Försvarsdepartementet

Datum	Diarienummer
2026-05-12	Ä 2026-742

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 (Fö2026/00576)

Tillväxtverket arbetar för konkurrenskraftiga företag och hållbar utveckling i alla delar av Sverige. Det gör myndigheten genom att skapa förutsättningar för stärkt konkurrenskraft, ökad innovation, stärkt omställningsförmåga och en hållbar utveckling i hela landet. Myndigheten arbetar inom tre politikområden - den regionala utvecklingspolitiken, landsbygdspolitiken och näringspolitiken - som är ömsesidigt förstärkande.

Remissvaret är skrivet utifrån dessa utgångspunkter.

Sammanfattning

- En tydligare roll för ENISA beträffande vägledning om NIS 2-tillämpning minskar risken för osäkerhet kring regelverket och ger bättre förutsägbarhet i tillämpningen både för myndigheter och företag.
- Effektivare och tydligare certifieringsprocess ger kortare handläggningstider för företagen. Förslaget om certifiering ger färre parallella och överlappande nationella krav och minskar behovet av tillsyn hos certifierade företag, liksom kraven på rapportering. Inträdeskostnaderna för mindre företag är däremot höga och det kan inte uteslutas att kostnaderna påverkar de mindre företagen utan tillräckliga rutiner för cybersäkerhet på ett för verksamheten avgörande sätt.
- Med ändringar i NIS 2 kan företag behöva byta, begränsa eller fasa ut vissa leverantörer. Det kan inte uteslutas att särskilt små och medelstora företag

påverkas på ett betydande sätt. Åtgärder för stärkt cybersäkerhet och att förebygga incidenter kan dock på sikt medföra besparingar för företagen.

- Förtydligandet om vilka entiteter som ska omfattas av NIS 2 medför en tydligare koppling till faktiskt risk, och till verksamhetens art och storlek i stället för branschtillhörighet. Detta torde minska risken för att företag omfattas i onödan. För små och medelstora företag, och företag som indirekt påverkas genom kundkrav, upphandlingar och leverantörskedjor kan detta dock medföra kostnader för nya processer, kompetenshöjning och externa tjänster.

- Tydligare regler för huvudsaklig etableringsland, är positivt för företag med verksamhet i flera medlemsstater. Tydligare tillsynsansvar minskar risken för dubbelrapportering och parallella tillsynssystem, vilket leder till minskade administrativa kostnader.

- Närmare koppling mellan krav i NIS 2-direktivet och cybersäkerhetsakten, och att riskhanteringsåtgärder i större utsträckning ska kunna uppfyllas genom EU-certifiering, ger mer harmoniserade regler och krav, som i sin tur leder till jämnare konkurrensvillkor och minskade kostnader för exempelvis juridisk rådgivning och anpassning till olika nationella regelkrav för företag med verksamhet i flera medlemsstater.

- Tydligare definition av vad som utgör en betydande incident underlättar för både myndigheteter i tillämpning och vägledning och för företag när resurser inte behöver bindas till lågrisk-incidenter. Det torde även inverka positivt på konkurrensvillkoren. Kostnader för incidentrapporteringen och vidtagande av säkerhetsåtgärder bedöms dock vara betydande, särskilt för de företag som tidigare inte omfattats av regleringen.

- Bättre samordning mellan rapporteringskrav i NIS 2, GDPR och sektorsspecifik EU-lagstiftning leder till minskad överrapportering och därmed minskade administrativa kostnader för företagen, liksom utjämnade konkurrensvillkor jämfört med tredjelandsaktörer.

- Nationella och regionala åtgärder bör vidtas för att mildra effekterna för små och mikro-företag. Genomförandet i svensk rätt (NIS 2-ändringarna) bör utformas så att de underlättar regelefterlevnaden i så hög utsträckning som möjligt. Myndigheterna bör tillhandahålla tydligt stöd till företagen i form av vägledningar, tolkningar, mallar och systemstöd med mera.

- Nationella föreskrifter, vägledning och stöd behöver utvärderas och effekterna dokumenteras. Sådan utvärdering kan med fördel remitteras till Regelrådet för synpunkter.

Kommentarer till förordningsförslaget

Stärkt och tydligare mandat för ENISA – särskilt stödbehov för små och medelstora företag

Tillväxtverket ställer sig positivt till att ENISAS roll förtydligas när det gäller policyutveckling, kunskapsutbyggnad och kunskapsspridning och stödjande verksamhet kring standardisering och övningar. Vi bedömer att detta får särskilt stor betydelse för små och medelstora företag. En tydligare roll när det gäller bland annat vägledning om NIS 2-tillämpning och, där exempelvis handböcker, mallar och bästa praxis tas fram, liksom metodstöd till tillsynsmyndigheter torde minska risken för

osäkerhet kring regelverk och ansvarsfördelning både för myndigheter och företag, och ge bättre förutsägbarhet i tillämpningen. Vi bedömer att detta är av särskild vikt för små och medelstora företag, då tillgången för dessa företag till praktisk, samlad och EU-harmoniserad vägledning kan vara avgörande, då många saknar egen juridisk och cybersäkerhetsrelaterad kompetens. Utifrån SMF-perspektivet är det därför centralt att ENISAs vägledning utformas som ett konkret stöd för genomförande, exempelvis genom bransch- och målgruppsanpassade exempel och mallar.

Reform av EU:s cybersäkerhetscertifiering – inträdeströsklar och risk för indirekt kravställning

Tillväxtverkets är positiv till att åtgärder föreslås för att effektivisera och förtydliga processerna så att handläggningstiderna kortas för företagen. Förslaget bidrar även till färre parallella och överlappande nationella krav. Vår bedömning är också att med förslaget om certifiering torde behovet av tillsyn till viss del minska hos certifierade företag, liksom kraven på rapportering.

Tillväxtverket delar bedömningen att effektivare och mer harmoniserade certifieringsprocesser på sikt kan innebära förenklingar och stärkt konkurrenskraft för företagen. Ur ett SMF-perspektiv behöver dock certifieringens praktiska effekter särskilt uppmärksammas. Certifiering riskerar i praktiken att bli ett affärsvillkor snarare än ett frivilligt verktyg, särskilt i leverantörskedjor till NIS 2-reglerade företag och vid offentlig upphandling. För små företag kan detta innebära höga initiala kostnader och komplexa processer som kan utgöra ett reellt hinder för marknadstillträde. För många SMF kan alternativ som självvärderingar fortsatt vara viktiga.

Förslaget medför positiva effekter för de företag som redan arbetar strukturerat med informationssäkerhet. På sikt kan det bli kostnadsbesparande även för små- och medelstora företag, även om inträdeströskeln är hög. Att högriskleverantörer kan nekas certifiering bidrar också till jämnare konkurrensvillkor. Det kan dock inte uteslutas att mindre leverantörer utan strukturerat arbete med cybersäkerhet kan riskera marknadsutträde, eller, för dem som önskar inträde, att inte kunna bära kostnaderna.

Nytt ramverk för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT) – tydliga indirekta effekter för små och medelstora företag

Tillväxtverket bedömer att förslaget medför att företag som är väsentliga eller viktiga entiteter enligt NIS 2 måste ta hänsyn till EU-identifierade leverantörskedjor i sin riskhantering och kan behöva byta, begränsa eller fasa ut vissa leverantörer. Företagen ges också mindre handlingsutrymme att själva avgöra vad som är acceptabel leverantörsrisk. Tillväxtverket anser att det är positivt i sig att företagen får hjälp att identifiera högriskleverantörer och nyckel-IKT-tillgångar. Men ser även att förslaget kan medföra att ansvar och risk förskjuts nedåt i värdekedjorna, då många små och medelstora företag verkar som underleverantörer inom kritiska sektorer och påverkas därmed av ökade krav på spårbarhet, dokumentation och leverantörskontroll, trots att de själva inte omfattas av NIS 2-direktivets tillämpningsområde. Detta riskerar att leda till en snedvriden konkurrens och till att mindre, lokala eller specialiserade leverantörer trängs undan. Samtidigt kan ramverket, rätt tillämpat och kombinerat med tydlig EU-samordning, bidra till ökad förutsägbarhet och mer likvärdiga konkurrensvillkor på den inre marknaden.

Förslaget kopplar IKT-leveranskedjor till certifiering, vilket innebär att certifiering kan bli praktiskt nödvändig för att få sälja till vissa kunder och företag kopplade till högriskleverantörer kan nekas certifiering. Certifieringskostnader är betungande för företag och framför allt för mindre företag som hittills inte arbetat systematiskt med cybersäkerheten. Förslaget bidrar till höga inträdeskostnader, men stärker på sikt konkurrenskraften för företag som verkar inom EU jämfört med aktörer från tredje land. Åtgärder för stärkt cybersäkerhet och att förebygga incidenter kan också på sikt medföra besparingar för företagen.

Kommissionens förslag till ändringar i NIS 2

Tillväxtverkets kommentarer

Vid genomförandet av NIS 2-direktivet fick medlemsstaterna stort utrymme för nationella val gällande krav på säkerhetsåtgärder, incidentrapportering, tillsyn och efterlevnadskontroll, vilket bidragit till fragmentering av den inre marknaden som inte varit önskvärd. Tillväxtverket anser att en mer harmoniserad tillsynsmodell minskar risken för olika nationella krav kopplat till bland annat tillsyn och därmed lägre oförutsedda kostnader och jämnare konkurrensvillkor.

Tillväxtverket instämmer i bedömningen att ändringarna i NIS 2, genom tydligare koppling till faktiskt risk samt verksamhetens art och storlek, kan minska risken för att företag omfattas i onödan. Samtidigt innebär utvidgningen och förtydligandena att fler företag än tidigare direkt kommer att omfattas av krav på riskhantering, incidentrapportering och styrning. För små och medelstora företag, liksom för företag som indirekt påverkas genom leverantörskedjor, kan detta innebära behov av nya processer, kompetenshöjning och externa tjänster.

Tillväxtverket delar bedömningen av att de förtydliganden som görs om gränsöverskridande verksamhet och behörig tillsyn medför att reglerna blir tydligare gällande huvudsaklig etableringsland, vilket är positivt för dessa företag. Att reglerna för tillsyn förtydligas medför vidare att ansvaret för tillsynen blir tydligare, vilket sannolikt minskar risken för dubbelrapportering och parallella system. Sammantaget torde detta leda till minskade administrativa kostnader.

Tillväxtverket kan konstatera att förslaget leder till en närmare koppling mellan krav i NIS 2-direktivet och cybersäkerhetsakten och att riskhanteringsåtgärder i större utsträckning ska kunna uppfyllas genom EU-certifiering. Tillväxtverket är positiv till mer harmoniserade regler och krav då det torde leda till jämnare konkurrensvillkor och minskade kostnader för exempelvis juridisk rådgivning och anpassning till olika nationella regelkrav för företag med verksamhet i flera medlemsstater. Vi ser dock en risk i försämrade konkurrensvillkor för mindre och specialiserade underleverantörer, vilket vi påtalar ovan. Certifiering är också förknippade med höga initiala kostnader, och särskilt betungande för de mindre företagen vilket redan anförts ovan.

Tillväxtverket konstaterar vidare att förslaget medför en tydligare definition av vad som utgör en betydande incident, vilket underlättar för både myndigheteter i tillämpning och vägledning och leder till minskade kostnader för företag när resurser inte behöver bindas till lågrisk-incidenter. Även detta torde inverka positivt på konkurrensvillkoren. Kostnader för incidentrapporteringen och vidtagande av säkerhetsåtgärder bedöms dock vara betydande, särskilt för de företag som tidigare inte omfattats av regleringen, men som med ändringen i NIS 2-direktivet nu kommer att omfattas. Förslaget medför vidare en bättre samordning mellan rapporteringskrav i NIS 2, GDPR och sektorsspecifik EU-lagstiftning, vilket torde leda till minskad överrapportering och därmed minskade administrativa kostnader för företagen, liksom utjämnade konkurrensvillkor jämfört med tredjelandsaktörer.

Många små och medelstora tillverkande företag, mindre importörer och distributörer har begränsad tillgång till juridisk och cybersäkerhetsrelaterad kompetens, samt en stark beroendeställning till större kunder och leverantörskedjor. I kombination med ökade krav på riskhantering, dokumentation och incidentberedskap innebär detta en påtaglig risk för att regelverken blir tillväxthämmande om de inte kombineras med riktat och företagsnära stöd. Detta gäller särskilt för små och mikro-företag som formellt inte omfattas av regleringen, men som i praktiken påverkas genom upphandlingar och avtalsvillkor. Vi ser därför ett behov av kompletterande nationella och regionala insatser med inriktning på bransch- och målgruppsanpassade utbildningar, vägledningar, mallar, checklistor och konkreta exempel. Tillgången till cybersäkerhetskompetens varierar mellan olika delar av landet och för många företag försvårar detta anpassningen. Regionalt förankrade stödinsatser är nödvändiga för att säkerställa att även företag utanför större tillväxt- och teknikmiljöer ges reella förutsättningar att anpassa sig till de nya kraven.

Tillväxtverket ser vidare ett behov av att nationella regler utformas så att de underlättar regelefterlevnaden i så hög utsträckning som möjligt. Expertmyndigheterna behöver bistå med tydligt stöd till företagen i form av vägledningar, tolkningar, mallar och systemstöd med mera.

Det finns behov av fortsatt analys av regelverkets effekter för berörda företag, särskilt för de små och medelstora. Nationella föreskrifter behöver därför utvärderas och dokumenteras med särskild betoning på företagseffekter. Sådan utvärdering kan med fördel remitteras till Regelrådet för synpunkter. Åtgärder i form av vägledning och olika stöd till företagen behöver också utvärderas.

Beslut i detta ärende har fattats av avdelningschef Anna Johansson.
Handläggare Annika LeBlanc har varit föredragande.

Anna Johansson

Annika LeBlanc