TechSverige

Datum
2026-05-18

Vår referens
RL

Finansdepartementet
fo.remissvar@regeringskansliet.se

Kopia till
fo.ech.remissvar@regeringskansliet.se

Remissvar avseende 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

TechSverige har givits möjlighet att avge remissvar avseende Europeiska kommissionens cybersäkerhetspaket.

TechSverige är den ledande bransch- och arbetsgivarorganisation som samlar kärnan av svensk tech – företag som utvecklar, levererar och möjliggör tech i Sverige och som verkar på den svenska, europeiska och globala marknaden. Vi företräder cirka 1 400 företag som sammantaget har närmare 100 000 medarbetare i Sverige.

TechSveriges uppdrag är att tillsammans med våra medlemmar skapa goda villkor för en konkurrenskraftig och ansvarstagande techbransch i Sverige.

Sammanfattning

TechSverige välkomnar ambitionen att på EU-nivå stärka säkerheten i kritiska sektorers digitala leveranskedjor, men vill betona att regelverket behöver säkerställa att det är förutsebart, proportionerligt och genomförbart i praktiken. Förslag om högriskleverantörer och utfasning kan annars få påtagliga konsekvenser för investeringar och leveranskedjor i digital infrastruktur, med följdeffekter i stora delar av ekonomin och samhället som är beroende av denna.

Särskilt viktigt är att åtgärder utformas med hänsyn till investeringscykler och att mer ingripande åtgärder används som en sista åtgärd. I annat fall finns en risk att investeringar i digital infrastruktur trängs undan, vilket kan påverka Sveriges position som en ledande digital ekonomi.

TechSverige understryker även behovet av förenkling, tydlig rollfördelning mellan EU och nationell nivå samt att certifiering och rapporteringskrav utformas så att de minskar, och inte ökar, den samlade regelbördan.

Förenkling och samordning av regelverk

Regeringen har i flera sammanhang betonat vikten av förenkling och minskade regelbördor för svenska företag, som en central del av arbetet med att stärka konkurrenskraft och investeringar. Mot denna bakgrund är det centralt att nya initiativ på EU-nivå utformas så att de bidrar till minskad komplexitet i praktiken.

Storgatan 19
114 82 Stockholm

+46 8 665 36 60

802410-1936
techsverige.se

Cybersäkerhetspaketet kommer att verka parallellt med andra regelverk, såsom NIS2, CRA och Dora. Om dessa inte samordnas riskerar de tillsammans att skapa ett komplext system där resurser i allt större utsträckning går till att hantera regelkrav snarare än att stärka säkerheten i praktiken. Det är därför särskilt viktigt att cybersäkerhetspaketet utformas i linje med befintliga regelverk. I annat fall finns en risk att det leder till ökade administrativa bördor, överlapp och dubbelarbete.

Säkerhetsfrågor präglas samtidigt av starka nationella intressen, vilket innebär att EU-regelverk ofta kompletteras med nationella åtgärder. Det är därför viktigt att den samlade regleringen utformas så att risken för överlapp och motstridiga krav begränsas.

För att bidra till förenkling är det vidare viktigt att certifiering utformas som ett frivilligt verktyg och inte i praktiken utvecklas till ett brett eller generellt krav, exempelvis genom att konsekvent efterfrågas i upphandlingar oavsett relevans eller proportionalitet. För aktörer som väljer att använda certifiering bör denna i möjligaste mån kunna ersätta, snarare än komplettera, andra krav på dokumentation och efterlevnadsbedömningar. Eventuella avgiftsmodeller bör utformas så att de inte skapar ytterligare trösklar, särskilt för mindre aktörer.

Högriskleverantörer, leveranskedjor och investeringsperspektiv

En central del av förslaget rör hanteringen av icke-tekniska risker i kritiska IKT-leveranskedjor och möjligheten att vidta åtgärder mot högriskleverantörer på ett harmoniserat sätt inom EU. Förslaget kan därmed få konsekvenser för aktörer som tillhandahåller digital infrastruktur, liksom för verksamheter som är beroende av denna.

TechSverige ser behovet av att hantera sådana risker, men vill betona att åtgärder med långtgående konsekvenser för investeringar och drift måste vila på en grundlig behovsanalys och utformas i nära dialog med berörda aktörer. I sammanhanget krävs också en analys av riskerna kopplade till minskade möjligheter till diversifiering bland IKT-leverantörer. Detta inkluderar tillgången till alternativa leverantörer och de potentiella konsekvenserna för verksamheter som är beroende av dessa leveranskedjor.

Vidare krävs tydliga, transparenta och riskbaserade kriterier. Det behöver klargöras vilket underlag som krävs för beslut, hur olika riskfaktorer vägs samman och hur åtgärder avgränsas. Utan sådan tydlighet riskerar regelverket att skapa osäkerhet kring investeringar och leverantörsval.

Samtidigt väcker den föreslagna utformningen av detta ramverk frågor om proportionalitet, rättssäkerhet och genomförbarhet, vilket talar för behov av fortsatt analys och bearbetning. Det är i detta sammanhang viktigt att mer ingripande åtgärder, såsom förbud eller krav på utfasning, används som en sista åtgärd när andra riskreducerande åtgärder inte är tillräckliga.

Investeringsperspektivet är i detta sammanhang avgörande. Digital infrastruktur byggs och moderniseras över långa tidshorisonter. Den i förslaget angivna tidsramen om 36 månader för utfasning saknar i många fall koppling till dessa investeringscykler och riskerar att bli svår att genomföra i praktiken.

Sverige har erfarenhet av liknande åtgärder genom villkor kopplade till utbyggnaden av 5G-nät. Erfarenheter visar att åtgärder i leveranskedjan kan påverka såväl tidsplaner som investerings- och kostnadsförutsättningar. Sammantaget understryker detta vikten av realistiska tidsramar, tydliga och förutsebara förutsättningar samt en nära dialog med berörda aktörer i utformningen av regelverket.

Mot denna bakgrund anser TechSverige att övergångsperioder bör utformas med hänsyn till investeringscykler i de sektorer som omfattas av regelverket, tillgångars livslängd och praktisk genomförbarhet. Det är också viktigt att tydligt analysera och beakta de ekonomiska konsekvenserna av föreslagna åtgärder. Särskilt viktigt är att det klargörs hur effekter på redan genomförda investeringar ska hanteras för att upprätthålla ett förutsägbart och attraktivt investeringsklimat.

Utan sådana avvägningar finns en risk att omfattande och oförutsägbara krav på utfasning tränger undan andra investeringar som är nödvändiga för att utveckla och stärka Sveriges digitala infrastruktur och därmed även den långsiktiga säkerheten och motståndskraften. Detta kan i förlängningen påverka Sveriges position som ett ledande land inom digital infrastruktur och nätutbyggnad.

Styrning, rapportering och roller

För att regelverket ska fungera i praktiken är Enisas roll viktig. TechSverige ser positivt på en stark europeisk samordning, men anser samtidigt att myndighetens roll bör ha ett tydligt fokus på vägledning, samordning och utveckling av gemensamma arbetssätt som bidrar till förenkling. Ett mer operativt ansvar riskerar att skapa överlappning med nationella myndigheter och därmed ökad komplexitet för berörda aktörer.

Förslaget om en gemensam ingång för incidentrapportering har potential att bidra till förenkling, men endast om det utformas på ett sätt som fungerar i praktiken. För att uppnå detta är det viktigt att trösklar och krav för incidentrapportering harmoniseras, så att företag inte möter olika bedömningar i olika medlemsstater. Det bör också säkerställas att företag inte behöver rapportera samma incident till flera instanser, utan att en verklig ”once-only”-princip tillämpas.

TechSverige vill även lyfta behovet av att hanteringen av känslig information säkerställs. I många fall rör det sig om uppgifter som omfattas av nationella säkerhetsintressen. Det bör därför övervägas en modell där rapportering i första hand sker till nationell myndighet, som därefter avgör vilken information som kan delas vidare på EU-nivå.

Avslutande synpunkter

Avslutningsvis vill TechSverige betona vikten av att hitta en fungerande balans mellan harmonisering och nationellt handlingsutrymme. Säkerhetsfrågor kommer även framöver att präglas av starka nationella intressen, och det är därför sannolikt att medlemsstater i vissa fall kommer att vidta ytterligare åtgärder. EU-regler bör i detta sammanhang ge en gemensam utgångspunkt som skapar förutsägbarhet för företag som verkar över gränserna. Samtidigt är det viktigt att utformningen av regelverket tar höjd för denna dynamik, så att den samlade effekten inte blir ökad komplexitet, överlappning eller motstridiga krav. Det avgörande är att marknaden inte hamnar i kläm i denna balans.

TechSverige vill även betona vikten av att industrins perspektiv tas till vara i den fortsatta utvecklingen av regelverket. De aktörer som berörs besitter avgörande kunskap om tekniska förutsättningar, marknadsdynamik och genomförbarhet. Ett strukturerat och meningsfullt deltagande från industrin är därför en förutsättning för att säkerställa ett regelverk som är effektivt, genomförbart och bidrar till såväl säkerhet som konkurrenskraft.

TechSverige ser fram emot den fortsatta dialogen i frågan.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Robert Liljeström
näringspolitisk expert