Säkerhetspolisen

REMISSVAR

Datum: 2026-05-12
Diarienummer: 2026-6435-3

Mottagare:
Försvarsdepartementet
103 33 Stockholm
Referens: Fö2026/00576

Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555)

Säkerhetspolisen har, utifrån de frågor som myndigheten har att bevaka, följande synpunkter på förslagen.

Det föreslagna ramverket för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT) i cybersäkerhetsakten föreslås gälla för verksamhetsutövare som omfattas av Europaparlamentet och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet). Frågan uppkommer hur de nu föreslagna revideringarna i cybersäkerhetsakten ska kunna utformas utan alltför omfattande inverkan på området nationell säkerhet, vilket är medlemsstaternas exklusiva ansvar. I Sverige har NIS 2-direktivet genomförts i första hand genom cybersäkerhetslagen (2025:1506). Vissa typer av verksamheter är undantagna helt eller delvis från cybersäkerhetslagens tillämpningsområde (jfr 1 kap. 12 §). För en enskild verksamhetsutövare som omfattas av NIS 2-direktivet men som också till någon del bedriver säkerhetskänslig verksamhet (en så kallad blandad verksamhetsutövare), gäller de olika åtgärdskraven etc. i cybersäkerhetslagen alla delar av verksamheten utom den säkerhetskänsliga delen. Hur avses ett framtida krav på att inte använda viss utrustning implementeras hos en sådan blandad verksamhetsutövare? Kommer dessa verksamhetsutövare att kunna fortsätta använda ”svartlistad” utrustning i den säkerhetskänsliga delen av sin verksamhet, eller kommer kraven i cybersäkerhetsakten att i praktiken gälla hela verksamheten? Beroende på hur frågorna besvaras kan det, ur ett nationellt säkerhetsperspektiv, framstå som olämpligt att överlåta rätten att besluta om förbud mot användningen av vissa leverantörer eller produkter från Sverige till EU.

I artikel 116 (2) förslås reglering av när en vägran att, med hänvisning till bland annat nationell säkerhet eller rikets försvar, lämna ut vissa typer av uppgifter till en frågeställande behörig myndighet i en annan medlemsstat, ska få göras. Enligt förslaget ska en sådan vägran inte få göras förrän efter konsultation/samråd har skett med kommissionen. Detta får tolkas som att en sådan vägran på något sätt ska kunna underställas kommissionens granskning. Säkerhetspolisen vill understryka att en sådan ordning måste anses stå i strid med artikel 346 fördraget om Europeiska Unionens funktionssätt (FEUF), enligt vilken ingen medlemsstat ska vara förpliktad att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.

I förslaget till revideringar av NIS 2-direktivet föreslås i artikel 27 att det register som Enisa ska upprätta ska utökas till att omfatta samtliga verksamhetsutövare som träffas av regleringen. Detta register kommer i sådant fall bland annat innehålla IP-adresser till samtliga NIS 2-verksamhetsutövare i EU. Detta kan kontrasteras mot nu gällande NIS-direktiv, enligt vilket (1) Enisa endast ska upprätta ett register över de kategorier av verksamhetsutövare som typiskt sett ofta bedriver gränsöverskridande verksamhet och (2) uppgifter om IP-adresser är undantagna från vad som ska vidarebefordras till Enisa. Av förslaget framgår inte tillräckligt tydligt varför det ska

anses motiverat att Enisa samlar in så stora mängder av uppgifter om samtliga NIS 2-verksamhetsutövare i EU. Att upprätta ett så omfattande register medför sådana sårbarheter ur säkerhetssynpunkt att det bör undvikas, om det inte är absolut nödvändigt.

_____

Detta remissvar har beslutats av biträdande rättsenhetschefen Ewa Bokwall efter föredragning av den seniora verksjuristen Robert Tolonen Scherman.