REMISSYTTRANDE

2024-04-15

FRA beteckning
Dnr 3.2:3065/24:2

Finansdepartementet
Finansmarknadsavdelningen
fi.remissvar@regeringskansliet.se
anna.stenberg@regeringskansliet.se

| Er handläggare | Ert datum | Er beteckning |
|---|---|---|
| Anna Stenberg | 2024-01-15 | Fi2024/00073 |
| FRA handläggare | FRA föreg. datum | FRA föreg. beteckning |
| Olle Molin | | |

# Promemorian Digital operativ motståndskraft för finanssektorn

Finansdepartementet har den 15 januari 2024 skickat promemorian Digital operativ motståndskraft på remiss och begärt svar senast den 15 april 2024. Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på promemorians förslag.

Sammanfattningsvis anser FRA att det finns anledning att i det fortsatta lagstiftningsarbetet göra en djupare analys avseende regleringens förhållande till nationella bestämmelser om säkerhet och sekretess. FRA har även en synpunkt vad gäller ställningstagandena avseende rapportering av informations- och kommunikationsteknikincidenter (IKT-incidenter) och cyberhot samt en kommentar avseende hotbildsstyrda penetrationstester.

Synpunkterna följer promemorians disposition.

### 5.5 Förhållandet till nationella bestämmelser om säkerhet

Avsnittet i promemorian som behandlar regleringens förhållande till nationella bestämmelser om säkerhet är kortfattat och konstaterar enbart att bestämmelserna i säkerhetsskyddslagen går före bestämmelserna i DORA-förordningen[1]. Frågan om säkerhetsskyddsklassificerade uppgifter kommer att omfattas av rapporteringsskyldigheten enligt DORA-förordningen behandlas inte.

[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.

FRA
Box 301
161 26 BROMMA

Telefon
010 – 557 46 00

Telefax

Org.nr
20 21 00 - 0365

FRA

FRA anser att det finns behov av en djupare analys av regleringens förhållande till bestämmelser om nationell säkerhet i den fortsatta lagstiftningsprocessen och att säkerhetsskyddsklassificerade uppgifter inte bör omfattas av rapporteringsskyldigheten. I betänkandet Nya regler om cybersäkerhet (SOU 2024:18) behandlas frågan om EU-regleringens förhållande till nationell rätt utförligt (se SOU 2024:18 s. 154–165). I det betänkandet föreslås även ett undantag för rapportering av säkerhetsskydds-klassificerade uppgifter.

**5.6 IKT-relaterade incidenter och Cyberhot**

I promemorian konstateras att det i första hand är Finansinspektionen som har nytta av information om IKT-relaterade incidenter.

FRA anser att det finns andra aktörer som också kan ha nytta av sådan information. Det kommer exempelvis att vara den nationella enheten för hantering av it-säkerhets-incidenter (CSIRT-enheten) som ska lämna stöd och råd till en verksamhetsutövare vid en IKT-relaterad incident.

**6 Hotbildsstyrda penetrationstester**

FRA tillstyrker att Finansinspektionen och Riksbanken ska ansvara för de hotbildsstyrda penetrationstesterna. FRA vill dock utifrån myndighetens erfarenheter påpeka att den aktuella typen av tester inte är resurseffektiva eftersom de fokuserar på att hitta en sårbarhet som sedan kan utnyttjas i stället för att identifiera så många sårbarheter som möjligt. De hotbildsstyrda penetrationstesterna tar inte heller höjd för att kvalificerade hotaktörer kan ta lång tid på sig för att identifiera sårbarheter och att det inte är säkert att de tekniker som historiskt identifierats kommer att användas vid ett riktat cyberangrepp.

FRA har i dag uppdrag att erbjuda stöd i cybersäkerhetsfrågor till de mest skyddsvärda verksamheterna och för inom ramen för det uppdraget en dialog med aktörer inom finanssektorn. Den dialogen omfattar bl.a. traditionella penetrationstester. Den metodik som FRA använder sig av vid penetrationstester medför att ett betydligt större antal sårbarheter kan identifieras. För att få ett så bra resultat som möjligt sker testerna i nära samarbete med de som sköter driften av it-systemet.

**9 Sekretess**

I avsnittet om sekretess behandlas inte frågan om några av de uppgifter som kan komma i fråga kan komma att omfattas av sekretess för säkerhets- eller bevakningsåtgärder enligt 18 kap. 8 § offentlighets- och sekretesslagen (2009:400), OSL, och eventuella följder av detta. Exempelvis skiljer sig sekretesstiden i den föreslagna 30 kap. 4 e § OSL mot sekretesstiden i 18 kap. 8 § OSL. I 30 kap. 4 e § anges att sekretessen för en

uppgift i en allmän handling ska gälla i 20 år och i 18 kap. 8 § OSL finns ingen sådan tid angiven. Uppgifter i incidentrapporter på cybersäkerhetsområdet omfattas normalt av sekretess enligt 18 kap. 8 § OSL (se t.ex. Kammarrätten i Göteborgs dom den 29 juni 2021 i mål nr 2144-21). Till detta kommer att frågan om sekretess för uppgifter med anledning av den typ av incidentrapportering som det är fråga om kommer att behandlas i ett kommande slutbetänkande från utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (se SOU 2024:18 s. 203). Det finns därför anledning att i det fortsatta lagstiftningsarbetet genomföra en djupare analys av regleringens förhållande till bestämmelserna i OSL.

---

**Allmänt om FRA**

FRA är en civil myndighet under Försvarsdepartementet med ca 1 000 anställda. FRA är en del av svensk underrättelsetjänst med uppgift att bedriva försvarsunderrättelseverksamhet till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Inom försvarsunderrättelseverksamheten ska FRA bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning.

FRA bedriver signalspaning i syfte att kartlägga bl.a. yttre militära hot, internationell terrorism, allvarliga yttre hot mot samhällets infrastrukturer, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets-, och försvarspolitik. All signalspaning är riktad mot utländska förhållanden och sker på uppdrag av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten. Uppdragsgivarna är fortlöpande i behov av underrättelserapportering och signalspaningsverksamheten bidrar kontinuerligt till att skydda Sverige och svenska intressen.

FRA bedriver även teknisk informationssäkerhetsverksamhet. FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt hänseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd.

Uppgifter rörande FRA:s verksamhet omfattas i stora delar av sekretess bl.a. enligt 15 kap. 2 § och 18 kap. 8 § OSL.

FRA

_____

I detta ärende har chefsjuristen Michaela Dráb beslutat. I den slutliga handläggningen har också deltagit juristen Olle Molin (C JUR:s kansli/rättsenheten), tillika föredragande.

Försvarets radioanstalt

Michaela Dráb

Olle Molin

Sändlista

Externt för kännedom
Försvarsdepartementet/EFU
Försvarsdepartementet/Rättssekretariatet

Internt FRA
GD
ÖD
C JUR
Bitr. C JUR
C GD:s stab
C KOM
AC
C Rätts