Myndigheten för civilt försvar

Remissvar

Datum	Ärendenummer
2026-05-15	MCF 2026-05641
Ert datum	Er referens
2026-03-23	Fö2026/00576

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

Regeringskansliet
Försvarsdepartementet
111 52 Stockholm

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

Övergripande synpunkter

Myndigheten för civilt försvar är positiv till en revidering av cybersäkerhetsakten och NIS 2-direktivet då en kontinuerlig utveckling av existerande regelverk bidrar till främjande av en hög nivå av cybersäkerhet inom EU. Myndigheten för civilt försvar belyser därtill följande:

- Ransomware nämns uttryckligen i flera av de föreslagna artiklarna. Myndigheten för civilt försvar konstaterar dock att det finns flera typer av cyberkriminella aktiviteter som kan få allvarliga konsekvenser och det bör således finnas ytterligare aktiviteter värda att nämna.
- Myndigheten för civilt försvar noterar lagstiftarens höga ambition för ENISA:s roll och uppgifter. ENISA är en viktig aktör som bidrar till att stärka den europeiska cybersäkerheten och Myndigheten för civilt försvar är således positiv till en revidering av dess mandat.
- Den föreslagna regleringen lägger stort fokus på hotaktörer. Myndigheten för civilt försvar anser att ett tydligare all-riskperspektiv bör inkluderas då inte bara de handlingar som orsakas av illvilja bör omfattas.

Specifika synpunkter

Artikel 3–70

ENISA är en viktig aktör i arbetet för en stärkt europeisk cybersäkerhet och ska som en del av sitt arbete samverka med medlemsstaterna. Myndigheten för civilt försvar vill därtill framhålla vikten av att medlemsstaterna involveras i de fall då de själva berörs. I den föreslagna regleringens artikel 5.1 (c) ska kommissionen, å medlemsstaternas vägnar, kunna begära assistans från ENISA. En sådan förfrågan bör komma från medlemsstaterna själva.

ENISA ska enligt den föreslagna regleringens artikel 11.1 (f) regelbundet ta fram en fördjupad rapport om incidenter och cyberhot som ska delas med ett antal aktörer. Rapporten kan antas bidra till en ökad kunskap inom området vilket i sin tur främjar cybersäkerhetsarbetet. Myndigheten för civilt försvar är därför positiv till uppgiften, men menar att rapporten dessutom ska göras publik, om än en mindre detaljerad version av denna.

Myndigheten för civilt försvar framhåller därtill vikten av effektiv informationsdelning i syfte att främja en säker cyberkrishantering. I den föreslagna regleringens artikel 12, som behandlar tidiga varningar, omnämns CSIRT-enheten vilket anses vara positivt. Myndigheten för civilt försvar menar dock att även cyberkrishanteringsmyndigheterna bör nämnas då det är dessa som agerar på den givna informationen. Det är således av stor vikt, för att säkerställa att aktuella samhällsfunktioner upprätthålls, att dessa får informationen så fort som möjligt. Informationen bör därtill ges oberoende av huruvida verksamhetsutövaren efterfrågar den eller inte. Myndigheten för civilt försvar anser att det kan bidra till ökat förtroende bland verksamhetsutövare och allmänheten i stort om aktuell CSIRT-enhet parallellt med ENISA kan gå ut med informationen vid en tidig varning.

Myndigheten för civilt försvar stödjer särskilt kombinationen av den förslagna regleringens artikel 44.1 och artikel 44.6, som slår fast att ENISA:s arbetsprogram antas och ändras genom beslut av ENISA:s styrelse. Detta stärker ett mer självständigt och effektivt ENISA vilket anses bidra till ökad cybersäkerhet inom unionen.

Artikel 98–117

Myndigheten för civilt försvar är positiv till att det skapas en förmåga att värna om EU:s digitala suveränitet. Proceduren riskerar dock att, när det används, generera negativa konsekvenser för såväl samhällets funktionalitet som för medlemsstaternas ekonomier. Av denna anledning bör medlemsstaterna ges ökat

mandat att ha inflytande över när och hur instrumentet används. Myndigheten för civilt försvar ser det som godtagbart att EU-KOM har det största inflytande över att begränsa tillhandahållandet av produkter och tjänster från tredjeland. Däremot bör medlemsstaterna ha rådighet över verksamhetsutövare inom EU:s jurisdiktion.

Myndigheten för civilt försvar vill vidare understryka vikten av att det finns en samordnande myndighet med en helhetssyn avseende de genomförandeförordningar som antas i enlighet med artikel 103. En sådan myndighet bör med fördel vara densamma som deltar i arbetet med de säkerhetsriskbedömningar som ska genomföras enligt artikel 99. I samverkan med relevanta tillsynsmyndigheter bör den samordnande myndigheten ha mandat att, utifrån den övergripande inriktning som ges av EU-kommissionen, utforma hur genomförandeförordningarna ska implementeras hos verksamhetsutövare inom den egna medlemsstaten.

Myndigheten för civilt försvar bedömer att den procedur som beskrivs i den föreslagna regleringens artikel 98–117 kommer att negativt påverka verksamhetsutövare som berörs av sådana förbud som kommissionen ges mandat att driva igenom. Den föreslagna regleringen kan generera fall då en verksamhetsutövare som redan är aktiv på den inre marknaden och som andra verksamhetsutövare är beroende av, förvärvas av en utländsk aktör varpå verksamhetsutövaren till följd av förvärvet klassificeras som högriskleverantör. Den föreslagna regleringen innebär följaktligen att denna verksamhetsutövare begränsas på olika sätt, vilket förväntas bli kostsamt och komplicerat för de verksamhetsutövare som är beroende av denna vilket i sin tur kan påverka samhällets funktionalitet. Myndigheten för civilt försvar anser, för att begränsa negativ inverkan på samhället, att denna typ av förvärv blockeras från början, snarare än att det genomförs och att verksamhetsutövaren därefter klassificeras som en högriskleverantör. Myndigheten poängterar därför vikten av att denna reglering ingår i ett samlat ramverk som inkluderar regelverket med koppling till utländska direktinvesteringar. Om förvärvet inte blockeras är det viktigt att verksamhetsutövarna ges tillräckligt med tid och resurser att anpassa sin verksamhet till att frångå beroendet av högriskleverantören.

Myndigheten för civilt försvar konstaterar att de tidsramar som följer av den föreslagna regleringens artikel 99.2 för när säkerhetsriskbedömningar ska framtas är snäva. Myndigheten noterar även att tidsramen löper från och med att en sådan efterfrågas och inte när den beslutats vilket minskar tiden ytterligare. Detta riskerar i sin tur att leda till svagt underbyggda analyser vilket i förlängningen skapar en risk för felriktade åtgärder. För att slutförda riskbedömningar ska kunna nyttjas

adekvat i enlighet med artikel 101, behöver arbetet genomföras inom rimliga tidsramar. Myndigheten för civilt försvar anser därför att tidsramen bör förlängas. En förlängd tidsram är dessutom av stor vikt för att säkerställa meningsfull involvering från medlemsstaternas sida.

Gällande säkerhetsriskbedömningar, i den föreslagna regleringens artikel 99, framhåller Myndigheten för civilt försvar vikten av att medlemsstater, via NIS Samarbetsgruppen, involveras på ett meningsfullt sätt vid framtagandet av säkerhetsriskbedömningar. Detta med hänsyn till att analyserna kan leda till slutsatser som i sin tur motiverar vissa handelspolitiska åtgärder och som därav är av stort intresse för medlemsstaterna. Kommissionen bör således inte utföra egna säkerhetsriskbedömningar utan involvering av medlemsstaterna.

Myndigheten för civilt försvar noterar därtill flera skrivningar om säkerhetsriskbedömningar som inte tydliggör att det rör sig om säkerhetsriskbedömningar av digitala leveranskedjor. Sådana skrivningar medför en risk för bedrivandet av riskbedömningar som fokuserar på digitala produkter eller tjänster, snarare än de leveranskedjor som möjliggör leveransen av den digitala produkten eller tjänsten.

Komplexiteten hos de leveranskedjor som möjliggör leveransen av digitala produkter och tjänster, innebär att det finns få digitala produkter som helt saknar komponenter, eller delkomponenter, med ursprung från en jurisdiktion som kan komma att betraktas som högrisk. Myndigheten för civilt försvar vill därför uppmärksamma de implikationer som förslaget kan leda till i de fall då alternativ till leverantörer som finns inom jurisdiktioner som klassificerats som högrisk är begränsade eller saknas helt. I sådana fall bör risken som orsakas av högriskleverantören vägas mot de konsekvenser som uppstår om en digital produkt eller tjänst inte kan nyttjas överhuvudtaget.

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