Finansdepartementet
Finansmarknadsavdelningen
103 33 Stockholm

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2024-00108

ER REF Fi2024/00073

Remissvar om promemorian Digital operativ motståndskraft för finanssektorn 2024-04-10

Riksbanken tillstyrker i stora drag Finansdepartementets förslag till lag med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn (DORA-förordningen) och ändringsförslagen i flera lagar på finansmarknadsområdet samt offentlighets- och sekretesslagen (2009:400) (OSL). Förslaget bidrar till att fördela ansvaret mellan Riksbanken och Finansinspektionen på ett ändamålsenligt sätt i enlighet med DORA-förordningen och att öka den finansiella stabiliteten kopplad till digital motståndskraft.

Riksbanken tillstyrker ansvarsfördelningen mellan Finansinspektionen och Riksbanken och samverkansparagrafen mellan myndigheterna. Införande av en sekretess-bestämmelse för DORA-tester tillstyrks, och att DORA-förordningen inte föranleder ändringar i säkerhetsskyddslagen. Även paragrafen om överklagande av Riksbankens beslut tillstyrks, dock bör Finansinspektionens beslut om testning gälla omedelbart för att testning ska kunna ske med korrekt tidsintervall i enlighet med DORA-förordningen.

Riksbanken avstyrker däremot förslaget till begränsningen i betaltjänstlagen, vilket i praktiken skulle innebära att Riksbanken i vissa fall inte får information om incidentrapportering.

Riksbanken efterfrågar i remissvaret vägledning från Finansdepartementet vad gäller fördelning av beslut och uppgifter inom vissa områden i den föreslagna tekniska standarden. Riksbanken vill även lyfta att invänta på yttrande vad gäller samverkan mellan Finansinspektionen och Riksbanken under den aktiva testfasen är förenat med avsevärda tids- och kostnadsökningar. Vidare kommer Riksbanken fortsätta utföra TIBER-tester vid sidan av DORA-testerna för de aktörer som inte träffas av DORA-förordningen, och Riksbanken vill betona vikten av att TIBER-testerna får ett lika tydligt sekretesskydd som DORA-testerna. Vidare anser Riksbanken att det kompletterande lagförslaget bör innehålla ett undantag för rapportering av incidenter. Remissvaret avslutas med ett medskick gällande informationsutbyte mellan finansiella entiteter.

Ansvariga myndigheter

Riksbanken tillstyrker förslaget att ansvaret för hotbildsstyrda penetrationstester ska delas mellan Finansinspektionen och Riksbanken samt med förslagets motiv och den föreslagna principen för ansvarsfördelning.

Riksbanken anser dock att mer vägledning kan ges för hur vissa beslut och uppgifter som finns i den föreslagna tekniska standarden[1] ska fördelas. Flera beslut faller naturligt under uppgiften att övervaka och samordna medan andra är mer svårplacerade. Exempel är beslut om en finansiell gruppering som är verksam i flera länder kan behöva genomföra flera tester, eller om Riksbankens deltagande i landsöverskridande tester som andra länder leder eller huruvida finansiella entiteter som använder samma IT-leverantör kan göra ett gemensamt test eller inte.

Samverkan mellan Finansinspektionen och Riksbanken

Riksbanken tillstyrker i huvudsak förslaget om samverkan mellan Finansinspektionen och Riksbanken. Riksbanken delar bedömningen att ingen myndighet ensidigt ska kunna fatta beslut som kan påverka den andra myndighetens verksamhet utan att myndigheten ges tillfälle att yttra sig. Riksbanken ser positivt på att ge Finansinspektionen möjlighet att yttra sig under förberedelsefasen, det bör dock förtydligas att Riksbanken under den aktiva testfasen kan vara mer restriktiv med när Finansinspektionen ska ges möjlighet att yttra sig.

Vid hotbildsstyrda penetrationstester är det viktigt att fokus är på lärandet och att höja den digitala operativa motståndskraften. Det är därför olämpligt att annat än under mycket särskilda omständigheter inleda tillsynsaktiviteter under ett pågående test. Förslaget till teknisk standard rekommenderar att den som övervakar ett hotbildsstyrt penetrationstest inte samtidigt ska vara inblandad i tillsynsaktiviteter för samma finansiella entitet. Beslut som tas under den aktiva fasen är ett led i en komplicerad process och tas ofta under sittande möten. Inväntande av yttrande från Finansinspektionen under den aktiva fasen skulle innebära en fördröjning av hela testprocessen och orsaka betydande merkostnader.

Sekretess

Riksbanken tillstyrker förslaget att det införs en ny sekretessbestämmelse som omfattar testning och processen enligt DORA-förordningen. Riksbanken vill även lyfta vikten av att det behövs ett tydligt sekretesstöd för de aktörer som inte omfattas DORA-förordningen men genomför TIBER-tester. Förslagsvis kan den nya sekretess-bestämmelsen utvidgas till att omfatta även TIBER-tester.

Sekretessen bör även omfatta samarbetet mellan Finansinspektionen och Riksbanken och de europeiska tillsynsmyndigheterna EBA, Esma och Eiopa. Riksbanken anser att även andra länders testmyndigheter bör nämnas med anledning av de landsöverskridande tester som kommer att utföras.

Överklagande och beslut som ska gälla omedelbart

Riksbanken tillstyrker förslaget rörande överklagande av Riksbankens beslut. När det gäller överklagande av Finansinspektionens beslut om vilka finansiella entiteter som ska testas ser Riksbanken en risk att testerna kan komma att försenas i det fall beslutet inte gäller omedelbart. Testning ska enligt art. 26 DORA-förordningen ske minst vart tredje år, ett överklagande av beslutet riskerar att den digitala operativa motståndskraften inte testas inom korrekt tidsintervall i enlighet med DORA-förordningen. En finansiell entitet har alltid möjlighet att begära inhibition vid ett eventuellt överklagande.

[1] Draft Regulatory Technical Standards specifying elements related to threat led penetration tests, https://www.esma.europa.eu/document/consultation-paper-draft-rts-tlpt

EU-direktiv på finansmarknadsområdet som ändras med anledning av DORA-förordningen

Riksbanken avstyrker förslaget att betaltjänstleverantörer som omfattas av DORA-förordningen bara bör incidentrapportera enligt DORA-förordningen, per det föreslagna nya tredje stycket i 5 b kap. 2 § lagen (2010:751) om betaltjänster. Det skulle i praktiken innebära att Riksbanken inte längre ska informeras när en betaltjänstleverantör som omfattas av DORA-förordningen underrättar Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident. Det föreslagna nya stycket bör förtydligas för att det ska framgå att Finansinspektionen även fortsatt ska vara skyldig att informera Riksbanken och andra relevanta berörda svenska myndigheter.

Enligt art. 19.6 DORA-förordningen ska den behöriga myndigheten, dvs. Finansinspektionen, skyndsamt lämna närmare uppgifter om IKT-relaterade incidenter till bland annat EBA, ECB, behöriga myndigheter enligt NIS2-direktivet samt andra relevanta offentliga myndigheter enligt nationell rätt.

Riksbanken noterar att förslaget till det nya tredje stycket får till konsekvens att Finansinspektionen inte kommer att vara skyldig att informera Riksbanken om allvarliga operativa incidenter eller säkerhetsincidenter som avser betaltjänsteleverantörer som omfattas av DORA-förordningen.

Samarbete mellan myndigheter

Riksbanken anser att det i avsnittet om samarbete mellan myndigheter bör lyftas att samarbete för utbyte av information även gäller andra centralbanker.

Centralbanker, behöriga myndigheter och ECB samarbetar idag vid hotbildstyrda penetrationstester. De länder som har implementerat ramverket TIBER-EU kommer att använda TIBER-ramverket för DORA-förordningens hotbildstyrda penetrationstester. Landsöverskridande hotbildstyrda penetrationstester kommer även fortsättningsvis att innebära ett nära samarbete vid enskilda test men även vid vidareutveckling av ramverket, erfarenhetsutbyte och utbildningar, där är därför lämpligt att även centralbanker nämns i det fortsatta lagstiftningsarbetet.

Förhållandet till nationella bestämmelser om säkerhet

Riksbanken delar bedömningen att DORA-förordningen inte föranleder ändringar i säkerhetsskyddslagstiftningen men anser att det i den kompletterande lagen till DORA-förordningen behövs införas ett undantag för rapportering av incidenter. Undantaget kan utformas likt undantaget i 1 kap. 4§ i lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

I 8 kap. 1 och 2 §§ säkerhetsskyddslagen (2018:585) finns bestämmelser om tystnadsplikt, samtidigt som det i DORA-förordningen finns en uppgiftsskyldighet för finansiella entiteter gentemot tillsynsmyndigheterna. För säkerhetskänslig verksamhet kan dessa bestämmelser överlappa, dvs. att det kan finnas en uppgiftsskyldighet enligt DORA-förordningen samtidigt som det föreligger en tystnadsplikt enligt säkerhetsskyddslagen. Det bör göras tydligt att uppgiftslämnande enligt uppgiftsskyldigheten i DORA-förordningen inte ska ses som ett obehörigt röjande av information enligt säkerhetsskyddslagen.

Med föreslaget upplägg ser Riksbanken en risk att en finansiell entitet som bedriver säkerhetskänslig verksamhet och ska delge säkerhetsskyddsklassificerade uppgifter kan tolka bestämmelserna att ett säkerhetsskyddsavtal behövs med Riksbanken. Vid ett hotbildsstyrt penetrationstest föreligger inte samarbete eller samverkan mellan den finansiella entiteten

och Riksbanken, utan Riksbanken har en övervakande och tillsynsliknande roll. Kravet på säkerhetsskyddsavtal bör inte utvidgas till sådana situationer.[2]

Riksbanken efterfrågar även ett resonemang vad bestämmelserna i säkerhetsskyddslagstiftningen och DORA-förordningen innebär för landsöverskridande tester på finansiella entiteter som bedriver säkerhetskänslig verksamhet.

Informationsutbyte mellan finansiella entiteter

Riksbanken vill slutligen göra följande medskick. Riksbanken anser att frågan huruvida en lagstiftningsåtgärd krävs eller inte angående informationsutbyte mellan finansiella entiteter i art. 45 i DORA-förordningen behöver utredas vidare.

Riksbanken är undantagen från DORA-förordningen men har ett behov av att delta i olika informationsutbyten med finansiella entiteter. Riksbanken är till exempel aktiv deltagare i det nationella cybersäkerhetscentrets finansforum. Promemorian saknar förslag på hur sekretessfrågan ska hanteras av offentliga myndigheter som deltar i samarbetet.

Praktiskt har samverkan inom finansforumet varit svårt, framför allt när det gäller automatiskt utbyte av information eftersom det från deltagande myndigheter inte alltid går att garantera sekretess. Den sekretess som 18 kap. 8 § OSL ger möjlighet till anses inte omfatta alla uppgifter som det finns skäl att sekretessbelägga. Den nya föreslagna 30 kap. 4 e § OSL synes inte vara tillämplig vid myndigheters deltagande i sådana forum. Även om den skulle vara tillämpbar innebär det raka skaderekvisitet en presumtion för att uppgifterna är offentliga och eftersom det då inte går att garantera att uppgifterna inte kommer att lämnas ut finns det hög risk att andra aktörer inte frivilligt vill dela med sig av denna typ av information.

Enligt Riksbankens bedömning behövs det därför en mer utförlig sekretessbestämmelse som omfattar information och underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg. Det är viktigt att sekretessen även gäller för automatiserad delning av information och att sekretessen följer med om uppgifterna exempelvis läggs in i system för att detektera intrång. För uppgifter som rör den egna verksamheten föreslås sekretessen bara gälla när de delas inom ramen för samarbetet.

Utformningen av en sekretessbestämmelse måste vara ett resultat av en avvägning mellan insyns- och sekretessintressena. Frivilligt samarbete mellan myndigheter och privata bolag i syfte att förbättra säkerheten hos de deltagande parterna försvåras kraftigt om inte sekretess kan garanteras. Behovet är därför att regler för absolut sekretess införs eller åtminstone ett omvänt skaderekvisit. En sådan sekretess föreslås inte omfatta den information som någon är skyldig att lämna in till en myndighet, exempelvis via incidentrapportering eller polisanmälan. Den medborgerliga makt-kontrollen bör inte nämnvärt försvagas genom att det inte är möjligt att hos myndighet A att begära ut information som berör myndighet B eller annan finansiell entitet och som kommit in genom frivilligt säkerhetssamarbete.

Det behövs även en sekretessbrytande bestämmelse som möjliggör för deltagande myndigheter att lämna ut uppgifter som omfattas av samarbetet. För flera av myndigheterna

[2] Prop. 2020/21:194 s. 32 andra stycket, se även resonemanget rörande Riksrevisionen i framställningen till riksdagen 2021/22:RS5 s. 62-63.

bakom finansforumet är det möjligtvis nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet (10 kap. 2 § OSL) men det går inte att hävda för Riksbanken. I enstaka fall skulle det gå att hävda att det står klart att intresset av ett utlämnande har företräde framför det intresse som sekretessen ska skydda (10 kap. 27 § OSL). Mer rutinmässiga utlämnanden får bara ske i undantagsfall med hänvisning till 10 kap. 27 § OSL och borde därför inte vara möjlig att använda för formaliserade samarbeten som i finansforumet.[3] Riksbanken, Riksgälden m.fl. skulle därför behöva en sekretessbrytande bestämmelse för deltagande i sådant samarbete.

På direktionens vägnar:

Erik Thedéen

Monika Gustavsson

Beslutet har fattats av direktionen (riksbankschefen Erik Thedéen, förste vice riksbankchefen Anna Breman samt vice riksbankscheferna Per Jansson, Martin Flodén och Aino Bunge) efter föredragning av cybersäkerhetsstrategen Joacim Häggmark. I den slutgiltiga handläggningen har avdelningschefen Olof Sandstedt och den seniora juristen Anna Forslind medverkat.

[3] Se prop. 1979/80:2 Del A s. 327.