FÖRSVARSMAKTEN

Svar

Datum
2026-05-13

Beteckning
FM2026-13975:2

Säkerhetsskyddsklass

Regeringskansliet,
Försvarsdepartementet samt Sändlista

Ert tjänsteställe, handläggare
Regeringskansliet, Försvarsdepartementet

Ert datum
2026-03-23

Er beteckning
Fö2026/00576

Vårt tjänsteställe, handläggare
FST CYBER, Lars-Erik Mickos

Vårt föregående datum

Vår föregående beteckning

Försvarsmaktens remissyttrande över Cybersäkerhetspaketet

Försvarsmakten har beretts tillfälle att yttra sig över Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS2-direktivet (EU 2022/2555) KOM (2026)11, 13.

Försvarsmaktens generella inställning till arbete med syfte att höja nivån på cybersäkerhet i samhället är mycket positiv. Med dagens samhällsutveckling är det av högsta vikt att regelverk och metoder kontinuerligt förbättras. Det är dock viktigt att detta arbete inte negativt påverkar Försvarsmaktens rådighet i att utföra sin uppgift.

Försvarsmakten har identifierat följande synpunkter på förslaget.

Strategisk infrastruktur med dubbla användningsområden

Enligt förslaget om ändringar i NIS 2-direktivet ska direktivet även omfatta ägare, innehavare och operatörer av sådan strategisk infrastruktur med både civil och militär användning som avses i ett förslag till EU-förordning om militära transporter som är under förhandling. I EU-kommissionens promemoria finns ingen närmare beskrivning av eller motivering till detta förslag. Förslaget hänvisar dessutom till en förordning som ännu inte är beslutad. Det gör det svårt att bedöma behovet och konsekvenserna av förslaget. Försvarsmakten anser att det finns en risk att tillämpningsområdet för NIS 2-direktivet utökas på ett sätt som inte är önskvärt vad gäller nationell säkerhet.

(LMI)

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
Försvarsmakten	Lidingövägen 24	08-788 75 00	08-788 77 78	exp-hkv@mil.se
107 85 Stockholm				www.forsvarsmakten.se

Ramverk för säkerhet i IKT-leveranskedjor

Förslaget till en ny cybersäkerhetsakt innehåller ett förslag om ramverk för säkerhet i IKT-leveranskedjor. Förslaget innebär begränsningar vad gäller användning av identifierade högriskleverantörer. Försvarsmakten instämmer i att det finns ett behov av att höja säkerheten i IKT-utrustning, och att det generellt är önskvärt att kunna utesluta användande av utrustning med tveksam säkerhet eller risk för andra leveranskedjeproblem. Det finns dock ett behov av att inom viss verksamhet som rör nationell säkerhet, där det även finns resurser och kompetens att hantera säkerhetsrisker, behålla rådigheten över val av leverantörer och utrustning.

Centralisering av certifieringar

I förslaget om ändringar i NIS2-direktivet (artikel 24) tillkommer att medlemsstater kan kräva uppfyllnad av certifieringar från Enisa/CSA ramverket. Dock kan dessa krav inte gå över den nivå som definierats i certifieringarna. Då varje land har en varierande säkerhetssituation är det svårt att definiera en fast nivå av säkerhet som är generisk men passar varje lands lokala behov och förutsättningar. Det finns en tydlig risk för att man väljer en nivå som motsvarar minsta gemensamma nämnare och därför lägger ett minimigolv av krav som inte får överskridas på grund av fullharmonisering. Försvarsmakten anser att en sådan utveckling inte skulle gagna Europas säkerhet. EU bör därför ge nationerna möjlighet att centralt definiera tilläggskrav till den överenskomna grundnivån för att certifiering ska vara giltig i medlemsstaten. Endast en leverantör som blir certifierad med alla medlemsstaters tilläggskrav kan då säga att dennes produkt är certifierad i hela EU.

Kryptografiska algoritmer

Kompetensen avseende kryptografiskt skydd av säkerhetsskyddsklassificerade uppgifter finns hos medlemsstaternas säkerhetsmyndigheter. Med hänsyn tagen till dess känsliga natur och det faktum att säkerhetsskyddsklassificerade EU-uppgifter generellt har direkt inverkan på nationell säkerhet, anser Försvarsmakten att det är olämpligt att ge Enisa uppgifter inom detta område. Uppgifterna i cybersäkerhetsakten artikel 18 punkt 3 bör därför avgränsas till användning av kryptografiska algoritmer när det avser skydd av icke säkerhetsskyddsklassificerade uppgifter.

Deltagande i beredningen av ärendet har varit försvarsjurist Sara Westerlund (FST JUR), Jan Wünsche (MUST SÄKK SÄKT) och chefsingenjör Patrik Fältström (CYBER).

Detta yttrande har fattats av överste Henrik Sjövall. I den slutliga handläggningen har deltagit Stf C FST CYBER FUNK Ann-Marie Löf och som föredragande informationssäkerhetsarkitekt Lars-Erik Mickos.

Sjövall, Henrik

Stf C FST CYBER

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

Inom myndigheten för kännedom
MUST SÄKK SÄKK
MUST SÄKK SÄKT
HKV FST JUR