REMISSYTTRANDE

2024-05-28

FRA beteckning
Dnr 2024FRA257-6

Försvarsdepartementet
Rättssekretariatet

Er handläggare	Ert datum	Er beteckning
Visnja Raguz	2024-03-06	Fö2024/00496
FRA handläggare	**FRA föreg. datum**	**FRA föreg. beteckning**
Olle Molin		

Nya regler om Cybersäkerhet (SOU 2024:18)

Försvarsdepartementet har den 6 mars 2024 skickat delbetänkandet Nya regler om Cybersäkerhet (SOU 2024:18) på remiss och begärt svar senast den 28 maj 2024. Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på förslagen i delbetänkandet.

FRA tillstyrker utredningens förslag om att FRA ska undantas från tillämpningsområdet för den föreslagna lagen om cybersäkerhet (cybersäkerhetslagen) och att skyldigheten att lämna uppgifter enligt cybersäkerhetslagen inte ska gälla säkerhetsskydds-klassificerade uppgifter. FRA avstyrker förslaget om att Inspektionen för strategiska produkter (ISP) ska omfattas av cybersäkerhetslagens tillämpningsområde. FRA har i övrigt några synpunkter och kommentarer avseende nya krav på kryptering och autentisering, genomförande av NIS2-direktivets[1] bestämmelser om standarder samt avsnittet om tillsyn. När det gäller förslagen i avsnitt 10 i delbetänkandet hänvisar FRA i huvudsak till vad som förts fram i FRA:s tidigare remissyttrande[2] avseende promemorian Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning.

Synpunkterna följer delbetänkandets disposition.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2055 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 (NIS2-direktivet).
[2] FRA:s dnr 2024FRA660-2.

FRA
Box 301
161 26 BROMMA

Telefon
010 – 557 46 00

Telefax

Org.nr
20 21 00 - 0365

FRA

5.5 Undantag för Sveriges säkerhet och brottsbekämpning

FRA tillstyrker utredningens förslag om att FRA ska undantas från den föreslagna cybersäkerhetslagens tillämpningsområde och att skyldigheten att lämna uppgifter enligt cybersäkerhetslagen inte ska gälla säkerhetsskyddsklassificerade uppgifter.

FRA noterar att utredningen har föreslagit att ISP ska omfattas av den nya cybersäkerhetslagen. Detta trots att inriktningen i direktivet till utredningen är att säkerhetskänslig verksamhet ska undantas och att det förts fram till utredningen att ISP inte bör omfattas av regleringen. Några närmare skäl för utredningens ställningstagande anges inte. FRA, som understödjer ISP inom exportkontroll genom att utvärdera produkters kryptologiska funktionalitet, anser att det finns en risk för att ISP:s verksamhet kan komma att påverkas negativt av att omfattas av regleringen. FRA avstyrker därför förslaget om att ISP ska omfattas av regleringen.

7.1.2 Riskhanteringsåtgärder

Nya krav på kryptering och autentisering i förslaget till cybersäkerhetslag

FRA uppfattar att det är utredningens avsikt att förslaget till 3 kap. 1 § cybersäkerhetslagen ska spegla innehållet i artikel 21.2 i NIS2-direktivet. FRA anser dock att den föreslagna lagtexten inte speglar punkterna i artikel 21.2 i NIS2-direktivet när det gäller åtgärder rörande användning av kryptering och autentisering.

I artikel 21.2 i NIS2-direktivet anges att riskhanteringsåtgärder i form av kryptering och lösningar för bl.a. multifaktorsautentisering ska göras när så är lämpligt. I utredningens förslag till 3 kap. 1 § cybersäkerhetslagen har orden ”när så är lämpligt” utgått. Genom att utesluta lämplighetskravet skulle det kunna tolkas som att utredningen avsett att göra kryptering och autentisering obligatoriskt, men samtidigt lämnat det öppet om hur stark kryptering som krävs. Det finns en risk att detta medför onödigt kostsamma obligatoriska åtgärder som inte heller är möjliga att granska. Utredningen motiverar inte denna innehållsförskjutning.

Enligt FRA:s mening innebär utredningens förslag i den här delen att det införs nya krav i förhållande till direktivet. Av det aktuella avsnittet framgår dock inte att detta är utredningens avsikt. Om avsikten är att det ska införas ett obligatoriskt krav på

kryptering och autentisering som går utöver NIS2-direktivets krav anser FRA att det måste analyseras djupare under det fortsatta lagstiftningsarbetet.

Genomförande av NIS2-direktivets bestämmelser om standarder

Enligt artikel 21.1 andra stycket i NIS2-direktivet ska relevanta europeiska och internationella standarder beaktas i tillämpliga fall. Detta följer även av artikel 25.1 där det framgår att medlemsstaterna, utan att föreskriva eller gynna användningen av viss teknik, ska uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.

Utredningen gör bedömningen att det inte är möjligt att i lag föreskriva att standarder ska beaktas utan att detta får uppmuntras på andra och frivilliga sätt.

Verksamhetsutövarna som träffas av NIS-2 direktivet måste bl.a. implementera cybersäkerhetsåtgärder så snart som möjligt för att undgå tillsynsåtgärder. Detta innebär att en verksamhetsutövare själv måste göra åtminstone en bedömning om vilka säkerhetsåtgärder som är lämpliga och proportionerliga och som kan antas möta tillsynsmyndighetens krav. Även om användning av standarder uppmuntras finns ett stort antal standarder som sannolikt alla i princip skulle kunna uppfylla kraven. Detta innebär dock inte att alla standarder löser problemet på ett så kostnadseffektivt sätt som möjligt.

Mot denna bakgrund menar FRA att det går att ställa sig frågan om artikel 21.1 och 25.1 i NIS2-direktivet om att uppmuntra till användning av standarder kan anses vara genomförda till fullo.

8 Tillsyn

I dagsläget bedriver de olika aktörerna i samhället sitt informationssäkerhetsarbete på delvis olika sätt, utifrån olika förutsättningar och behov, baserat på flera olika regelverk och delvis olika uppfattningar om hot och risker. För att komma tillrätta med detta pågår ett arbete med att utveckla en nationell modell för systematiskt informations-säkerhetsarbete.

Utredningen pekar i avsnitt 8.4.1 på att antalet sektorer ökar i antal från nuvarande sju till 18 och föreslår att det ska finnas en tillsynsmyndighet för varje sektor. I avsnitt 8.4.5

föreslås att tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder samt systematiskt och riskbaserat informationssäkerhetsarbete inom sitt tillsynsområde.

FRA anser att detta riskerar att ytterligare fragmentera styrningen av det nationella arbetet med informationssäkerhet och att det därför är angeläget att utveckla en nationell modell för systematiskt informationssäkerhetsarbete. En sådan nationell modell ersätter inte föreskrivande myndigheters uppgifter utan syftar i stället till att på sikt harmonisera det nationella regelsystemet genom bl.a. gemensam terminologi och en gemensam klassningsmodell med tillhörande skyddsnivåer och säkerhetsåtgärder.

Arbetet med en nationell modell för systematiskt informationssäkerhetsarbete skulle med fördel kunna bedrivas inom Nationellt cybersäkerhetscenter (NCSC), som i promemorian Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning, föreslås få i uppdrag att verka för ett enhetligt informationssäkerhets- och cybersäkerhetsarbete.

10 Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

Utredningens förslag
Utredningen föreslår att Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt, CSIRT-enhet samt cyberkrishanteringsmyndighet i Sverige.

I promemorian Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning föreslås att NCSC blir en del av FRA och att FRA därmed får huvudansvar för NCSC. I promemorian görs även bedömningen att verksamheten i CERT-SE, som i dag är CSIRT-enhet, bör överföras till FRA samt att FRA bör utses till nationell cyberkrishanteringsmyndighet.

Som framgår av FRA:s remissvar den 24 maj 2024[3] avseende promemorian välkomnar FRA promemorians förslag och instämmer i dess bedömning. I remissvaret för FRA även fram att det finns anledning att utreda om FRA ska utses till gemensam kontaktpunkt enligt NIS2-direktivet och att det finns anledning att överväga att flytta andra relevanta uppgifter som exempelvis det systematiska informationssäkerhetsarbetet till NCSC.

[3] FRA:s dnr 2024FRA660-2

De närmare rättsliga, organisatoriska och praktiska förutsättningarna för en verksamhetsöverföring behöver utredas ytterligare i ett annat sammanhang. Som framgår av remissvaret anser FRA att en sådan utredning med fördel även omfattar frågorna om tilldelandet av uppgifterna som cyberkrishanteringsmyndighet, gemensam kontaktpunkt och det systematiska informationssäkerhetsarbetet. FRA ser fram emot att delta i en sådan utredning.

FRA bör representera Sverige i en undergrupp för postkvantkryptografi

Den Europeiska kommissionen har i en rekommendation av den 11 april 2024[4] beskrivit hur kryptografi ska utvecklas enligt NIS2-direktivet för att klara av hoten från kvantdatorer. För att uppmuntra medlemsstaterna att samordna sina åtgärder på unionsnivå rekommenderar kommissionen medlemsstaterna att inrätta ett särskilt forum. Vidare rekommenderas att forumet inrättas som en undergrupp till samarbetsgruppen för nät- och informationssäkerhet.

FRA har bl.a. i uppdrag att upprätthålla kompetensen för de nationella behoven i fråga om kryptologi[5] och bör därför representera Sverige i en undergrupp för postkvantkryptografi.

Den aktuella samarbetsgruppen regleras i artikel 14 i NIS2-direktivet. Av 22 § i förslaget till förordning om cybersäkerhet framgår att det är den gemensamma kontaktpunkten som ska vara Sveriges representant i samarbetsgruppen som inrättats enligt artikel 14 i NIS2-direktivet.

Det är viktigt att Sverige tidigt finns representerat i undergruppen för postkvantkryptografi för att ha möjlighet att påverka. Oavsett vilken myndighet som utses till gemensam kontaktpunkt enligt NIS2-direktivet bör därför FRA så snart som möjligt få uppgiften att representera Sverige i undergruppen för postkvantkryptografi.

---

[4] Kommissionens rekommendation (EU) 2024/1101 av den 11 april 2024 om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi.
[5] 2 a § förordningen (2007:937) med instruktion för FRA.

FRA

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

Försvarets radioanstalt

Jessica Sjöstrand

Olle Molin

Sändlista

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