företagarna

Försvarsdepartementet
Avdelningen för försvarsunderrättelser,
Säkerhets- och cyberfrågor,
Enheten för cyber-och hybridfrågor

Stockholm	Vår referens	Dnr
2026-05-13	Jacob Ämtvall	Fö2026/00576

Remissyttrande

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

Företagarna välkomnar möjligheten att lämna synpunkter på 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.

Förslaget i korthet
Förslagen till ändringar i cybersäkerhetsakten KOM (2026) 11 och riktade ändringar i NIS 2-direktivet (KOM 2026) 13 syftar till att modernisera och stärka EU:s rättsliga ramverk för cybersäkerhet, förenkla efterlevnad och skapa ett mer sammanhållet skydd mot cyberhot. Förslagen till förändringar i cybersäkerhetsakten innebär huvudsakligen ett stärkt mandat för EU:s cybersäkerhetsbyrå Enisa, ett reformerat ramverk för cybersäkerhetscertifiering som syftar till att skapa snabbare processer, en ny certifieringsordning för NIS 2 och en förenklad styrning på EU nivå samt ett nytt ramverk för IKT-leveranskedjor för att hantera icke-tekniska risker i leveranskedjor för informations- och kommunikationsteknik (IKT).

Förslaget om riktade ändringar i NIS 2-direktivet KOM (2026) 13 syftar till att förenkla och förtydliga NIS 2 direktivet samt anpassa den till den nya cybersäkerhetsakten enligt ovan förslag. Förslagen innebär i huvudsak att nya verksamhetstyper inkluderas, i form av leverantörer av europeiska identitetsplånböcker och europeiska företagsplånböcker samt operatörer av undervattensinfrastruktur för dataöverföring (t.ex. fiberkablar till havs) och strategisk infrastruktur med *dual use* (civil och militär användning), ett nytt krav om rapportering av utpressningsangrepp (ransomware) för påverkade verksamheter som på begäran av behörig myndighet måste informera att de mottagit krav på lösensumma, stärkt tillsyn och införande av certifiering för efterlevnad.

Företagarnas inställning
Företagarna ser positivt på att cybersäkerhetsfrågan fortsatt prioriteras för att skapa ökad säkerhet och större motståndskraft. Samtidigt är det av yttersta vikt för små och medelstora företag att lagrum och riktlinjer är tydliga och inte skapar en oskälig administrativ börda eller oskäliga kostnader för företag som inte har förutsättningar att ha relevant expertis inom den egna organisationen. Företagarna välkomnar därför regeringens avsikt, så som den uttrycks i faktapromemorian (2025/26:FPM78), att verka för att reglerna i och med förestående förslag ska vara proportionerliga och att konsekvenserna av ramverket för IKT-leveranskedjor behöver analyseras noggrant.

I Företagarnas remissyttrande om SOU 2024:18 *Nya regler om cybersäkerhet*, som låg till grund för den cybersäkerhetslag som genomför NIS 2-direktivet i Sverige, framfördes i huvudsak synpunkter om en otillräcklig konsekvensanalys av vilka kostnader reglerna skulle medföra för företag, risk för oproportionerlig administrativ börda kopplat till anmälningsskyldighet och kraven på

riskhanteringsåtgärder, vikten av stöd till småföretag och att verksamhetsutövare enkelt ska kunna förstå hur man ska agera för att undvika sanktioner. [1]

I och med förestående förslags inriktning ser Företagarna en risk för att de farhågor som vi tidigare uttryckt kring SOU 2024:18 kvarstår och i hög grad riskerar att förvärras, bland annat genom att småföretag som tidigare varit undantagna från de mest betungande administrativa bördorna nu direkt eller indirekt ändå påverkas av de nya kraven. Ökad administrativ börda och kostnader kan uppstå till följd av det föreslagna ramverket för IKT-leverantörer, där småföretag i en leverantörskedja inte bara måste förhålla sig till sin kunds krav, utan också aktivt bevaka om deras egna underleverantörer (av mjukvara, hårdvara etc.) hamnar på en europeisk "högrisklista". Detta skulle kunna tvinga fram dyra och oplanerade byten av system. På motsvarande sätt kan småföretag i en leverantörskedja komma att omfattas av incidentrapporteringskravet indirekt, genom att deras större kunder omfattas av lagen och därmed måste säkra sin leverantörskedja. Företagarna är inte principiellt mot någon av de två ovan nämnda regelskärpningarna, men vi vill betona vikten av att utförlig konsekvensanalys av reglerna genomförs och lämpliga åtgärder vidtas för att stödja småföretag i de här frågorna. Småföretagare som inte har förutsättningar att anskaffa den teknik och kompetens som krävs för efterlevnad riskerar annars att drabbas oproportionerligt hårt. Av samma anledning och för att undvika onödig byråkrati ser Företagarna det som nödvändigt att incidentrapporteringssystemet organiseras med single entry point, d.v.s. en-väg-in till en nationell CSIRT.

Även om kraven på postkvantkryptering är framåtblickande vill Företagarna tydligt betona att de inte får utformas på ett sätt som blir kostnadsdrivande för de småföretag som indirekt påverkas via leverantörskedjan. Kostnader för regelefterlevnad måste täckas av intäkter i den reguljära verksamheten och långtgående regelkrav kan bli ekonomisk betungande för i synnerhet småföretag. Tydlighet, förutsebarhet, god framförhållning och dialoger som inkluderar småföretagare är därför av stor betydelse inför inrättandet av dessa krav och instruktioner måste ges till ansvariga myndigheter att arbeta med detta.

Förslaget om att kunna använda en EU-certifiering för att bevisa regelefterlevnad kan potentiellt minska svårigheterna för verksamhetsutövare att överblicka och förstå hur man ska agera för att undvika sanktioner. I teorin skulle ett småföretag kunna skaffa en certifiering och därmed på ett enkelt sätt visa alla sina kunder att det uppfyller kraven. Detta skulle kunna minska administrationen jämfört med att svara på varje kunds unika säkerhetsenkäter och revisioner. Samtidigt riskerar certifieringen att bli ett de facto-krav från kunderna, vilket skapar en ny kostnad då många småföretagare med stor sannolikhet kommer att behöva anlita externa konsulter för certifieringsarbetet. Det är därför av stor vikt att certifieringen i praktiken är frivillig och finansieras av det offentliga för att undvika att ytterligare kostnader förs över på företagen.

Företagarna anser att syftet med föreslagna ändringar – att stärka cybersäkerheten i hela EU – är gott. Samtidigt vill vi betona att vägen dit riskerar att bli kostsam och administrativt tung för småföretag, vilket vi varnat för i tidigare remissyttrande. Om de föreslagna skärpningarna gör den regulatoriska miljön än mer komplex blir det svårare, inte enklare, för en icke-expert att överblicka sina skyldigheter. Det ytterligare lager av krav som föreslås läggas ovanpå det befintliga NIS 2-regelverket gör det också ännu svårare att beräkna den kumulativa kostnaden för ett enskilt svenskt företag.

Avslutningsvis vill Företagarna uppmana lagstiftaren, Försvarsmakten, Myndigheten för civilt försvar och andra sektorsansvariga myndigheter att skyndsamt upprätta och stärka befintliga dialoger med det privata näringslivet och på ett tydligt sätt inkludera småföretagarperspektiv. Behovet av dessa insatser stärks ytterligare i och med de föreslagna ändringarna.

Jacob Ämtvall
Näringspolitisk expert
Företagarna

Pernilla Norlin
Samhällspolitisk chef
Företagarna

[1] Se Företagarnas remissvar Fö2024/00496