FOI - Totalförsvarets forskningsinstitut
164 90 Stockholm

08-555 030 00
registrator@foi.se

Datum: 2024-04-08
Diarienummer: FOI-2024-85:1

Christian Vestlund
Cyberförsvar och ledningsteknik
Cyberförsvar

Remissvar gällande Promemorian Digital operativ motståndskraft för finanssektorn, Fi2024/00073

Sammanfattning av FOI:s synpunkter

Totalförsvarets forskningsinstitut (FOI) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet. Remissvaret utgår huvudsakligen från två perspektiv: totalförsvar och informations-/cybersäkerhet.

FOI tillstyrker förslaget som lämnas i promemorian. Dock finns ett antal synpunkter och kommentarer på förslaget.

Det är bra att det införs tydlig lagstiftning för hanteringen av cybersäkerhet för IKT-system inom finanssektorn. IKT-system hos finansiella entiteter har en viktig roll i dagens samhälle där fler och fler tjänster digitaliseras. Då kritiska funktioner i det svenska finansiella systemet är nästan enbart digitala[1] är det av stor betydelse att upprätthålla god cybersäkerhet.

FOI anser att säkerhetsskyddslagen (2018:585) inte omhändertagits tillräckligt väl i promemorian. Promemorian påpekar att vissa finansiella entiteter omfattas av både DORA-förordningen och säkerhetsskyddslagen, men konsekvenserna för dessa entiteter beskrivs inte.

Övergripande kommentarer

Nedan följer de övergripande kommentarer som FOI har på promemorian. Dessa kommentarer berör innehåll som är spritt på flera ställen i betänkandet och kan därmed inte hänföras till ett enskilt avsnitt.

Säkerhetsskydd

Finansiella entiteter utgör en samhällsviktig funktion och är av betydelse för totalförsvaret. I vissa fall är finansiella entiteter också av betydelse för Sveriges säkerhet, vilket omnämns i kapitel 5.5 i promemorian. Bedömningen i kapitel 5.5 är att DORA-förordningen inte föranleder ändringar i nationella bestämmelser

[1] Elestedt L., Nilsson U., Rosenvinge C.-J. (2021). *Ekonomisk kommentar – En cyberattack kan påverka den finansiella stabiliteten*, Sveriges Riksbank.

om säkerhet, specifikt säkerhetsskyddslagen (2018:585). FOI instämmer i bedömningen men anser att det saknas tydliga resonemang om relationen mellan arbetet som finansiella entiteter är tänkta att bedriva enligt DORA-förordningen och säkerhetsskyddsarbetet som entiteterna bedriver i dagsläget.

Det kan komma att uppstå överlapp mellan arbete som föreskrivs i DORA-förordningen och säkerhetskyddsarbete som föreskrivs av säkerhetsskyddslagen. Exempelvis kan uppgiftsskyldigheten i 2 kap. 2 § i kapitel 2.1 innebära att säkerhetsskyddsklassificerad information kan komma att begäras ut av Riksbanken. Ovanstående berörs inte i konsekvensanalysen.

För fall där DORA-förordningen och säkerhetsskyddslagen överlappar bör det tas fram tydliga vägledningar för hur finansiella entiteter ska agera.

Sekretess

Flera kapitel i promemorian omnämner sekretess och utbyte av information mellan myndigheter och finansiella entiteter. Dock saknas beskrivningar om säkerhetsskyddsklassificerad information ingår i utbytet och eventuella konsekvenser om den typen av information ingår i utbytet.

Säkerhetsskyddsklassificerade uppgifter är sådana uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller skulle omfattas av sekretess om lagen hade varit tillämplig. Enligt SÄPO:s vägledningar[2] ska alla aktörer som bedriver säkerhetskänslig verksamhet göra en bedömning huruvida en uppgift är säkerhetsskyddsklassificerad. Inom ramen för finansiella entiteters arbete med IKT-säkerhet kan det förekomma uppgifter som är säkerhetsskyddsklassificerade om en entitet bedömt att uppgifter är av relevans för Sveriges säkerhet. Även sekretess enligt andra lagrum än de som omnämns i promemorian kan förekomma, exempelvis 18 kap 8 §.

Kapitel 9 om sekretess tar inte upp hantering av säkerhetsskyddsklassificerade uppgifter. Kapitlen 6.2, 11 och 12 belyser specifikt utbyte av uppgifter som omfattas av sekretess, men inget av kapitlen beskriver scenarion som innefattar säkerhetsskyddsklassificerad information.

Då uppgifter kan behöva utlämnas till organisationer utanför Sverige enligt DORA-förordningen bör hanteringen av uppgifter som omfattas av sekretess tydligt beaktas, speciellt i de fall där säkerhetsskyddsklassificering av uppgifter kan förekomma. Det framgår inte i promemorian om förekomsten av säkerhetsskyddsklassificerade uppgifter kan föranleda specifika åtgärder, såsom säkerhetsskyddsavtal, för att kunna genomföra hotbildsbaserade penetrationstester.

Uppgiftsskyldighet

Det är bra att Riksbanken ges möjlighet att begära uppgifter enligt 2 kap. 2 § i den föreslagna kompletterande lagen. Ur ett cybersäkerhetsperspektiv behövs ofta en

[2] SÄPO (2023). *Vägledning i säkerhetsskydd – Informationssäkerhet.*

stor mängd information för att göra bedömningar av cybersäkerhet, detta inkluderar att göra bedömningar av testplaner för penetrationstester.

Uppgiftsskyldigheten ger Riksbanken bred befogenhet att begära ut information från finansiella entiteter. I praktiken får Riksbanken möjlighet att begära ut all information om en finansiell entitets IKT-system. En potentiell konsekvens är att Riksbanken kan komma att inneha stora mängder information om flera finansiella entiteters IKT-system, vilket utgör en måltavla för antagonister som vill påverka samhällsviktig verksamhet i Sverige. Samma resonemang gäller också för Finansinspektionens tillsynsarbete.

Kapitel 19 – Konsekvensanalys

Utöver kommentarerna om säkerhetsskydd, sekretess och uppgiftsskyldighet anser FOI att konsekvensanalysen bör vara mer detaljerad i termer av kostnader och hur tredjepartsleverantörer påverkas.

De ekonomiska konsekvenserna beskrivs överlag som begränsade, men det finns ingen beskrivning om vad begränsat innebär. Promemorian påpekar samtidigt att det är svårt att göra en bedömning av de ekonomiska konsekvenserna för Finansinspektionen, vilket inte påpekas för de övriga entiteterna. Konsekvenserna för exempelvis Riksbanken bör också anses vara svåra att uppskatta då det dels inte framgår i hur stor utsträckning man idag utför uppgifter enligt TIBER-EU, dels för att det i DORA-förordningen påpekas att tekniska standarder för genomförandet av den hotbildsstyrda penetrationstestningen ska utvecklas[3]. Det saknas resonemang kring om Riksbankens nuvarande resurser är tillräckliga för att genomföra arbete enligt TIBER-EU när antalet entiteter som ska testas ökar.

Konsekvensanalysen för företag är inte tydlig om konsekvenserna också inkluderar tredjepartsleverantörer. Då dessa också inkluderas i tillsyn och den hotbildsbaserade penetrationstestningen bör konsekvensernas omfattning för dem beskrivas.

Konsekvensanalysen i kapitel 19 omnämner inte eventuella tillkommande risker med att hantera stora mängder information om finansiella entiteters IKT-system.

FOI anser att påståendet "I ett längre perspektiv kan de nya kraven innebära kostnadsbesparingar för företagen ..." på sidan 125 är motsägelsefullt då tidigare avsnitt beskriver ökade kostnader för företagen. Att risken för driftavbrott minskar med förbättrad IKT-säkerhet är en rimlig bedömning men kan inte likställas med kostnadsbesparingar utan tydligare motiveringar.

[3] Se exempelvis artikel 26.11 i DORA-förordningen.

Detta remissvar har beslutats av överdirektör Lena Nyberg efter föredragning av forskningsingenjör Christian Vestlund. I den slutliga handläggningen har även chefjurist Eva Liljefors och särskild rådgivare Mikael Wiklund deltagit.

Lena Nyberg

Christian Vestlund

Sändlista
Finansdepartementet
Anna Stenberg, Regeringskansliet

För kännedom
Försvarsdepartementet

Internt FOI
Registrator
GD-sekreterare
Särskild rådgivare
Chefsjurist
AC