REMISSYTTRANDE

2026-05-13

FRA beteckning
Dnr 2026FRA679-2

Försvarsdepartementet
Enheten för cyber- och hybridfrågor

Er handläggare
Felix Nolte

Ert datum
2026-03-24

Er beteckning
Fö2026/00576

FRA handläggare
Karin Adamsson

Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11,13

Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på Europeiska kommissionens (kommissionen) cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555), nedan förkortad kommissionens cybersäkerhetspaket.

Inledning och sammanfattning av FRA:s synpunkter

FRA ställer sig huvudsakligen positivt till förslagen i kommissionens cybersäkerhetspaket. Från den 1 juli 2026 kommer FRA att ta över ett antal roller och uppgifter som i dag innehas och utförs av Myndigheten för civilt försvar. Flera av dessa roller aktualiseras även i kommissionens cybersäkerhetspaket, däribland rollen som nationell CSIRT-enhet, cyberkrishanteringsmyndighet och gemensam kontaktpunkt. Dessa roller kommer att utföras genom det nationella cybersäkerhetscentret (NCSC) vid FRA.

NCSC har genom förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt givits ett brett uppdrag att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. FRA bedömer att förslagen i kommissionens cybersäkerhetspaket kommer att påverka NCSC:s arbete bland annat genom NCSC:s roll som CSIRT-enhet och omfattningen av FRA:s föreskriftsrätt.

FRA
Box 301
161 26 BROMMA

Telefon
010 – 557 46 00

E-post
fra@fra.se

Org.nr
20 21 00 - 0365

Föreslagna ändringar i cybersäkerhetsakten (EU 2019/881)

FRA välkomnar en förstärkt Europeiska unionens cybersäkerhetsbyrå (Enisa) som med större kapacitet kan bidra med stöd och annat förmågehöjande arbete. Det är dock viktigt att Enisa inte genom operativt arbete går in på områden som medlemsstaterna ansvarar för genom sina nationella myndigheter (främst i egenskap av nationell CSIRT-enhet), enskilt eller i samverkan med andra medlemsstaters behöriga myndigheter. Detta är särskilt relevant rörande arbetet med krishantering och annat stöd vid hantering av incidenter.

Enisas roll rörande sårbarhetshantering blir särskilt viktigt när regelverk såsom EU:s cyberresiliensförordnings krav på rapportering träder i kraft den 11 september 2026. Systemet för sårbarhetshantering kan komma att behöva utvecklas mycket snabbt för att följa den tekniska utvecklingen på området och då behövs ett agilt hanterande av Enisa. Förslaget att Enisa bör upprätthålla en europeisk databas med kända utnyttjade sårbarheter (Known Exploited Vulnerabilities - KEV) välkomnas.

FRA välkomnar en utveckling av det europeiska ramverket för cybersäkerhetscertifiering. Syftet med cybersäkerhetscertifiering är bland annat att verksamhetsutövare ska kunna visa efterlevnad av de krav på säkerhetsåtgärder som uppställs i NIS 2-direktivet. Ramverket för cybersäkerhetscertifiering kan därför användas av föreskrivande myndigheter, såsom FRA och Post- och telestyrelsen, inom ramen för genomförande av säkerhetsåtgärder enligt cybersäkerhetslagen (2025:1506) eller att dessa anges i allmänna råd. Förslaget om cybersäkerhetscertifiering kan även, om det utformas ändamålsenligt, vara ett ytterligare stöd för att få organisationer att lyfta sig till den grundläggande nivån av cybersäkerhetsskydd som krävs utifrån deras respektive riskexponering. Det skulle även underlätta för tillsynen av sådana verksamhetsutövare och sätta fokus på faktiska åtgärder för att höja skyddsnivån. Detta går även ihop med möjligheten att certifiera utlokaliserade säkerhetstjänster (MSS). Det finns kopplingar mellan detta och det arbetet som genomförs i Sverige av ett antal myndigheter inom ramen för aktiviteter i handlingsplanen för den svenska nationella cybersäkerhetsstrategin.

Föreslagna ändringar i NIS 2-direktivet (EU 2022/2555)

FRA välkomnar förslaget om utökade rapporteringskrav i fråga om utpressningsangrepp för att öka förståelsen kring denna angreppsmetod. Hotaktörernas utvecklade och skiftande tillvägagångssätt vid utpressningsattacker kan komma att kräva en mer neutral utformning av bestämmelsen för att säkerställa att den behåller sin relevans. I det fortsatta nationella lagstiftningsarbetet bör det tydliggöras hur mottagna uppgifter kring en utpressningsattack överlämnas av den nationella CSIRT-enheten till en brottsutredande myndighet.

När kommissionen antar en genomförandeakt ska kommissionen bedöma behovet av en sådan akt för att förbättra den inre marknadens funktion enligt artikel 21.5. Artikel 21.5 knyts till artikel 5, vilken reglerar direktivets minimiharmonisering. FRA konstaterar att förslaget hindrar ytterligare krav på nationell nivå inom de områden där genomförandeakter har antagits. Detta kan i sin tur komma att påverka handlingsutrymmet och djupet på de krav som FRA kan ställa inom ramen för myndighetens föreskriftsrätt enligt cybersäkerhetslagen och cybersäkerhetsförordningen (2025:1507).

FRA välkomnar förslag till stöd för harmonisering genom ensade riktlinjer från kommissionen av de frågeformulär som ställs till underleverantörer av viktiga och väsentliga verksamhetsutövare enligt cybersäkerhetslagen. Det får dock inte innebära att ytterligare rådgivning på nationell nivå försvåras.

Krav på nationella policies för migrering till postkvantkryptografi som en del av den nationella cybersäkerhetsstrategin, kan ses i ljuset av att det redan pågår arbete kring detta genom den vägkarta för postkvantkryptografi som utförs inom NIS samarbetsgrupp (NIS CG) och av medlemsstaterna. Även i Sverige pågår sådant arbetet genom NCSC och samverkande myndigheter. Förslaget välkomnas som en del av det arbete som redan utförs på området.

Förslagen rörande hantering av risk i IKT-leveranskedjor behöver utformas på ett sätt som möjliggör fortsatt fokus på tekniska risker i IKT-produkter och -tjänster. Hanteringen av icke-tekniska risker, såsom utländskt inflytande på en leverantör, behöver ske inom ramen för politiska överväganden. De nya verktygen som föreslås behöver balansera tekniska och icke-tekniska, strategiska krav. Detta för att möjliggöra hänsyn till nationella prioriteringar och hänsyn till nationella behöriga myndigheters uppdrag.

FRA välkomnar i stort ansatsen att förenkla regelverket och verka för större harmonisering i kravställning. Det får dock inte ske genom införande av nya regelbördor och administrativa processer. Det övergripande målet behöver vara cybersäkerhetsåtgärder som ger maximal skyddseffekt i de verksamheter som omfattas av regelverken.

I detta ärende har generaldirektören Björn Lyrvall beslutat. I den slutliga handläggningen har även avdelningschefen John Billow och enhetschefen Jessica Öhlund Andersson deltagit. Juristen Karin Adamsson har varit föredragande.

Försvarets radioanstalt

Björn Lyrvall

Karin Adamsson

Sändlista

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