SVENSKT NÄRINGSLIV

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
Felix Nolte

Vår referens/dnr:
2026-71

Er referens/dnr:
Fö2026/00576

2026-05-12

Remissvar

Remittering av 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

Svenskt Näringsliv välkomnar målet att stärka EU:s cybersäkerhet och minska fragmentering på den inre marknaden. Tyvärr tar inte Europeiska kommissionen tillfället i akt att betydligt underlätta regelefterlevnaden och effektivisera den komplexa uppsättningen regler för cybersäkerhet som antagits på senare år. Reglerna som styr cybersäkerhet behöver vara så effektiva som möjligt och proportionerligt begränsa den kostsamma regulatoriska bördan.

Övergripande synpunkter

- Behov av regelförenkling inom hela cybersäkerhetsområdet
- Tydlig lagstiftning; undvik delegerade- och genomförandeakter
- Starkt stöd för Enisa, men den ska inte bli en operativ supermyndighet
- Single Entry Point (SEP); en efterfrågad förenkling för all incidentrapportering
- Frivillig certifiering, ”presumption of conformity” och marknadsdriven standardisering
- Vikten av pålitliga IKT-leveranskedjor och digital kapacitet centralt för konkurrenskraften

Synpunkter

Regelförenkling efterfrågas av näringslivet

CSA2 behöver förändras i syfte att minska den administrativa bördan som på senare år blivit mycket omfattande inom cybersäkerhetsområdet med NIS2-direktivet, direktivet om kritiska enheters resiliens (CER), Cyber Resilience Act (CRA), RED-DA 2022/30, Cyber Solidarity Act, 5G Cybersecurity Toolbox (5G Toolbox) och Digital Operational Resilience Act (Dora). Särskild vikt behöver läggas vid att utforma reglerna riskbaserat, proportionerligt och sektorsanpassat samt

att undvika överlappande krav med till exempel NIS2, CRA och Dora. Processer måste utformas förutsebart och övergångsperioder bli realistiska och sektorsanpassade.

Lagstiftningsprocessen

Svenskt Näringsliv är en stark förespråkare för den vanliga lagstiftningsprocessen som möjliggör meningsfullt och transparent intressentengagemang. Dessutom är det betydligt enklare för företag att klara regelefterlevnaden med tydliga och förutsägbara materiella krav i lagstiftningen. Därför förordar vi att CSA2-kraven regleras direkt i CSA2 baserat på obligatoriska konsekvensbedömningar och transparent intressentengagemang, snarare än genom genomförandeakter.

Om delegerade eller genomförandeakter används bör de ha ett tydligt avgränsat omfång och de måste präglas av transparens, åtföljas av gedigna konsekvensanalyser och arbetet med dem måste ge berörda aktörer möjlighet till insyn och verklig samverkan.

Enisa: starkt stöd – men ska inte bli en operativ supermyndighet

Enisas verksamhet är viktig för att öka medvetenheten om cybersäkerhet för att stärka Europas cybermotståndskraft.

Enisa ska vara ett tekniskt och stödjande expertorgan, utan dubbelarbete med nationella myndigheter och utan att utvecklas till ett operativt tillsyns- och beslutsorgan gentemot företag. Om nya funktioner införs (t.ex. ransomware-stödcenter, CSIRT-kopplingar, avgiftsbelagda verktyg) kan det driva Enisa i en mer operativ riktning. Det är mycket viktigt med tydliga mandatgränser.

Svenskt Näringsliv välkomnar artikel 13 om att Enisa i samarbete med Europol och CSIRT eller andra behöriga myndigheter ska inrätta en helpdesk och dela information om cyberhot och incidentlandskapet. Enisa ska ge råd till företag och tillhandahålla hotbedömningar.
Enisas budget bör stå i proportion till arbetsuppgifterna med att bidra till harmonisering och cybersäkerhet genom rådgivning till medlemsstater och näringslivet.

Single Entry Point (SEP): en väg in, men inte central datalagring

Vad gäller incidentrapportering förordar Svenskt Näringsliv att all sådan rapportering samordnas genom en-väg-in (Single Entry Point) på det sätt som är föreslaget i Digital Omnibus, men till nationella system utan att Enisa centralt lagrar incidentdata. Vi förespråkar en modell där företagen rapporterar en gång till en nationell CSIRT som har ansvar att föra informationen vidare till Enisa. Skulle inte det förslaget vinna gehör bör en väg in för incidentrapportering samordnas med framför allt Cyber Resiliens Act (CRA) för att förhindra överlappande skyldigheter och byråkrati.

Förslaget (i samband med Digital Omnibus) att Enisa kan upprätta en Single Information Point (SIP) är positiv för att säkerställa harmonisering.

Förenkling på riktigt: frivillig certifiering, ”presumption of conformity” samt standardisering på rätt sätt

Certifiering ska förbli frivillig och fungera som förenklingsverktyg, bland annat genom antagande om överensstämmelse (presumption of conformity). Konstruktioner som gör certifiering ”obligatorisk i praktiken” via upphandling eller indirekta marknadskrav utan konsekvensanalys måste undvikas.

De föreslagna artiklarna 46 och 47 innebär ytterligare ekonomisk börda och osäkerhet för företag. Dessa avgifter bör tas bort. Cybersäkerhetscertifiering tjänar ett viktigt politiskt mål och bör finansieras genom offentliga budgetar snarare än att påföra industrin ytterligare kostnader. Standarder ska vara marknadsdrivna och tas fram på sedvanligt sätt i etablerade standardiseringsprocesser. SN är därför emot att Enisa ges i uppdrag att ”skapa standarder” eller kringgå etablerad internationell/europeisk standardisering. Enisa ska inte ges rätt att skriva tekniska specifikationer, artikel 77.

Riskbaserad flexibilitet kring självbedömning (self-assessment) bör gälla både för låg- och medelriskprodukter/tjänster för att inte onödigt begränsa innovation.
Om ECCF genomförs bör det endast tillämpas på icke-produktkategorier, dvs. tjänster, som inte omfattas av CRA, förbli helt frivilligt och utgå från befintliga standarder.

Pålitliga IKT-leveranskedjor och digital kapacitet

Säkra och pålitliga IKT-leveranskedjor är avgörande både för att viktiga och kritiska enheter ska fungera korrekt och för samhället som helhet. Förslaget innehåller legitima intressen såsom behov av EU-harmonisering i hantering av icke-tekniska risker (jfr fragmenterad 5G-toolbox-genomförande). Parallellt med förslagen måste dock EU möjliggöra digitala kapacitet genom regler som stärker EU-baserad innovation och utveckling, samtidigt som tillgången till banbrytande global teknik värnas.

Eftersom många europeiska företag också är etablerade i tredjeländer bör definitionen av högriskleverantörer begränsas till sådana enheter som kontrolleras av ett tredjeland eller av en medborgare i ett sådant tredjeland.

Svenskt Näringsliv föreslår ändring i artikel 2 (39):
‘high-risk supplier’ means either of the following:
(a) an entity ***controlled by*** *a third country posing cybersecurity concerns designated in accordance with Article 100, or* ***by an entity with its registered head office*** *in such third country, or by a national of such third country;*
(b) an entity designated in accordance with Article 103(7) and entities controlled by that

Kriterier och processer för att hantera icke-tekniska risker måste vara effektiva, men inte på bekostnad av ingående konsekvensanalyser, proportionalitetsbedömningar, transparens och realistiska övergångsperioder anpassade för olika sektorer.
Innan någon åtgärd som innebär intrång i äganderätten genomförs måste den noga utredas och endast komma i fråga om det är uppenbar och betydande risk för en entitets eller infrastrukturs motståndskraft.

Åtgärdsdrabbade företag hamnar i ett konkurrensmässigt underläge och ska därför få ersättning av medlemsstaterna eller EU för att täcka de offentligt motiverade kostnaderna. För NIS2, Annex II-företag, skulle det vara proportionerligt att kraven är begränsade till framåtblickande och riskbaserade ledningsåtgärder.

SVENSKT NÄRINGSLIV

Göran Grén Carolina Brånby