Teknikföretagen

REMISSVAR
2026-05-18

Försvarsdepartementet

Via e-post: fo.remissvar@regeringskansliet.se
Kopia:
fo.ech.remissvar@regeringskansliet.se
dnr: Fö2026/00576

# Remiss av Europeiska kommissionens cybersäkerhetspaket med förlag om ändringar i cybersäkerhetsakten mm, KOM (2026)11,13

Teknikföretagens drygt 4 500 medlemsföretag står för en tredjedel av Sveriges export och över en miljon jobb. Vår uppgift är att stärka våra medlemmars konkurrenskraft och driva den hållbara utvecklingen framåt. Tillsammans med företag över hela landet formar vi teknikbranschens framtid – för vi är tekniksverige.

Teknikföretagen välkomnar EU-kommissionens ambition att stärka EU:s cybersäkerhet och minska fragmenteringen på den inre marknaden då vi alla, i stor utsträckning, är sammankopplade och beroende av varandra. Vår utgångspunkt är att EU:s cyberregelverk behöver vara effektivt och sammanhållet, men också vara tydligt riskbaserade, proportionerliga och rättssäkra. De får heller inte skapa överlappande eller motstridiga krav i förhållande till befintlig lagstiftning på nationell eller EU-nivå.

**Övergripande synpunkter**

- Regelverket bör utformas riskbaserat och proportionerligt, med tydliga definitioner, förutsebara processer och realistiska övergångsperioder.
- Förslagen bör minska – inte öka – den samlade administrativa bördan och undvika överlapp med bl.a. NIS2, CRA och DORA.
- De materiella reglerna bör i så hög grad som möjligt framgå av lagstiftningen. 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.
- Åtgärder som kan leda till restriktioner i IKT-leveranskedjor behöver bygga på objektiva kriterier och en ordning som säkerställer rättssäkerhet och likabehandling.
- ENISA bör fortsatt vara ett tekniskt och stödjande expertorgan. Nya uppgifter bör utformas så att dubbelarbete med nationella myndigheter undviks och att ENISA inte utvecklas till ett operativt tillsyns- eller beslutsorgan.

**Ramverk för säkerhet i IKT-leveranskedjor**

Teknikföretagen delar regeringens preliminära bedömning att ett EU-gemensamt ramverk kan bidra till ökad harmonisering och framdrift i EU:s samlade säkerhetsarbete. Samtidigt är det avgörande att ramverket utformas balanserat och rättssäkert, med tydliga kriterier och processer som ger förutsebarhet för berörda aktörer.

Bedömningar av icke-tekniska risker bör vila på objektiva, på förhand fastställda och kommunicerade kriterier och en transparent process. Förslaget bör tydligt ange vilka typer av underlag som kan beaktas och hur olika riskfaktorer vägs.

Åtgärder bör vara proportionerliga i förhållande till identifierad risk och ta hänsyn till konsekvenser för berörda verksamheter, resiliens och investeringar. Restriktioner bör vara riktade och, där det är relevant, avgränsade utifrån entiteters storlek och hur kritiska de är.

Innan beslut om långtgående åtgärder (t.ex. stopp för nya investeringar eller krav på utfasning) tas behöver det finnas krav på strukturerad konsekvensbedömning, inklusive tillgång, kostnader, tidslinjer och påverkan på driftsäkerhet.

Berörda leverantörer måste garanteras rätt till försvar och möjlighet att bemöta underlag innan eventuella utpekanden eller restriktioner beslutas.

Om utfasning av installerad utrustning aktualiseras måste tidsfrister vara realistiska och baserade på marknadens kapacitet, för att undvika oavsiktliga risker för kontinuitet och säkerhet.

**Cybersäkerhetscertifiering**

Certifiering bör fortsatt vara frivillig och användas som ett förenklingsverktyg. EU bör undvika konstruktioner som gör certifiering ”obligatorisk i praktiken” via upphandling eller indirekta marknadskrav utan tydlig konsekvensanalys.

Teknikföretagen ser positivt på att certifieringsresultat kan bidra till presumtion om överensstämmelse, förutsatt att det faktiskt minskar dubbelarbete mellan regelverk och inte adderar administrativ börda eller kostnader.

Standarder bör fortsatt tas fram inom etablerade europeiska och internationella standardiseringsprocesser. ENISA:s roll bör vara stödjande och teknisk – inte att utforma egna tekniska specifikationer som kringgår ordinarie processer.

**ENISA:s mandat, styrning och finansiering**

Teknikföretagen välkomnar en stärkt roll för ENISA som EU:s tekniska expertorgan, men betonar behovet av tydliga mandatgränser så att ENISA inte får en operativ roll som duplicerar nationella myndigheters uppdrag eller skapar parallella processer gentemot företag.

Nya uppgifter bör dimensioneras och prioriteras så att de ger konkret nytta (t.ex. stöd, samordning och kapacitetsuppbyggnad) utan att leda till ökad rapporteringsbörda eller otydligt ansvar mellan EU- och nationell nivå.

Eventuella avgiftsmöjligheter bör analyseras noga. Avgifter eller betalväggar får inte skapa trösklar för användning av gemensamma verktyg som är centrala för EU:s cybersäkerhetsförmåga, särskilt för mindre aktörer.

**NIS2 – Gemensam incidentrapportering**

Teknikföretagen stödjer ambitionen om en en-väg-in för incidentrapportering, men den bör utformas som en gemensam ingång till nationella rapporteringssystem och bygga på interoperabilitet, så att företag kan rapportera ”en gång” utan duplicering. Här bör erfarenhet kunna dras av den redan inrättade strukturen kring incidentrapportering under cyberresiliensakten.

Modellen bör undvika parallella rapporteringsspår till olika myndigheter och säkerställa harmonisering och ensning i fråga om i definitioner, mallar och tidsfrister i förhållande till angränsande regelverk.

För Teknikföretagen

Maria Rosendahl
Näringspolitisk chef

My Bergdahl
Näringspolitisk expert