



KORTRAPPORT

Företagen behöver stärka sitt säkerhetsskyddsarbete

20 december 2023

Sammanfattning

De finansiella företagen behöver stärka sitt säkerhetsskyddsarbete. Det visar en fördjupad analys som Finansinspektionen (FI) har gjort under 2023 av säkerhetsskyddsarbetet hos de företag som har anmält sig till FI som verksamhetsutövare enligt säkerhetsskyddslagstiftningen.

Det kraftigt försämrade säkerhetspolitiska läget ökar risken för att svenska intressen utsätts för olika angrepp. Eftersom säkerhetsskyddet ska vara en tröskel för antagonistiska angrepp, vill FI betona vikten av ett effektivt och ändamålsenligt säkerhetsskyddsarbete.

Vi förväntar oss att de finansiella företagen löpande utvärderar och uppdaterar sina säkerhetsskyddsanalyser. Analyserna ska besvara följande frågor: vad ska skyddas, mot vad ska det skyddas och hur ska det skyddas. Det systematiska säkerhetsskyddsarbetet ska sedan ta avstamp i analysens bedömningar.



Tillsyn av säkerhetsskyddsarbetet

I denna rapport redogör vi på ett generellt plan för slutsatserna av den fördjupade analys av verksamhetsutövarnas säkerhetsskyddsorganisationer och säkerhetsskyddsanalyser som FI har gjort under 2023. I detta avsnitt beskriver vi vad säkerhetsskydd är och vilka regler som de berörda finansiella företagen i huvudsak behöver följa när det kommer till säkerhetsskyddsarbetet. Vi tar också upp FI:s roll som tillsynsmyndighet enligt säkerhetsskyddslagstiftningen. Vi redogör närmare för några av de bestämmelser som är centrala för den fördjupade analysen. I rapporten beskriver vi också ramarna för, och syftet med, den fördjupade analysen.

Bakgrund

Säkerhetsskydd handlar om att vidta förebyggande åtgärder mot spioneri, sabotage, terrorism och andra brott som kan hota Sveriges säkerhet. Det handlar också om att skydda säkerhetsskyddsklassificerade uppgifter. Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet. Kraven på säkerhetsskydd gäller för alla som driver säkerhetskänslig verksamhet. Den som driver säkerhetskänslig verksamhet kallas verksamhetsutövare.

Här är de viktigaste författningarna som reglerar säkerhetsskyddsarbetet för verksamhetsutövarna:

- säkerhetsskyddslagen (2018:585)
- säkerhetsskyddsförordningen (2021:955)
- Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd
- Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten
- Finansinspektionens föreskrifter (FFFS 2022:17) om säkerhetsskydd.

En central fråga som regleras i säkerhetsskyddslagstiftningen är skyldigheten för verksamhetsutövare att ta fram säkerhetsskyddsanalyser. Enligt 2 kap. 1 § säkerhetsskyddslagen ska den som till någon del driver säkerhetskänslig verksamhet utreda behovet av säkerhetsskydd och dokumentera det i en säkerhetsskyddsanalys.

En säkerhetsskyddsanalys ska bland annat innehålla en beskrivning av

- den säkerhetskänsliga verksamheten
- varför den är säkerhetskänslig
- vilka skyddsvärden som finns i verksamheten
- vilka skyddsnivåer verksamheten har och vilka hot som finns mot den
- vilka sårbarheter verksamheten har
- vilka säkerhetsskyddsåtgärder som behövs för att skydda verksamheten

Säkerhetsskyddsanalysen är grunden i ett systematiskt säkerhetsskyddsarbete. Enligt 2 kap. 1 § säkerhetsskyddförordningen ska analysen uppdateras vid behov och minst vartannat år. Säkerhetsskyddsanalysen ska fastställas av verksamhetsutövarens högsta chef.

En annan central reglering är kravet i 2 kap. 7 § säkerhetsskyddslagen på att en verksamhetsutövare ska ha en säkerhetsskyddschef, om det inte är uppenbart att det inte behövs. Säkerhetsskyddschefen ska vara direkt underställd chefen för verksamhetsutövarens verksamhet (det vill säga verkställande direktören) om en sådan finns, och annars verksamhetsutövarens ledning. Säkerhetsskyddschefen ska leda, samordna och kontrollera säkerhetsskyddsarbetet inom verksamheten. Detta ansvar kan inte delegeras.

Säkerhetsskyddsarbetet ska vara ständigt pågående hos en verksamhetsutövare. Det bygger bland annat på en kontinuerlig identifiering av skyddsvärda tillgångar, att säkerhetsskyddsanalysen hålls uppdaterad och att säkerhetsskyddsplaner upprättas och följs upp. Det innebär även att verksamhetsutövaren omhändertar fysisk säkerhet, informationssäkerhet och personalsäkerhet. För att säkerhetsskyddsarbetet ska bli effektivt och ändamålsenligt behöver det införas i den löpande verksamheten och i riskhanteringen.

Enligt säkerhetsskyddslagstiftningen är FI tillsynsmyndighet för enskilda verksamhetsutövare inom området finansiella företag och motsvarande utländska företag etablerade i Sverige. Det innebär att FI ska se till att verksamhetsutövarna följer säkerhetsskyddslagstiftningen. FI kan bland annat fatta beslut om åtgärdsföreläggande och sanktionsavgifter mot verksamhetsutövare som inte lever upp till regelverkets krav. FI har även möjlighet att besluta om förbud mot överlåtelser och utkontrakteringar av säkerhetskänslig verksamhet. För att vi ska kunna utöva tillsyn ska ett finansiellt företag som har identifierat att det driver säkerhetskänslig verksamhet anmäla det till FI utan dröjsmål.

Utöver tillsyn ska FI ge vägledning om säkerhetsskydd för verksamhetsutövare inom området finansiella företag.

Fördjupad analys av företagens säkerhetsskyddsarbete

FI:s tillsyn delas normalt sett upp i löpande tillsyn, fördjupade analyser och undersökningar. Fördjupade analyser syftar till att FI ska få en ökad förståelse för och kunskap om en specifik frågeställning. Fördjupade analyser kan inte ligga till grund för ingripande- eller sanktionsbeslut, men kan användas som underlag för beslut att starta och sedan göra en undersökning av ett eller flera företag.

Under 2023 har FI gjort en fördjupad analys av verksamhetsutövarnas säkerhetsskyddsorganisationer och säkerhetsskyddsanalyser. Syftet med den

fördjupade analysen är att ge oss en bättre bild av hur verksamhetsutövare under FI:s tillsynsansvar har organiserat sitt säkerhetsskyddsarbete och hur de arbetar med sin säkerhetsskyddsanalys.

Den fördjupade analysen omfattar de företag som har anmält till FI att de driver säkerhetskänslig verksamhet. Inom ramen för den fördjupade analysen har vi tittat på hur verksamhetsutövarna har organiserat sitt säkerhetsskyddsarbete, vilka resurser de har tillsatt i arbetet samt hur styrningen och rapporteringen av säkerhetsskyddsarbetet ser ut. Vi har även tittat på hur verksamhetsutövarna har tagit fram sina säkerhetsskyddsanalyser, vilka skyddsvärden och hot som har identifierats och vilka åtgärder som företagen har vidtagit för att skydda den säkerhetskänsliga verksamheten.

Genom den fördjupade analysen har FI fått en bättre förståelse för hur verksamhetsutövarna har organiserat sitt säkerhetsskyddsarbete, hur de har tagit fram sin säkerhetsskyddsanalys och vad den innehåller. Vi har även fått en indikation på hur långt verksamhetsutövare inom området finansiella företag har kommit i sitt säkerhetsskyddsarbete.

Slutsatser

Vi konstaterar att flera företag arbetar med säkerhetsskyddsfrågorna i den egna verksamheten. Men FI anser att de behöver stärka sitt säkerhetsskyddsarbete ytterligare.

De ökade spänningarna i omvärlden och den pågående ryska invasionen av Ukraina har kraftigt försämrat det säkerhetspolitiska läget, vilket ökar risken för att svenska intressen utsätts för olika angrepp. Eftersom säkerhetsskyddet ska vara en tröskel för antagonistiska angrepp vill FI betona vikten av ett effektivt och ändamålsenligt säkerhetsskyddsarbete.

En förutsättning för ett välfungerande säkerhetsskyddsarbete är att verksamhetsutövarna prioriterar arbetet med säkerhetsskyddsanalysen. Det är säkerhetsskyddsanalysen som är grunden för ett strukturerat och systematiskt säkerhetsskyddsarbete; det är i den som verksamhetsutövaren besvarar frågorna om vad som ska skyddas, mot vad det ska skyddas och hur det ska skyddas. En bristfällig säkerhetsskyddsanalys riskerar att leda till felaktiga säkerhetsskyddsåtgärder och därmed ett fel- eller underdimensionerat säkerhetsskydd. Säkerhetsskyddsanalysen behöver därför tydligt svara på

- vilken eller vilka delar av verksamheten som är säkerhetskänsliga
- vilka skyddsvärden som har identifierats (på den detaljnivå som krävs)
- mot vad och hur dessa skyddsvärden ska skyddas.

Analysen behöver dessutom uppdateras löpande, vid behov eller åtminstone vartannat år.

Ytterligare förutsättningar för ett välfungerande säkerhetsskyddsarbete är att

- det finns en organisation som ansvarar för säkerhetsskyddsarbetet
- det finns tillräckligt med resurser för arbetet
- säkerhetsskyddsarbetet införs i den löpande verksamheten och i riskhanteringen genom styrdokument, mandat och regelbunden rapportering.

Vi förväntar oss att verksamhetsutövarna inom området finansiella företag löpande utvärderar och uppdaterar sina säkerhetsskyddsanalyser. Analyserna ska besvara följande frågor: vad är det som ska skyddas, mot vad ska det skyddas och hur ska det skyddas. Det systematiska säkerhetsskyddsarbetet ska ta avstamp i analysens bedömningar.