Myndigheten för civilt försvar

Remissvar

Datum	Ärendenummer
2026-04-21	MCF 2026-01779
Ert datum	Er referens
Ange datum	Ange er referens

Enheten för nationell centersamverkan (CS-SC-NC)
Ida Sahlin
010-240 4250
Ida.Sahlin@mcf.se

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Betänkandet SOU 2025:115 Kompletterande bestämmelser till EU:s cyberresiliensförordning

Övergripande synpunkter

Myndigheten för civilt försvar stödjer utredningens inriktning och betonar vikten av tydlig kompletterande reglering för att främja en rättssäker implementering av cyberresiliensförordningen. Myndigheten för civilt försvar vill därtill belysa följande:

- Myndigheten för civilt försvar ställer sig positiv till utredningens förslag i kapitel 5–9 och tillstyrker särskilt utredningens förslag i kapitel 12.
- Bestämmelser kring sekretess för sårbarhets- och incidentrapportering är av stor vikt för att säkra förtroende och ökad informationsdelning mellan verksamhetsutövare och CSIRT-enhet. Därtill måste säkerställas att en sådan sekretess inte hindrar att åtgärder kan vidtas för att skydda samhällets funktionalitet, varför Myndigheten för civilt försvar delar utredningens förslag att införa en sekretessbrytande bestämmelse. Denna bestämmelse måste dock inkludera sårbarheter och incidenter såväl som cyberhot, i den mening som avses i EU:s legala definitioner.

Specifika synpunkter

Sekretess

Myndigheten för civilt försvar ser positivt på utredningens förslag om sekretesskydd för uppgifter i sårbarhets- och incidentrapporter, men vill betona vikten av att en sådan sekretess inte hindrar att åtgärder kan vidtas för att skydda samhällets funktionalitet. Uppdraget som CSIRT-enhet enligt artikel 11.3 i NIS2-direktivet föreskriver bl.a. att medlemsstaterna ska säkerställa att deras CSIRT-

enheter snabbt sprider information om sårbarheter och cyberhot för att skydda andra aktörer i samhället och det är därför viktig att denna möjlighet ges.

Det behöver säkerställas att sekretess inte hindrar att informationsdelning möjliggörs, framförallt vid sådana sårbarheter och cyberhot som är av den digniteten att de medför betydande cybersäkerhetsrisker i cyberresiliensförordningens mening. I vissa fall är det nödvändigt att göra sådana uppgifter tillgängliga för användare och ibland även allmänheten för att kunna genomföra en snabb och effektiv hantering av cybersäkerhetsriskerna. I de fall tillverkaren inte själv spridit nödvändig information behöver det finnas en möjlighet för CSIRT-enheten, även sett till NCSC:s uppgifter i övrigt, att skyndsamt säkerställa att berörda får ta del av nödvändiga uppgifter. Uppgifterna rör själva sårbarheten eller cyberhotet samt sådana korrigerade eller riskreducerande åtgärder som användare kan vidta.[1] Detta gäller i situationer där intresset av att uppgiften kommer till enskildas eller allmänhetens kännedom är större än det intresse som sekretessen ska skydda, såsom den enskilda tillverkarens risk för skada.

Mot bakgrund av detta resonemang är Myndigheten för civilt försvar positiv till tillägget i den sekretessbrytandebestämmelsen (18 e §) av art 14.8 och 17.2. Detta tillägg möjliggör informationsdelning till enskilda kring sårbarheter och incidenter, samt till allmänheten kring allvarliga incidenter. Myndigheten för civilt försvar önskar dock att även inkludera ”cyberhot” i denna sekretessbrytande bestämmelse. Tillägget av ”cyberhot” gör exempelvis att det blir möjligt att publikt informera om att en programvara har en inbyggd modul som en hotaktör har tvingat leverantören av programvaran att inkludera och som utför hotande aktivitet när programvaran körs. Detta skiljer sig ifrån sårbarheter i det avseendet att programvarans modul direkt kan utföra angrepp, istället för att det finns något inbyggt som möjliggör ett framtida angrepp.

Stöd till företag

Myndigheten för civilt försvar är enig med utredningens förslag gällande stöd till företag i kapitel 12. Utredningen framhåller att stödet till företag ska samordnas med nationella cybersäkerhetsaktörer vilket ger Myndigheten för civilt försvar en tydlig roll i stödsystemet. Myndigheten för civilt försvar i egenskap av NCC-SE, välkomnar utredningens förväntan att NCC-SE ska vara en del av helheten.

[1] Exempelvis har CSIRT-enheten följande uppgifter enligt NIS2-direktivet artikel 11, p. 3b: ”Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.”.

Myndigheten för civilt försvar välkomnar därtill utredningens förslag att ge Myndigheten för civilt försvar uppdraget att samordna statens stöd på området. Genom detta uppdrag ges myndigheten, i egenskap av NCC-SE, möjlighet att ytterligare bidra till ökad tydlighet i systemet.

Myndigheten för civilt försvar noterar dock att detta uppdrag kommer att flyttas till NCSC vid FRA från och med 1 juli 2026. Myndigheten för civilt försvar poängterar därför vikten av att de legala och finansiella förutsättningarna för att genomföra uppdraget ges direkt till NCSC vid FRA.

I detta ärende har överdirektör Anna Starbrink beslutat. Ida Sahlin har varit föredragande. I den slutliga handläggningen har också avdelningschefen Åke Holmgren, enhetschefen Johan Turell och sektionschefen Emma Söderberg deltagit.

Anna Starbrink

Ida Sahlin