Remissvar

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

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

2024-05-21

FI dnr 24-7220
(Anges alltid vid svar)

Nya regler om cybersäkerhet (SOU 2024:18)

Ert dnr: Fö2024/00496

Sammanfattning

Finansinspektionen (FI) tillstyrker, utifrån de utgångspunkter som myndigheten har att beakta de förslag som utredningen lämnar. FI lämnar nedan ett antal mindre synpunkter på förslagen i betänkandet.

Allmänna synpunkter

FI är tillsynsmyndighet över finansiella företag som lyder under flera olika regelverk. Från FI:s perspektiv är det därför viktigt att regleringen när det gäller digital operativ motståndskraft och cybersäkerhet är så sammanhängande och tydlig som möjligt. Det är också en fördel om rapportering kan ske på ett så enhetligt sätt som möjligt. NIS2-direktivet är ett av flera initiativ på senare tid – både från EU och på nationell nivå – som på olika sätt bidrar till att stärka den finansiella sektorns motståndskraft mot operativa risker, i synnerhet när det gäller digitala tjänster inom sektorn. Det mest betydande regelverket på området är Dora-förordningen som ska börja tillämpas den 17 januari 2025 och innehåller omfattande krav på riskhantering och incidentrapportering.[1]

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

Utöver de krav som ställs på de finansiella företagen, handlar en viktig del av att uppnå god motståndskraft om hur myndigheter ska organisera sig och samverka för att hantera incidenter och kriser. Även här bör tydlighet vara vägledande.

Utifrån dessa utgångspunkter har FI följande kommentarer till delbetänkandet.

Undantag från lagens tillämpningsområde

FI välkomnar det undantag från delar av lagens tillämpningsområde som utredningen föreslår när det gäller verksamhetsutövare som omfattas av Dora-förordningen (1 kap. 9 § lagen om cybersäkerhet och 5 § förordningen om cybersäkerhet jämte bilaga, se även s. 153).

För att göra det mer överskådligt vilka verksamhetsutövare som är undantagna från lagens tillämpningsområde kan det övervägas om det är tydligare att reglera undantaget direkt i den föreslagna lagen. De argument som utredningen framhåller för att regeringen ska peka ut författningar i en bilaga till förordningen (s. 153) gör sig enligt FI inte gällande med samma styrka när det gäller Dora-förordningen. Skälen till Dora-förordningen (skäl 16) respektive NIS2-direktivet (skäl 28) är så pass tydliga i frågan. Samtidigt ser FI fördelar med att undantag från lagen kan regleras på ett enhetligt sätt och med den högre grad av flexibilitet som en förordning medger. Den osäkerhet som kan uppstå i och med att lagen bereds för sig och tidsmässigt separat från förordningen, bör gå att lösa genom tydlig kommunikation under lagstiftningsprocessen.

FI förmodar att en liknande lösning kommer att föreslås för berörda finansiella företag när det gäller tillämpligheten av CER-direktivet[2], givet artikel 8 i CER-direktivet. I linje med vad FI anfört ovan om intresset av enhetlig reglering förordar FI att undantaget i fråga om CER-direktivet sker på ett sätt som, om förutsättningarna medger, följer undantaget i NIS2-direktivet och den föreslagna lagen samt förordningen om cybersäkerhet. Det är angeläget att det för berörda företag är tydligt vilka regler som ska tillämpas, särskilt om den lagstiftning som genomför de olika direktiven träder i kraft vid olika tidpunkter.

[2] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Clearing och avveckling av betalningar

Som FI tidigare uppmärksammat omfattas inte företag som bedriver clearing och avveckling av betalningar av Dora-förordningen.[3] I dag regleras dessa så kallade clearingorganisationer i 19 kap. lagen (2007:528) om värdepappersmarknaden. Den 1 juli 2024 träder en ny lag (2024:114) om clearing och avveckling av betalningar i kraft. Den nya lagen reglerar institutstypen clearingbolag och innehåller bland annat bestämmelser om informations-, it-, och cybersäkerhet. Kraven är dock inte lika omfattande som i Dora-förordningen.

Clearingbolag har som tillhandahållare av den finansiella infrastrukturen för betalningar en central betydelse på finansmarknaden. FI anser därför att dessa bolag behöver omfattas av en reglering som motsvarar de krav som framgår av Dora-förordningen.

Även om NIS2-direktivet och den föreslagna lagen om cybersäkerhet inte innehåller exakt samma krav som Dora-förordningen, kan ett sätt att ställa krav på clearingbolagens cybersäkerhet som bättre svarar mot kraven i Dora-förordningen vara att låta dessa bolag omfattas av lagen om cybersäkerhet. Eftersom NIS2-direktivet är ett minimidirektiv (se artikel 5), är det som utredningen noterar möjligt att fler sektorer än vad som följer av direktivet kan omfattas av regleringen (s. 72). FI noterar visserligen de tidsmässiga skäl som gör att saken svårligen kan lösas inom ramen för det här lagstiftningsärendet, men anser ändå att en sådan lösning bör övervägas.

Förhållandet till Myndigheten för samhällsskydd och beredskap

Av 29 och 30 §§ i förordningen om cybersäkerhet följer ett antal uppgifter för den CSIRT-enhet som föreslås ska inrättas på Myndigheten för samhällsskydd och beredskap (MSB) samt hur de ska följa upp gjorda incidentrapporter. Bemyndigandet för regeringen att meddela föreskrifter i denna del följer av 3 kap. 8 § i den föreslagna lagen om cybersäkerhet. Eftersom finansiella företag som ska följa Dora-förordningen är undantagna från 3 kap. i den föreslagna lagen, ska dessa företag inte heller lämna några incidentrapporter direkt till CSIRT-enheten. Av sista meningen i skäl 28 till NIS2-direktivet framgår att CSIRT-enheterna kan inbegripa finanssektorn i

[3] Se rapporten *Förstärkt digital motståndskraft hos företag i den finansiella sektorn* av den 6 maj 2022 (FI dnr 22-10015), s. 17.

sin verksamhet. Mot denna bakgrund bör det tydliggöras i den fortsatta beredningen på vilket sätt som CSIRT-enheten ska agera i förhållande till den finansiella sektorn, det vill säga hur 29 och 30 §§ i den föreslagna förordningen ska tillämpas.

Konsekvenser för FI

En uppgift för FI enligt de föreslagna reglerna är att i egenskap av tillsynsmyndighet ta emot anmälningar och upprätta ett register över verksamhetsutövare (2 kap. 2 § lagen om cybersäkerhet respektive 14 § förordningen om cybersäkerhet). FI kommer inom ramen för sitt tillsynsansvar enligt Dora-förordningen att införa flera system i syfte att hantera tillsyn och rapportering. Givet att Dora-förordningen och NIS2-regleringen är sammanlänkade förutser FI att det i systemen kommer behöva byggas in funktioner för att utskilja verksamhetsutövare som anges i NIS2-direktivet och sådan incidentrapportering som ska föras vidare till CSIRT-enheten. Detta medför ökade kostnader för FI.

FINANSINSPEKTIONEN

Daniel Barr
Generaldirektör

Michael Geller
Senior riskexpert

I detta ärende har generaldirektören Daniel Barr beslutat. Seniora riskexperten Michael Geller har varit föredragande.

Kopia till visnja.raguz@regeringskansliet.se