Totalförsvarets forskningsinstitut

Datum
2026-04-13

Diarienummer
FOI-2026-209

Er referens
Fi2026/00065

Vår handläggare

Remissvar gällande betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Totalförsvarets forskningsinstitut (FOI) har tagit del av betänkandet och har – från de utgångspunkter myndigheten har att beakta – följande synpunkter.

FOI tillstyrker betänkandets förslag, och lämnar härutöver följande kommentar.

Avseende kapitel 12 Stöd till företag

Kapitlet inleds med en beskrivning av de krav och möjligheter som cyberresiliensförordningen medför avseende stöd till de aktörer som berörs av densamma:

> Artikel 33 i EU:s cyberresiliensförordning innehåller bestämmelser om stödåtgärder för företag. Vidare innehåller artikel 10 i EU:s cyberresiliensförordning bestämmelser om hur kompetensen i en cyberresilient digital miljö ska förbättras.

Dessa två artiklar täcker två områden. För det första åtgärder för att myndigheter och företag effektivare ska kunna införa de standarder och rutiner som förordningen kräver. För det andra åtgärder för kompetenshöjning av *"... tillverkares anställda, konsumenter, utbildningsanordnare och även offentliga förvaltningar…"*. Detta är något som tidigare utredningar har slagit fast som ett bristområde hos svenska organisationer (se till exempel kapitel 3.4 och 3.6 i Skr. 2024/25:121 *Nationell strategi för cybersäkerhet 2025-2029 rörande behovet av cybersäkerhetskompetens i svenska verksamheter*).

Stöd för införande av rutiner täcks väl i kapitlet. Betänkandet tar upp risk för flaskhalsar, kompetensbrist och förseningar i förmågan att implementera direktivet. Betänkandet lämnar också förslag på myndigheter som bör få extra uppgifter att speciellt stödja de ansvariga myndigheterna och företagen med implementationen under en övergångsperiod.

De företag som behöver hjälp med införandet av nya rutiner, roller och procedurer kan emellertid förväntas ha en brant uppförsbacke vad avser att korrekt utföra de uppgifter som definieras i standarderna. Införandet av exempelvis en rutin för hot- och riskbedömning i projektarbetet kräver kompetens i att korrekt bedöma hot och risker.

I avsaknad av befintlig cybersäkerhetskompetens riskerar förordningens syfte – att öka säkerheten – att inte uppnås i avsedd utsträckning.

Med beaktande av synpunkterna ovan föreslår FOI därför att följande två aspekter övervägs i den fortsatta beredningen.

- Att relevanta myndigheter åläggs att medvetandegöra de företag och myndigheter som berörs av lagstiftningen avseende behovet av att utbilda och kompetensutveckla sin befintliga personal i generellt cybersäkerhetsarbete under övergången till den nya regleringen.
- Att relevanta myndigheter åläggs, på samma sätt som vid införandet av standarder och regelefterlevnad, ge stöd till de berörda organisationerna för att säkerställa att de kan uppnå en tillräcklig grad av generell cybersäkerhetskompetens i sin verksamhet.

FOI
Totalförsvarets forskningsinstitut

Datum 2026-04-13

Beteckning FOI-2026-209

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av forskare David Lindahl. I den slutliga handläggningen har även stabschef Niclas Karlsson, säkerhetschef Johan Bäckström, jurist Alexander Engvers och handläggare Pär Eriksson deltagit.

Jens Mattsson

David Lindahl

Sändlista:
Finansdepartementet
103 33 Stockholm
finansdepartementet.registrator@regeringskansliet.se

Internt FOI:
Registrator
ÖD-sekreterare
Stabschef
Chefsjurist
Avdelningschef Cyberförsvar och ledningsteknik