föreslår FI inte några förändringar i fråga om de gällande regelverken för de finansiella företagens hantering av cyberrisker innan förordningens slutliga utformning är beslutad. FI vill dock redan nu uppmärksamma att risken är stor för att betalningssystem, såsom Bankgirot, inte kommer att omfattas av förordningens bestämmelser. Eftersom dessa företag har en central betydelse på finansmarknaden anser FI att de behöver omfattas av en reglering som åtminstone motsvarar de regler som framgår av Dora-förordningen. Vi vill också framhålla att det kan finnas ytterligare behov av att fylla ut förordningens regler.

FRA:s möjlighet att bistå vissa finansiella företag

I juni 2021 kom FRA in med en hemställan till regeringen om ändring i den förordning som styr myndighetens verksamhet.[22] FRA föreslår att kretsen av aktörer som myndigheten får ge stöd till inom informationssäkerhetsområdet ska utvidgas till att även omfatta andra verksamhetsutövare än myndigheter och statligt

[22] FRA, Hemställan om ändring av 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt (Dnr 1.1:3835/21:1).

ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Som FRA konstaterar i sin begäran bedrivs en stor del av den skyddsvärda verksamheten utanför myndigheterna och de statligt ägda bolagen. Exempelvis driver privata finansiella företag verksamhet som är av mycket stor betydelse för Sveriges säkerhet. Som instruktionen är utformad i dag har FRA inte möjlighet att bistå dessa företag trots det starka skyddsintresset.

FI ställer sig bakom FRA:s hemställan och instämmer i de argument som myndigheten anför. När det gäller frågor om cybersäkerhet bör samhället inte, utan starka skäl, göra skillnad mellan sådan känslig verksamhet som drivs av en privat respektive en offentlig aktör. Som vi konstaterar i inledningen till denna rapport ökar sannolikheten för en sektor att bli utsatt för cyberangrepp om en antagonistisk angripare uppfattar att sektorns skydd mot cyberhot är svagt. Mot den bakgrunden anser FI att regeringen, så snart som möjligt, bör ändra FRA:s instruktion i enlighet med hemställan så att relevanta privata företag har möjlighet att få bistånd av FRA.

FRA har mycket hög teknisk kompetens inom informationssäkerhetsområdet och kan genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. Mer konkret innebär detta att FRA kan vägleda myndigheter och statligt ägda företag om säkerheten i deras it-system. Myndigheten kan även utföra avancerade säkerhetsgranskningar för att upptäcka brister i en myndighets eller ett företags it-system. FI anser, som nämns ovan i tillsynsavsnittet, att sådana säkerhetsgranskningar kan vara mycket värdefulla för finanssektorn och att alla systemviktiga finansiella företag bör bli föremål för en granskning av detta slag. Med systemviktiga företag avser FI som nämns ovan samtliga kreditinstitut i tillsynskategori 1 och 2, särskilt betydande filialer samt större finansiella infrastrukturföretag. Takten i genomförande av granskningarna är givetvis beroende på FRA:s resursläge och prioriteringar. Efter att en säkerhetsgranskning genomförts har FI möjlighet att följa upp resultatet inom ramen för tillsynen.

FRA har även tagit fram ett varningssystem som kan upptäcka avancerade it-angrepp som normalt inte fångas av kommersiella antivirusskydd som privata företag själva kan förvärva. Systemet kallas TDV (tekniskt detekterings- och varningssystem) och fungerar som ett avancerat antivirusskydd.[23] Skulle FRA:s hemställan leda till ändringar i nämnda instruktion ges även en möjlighet att installera TDV hos de systemviktiga finansiella företagen. Det skulle innebära en konkret höjning av nivån på företagens cyberskydd.

[23] Se https://www.fra.se/cyberforsvar/dethargorfra.4.60b3f8fa16488d849a54ec.html (hämtat 2022-04-26).

Gemensam nationell styrning av cybersäkerhetsfrågor

Cyberhoten är en viktig angelägenhet för flera olika delar av det svenska samhället. Både näringslivet och offentlig verksamhet berörs. Flera departement inom Regeringskansliet och olika myndigheter har ansvar för hanteringen av cyberhot och för cybersäkerhet i olika aspekter och för olika sektorer.[24] Det finns en risk för att insatserna inte utformas från en gemensam hotbild och inte inriktas på ett samlat och effektivt sätt. Mot bakgrund av att cyberriskerna har ökat under senare år, finns det anledning att tillfälligt skapa en gemensam styrning av all verksamhet som rör samhällets cybersäkerhet. Eftersom frågorna berör många olika samhällssektorer behövs i detta skede en övergripande bild av samhällets samlade behov så att en genomtänkt prioriteringar mellan de olika sektorernas behov kan göras. Givet cyberriskernas samhällsbetydelse bör detta vara en övergripande angelägenhet för regeringen.

FI anser därför att regeringen bör överväga att inrätta ett särskilt cybersäkerhetsråd i Statsrådsberedningen, förslagsvis under ledning av statsministerns statssekreterare. Syftet med rådet bör vara att utifrån en gemensam och samlad hotbild över cyberhoten mot det svenska samhället fastställa en gemensam styrning för cybersäkerhetsfrågor, inbegripet prioriteringar av behov mellan de olika sektorerna. FI menar att ett sådant cybersäkerhetsråd kan starkt bidra till en förbättrad styrning och en ökad tydlighet när det gäller samhällets arbete med cybersäkerhet. I takt med att samhällets förmåga att hantera cybersäkerhetsfrågor byggs upp kan behovet av cybersäkerhetsrådet minska varefter cybersäkerhetsfrågorna fortsatt kan hanteras inom ramen för Regeringskansliets och berörda myndigheters ordinarie verksamheter.

Som tidigare nämnt pågår nu etableringen av NCSC. Även här finns det skäl att vidta åtgärder för att uppnå ökad tydlighet. NCSC är inte en egen myndighet utan en så kallad fördjupad myndighetssamverkan mellan de myndigheter som fått i uppdrag att bedriva verksamheten.[25] Även om denna organisationsform kan medföra vissa fördelar genom att göra det möjligt att samla flera kompetenta myndigheters resurser finns det tydliga utmaningar, inte minst gällande verksamhetens styrning.

NCSC styrs på en övergripande nivå av regeringen genom dess beslut att inrätta centret och genom styrningen av de samverkande myndigheterna. Men mer

[24] Utredningen om civilt försvar föreslår i sitt slutbetänkande att ett särskilt beredskapsområde för cybersäkerhet ska inrättas. Området ska bestå av Säkerhetspolisen, MSB, Försvarsmakten och FRA. Till skillnad från övriga områden pekar inte utredningen ut en myndighet utan anser att området ska vara ett samarbete mellan de nämnda myndigheterna.
[25] Svar på uppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter den 19 december 2019. Se även 2020/21:1, utgiftsområde 6, s. 14.

operativa beslut tas gemensamt av de fyra myndigheterna FRA, Försvarsmakten, MSB och Säkerhetspolisen. En beslutsordning som bygger på konsensus kan möta särskilda utmaningar när snabba beslut och avvägningar måste göras i en krissituation. FI:s rekommendation är att regeringen ser över formen för centret i syfte att på längre sikt hitta den mest ändamålsenliga organisationsmodellen. När NCSC:s verksamhet fått en mer konkret struktur kan det finns anledning att överväga om centret bör övergå i myndighetsform.

Som ett första steg bör tidplanen för centrets etablering ses över. FI bedömer att det är önskvärt att centret är fullt fungerande redan i slutet av 2023 i stället för 2025 som nu planeras. I detta syfte bör regeringen överväga att tillskjuta extra medel till de myndigheter som ingår i centret. De ska användas för att snabbare rekrytera personal till NCSC.

Det finns även goda skäl för de myndigheter som har ett ansvar för finansiell stabilitet (FI, Riksbanken och Riksgälden) att inleda ett mer formaliserat samarbete med NCSC. Med stöd av ett samarbetsavtal bör myndigheterna och centret kunna utbyta erfarenheter och kunskap. Det bör även vara möjligt för anställda att tjänstgöra växelvis vid myndigheterna och NCSC samt i de med centret samverkande myndigheterna. Detta skulle bidra till en stärkt kompetens hos de finansiella stabilitetsmyndigheterna i frågor om cybersäkerhet, och om finansiell stabilitet hos centret. Ett sådant samarbetsavtal skulle även kunna tjäna som en förebild för centrets samverkan med andra samhällssektorer.

Under våren 2022 har det inletts en dialog mellan FI, Riksbanken, Riksgälden och MSB där syftet är att skapa en struktur för samverkan mellan myndigheterna som har ansvar för finansiell stabilitet, NCSC och de samverkande myndigheterna samt privata aktörer i den finansiella sektorn. Syftet är att etablera ett forum för att utbyta information, lägesbilder och uppgifter om aktuella metoder och tillvägagångssätt hos antagonister. Förhoppningsvis kan strukturen bli verklighet inom en snar framtid. Även detta kan tjäna som en förebild för hur samverkan mellan det privata och det offentliga inom andra sektorer kan tas fram.

Öka viljan att rapportera och polisanmäla cyberangrepp

Att vi har en rättvisande bild av inträffade it-incidenter, allt från antagonistiska angrepp till handhavandefel, är centralt för att förstå de konkreta cyberhoten och sedan kunna välja effektiva åtgärder som stärker den digitala motståndskraften i samhället, inte minst i den finansiella sektorn.

Anmälningsgraden när det gäller dataintrång mot företag är i dag extremt låg.[26] Det är angeläget att viljan att anmäla denna typ av brott ökar så att omfånget och inriktningen på cyberangrepp tydliggörs och det därmed skapas en skarpare hotbild som kan ligga till grund för förebyggande cybersäkerhetsarbete. En ökad vilja att anmäla skulle också ge förutsättningar för att fler ansvariga ställs inför rätta och att brottsligheten minskar. FI bedömer att flera olika åtgärder behövs. En möjlig åtgärd är ett resurstillskott till såväl Polismyndighetens nationella it-brottscentrum som de regionala it-brottscentrumen. Ökade resurser kan leda till att fler brott klaras upp. Det kan i sin tur få fler företag att känna sig motiverade att anmäla om de utsätts för brott.

Både MSB och Polismyndigheten bedömer att antalet it-incidenter som rapporteras inte alls motsvarar det antal incidenter som inträffar. Anledningarna till den låga rapporteringen av it-incidenter kan vara flera. Men svårigheten att bedöma när en it-incident ska rapporteras och till vem brukar lyftas upp som en anledning av berörda aktörer inte bara i finansiell sektor.

Det är därför angeläget att vidta åtgärder för att både underlätta och uppmuntra berörda aktörer att rapportera sina inträffade it-incidenter. Aktörerna kan få tillgång till ett samlat stöd för sin it-incidentrapportering genom att en webbportal etableras med en gemensam ingång för flera former av central it-incidentrapportering till myndigheter, såsom it-incidentrapportering enligt Dora, lagen (2018:1174) om informationssäkerhet för samhällsviktiga tjänster (NIS-regleringen), lagen (2003:389) om elektronisk kommunikation, dataskyddsförordningen (GDPR) samt polisanmälan. Åtgärden bör kombineras med kunskapshöjande insatser, exempelvis i form av en kampanj, riktade till aktörerna. Uppgiften att driva och samordna samverkan kring webbportalen skulle, med hänsyn till den breda ansatsen, kunna ges till MSB.

I dagsläget tar MSB emot samlad incidentrapportering från aktörer som driver bankverksamhet och finansmarknadsinfrastruktur enligt NIS-regleringen. Dessa rapporter blir en del av den samlade incidentrapporteringen från alla de verksamheter som omfattas av NIS-regleringen och ligger till grund för MSB:s återkoppling i form av analyser av hot och risker samt rekommenderade åtgärder. De bidrar också till att ge en övergripande bild av samhällets informations- och cybersäkerhet.

Genomförandet av Dora och det föreslagna NIS 2-direktivet innebär en uppdelning av incidentrapporteringen från berörda aktörer i den finansiella sektorn till

[26] Polismyndigheten uppskattar att enbart några få procent av de begångna brotten anmäls. Se även Svenskt Näringslivs rapport Företagen och it-säkerheten – hotbilder, motåtgärder och behov från mars 2021. Av rapporten, som redogör för en intervjuundersökning med säkerhetsansvariga i ett representativt urval av företagen i Stockholmsbörsens så kallade OMX30-index, framgår bland annat att de flesta storföretag anser att en polisanmälan i praktiken är ett slöseri med tid.

ansvariga myndigheter. Uppdelningen kan leda till sämre förutsättningar för myndigheterna att tillhandahålla en samlad bild av inträffade incidenter vilket i sin tur minskar synergieffekterna som finns i den nuvarande ordningen. Om incidentrapporteringen från aktörer inom finanssektorn inte längre kommer in till MSB minskar också möjligheterna för myndigheten att erbjuda tematiska analyser för sektorn. För att bevara dessa möjligheter bör relevant information om inträffade incidenter i den finansiella sektorn kunna delas mellan FI och MSB.

Det är även viktigt att öka företagens förståelse av hur deras incidentrapporter behandlas av myndigheterna. FI anser att den ovan nämnda strukturen för samverkan med, bland andra, NCSC och företagen i den finansiella sektorn, på sikt, kan göra det möjligt att lämna återkoppling till företagen och stärka förståelsen för hur myndigheterna arbetar med den information som de tar emot. Utöver detta är det naturligtvis viktigt att varje ansvarig myndighet upprätthåller en god kommunikation med företagen i den finansiella sektorn om vikten och nyttan av såväl incidentrapportering som polisanmälningar.

En ny struktur för krishantering

Om ett finansiellt företag eller en myndighet med operativ verksamhet inom det finansiella området, utsätts för ett cyberangrepp är det i första hand företagets eller myndighetens eget ansvar att bemöta och hantera angreppet. Ett finansiellt företag som hanterar ett cyberangrepp ska sedan rapportera det enligt föreskrifter till MSB, Riksbanken och FI. Incidenthanteringen kan därmed följas av myndigheterna. Riksbanken och FI kan om det finns behov föra informationen vidare inom det Finansiella stabilitetsrådet. Stabilitetsrådet är det forum där myndigheterna kan samordna hur de hanterar hot mot den finansiella stabiliteten och diskutera olika åtgärder som respektive myndighet vidtar inom ramen för sitt ansvarsområde med anledning av uppkomna situationer.

Vid ett svårt cyberangrepp som kan innebära en fara för den finansiella stabiliteten är det naturligt att myndigheterna inom Finansiella stabilitetsrådet samverkar för att ta fram en gemensam lägesbild och diskutera åtgärder. En viktig aktivitet är att bestämma den information som bör lämnas till andra myndigheter och allmänheten. Stabilitetsrådets myndigheter har dock inte den kompetens eller de mandat som kan krävas för att ensamma hantera ett stort och brett cyberangrepp mot den finansiella sektorn. Till skillnad från vad som är fallet vid en konventionell finansiell kris kan de störningar och skador som uppstår till följd av en cyberattack inte avhjälpas genom exempelvis ett likviditetstillskott eller en statlig garanti. Det finns därför skäl att överväga en ny struktur för krishantering när det gäller systemhotande operationella störningar såsom cyberattacker mot den finansiella sektorn.

Fokus bör ligga på att upprätthålla kritiska finansiella funktioner genom kontinuitetsarrangemang (reservfunktioner) respektive inom rimlig tid återställa ordinarie funktioner. Dessutom är det möjligt att det finns en säkerhetspolitisk och/eller brottsbekämpande dimension vid större cyberangrepp. Det gör att även andra myndigheter än FI, Riksbanken och Riksgälden kan behöva kopplas in för att dels bidra med relevant information och kunskap, dels begränsa spridning av skada. Vid angrepp av detta slag blir därför behovet extra stort av att agera samordnat och att dela information koordinerat.

I en konkret krishantering kan det behöva tillföras teknisk förmåga för att få igång verksamheten. Vissa större finansiella företag har egen kapacitet av detta slag, men vid mer allvarliga angrepp måste man räkna med att man kan behöva tillföra kompetens, särskilt till mindre företag. Sådan teknisk kompetens kan hyras in från kommersiella it-säkerhetsföretag. Djup kompetens finns också hos myndigheter som Säkerhetspolisen, Försvarsmakten och FRA. Eftersom en effektiv avvärjning, utöver teknisk kompetens, förutsätter ingående kunskap om det enskilda företagets it-miljö är det inte givet att FRA, Säpo och Försvaret har komparativa fördelar att bistå under alla cyberangrepp. Men om ett cyberangrepp på allvar hotar det finansiella systemets funktionsförmåga och potentiellt även Sveriges säkerhet bör dessa myndigheters kompetenser kunna mobiliseras för att avvärja hot mot samhällsviktiga funktioner.[27]

I dag finns det inget gemensamt forum i Sverige för att hantera operationella kriser för finansiella företag. FI:s uppfattning är dock att det behövs en sådan centralt placerad aktör som har goda kontakter hos de olika relevanta myndigheterna samt hos de större finansiella företagen, och som får i uppdrag att samordna agerandet vid allvarliga cyberattacker som drabbar ett eller flera finansiella företag och riskerar att utvecklas till en allvarlig kris för den finansiella sektorn.

Här kan inspiration hämtas från Danmark där en sådan ordning redan existerar. I regi av den danska centralbanken – en myndighet under den danska regeringen – samarbetar myndigheter och de finansiella företagen inom ramen för *Finansielt Sektorforum for Operationel Robusthed* (FSOR). Vid sidan av att analysera hotbilder, agerar FSOR som en samordnande aktör under en cyberattack. FSOR har ett nära samarbete med bland andra den danska cybersäkerhetsmyndigheten,

[27] Försvarsmaktens möjligheter att lämna stöd är reglerade i förordningen (2002:375) om Försvarsmaktens stöd till civil verksamhet. Av förordningen framgår det att Försvarsmakten kan lämna stöd till en enskild om de har resurser som är lämpliga för uppgiften och det inte allvarligt hindrar dess ordinarie verksamhet (6 §). Vidare ska full kostnadstäckning uppnås (16 §). En förutsättning för att FRA ska kunna bistå en enskild är att myndighetens ovan nämnda hemställan om förordningsändring beviljas.

polisen och tillsynsmyndigheten. FSOR har även ett nära samarbete med NFCERT.[28]

FI föreslår att det i Sverige bildas ett liknande forum som omfattar både privata finansiella aktörer och relevanta myndigheter med uppgift att samordna operativ hantering av cyberrelaterade kriser i systemviktiga finansiella företag. Det rör sig om en koordinerande roll utan möjlighet att besluta över andra myndigheters och företags verksamheter. I enlighet med ansvarsprincipen ska alla aktörer ha kvar sina vanliga mandat och sitt vanliga ansvar, men de bör kunna göra ett bättre arbete genom samordning.

Uppdraget att leda detta forum för krishantering kan ges till en befintlig aktör alternativt till en myndighet som, för ändamålet, inrättar ett särskilt organ. För att snabbare uppnå önskad effekt anser FI att det är lämpligt att börja med att lägga ansvaret på en befintlig myndighet med förutsättningar att klara uppgiften. FI bedömer att det är i huvudsak tre olika myndigheter som idag har ett relevant ansvar för frågor om cybersäkerhet och därför kan komma i fråga.

Riksbanken ansvarar för RIX, det centrala betalningssystemet som banker, andra finansiella institut och Riksgälden använder för att göra betalningar mellan varandra. Riksbanken har således redan idag en operativ roll i det finansiella systemet. Det följer vidare av förslaget till den nya riksbankslag som föreslås träda i kraft den 1 januari 2023 att Riksbanken ska ansvara för att allmänheten ska kunna göra betalningar under fredstida krissituationer och vid höjd beredskap.[29] Samtidigt behöver det beaktas att regeringen inte kan utöva styrning över Riksbanken som är en myndighet under riksdagen. I en akut krissituation kan detta ge upphov till styrningssvårigheter.

Även FI kan ta en central roll i en sådan struktur mot bakgrund av den kunskap om de finansiella företagen och deras arbete mot cyberrisker som vi får i vår tillsyn, vår allmänna erfarenhet av den svenska finansmarknaden och hantering av finansiella kriser samt rollen som bevakningsansvarig myndighet med ansvar för beredskapen i den finansiella sektorn.[30] En statlig utredning har, som tidigare nämnt, föreslagit att FI ska få utökat ansvar och vara sektorsansvarig myndighet för beredskapen i hela den finansiella sektorn.

[28] NFCERT (Nordic Financial Computer Emergency Response Team) startades år 2017 i Norge som en ideell förening. NFCERT har i dag drygt 220 finansiella företag som medlemmar, de flesta av dem i Danmark eller Norge. De har även medlemmar i de övriga nordiska länderna. NFCERT tillhandahåller en plattform för operativ informationsdelning, utför analys av hot, tar fram hotbildsanalyser samt koordinerar responsen vid en eventuell cyberattack.
[29] Se 5 kap. 1 § i förslaget till ny riksbankslag i prop. 2021/22:41 En ny riksbankslag.
[30] Prop. 1994/95:47 Riksbankens och Finansinspektionens beredskapsansvar.

Slutligen kan MSB komma i fråga. Myndigheten har i dag ansvar för att koordinera och stödja krishanteringsarbetet i samtliga av samhällets sektorer. Enligt sin instruktion ska MSB även agera vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.[31] MSB har stor erfarenhet av krishantering inom flera sektorer även om myndigheten inte har någon specifik kompetens gällande den finansiella sektorn.

Det är viktigt att den myndighet som ges denna uppgift har god kännedom om relevanta aktörer när det gäller cyberskyddet i den svenska finansiella sektorn samt en god uppfattning om den svenska finansmarknadens funktionssätt i allmänhet och betalningar i synnerhet.

Det är även av stor vikt att de företag och myndigheter som ingår i detta organ är representerade på tillräckligt hög nivå i arbetet. I detta sammanhang kommer organet att behöva arbeta nära tillsammans med bland andra FI, Finansiella stabilitetsrådet, FRA, MSB, NCSC, Regeringskansliet, Riksbanken, Riksgälden och Säkerhetspolisen. Organet bör alltså även ha erfarenhet av och förmåga att genomföra krisövningar, vilket vi återkommer till nedan.

Mot denna bakgrund föreslår FI att regeringen skyndsamt utreder hur ett sådant krishanteringsorgan utformas på lämpligaste sätt samt vilken myndighet som bör ges huvudansvaret.

Övnings- och testverksamheten

Berörda myndigheter och företag behöver förbereda sig för att operativt kunna hantera en attack och begränsa dess skadeverkningar genom övningar av planer och rutiner för krishantering. Det är enbart genom återkommande, väl strukturerade och realistiska övningar som myndigheternas och företagens förmåga att hantera en kris kan utvecklas och upprätthållas över tid. Eftersom ett cyberangrepp och dess följdverkningar kan vara av olika art, omfattning och spridning och beröra många olika intressenter, är det flera funktioner som behöver övas. Här märks bland annat avvärjning av angrepp (tekniskt bemötande), åtgärder för att begränsa spridning till andra system och aktörer, lokalisering och neutralisering av angreppsinstrument (skadlig kod), att sätta igång kontinuitetsåtgärder, att dela information med andra företag och berörda myndigheter, samordna agerande mellan företag, samt mellan företag och berörda myndigheter, och även extern kommunikation.

Man kan grovt klassificera övningar enligt följande.

1. Krishanteringsövningar: samordning och kommunikation inom olika intressentkretsar.

[31] 11b § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

2. Test av operationell motståndskraft mot cyberangrepp: analys och dokumentation av operationella konsekvenser av en definierad allvarlig störning.
3. Tekniska intrångstester av typen TIBER.[32]

Övningar som berör cybersäkerheten i den finansiella sektorn förekommer redan i dag. Fokus ligger i de flesta fall på samordning och kommunikation vid kris.

Finansiella stabilitetsrådet ordnar sedan ett antal år tillbaka krisövningar för de myndigheter som ingår i rådet. Övningarna omfattar emellertid enbart de fyra myndigheterna. Sedan övningarna påbörjades har enbart den som hölls i oktober 2021 haft cyberfrågor som tema. Det finns inte heller i dagsläget planer på ytterligare övningar på detta tema.

Finansiella sektorns privat-offentliga samverkan (FSPOS) ordnar också regelbundet övningar som inbegriper både myndigheter och finansiella företag. Även dessa övningar kan beröra olika typer av krisscenarier. Enligt uppgifter från FSPOS avser organisationen att senare i år ordna en övning utifrån ett scenario som inbegriper en cyberattack.

De nordiska och baltiska myndigheterna för finansiell stabilitet genomförde i januari 2019 en gemensam finansiell krisövning inom ramen för den nordisk-baltiska stabilitetsgruppen (Nordic-Baltic Stability Group, NBSG).[33] Övningen involverade 31 myndigheter från Danmark, Estland, Finland, Island, Lettland, Litauen, Norge och Sverige samt berörda myndigheter från den europeiska unionen. Övningen utgick från ett hypotetiskt krisscenario som involverade fiktiva finansinstitut i de nordiska och baltiska länderna och testade de olika myndigheternas krishanteringsförmåga och regionala samarbete. De nordiska och baltiska länderna har enats om att genomföra regelbundna finansiella krisövningar inom ramen för NBSG. Nästa övning planeras till andra halvan av 2023 och kommer då ha cyberfrågor som tema.

Därutöver finns det ett antal övningar av mer allmän karaktär som fokuserar på cyberfrågor, men utan ett särskilt fokus på den finansiella sektorn. Dessutom sker generella krisövningar inom övningsserien Nationell informationssäkerhetsövning (NISÖ) där aktörer från privat och offentlig sektor deltar.

FI kan konstatera att de övningar som hålls företrädesvis är partiella i den meningen att det som övas är hur till exempel de finansiella stabilitetsmyndigheterna sinsemellan ska samverka om ett finansiellt företag hamnar i kris. Det saknas en bred övningsform där det flerdimensionella samspelet mellan finansiella stabilitetsmyndigheter, företag inom den finansiella sektorn och

[32] TIBER är en förkortning för *Threat Intelligence-based Ethical Red Teaming*.
[33] NBSG omfattar finansdepartement, centralbanker samt tillsyns- och resolutionsmyndigheter i de åtta nordiska och baltiska länderna.

säkerhetsmyndigheter samövas under just ett cyberangrepp med systemmässiga följdverkningar. Utöver att koordinera insatser i händelse av en cyberattack, bör det nya organ som föreslås i avsnittet ovan ges ansvar för att koordinera övningsverksamheten för samhällets förmåga att klara en cyberattack mot den svenska finansiella sektorn.

Förutom övningar med inriktning på samordning och kommunikation är det av stor vikt att det genomförs övningar där olika systems och företags motståndskraft mot otillbörlig påverkan testas. Ett viktigt sådant test är det så kallade TIBER-ramverket. Ramverket syftar till att viktiga aktörer inom den finansiella sektorn ska få en bättre bild av sin förmåga att stå emot cyberangrepp, och ger således en grund för att stärka motståndskraften i det finansiella systemet. Testen innebär att en cyberattack under kontrollerade former simuleras mot en organisations anställda, processer och teknik. Testen syftar till att identifiera brister för att sedan kunna förbättra motståndskraften. I dagsläget utförs sådana tester för de systemviktiga finansiella företagen i Sverige i Riksbankens regi inom ramen för vad som kallas TIBER-SE. FI:s bild är att TIBER-SE är ett välfungerande testformat. Det kan därför vara motiverat att utsträcka detta test till att omfatta fler företag.

Vid sidan av TIBER-SE är det önskvärt att göra andra typer av intrångstester i de finansiella företagen. Sådana tester kan utföras av privata it-säkerhetsföretag och myndigheter. Ett så kallat *white box*-test ger granskaren möjlighet att inrikta testet på de svagheter som granskaren bedömer vara mest betydande, i kontrast till de typer av test, såsom TIBER, som sker i enlighet med ett i förväg bestämt ramverk. Testen utmynnar i en rapport till den granskade organisationen om vilka brister som behöver åtgärdas. En sådan rapport kan även kompletteras med vägledning och utbildning av hur bristerna bör åtgärdas samt följas upp i FI:s tillsyn.

Tillsyn över bank-id och andra e-legitimationer

Bank-id utfärdas av bankerna och är den e-legitimation som dominerar på den svenska marknaden. Denna e-legitimation sköts av Finansiell ID-teknik BID AB som ägs av ett antal banker. Antalet innehavare av bank-id är, enligt statistik från Finansiell ID-teknik BID AB, cirka 8,3 miljoner och antalet användningstillfällen var under år 2021 cirka 6,3 miljarder.[34] Bank-id är således en central tjänst, inte enbart för betalningar, utan för den som till exempel söker vård, tecknar avtal om olika tjänster eller behöver komma åt känslig information. Till skillnad från fysiska legitimationer förlitar sig samhället på att en privat tjänst, bank-id, ska fungera, även i ett utsatt läge.

FI bedömer att en cyberattack som slår ut bank-id kan få allvarliga konsekvenser för flera delar av det svenska samhället. Det finns därför skäl för samhället att

[34] Detta innebär att cirka 91 procent av alla svenskar över 12 år har bank-id och att tjänsten användes i gemensnitt 701 gånger per år och person av svenskar över 12 år.

ställa krav på att vissa samhällsviktiga tjänster ska acceptera flera olika elektroniska legitimationer.

Det bör i sammanhanget noteras att bank-id enbart står under begränsad tillsyn.[35] Mot bakgrund av tjänstens centrala betydelse och de begränsade möjligheter som det allmänna har att utöva tillsyn över den, kan FI konstatera att dagens ordning inte är tillfredsställande. FI anser att det allmännas möjlighet att utöva tillsyn över bank-id, och andra liknande tjänster, behöver ses över så att de omfattas av tydligare reglering och tillsyn. Sådan reglering och tillsyn bör inbegripa tydliga krav på säkerhetsnivå, redundans, lednings- och ägarprövning samt ge möjligheter för den ansvariga tillsynsmyndigheten att genomföra tillsyn som inte enbart är händelsestyrd. FI anser vidare att vi inte är en lämplig myndighet för att utöva sådan tillsyn, eftersom det saknas ett naturligt samband mellan tillsyn av finansiella företag och elektroniska legitimationer.

År 2019 överlämnades betänkandet *SOU 2019:14 Ett säkert statligt ID-kort – med e-legitimation till regeringen,* som innehöll ett förslag om en statlig e-legitimation. Betänkandet har remitterats men har inte lett till lagstiftning.[36] Givet dagens otillfredsställande ordning ser FI att det finns starka skäl att fortsätta arbetet med att ta fram en statlig e-legitimation, särskilt om ökad tillsyn över de privata alternativen inte skulle vara möjlig.

[35] Enligt det förslag till ny riksbankslag som föreslås träda ikraft den 1 januari 2023 ska företag som är av särskild betydelse för genomförandet av betalningar vidta åtgärder för att kunna bedriva sin verksamhet i händelse av en fredstida kris eller krig. Dessa företag ska även delta i Riksbankens beredskapsplanering samt se till så att deras anställda för den utbildning som behövs. I förarbetena till den nya riksbankslagen framgår att Finansiell ID-teknik BID AB kan vara att anse som ett sådant företag (se SOU 2019:46 En ny riksbankslag s. 1805).

[36] Frågan om reglering och tillsyn av bank-id och andra e-legitimationer ligger inom ramen för det mandat som den statliga Betalningsutredningen har. Utredningen pågår och ska lämna sitt slutbetänkande senast den 30 november 2022.

Bedömning av ökat resursbehov

Ökad tillsyn

FI har i nuläget mycket begränsad förmåga att utöva specifik tillsyn av cyberrisker. Statens budget för 2022 gav FI ett tillskott på 8 miljoner kronor för detta ändamål. Det innebär att FI kraftigt kan öka sina tillsynsinsatser, men från mycket låga nivåer. Utökade resurser är nödvändigt för att FI ska kunna bedriva en mer ambitiös tillsyn och det måste vara en långsiktig utökning. FI behöver rekrytera cybersäkerhetsexpertis samtidigt som flera andra organisationer och företag också försöker möta ett växande behov.

Löneläget för personer med önskad kompetens inom cybersäkerhet är högt och det råder en generell brist på efterfrågad kompetens. FI behöver därför på olika sätt även öka sin attraktionskraft som arbetsgivare för denna personalgrupp. En tydlig signal från regering och riksdag om att FI ska göra en långsiktig satsning på cybersäkerhet som inkluderar en ny strategi, en uppbyggnad av kritisk kunskapsmassa och en möjlighet till kompetensutveckling skulle bidra till att FI kan bli en attraktiv miljö att arbeta i.

FI behöver göra kraftfulla förstärkningar avseende it- och cybersäkerhets-kompetensen. Frågorna är stora, tekniska och komplexa och kräver stort och långsiktigt fokus från organisationen. FI behöver utveckla kompetensen för att bättre kunna förstå och bedöma dessa risker både inom it-risktillsynen och inom säkerhetsskyddstillsynen. Dessutom krävs dessa förmågor för att fylla den krishanterande roll som följer av att vara sektorsansvarig myndighet som Utredningen om civilt försvar föreslagit. Det är vidare en hel tillsynskedja som behöver förstärkas där viktiga länkar utgörs av analysstöd, ett utvecklat systemstöd och juridisk expertis vid sidan av cybersäkerhetskompetens.

Det nya regelverket, Dora-förordningen, kommer också att innebära att en större översyn av de nationella regelverken måste göras för att identifiera brister, exempelvis i form av överlapp eller glapp. Regelutvecklingen på nivå två, det vill säga, att ta fram delegerade akter inom EU, kommer att ta vid när förordningen har antagits. Det är två viktiga arbetsströmmar som tar resurser i anspråk från det faktiska tillsynsarbetet.

FI har som mål att successivt stärka vår förmåga att bedriva en effektiv tillsyn för cybersäkerhet. De nivåmedel som tilldelades 2022 bedöms vara tillräckliga för innevarande år. Svårigheterna att rekrytera personer med rätt kompetens gör att det inte går att växla upp ambitionsnivån snabbare. För 2023 bedöms ytterligare 6 miljoner kronor tillskjutas anslaget för detta ändamål. För 2024 bedöms ytterligare 8 miljoner kronor och för 2025 ytterligare 4 miljoner tillskjutas, det vill säga totalt 18 miljoner kronor ytterligare i nivå från 2025. Med denna ambitionsökning

bedöms tillsynskapaciteten på sikt stärkas till en adekvat nivå samtidigt som en balans till övriga tillsynsområden behålls.

Anslagsförändringar	2022	2023	2024	2025
Tillskott BP 2022 (nivå)	8	8	8	8
Nytt äskande (nivå)		6	14	18

Det föreslagna resurstillskottet bedöms tillräckligt för att täcka kostnaderna för att stärka hela tillsynskedjan inklusive nödvändiga systemstöd, ny databas för utlagd verksamhet och för fortbildning inom området. Med dessa resurser bedöms också i snitt två cyberriskexperter kunna avdelas för varje systemviktigt företag. FI:s verksamhet är avgiftsfinansierad. En höjd ambitionsnivå ska finansieras med ökade avgifter, som innebär att statens budgetsaldo, lånebehov eller finansiellt sparande inte påverkas. De takbegränsade utgifterna beräknas dock öka med anslagstillskottet.

Diskussion om övriga åtgärder

Nedan diskuterar FI övriga åtgärdsförslag utifrån ett resursperspektiv. Förslagen har delvis karaktären av idéuppslag. Vidare rör de även andra myndigheters ansvarsområden. Sammantaget innebär det att förslagen varit svåra att kostnadsbestämma. FRA:s hemställan om att få möjligheten att bistå finansiella företag innebär inte några nya kostnader. FRA anser att detta kan prioriteras inom den ram som finns.

Nationellt cybersäkerhetscenter ska successivt byggas upp fram till 2025. Finansieringstrappan som har aviserats är 50 miljoner 2021, 60 miljoner 2022–2023, 120 miljoner 2024 och 150 miljoner i nivå från 2025. FI anser att det är angeläget att centrets förmåga ökas så snabbt som möjligt. En höjning av aktuella myndigheters anslag för 2023 bör övervägas av denna anledning. Finansiering föreslås ske inom aviserad försvarssatsning.

FI föreslår att ett organ ska få ett uttryckligt mandat att koordinera övningsverksamheten i fråga om samhällets förmåga att klara en cyberattack eller en annan allvarlig operationell störning mot den svenska finansiella sektorn. Organet bör även tilldelas uppdraget att hantera situationer där ett systemviktigt finansiellt företag utsätts för en allvarlig cyberattack. För dessa båda uppgifter kan organet behöva lämplig finansiering. Sådan finansiering torde kunna komma från anslaget 2:4 Krisberedskap under utgiftsområde 6 Försvar och samhällets krisberedskap.

En gemensam portal för mottagande av rapportering av it-incidenter bör minska myndigheternas samlade kostnader och därmed vara självfinansierande. Om bank-

id och andra e-legitimationer regleras så att en aktiv tillsyn möjliggörs kommer ökade kostnader för tillsynen att uppstå. Tillsynen bör avgiftsfinansieras.