Enheten för strategi och samordning (CS-ST)
Isaac Mintz
010-2404582
Isaac.Mintz@msb.se

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Remissvar - Promemorian Digital operativ motståndskraft för finanssektorn Fi2024/00073

Sammanfattning

MSB instämmer i merparten av promemorians förslag på nationella lagstiftningsåtgärder och kompletterande bestämmelser till EU-förordningen. Vi anser dock att promemorian inte tillräckligt belyst vissa frågor och aspekter som kommer att ha betydelse vid den praktiska tillämpningen, särskilt i förhållande till annan EU-reglering som nu implementeras.

Sammanfattningsvis har myndigheten följande synpunkter.

Avseende tillämpningsområdet:

- Förtydliga hur överlappningen med unionsrättsakterna direktivet (2022/2555) om åtgärder för en hög gemensam cybersäkerhet i hela unionen (NIS2-direktivet)[1] och direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft (CER-direktivet)[2] ska hanteras.
- Förtydliga att de entiteter som undantas från tillämpningsområdet i DORA behöver göra en bedömning om de omfattas av NIS2-regleringen.

Avseende tillsyn:

- Stärka informationsutbytet kring kritiska tredjepartsleverantörer.

Avseende ingripanden och sanktioner:

- Reglerna om ingripande mot vissa företrädare bör så långt som möjligt spegla motsvarande regler i NIS2.

Avseende incidentrapportering:

- Säkerställa att arbetet med framtagande av föreskrifter och mallar om incidentrapportering så långt som möjligt samordnas med motsvarande arbete för NIS2 och CER.

[1] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

[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

- Utöka och förtydliga samverkan mellan Finansinspektionen, berörd tillsynsmyndighet, Riksbanken, den gemensamma kontaktpunkten, cyberkrishanteringsmyndighet samt CSIRT-enheten som utsetts i enlighet med direktiv (EU) 2022/2555.
- Förtydliga relationen till cyberkrishanteringsområdet.
- Den gemensamma kontaktpunkten enligt NIS2-direktivet skall få ta del av de frivilliga rapporter om allvarligare cyberhot som skickas in av finansiella entiteter som lyder under DORA.

Behov av fördjupad analys

Avseende tillämpningsområdet

MSB anser att det som stöd för organisationerna i den finansiella sektorn behöver förtydligas i förarbetena till den nationella regleringen kopplad till DORA-förordningen, att de som undantas från DORA behöver analysera om de omfattas av de nationella NIS2- eller CER-regelverken. I NIS2, Bilaga I, finns de högkritiska sektorerna: Bankverksamhet (med underkategorin: Kreditinstitut) och Finansmarknadsinfrastruktur (med underkategorierna: Operatörer av handelsplatser och Centrala motparter). Inom CER, bilaga Sektorer, undersektorer och kategorier av entiteter, finns samma sektorer och underkategorier. Inom dessa sektorer skulle entiteter som undantas DORA ändå kunna omfattas av NIS2 och CER.

Med hänvisning till avsnitt 4.3 Tillämpningsområde i promemorian:

- ” DORA-förordningen är tillämplig på de flesta fysiska och juridiska personer som är verksamma inom den finansiella sektorn förutom betalningssystemoperatörer och enheter som deltar i betalningshantering (artikel 2 och 58). Förvaltare av alternativa investeringsfonder, försäkrings- och återförsäkringsföretag, tjänstepensionsinstitut och försäkrings- och återförsäkringsförmedlare som inte uppfyller vissa storlekskrav undantas från tillämpningsområdet. Från förordningens tillämpningsområde undantas även postgiroinstitut, försäkringsförmedlare som bedriver förmedling som sidoverksamhet och personer som omfattas av artikel 2 och 3 i Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU. Förordningen ger även möjlighet att undanta bl.a. Svenska skeppshypotekskassan från tillämpningsområdet.”

Storlekskravet i NIS2 beskrivs i art. 2.1. som refererar till artikel 1 och 2 i 2003/361/EG där medelstora företag definieras. Därutöver finns det entiteter som omfattas av NIS 2 oavsett storlek, vilket beskrivs i art. 2.2, 2.3 och 2.4 NIS 2. Exempelvis tillhandahållare av betrodda tjänster. Vidare, om en störning av den tjänst som entiteten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser, samt på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller

ekonomisk verksamhet. Oavsett entiteternas storlek är NIS2-direktivet även tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER, art. 6.

Storlekskraven adresseras i *Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven* (SOU 2024:18) 1 kap 8 § förslag till Cybersäkerhetslag:

- 8 § ”Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om”,
    - ”1. verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner, 2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller 3. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.”

Vilka entiteter som kommer att omfattas av NIS2 kommer specificeras i den kommande nationella NIS2-regleringen utifrån NIS2-direktivets trösklar gällande storlek och omsättning. Dessutom kan aktörer som faller under tröskelvärdena komma att omfattas om de pekas ut i föreskrifter.

Antalet regelverk med påverkan på informations- och cybersäkerhetsområdet ökar nu påtagligt. För att underlätta för privata och offentliga organisationer så ser MSB därför ett generellt behov av att det från centralt håll ges ledning i hur de olika regelverken förhåller sig till varandra och vilka organisationer som ska efterleva vilket regelverk. Detta behov gör sig särskilt gällande här eftersom de entiteter som är undantagna DORA:s tillämpningsområde med stor sannolikhet kommer att omfattas av NIS2-regleringen.

Synpunkter avseende tillsyn

Stärkt informationsutbyte kring kritiska tredjepartsleverantörer

Ur NIS2-utredningens förslag till ny cybersäkerhetsförordning:

- 16 § ”Om tillsynsmyndigheten bedriver tillsyn över en verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i DORA-förordningen ska tillsynsmyndigheten informera det tillsynsforum som inrättats enligt artikel 32 i samma förordning.”

För att denna informationsskyldighet ska kunna uppfyllas föreslår MSB att det införs motsvarande bestämmelser som ålägger den relevanta DORA-funktionen (Finansinspektionen, tillsynsforum eller de ledande tillsynsmyndigheterna) att informera berörd NIS2-tillsynsmyndighet om vilka entiteter som klassificeras som kritiska tredjepartsleverantörer. Det bör även tydliggöras hur informationsutbytet ska göras.

Avseende ingripanden och sanktioner

Förslaget i promemorian om Finansinspektionens befogenheter att kunna ingripa mot person som ingår i en finansiell entitets styrelse eller dess verkställande direktör, eller

ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter enligt DORA-förordningen, bör så långt som möjligt ensas med motsvarande regler och krav i NIS2, art. 32.5 b).

Synpunkter avseende incidentrapportering

Harmoniserad rapportering

I *Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven* (SOU 2024:18) föreslås att MSB ska utgöra gemensam kontaktpunkt, utgöra cyberkrishanteringsmyndighet samt inneha rollen som CSIRT-enhet under NIS2.

MSB framhåller att det är av stor vikt att incidentrapporteringen inom DORA sker på likartat sätt som incidentrapporteringen i NIS2. Detta för att de uppgifter om incidenter och anmälan om cyberhot som sedermera ska överlämnas till MSB från Finansinspektionen ska vara jämförbara med de uppgifter som MSB erhåller inom ramen för rapporteringen enligt NIS2. Jämförbara uppgifter är en förutsättning för att MSB ska kunna genomföra samlade analyser av innehållet i rapporteringen enligt NIS2, CER och DORA och därmed skapa en heltäckande lägesförståelse som även inkluderar den finansiella sektorn. En sådan heltäckande lägesförståelse bidrar till det samlade arbetet med stärkt motståndskraft i samhällsviktig verksamhet och totalförsvar.

När det gäller hanteringen av incidentrapporter enligt DORA i förhållande till NIS2-direktivet berörs i promemorian både med vilka information ska delas och vad som ska delas. I promemorian anges att information om inträffade IKT-incidenter ska delas med behöriga myndigheter och CSIRT-enheter enligt NIS2-direktivet. Eftersom de behöriga myndigheterna, inklusive den gemensamma kontaktpunkten, cyberkrishanteringsmyndigheten och CSIRT-enheten i NIS2 har delvis olika roller och uppgifter när det gäller hanteringen av incidenter så är MSB av den uppfattningen att samtliga av dessa behöver skyndsamt få tillgång till information om incidenter rapporterade enligt DORA. Med hänsyn till den tidskritiska natur som IKT-incidenter kan ha är det enligt MSB:s mening resurseffektivast att samtliga berörda myndigheter enligt NIS2-direktivet delges informationen samtidigt. För säker informationsdelning rekommenderas användning av den tekniska lösning WIS som MSB nu etablerar för hantering av incidentrapportering enligt NIS2 och CER-direktiven. WIS är ett välanvänt verktyg för informationsdelning inom krisberedskapssystemet med mera som nu kommer att få ytterligare funktionalitet som möjliggör säker hantering av incidentrapporter.

När det gäller vilken information som ska delas förs ett resonemang om i vilken utsträckning Sverige ska nyttja möjligheterna att ålägga finansiella entiteter att använda de mallar som tas fram på EU-nivå.[3] I promemorian konstateras att det är angeläget att myndigheter får tillräcklig och korrekt information om vad som inträffat så att relevanta åtgärder kan vidtas.[4] Vidare anförs att det får anses som tillräckligt att Finansinspektionen skyndsamt delar inkomna uppgifter med bl.a. den behöriga myndigheten, den gemensamma kontaktpunkten eller de CSIRTS-enheter som utsetts eller inrättats enligt NIS2-direktivet (artikel 19.6). Mot bakgrund av myndighetens långvariga erfarenhet av

[3] Sid 67f Promemorian

incidentrapportering anser MSB att en lösning där innehållet i vad som ska rapporteras inte närmare inriktas riskerar att få till resultat att inte bara jämförbarheten mellan incidenter som rapporterats in enligt DORA respektive NIS2- och CER-regleringen går förlorad utan även möjligheten för berörda myndigheter, inklusive Finansinspektionen, att vidta relevanta åtgärder begränsas.

Med hänsyn till finanssektorns centrala betydelse för samhällets funktionalitet och de många beroenden som finns mellan finanssektorn och andra NIS2-sektorer är detta enligt myndighetens mening olyckligt, inte minst för pågående arbete med att stärka motståndskraften i samhällsviktig verksamhet och totalförsvar.

För att uppnå syftet med den informationsdelning som ska ske med myndigheter och enheter enligt NIS2-direktivet inklusive att hitta en ur statens perspektiv resurseffektiv lösning föreslår MSB att incidentrapportering enligt DORA, som ovan nämndes, samordnas med de lösningar som nu byggs upp för att omhänderta motsvarande funktion inom NIS2. Samordningen behöver enligt MSB:s mening inte bara ske rörande kanalerna för informationsdelning utan även rörande inrapporterat innehåll. Ett effektivt sätt att säkerställa både samordning mellan incidentrapportering enligt de båda regelverken och att Finansinspektionen får den information som behövs för tillämpningen av DORA är att använda samma incidentrapporteringsformulär vid incidentrapportering enligt NIS2 och DORA med en möjlighet att addera frågor vid DORA-rapportering om det bedöms saknas någon ur finanssektorns perspektiv.

Arbetet att nyttja synergier och bygga upp incidentrapportering på ett sådant samlat sätt som här föreslås förutsätter, precis som när det gäller penetrationstester, samverkan och informationsdelning mellan myndigheterna. Behovet av tydligare rättsligt stöd för delning av känslig information mellan Finansinspektionen och Riksbanken beskrivs i promemorian.[5] Där konstateras att möjligheten för Finansinspektionen och Riksbanken att utföra sina uppgifter enligt DORA-förordningen och kompletteringslagen bör kräva ett nära samarbete, med ett omfattande och kontinuerligt informationsutbyte. Givet inriktningen att och behoven av att knyta samman DORA med NIS2- och CER-direktiven rörande informationsdelning ser MSB att motsvarande samverkan och informationsdelning skulle behöva etableras mellan Finansinspektionen och MSB. Myndigheten föreslår därför att en ytterligare regel om informationsdelning införs i 1 kap förslaget till kompletteringslag.

Samverkan
4 § Finansinspektionen och Myndigheten för samhällsskydd och beredskap ska lämna varandra de uppgifter som respektive myndighet behöver för samverkan kring incidentrapportering och informationsdelning avseende hot, sårbarheter och risker.

Information som lämnats till Finansinspektionen enligt artikel 19 punkt 4 ska skyndsamt delas med berörd tillsynsmyndighet, den gemensamma kontaktpunkten, cyberkrishanteringsmyndigheten och CSIRT-enheten som utsetts i enlighet med direktiv (EU) 2022/2555.

[5] Sid 72f Promemorian

Relationen till cyberkrishantering

MSB vill även tydliggöra vikten av att nationell tillämpning av DORA förhåller sig till utvecklingen och bestämmelserna i NIS2-direktivet, Cyberkrishanteringsmyndigheten och den nya funktionen för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur. Samverkan och informationsutbyte mellan de behöriga myndigheterna inom respektive uppdrag kommer att vara avgörande för en lyckad nationell implementering av de båda unionsrättsakterna.

EU-kommissionen har meddelat att DORA-förordningen inte utgör lex specialis inom cyberkrishanteringsområdet där istället den särskilt utsedda Cyberkrishanteringsmyndigheten kommer att ha ett utpekat ansvar och leda arbetet. Utöver det har EU-CyCLONe (art. 16 NIS 2) samordningsansvar gällande storskaliga cybersäkerhetsincidenter[6] och cyberkriser. Det betyder att relevant information inte enbart bör lämnas till de behöriga myndigheterna och den ledande tillsynsmyndigheten enligt DORA. MSB föreslår med anledning av ovan följande ändring i 5 b kapitlet 3 § 1 stycket Förslag till lag om ändring i lagen (2010:751) om betaltjänster:

Finansinspektionen ska så snart det kan ske informera Riksbanken *samt den gemensamma kontaktpunkten, Cyberkrishanteringsmyndigheten, den nationella CSIRT-enheten enligt direktiv (EU) 2022/2555*, andra berörda svenska myndigheter, Europeiska bankmyndigheten och Europeiska centralbanken.

Frivillig rapportering om allvarligare cyberhot

I avsnitt 5.6 i promemorian[7] föreslås att möjligheten att bestämma att finansiella entiteter som frivilligt rapporterar om allvarliga cyberhot också får vidarebefordra en anmälan till den särskilt utsedda NIS2-myndigheten inte bör utnyttjas.

Mot bakgrund av ovan beskrivna behov av en samlad lägesuppfattning som stöd för arbetet med att stärka totalförsvaret ser MSB det som problematiskt att inte nyttja de möjligheter till informationsdelning och incidentrapportering som ges. Myndigheten rekommenderar därför att finansiella entiteter ges möjlighet att frivilligt dela den här typen av information med berörda myndigheter enligt NIS2.

Övriga synpunkter

MSB anser att det är viktigt att säkerställa enhetlig användning av begreppet *kontinuitetsplan*, och att detta skiljs från *beredskapsplan*, i de olika lagtexterna.

Exempel i avsnitt 2.2: I detta förslag används begreppet *beredskapsplan* där det borde stå *kontinuitetsplan.* I avsnitt 2.8: I detta förslag används begreppen *IKT-plan* (oklar innebörd) och *IKT-kontinuitetsplan.* Sannolikt kan båda ersättas med *kontinuitetsplan.*

[6] Hänvisning till definitionen i artikel 6 i NIS2-direktivet
[7] Sid 65f Promemorian

I detta ärende har generaldirektör Charlotte Petri Gornitzka beslutat. Isaac Mintz har varit föredragande. I den slutliga handläggningen har också biträdande avdelningschefen Ronny Harpe och enhetschefen Johan Turell deltagit.

Charlotte Petri Gornitzka Isaac Mintz

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984