Datum 2026-05-18

Informationsklass Öppen

Diarienr (åberopas) A191.775/2026 Saknr 000

Polismyndigheten

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

fo.ech.remissvar@regeringskansliet.se

Er referens Fö2026/00576

# Cybersäkerhetspaket; förändringar i EU:s cybersäkerhetsakt och i NIS 2-direktivet

## Sammanfattning

Polismyndigheten ställer sig i stort bakom regeringens preliminära svenska ståndpunkter. Polismyndigheten lämnar därutöver synpunkter enligt följande.

## Polismyndighetens synpunkter

### Ändringar i cybersäkerhetsakten (avsnitt 1.2.1)

#### Enisas mandat uppdateras för att reflektera nya uppgifter i EU:s samlade cyberreglering

Polismyndigheten är positiv till förslaget om en ökad roll och nya funktioner för Enisa inom sårbarhetshantering och hotunderrättelser. Förslaget bör, om det genomförs, kunna ge bättre stöd till nationella rättsvårdande myndigheters arbete samt öka förutsättningarna för ett starkt internationellt samarbete.

#### Ett nytt ramverk för EU-harmoniserat tillvägagångssätt avseende stärkt säkerhet i IKT-leveranskedjor

Polismyndigheten ser positivt på det föreslagna ramverket för att identifiera högriskleverantörer och motverka ”icke-tekniska risker”, t.ex. påverkan från tredjeland, i syfte att skydda kritisk infrastruktur mot statligt understödda cyberhot och sabotage. Polismyndighetens bedömning är att ett sådant ramverk bör kunna ha en stark brottsförebyggande effekt. Detsamma gäller kommissionens förslag som syftar till att säkerställa en harmoniserad ansats till icke-tekniska sårbarheter i 5G-nät.

**Postadress** Polismyndigheten 106 75 Stockholm
**Besöksadress** Polhemsgatan 30 Stockholm
**Telefon** 114 14
**Webbplats** polisen.se
**E-post** registrator.kansli@polisen.se

Polismyndigheten omfattas inte av NIS 2-direktivet och cybersäkerhetslagen[1]. Förslagen om tillvägagångssätt för att stärka säkerheten i IKT-leveranskedjor kan likväl komma att påverka Polismyndigheten.

Förslaget till ramverk innehåller en interventionsmekanism och förslag på begränsningar för identifierade högriskleverantörer bl.a. i förhållande till hur NIS 2-entiteter får nyttja sådana leverantörer, där kommissionen via genomförandeförordningar ska kunna förbjuda respektive kräva utfasning av utrustning från leverantörerna eller införa krav på riskreducerande åtgärder avseende användning av utrustning från leverantörerna. Därtill föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att delta i offentliga upphandlingar inom EU som rör tillhandahållande av komponenter för viktiga IKT-tillgångar. Exempel på utrustning som kan omfattas av ramverket är komponenter i mobilnät, fiber och satellit.

Ramverket kan således få till effekt att leverantörer till Polismyndigheten direkt eller indirekt påverkas av sådana förbud eller restriktioner och att Polismyndigheten som en följd av detta förhindras att köpa in strategiskt intressanta eller nödvändiga komponenter alternativt med relativt kort varsel tvingas att byta ut redan upphandlade komponenter. Ramverkets potentiella negativa konsekvenser ur ett brottsbekämpande perspektiv behöver därför analyseras särskilt.

### Ändringar i NIS 2-direktivet (avsnitt 1.2.2)

Polismyndigheten ser positivt på förslaget om krav på harmoniserad insamling av uppgifter om utpressningsprogram, s.k. ransomware-angrepp. Förslaget skulle, om det genomförs, ge brottsbekämpande myndigheter bättre lägesbilder och avsevärt mer och viktig data för att spåra och bekämpa cyberkriminalitet.

### Enisas mandat (avsnitt 2.1.2)

Polismyndigheten instämmer i regeringens hållning att det behövs mer analys i frågan om utvidgningen av Enisas mandat, och att det slås vakt om att Enisas roll inte blir övervägande operativ i förhållande till övriga uppgifter av stödjande karaktär. Exempelvis kan en utökad operativ roll för Enisa leda till duplicering eller överlappning med nationella myndigheters ansvar. Är dessa roller otydliga kan det allvarligt försvåra samordningen och därmed begränsa andra myndigheters insatser, exempelvis vid faktiska it-incidenter.

Polismyndigheten bedömer att förslaget om att ge Enisa nya arbetsuppgifter genom upprätta av en ny stödfunktion för att bemöta utpressningsangrepp, s.k. ransomware, samt uppgift att tillhandahålla verktyg för säker

[1] 1 kap. 12 § cybersäkerhetslagen (2025:1506).

kommunikation och verktyg som kan användas vid bedömning av överenstämmelse med certifieringsordningar är positivt.

Polismyndigheten är liksom regeringen positiv till att det nuvarande nätverket för nationella sambandspersoner inte finns med i det nya förslaget, då ett avvecklande av nätverket kan frigöra resurser och istället främja användning av uppbyggda kanaler för kommunikation mellan intressenter i medlemsstater och EU-nivå (såsom via nationella samordningscentrum i NCC-nätverket).

Polismyndigheten instämmer även i regeringens bedömning om att den föreslagna modellen där varje medlemsstat åläggs att bidra med två sekonderade nationella experter till Enisa behöver analyseras ytterligare. Förslaget i denna del innebär ett direkt personellt ianspråktagande av personal med mycket hög cyberkompetens. Denna typ av kompetens är eftertraktad och svårersättlig, inte minst för Polismyndigheten.

Yttrandet har beslutats av juristen Lars Stark efter föredragning av juristen Eric Åmell.

**POLISMYNDIGHETEN**

Lars Stark

Eric Åmell

Dokumentet har fastställts digitalt och har inga underskrifter.

**Kopia till**
Justitiedepartementet (INS)
Arbetstagarorganisationerna
Rikspolischefens kansli