RAPPORT

Delredovisning av tillsynsuppdraget över it-risker

30 september 2022

Dnr 22-25815

Innehåll

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

Sammanfattning

Finansinspektionen (FI) arbetar sedan länge med informations- och cybersäkerhetsrisker inom ramen för den löpande tillsynen av de finansiella företagen. Det säkerhetspolitiska läget har inskärpt allvaret i och vikten av detta arbete.

FI har sedan årets början behövt ändra inriktningen på tillsynen på informations- och cybersäkerhetsområdet. Detta för att ytterligare driva på de finansiella företagen att fortsätta att öka motståndskraften och utveckla förmågan att hålla igång kritiska finansiella tjänster även vid en allvarlig cyberattack eller annan it-incident. Den ändrade inriktningen har främst bestått i en tät dialog med företagen under tillsyn, istället för riktade tillsynsaktiviteter. Vi har också fördjupat vårt samarbete med andra berörda myndigheter, bland annat Riksbanken. FI har dessutom varit drivande i att Nationellt cybersäkerhetscenter inom kort påbörjar en pilotverksamhet för privat och offentlig samverkan, för ökad cybersäkerhet i finanssektorn.

Så har tillsynen över it-riskerna stärkts

Uppdraget

Genom ändring av regleringsbrevet för budgetåret 2022 beslutade regeringen den 22 juni 2022 att FI senast den 1 oktober 2022 ska delredovisa hur tillsynen av de finansiella företagens hantering av informations- och cybersäkerhetsrisker (i fortsättningen kallade it-risker) hittills har stärkts under 2022 (FI dnr 2022/02084).

FI redovisar uppdraget i form av denna rapport.

Så arbetar FI med it-risktillsynen

FI arbetar sedan länge med tillsyn över it-risker hos de finansiella företagen. FI utövar tillsynen enligt de regler som gäller för hantering av operativa risker inom de olika delsektorerna av finansmarknaden. Sedan december 2021 utövar FI dessutom tillsyn över finansiella företag enligt säkerhetsskyddslagstiftningen.

I it-risktillsynen arbetar FI med riktade tillsynsaktiviteter som undersökningar och kartläggningar samt händelsestyrda insatser vid incidenter i finansiella tjänster. Vi utövar också löpande tillsyn samt bedömer it-, informations- och cyberriskexponering inom ramen för bankernas översyns- och utvärderingsprocess (ÖUP). Syftet med it-tillsynen är att, så långt det är möjligt, förebygga problem som kan hota det enskilda företagets och i förlängningen det finansiella systemets stabilitet. Genom vår tillsyn kan vi driva på de finansiella företagen så att de fortsätter att förbättra sina interna kontrollsystem, vilket i sin tur leder till att de utvecklar de förmågor som krävs för att hålla igång kritiska finansiella tjänster i samband med cyberattacker och andra slags avbrott. Vår tillsyn tar avstamp i myndighetens riskidentifieringsprocess och samlade kunskap om de finansiella företagen.

Som FI tidigare i år framhöll i rapporten Förstärkt digital motståndskraft hos företag i den finansiella sektorn (dnr 22-10015), ser vi ett behov av en kraftig ambitionshöjning i tillsynen över finansiella företags cyberrisker. FI har under året vidtagit flera åtgärder i detta syfte, som vi beskriver nedan.

Årets arbete

Ett av FI:s prioriterade områden för 2022 är att granska hur de finansiella företagen skyddar sig mot it-incidenter och cyberattacker.

Ändrad inriktning

Med anledning av det försämrade säkerhetspolitiska läget, inte minst i samband med Rysslands invasion av Ukraina, har tillsynsarbetet bytt riktning. Istället för ett planerat tillsynsarbete har en tät dialog och samtal med företagen prioriterats. Dialogen var särskilt intensiv i början av året och har syftat till att nära följa hur företagen har hanterat de ökade riskerna för cyberangrepp i och med de förändrade läget. Dialogen har varit högst prioriterad och därför tagit mycket resurser i anspråk.

Därutöver har FI prioriterat att fördjupa samarbetet och samverkan med andra myndigheter, som Riksbanken och Riksgälden, men även med myndigheter med ett särskilt ansvar för cybersäkerheten i samhället, exempelvis Försvarsmakten, Försvarets radioanstalt (FRA), Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen. Det har vi bland annat gjort i samband med den ovan nämnda dialogen med företagen under tillsyn. Dialogen har varit ett mycket viktigt verktyg där vi gemensamt med andra myndigheter och finanssektorn har arbetat förebyggande och stärkt motståndskraften. FI har även varit fortsatt aktiv i Finansiella stabilitetsrådets arbete med att ta fram en gemensam handlingsplan för cybersäkerhet i den finansiella sektorn. Enligt planerna ska arbetet slutredovisas inför rådet vid dess möte i december i år. Vidare har FI arbetat med Nationellt cybersäkerhetscenter för att pilotverksamheten för privat och offentlig samverkan för ökad cybersäkerhet i finanssektorn snarast ska komma igång.

Kommande reglering

Som vi framhöll i rapporten Förstärkt digital motståndskraft hos företag i den finansiella sektorn, behöver FI ta fram en tillsynsstrategi för en mer genomgripande och frekvent tillsyn, ett arbete som är påbörjat. FI behöver också utveckla en databas för utlagda verksamheter som ska möjliggöra analysen av koncentrationsrisker av tredjepartsleverantörer, något som kommande förordning om digital operativ motståndskraft (Dora-förordningen) tar sikte på.

Förhandlingarna kring Dora-förordningen pågår och FI har deltagit i arbetet såväl nationellt som internationellt. Nationellt har FI varit ett stöd till Finansdepartementet i översynen av översättningar och begrepp. Internationellt har samtliga tre europeiska tillsynsmyndigheter – Europeiska bankmyndigheten (EBA), Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) och Europeiska värdepappers- och marknadsmyndigheten (Esma) – enats om en enkät som har skickats ut via nationella tillsynsmyndigheter till bland annat banker, infrastrukturbolag och försäkringsbolag. Syftet med enkäten är att skapa sig en bild av hur förberedelsearbetet kan behöva se ut med fokus främst på tredjepartsrisker. Svaren på enkäten ska sammanställas och kvalitetssäkras av respektive nationell myndighet innan de ska återrapporteras till de europeiska tillsynsmyndigheterna

senare i höst. Enkäten är även ett bra underlag för FI i analysen inför att vi ska utveckla databasen med uppgifter om utkontraktering och tredjepartsleverantörer.

Tillsynsaktiviteter och internt utvecklingsarbete

Under året har resurser lagts på att hantera en större central tillståndsansökan samt ett antal undersökningar där en har avslutats och två fortfarande pågår. Esma har gjort en utvärdering av it-risker hos företag med avvecklingsverksamhet, där FI:s it-kompetenscenter har deltagit genom att ta fram underlag samt vara med på möten. Inom ramen för den löpande tillsynen har särskilda fokusområden belysts såsom risker vid utkontraktering, men även uppföljning av åtgärdsplaner som har tagits fram i tidigare undersökningar där hantering av it-risker har granskats. I den löpande tillsynen har FI hållit kvartalsvisa möten med de stora bankerna.

Utöver det som nämns ovan har vi lagt mycket arbete på att bygga upp FI:s it-kompetenscenter och det nya tillsynsuppdraget inom säkerhetsskydd, som är organiserat under it-kompetenscentret. FI:s ambition har varit att utöka personalen i it-kompetenscentret. En utmaning är att rekrytera i en omfattning som taktar med behovet, och ett skäl till det är den hårda konkurrens på arbetsmarknaden som leder till att rekryteringarna har dragit ut på tiden.

När det gäller FI:s tillsyn enligt säkerhetsskyddslagstiftningen har arbetet bestått av att ta fram rutiner och processer för de nya arbetsuppgifterna, möten med bransch-organisationer och enskilda företag samt samarbete med andra myndigheter. Utöver det har vi genomfört interna och externa workshoppar och utbildningar för att höja kompetensen. FI har också tagit fram föreskrifter som ska komplettera Säkerhetspolisens föreskrifter (PMFS 2022:1). Föreskrifterna remitterades före sommaren och planen är att FI:s styrelse ska fatta beslut senare i år.

It-risker, med stort fokus på cyberrisker, var ett enskilt tema i den djupgående analys (FSAP) som Internationella valutafonden (IMF) inledde i början av 2022. Granskningen pågick till efter sommaren. Minst två anställda arbetade på heltid med att förbereda underlag och delta i intervjuer.

FI:s arbete närmaste tiden

I takt med att mer resurser tillsätts kommer ytterligare riktade tillsynsaktiviteter att kunna genomföras även om omvärldsläget är en styrande faktor för hur FI ska planera och prioritera sitt tillsynsarbete. Som vi beskriver i rapporten Förstärkt digital motståndskraft hos företag i den finansiella sektorn har FI arbetat fram metoder för tillsynen som tar avstamp i fem förmågor utifrån internationell standard. Metoden kan anpassas och appliceras effektivt på finansiella företag oavsett verksamhet. Arbetet med att ytterligare utveckla och effektivisera samarbetet med andra myndigheter står fortfarande högt på agendan och kommer att fortsätta under året. Utbildningar inom såväl säkerhetsskyddsområdet som it-

riskområdet kommer att prioriteras en tid framöver, och även kommunikationsinsatser gentemot berörda företag kommer att behövas.

FI planerar dessutom för en organisationsförändring våren 2023. Planerna innebär att ett nytt verksamhetsområde bildas, vilket kommer skapa bättre förutsättningar för FI att stärka arbetet med bland annat it-risker och svara mot de ökade förväntningarna på tillsynen över dessa.

Avslutningsvis kan vi konstatera att det försämrade säkerhetspolitiska läget i vårt närområde har gjort att frågor om den finansiella sektorns digitala motståndskraft har kommit i fokus allt mer. Som vi beskriver ovan har det lett till flera olika insatser som inte varit planerade i förväg. Tillsammans med ökade krav på FI att delta i internationella processer, som förhandlingarna av Dora-förordningen och IMF:s analys, och det svåra rekryteringsläget, har det varit både nödvändigt och naturligt för FI att omprioritera verksamheten. Mot bakgrund av de samarbeten som har etablerats under året och pågående rekryteringar, kommer FI att kunna öka myndighetens tillsyn över finansiella företags hantering av it-risker framöver.