Regeringskansliet

Faktapromemoria
Riksdagsår: 2025/26
FPM-nummer: 78
2026-02-23

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

Försvarsdepartementet

Dokumentbeteckning

COM(2026) 11 Celexnummer 52026PC0011

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

COM(2026) 13 Celexnummer 52026PC0013

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

Sammanfattning

Kommissionen presenterade den 20 januari 2026 ett cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555).

I förordningen om ändringar i cybersäkerhetsakten (CSA 2) föreslås ändringar avseende mandatet för EU:s cybersäkerhetsbyrå (Enisa) i syfte att bl.a. klargöra och i vissa fall utöka Enisas ansvar och uppgifter. Därtill föreslås ändringar i

ramverket för europeisk cybersäkerhetscertifiering syftandes till att effektivisera och förtydliga processerna i ramverket. Vidare finns också förslag om ett nytt ramverk för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT) som syftar till att harmonisera och stärka EU:s arbete med säkerhet i IKT-leveranskedjor.

I direktivet föreslås riktade ändringar i NIS 2-direktivet. Förslagen innebär bl.a. vissa ändringar i vilka entiteter som omfattas av NIS 2-direktivet och följdändringar utifrån CSA 2-förslaget. Regeringen är preliminärt positiv till förtydliganden av Enisas existerande uppgifter avseende bl.a. policyutveckling, kunskapsbyggnad och kunskapsspridning, stödjande verksamhet kring standardisering och övningar. Regeringen anser dock att mer analys behövs i frågan om utvidgningen av Enisas mandat, vilket hänför sig till att Enisa ska inta en mer operativ roll samt att byrån ska kunna ta ut avgifter för viss verksamhet.

Regeringen är också preliminärt positiv till att ramverket för cybersäkerhetscertifiering effektiviseras och förtydligas. Regeringens ingångsvärde i förhandlingarna är att verka för förändringar som får verkliga effekter.

Regeringen välkomnar att kommissionen undersöker sätt att stärka säkerheten i kritiska IKT-leveranskedjor. Hur ramverket är tänkt att fungera och vilka effekter det kan få kräver emellertid ytterligare analys.

Slutligen välkomnar regeringen kommissionens förslag om att införa ändringar i NIS 2-direktivet som syftar till att förtydliga hur regelverket ska tillämpas.

Regeringen avser verka för att regler och processer utformas så att konsekvenserna är proportionerliga och inte medför större begränsningar eller kostnader än vad som är nödvändigt.

1. Förslaget

1.1 Ärendets bakgrund

Mot bakgrund av bl.a. ökade hot och sårbarheter i cyberrymden, kopplat till EU:s inre marknad, har kommissionen under de senaste åren tagit fram en rad bindande rättsakter och rekommendationer.

1.1.1 EU:s verktygslåda för 5G-säkerhet

Baserat på bl.a. EU:s samordnade riskanalys av cybersäkerheten i 5G-nät publicerade samarbetsgruppen[1] den 29 januari 2020 EU:s verktygslåda för 5G-säkerhet. Verktygslådan innehåller rekommenderade åtgärder som kan vidtas för att reducera identifierade risker. Åtgärderna, vilka inte är bindande för medlemsstaterna, omfattar bland annat att stärka säkerhetskraven för operatörer av mobilnät, bedöma leverantörers riskprofil och tillämpa relevanta begränsningar eller uteslutningar av leverantörer som utgör en hög risk samt säkerställa att varje operatör har en strategi för att undvika eller begränsa beroendet av en enda leverantör.

1.1.2 Cybersäkerhetsakten

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) innehåller två huvudsakliga delar: (1) ett mandat för EU:s cybersäkerhetsbyrå, Enisa, och (2) ett ramverk för europeisk cybersäkerhetscertifiering (ECCF). ECCF infördes för att ersätta nationella certifieringsordningar med europeiska ordningar som möjliggör harmoniserade och standardiserade bedömningar av cybersäkerhetsnivån för produkter och tjänster på den inre marknaden. Europeiska certifieringsordningar bedömdes också kunna skapa förenklade villkor för både kunder och leverantörer. Enisa fick i cybersäkerhetsakten en central roll i att stötta kommissionen i certifieringsarbetet, bl.a. att bistå kommissionen i dess roll som ordförande för den europeiska gruppen för

[1] *Samarbetsgruppen för nät- och informationssäkerhet*, inrättades genom Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).

cybersäkerhetscertifiering (ECCG) och uppgiften att ta fram utkast på certifieringsordningar som beställs av kommissionen.

1.1.3 NIS 2-direktivet

Europaparlamentet och rådet antog den 14 december 2022 direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet). NIS 2-direktivet, som ersatte det tidigare NIS-direktivet från 2016, syftar till att höja den gemensamma cybersäkerhetsnivån inom EU. Direktivet omfattar 18 sektorer och innehåller skärpta cybersäkerhetskrav för både privata och offentliga aktörer. I Sverige har NIS 2-direktivet genomförts i huvudsak genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507).

1.1.4 Inre säkerhetsstrategin

Kommissionen presenterade i april 2025 dokumentet ProtectEU: Europeisk strategi för inre säkerhet[2]. I strategin aviserade kommissionen delar av det som nu presenteras i CSA 2-förslaget. I strategin anges bland annat att EU behöver en gemensam strategi om säkerhet och motståndskraft för IKT-leveranskedjor och IKT-infrastruktur, i syfte att motverka rådande fragmentering på den inre marknaden samt för att undvika kritiska beroenden och att säkra EU:s kritiska infrastruktur. Molntjänster och telekommunikationstjänster uppges vara centrala för leveranskedjorna för kritisk infrastruktur och kommissionen indikerar att kritiska entiteter bör välja sådana tjänster utifrån en lämplig cybersäkerhetsnivå, med beaktande av inte bara tekniska risker utan också strategiska risker och beroendeförhållanden. I strategin framhålls att EU:s verktygslåda för 5G-cybersäkerhet[3] har varit en lämplig ram för att skydda 5G-näten men att medlemsstaterna inte tillämpat verktygslådan tillräckligt effektivt. Allvarliga säkerhetsbrister beskrivs därför vara olösta, särskilt avseende utfasning av leverantörer som bedömts utgöra hög risk.

[2] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om ProtectEU: Europeisk strategi för inre säkerhet, KOM 2025/148.

[3] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén - Säker 5G utbyggnad i EU – Genomförande av EU:s verktygslå, KOM (2020) 50.

1.1.5 Förslaget om förordning om digitala nät

I samband med CSA 2-förslaget presenterade kommissionen den 21 januari ett förslag till förordning om digitala nät (Digital Networks Act, DNA).[4] Förslaget innehåller bland annat villkor som får förenas med anmälan och radiospektrumtillstånd som avser efterlevnad av de krav som föreslås i CSA 2.

1.2 Förslagets innehåll

1.2.1 Ändringar i Cybersäkerhetsakten

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

Enisas mandat föreslås förtydligas för att inkorporera alla de uppgifter som tillkommit Enisa i och med nya rättsakter som har införts sedan EU:s cybersäkerhetsakt trädde i kraft 2019. I vissa delar utökas också Enisas roll enligt kommissionens förslag. Kommissionen uppskattar också att förslaget skulle kräva en budgetökning för Enisa där byråns årliga budget från 2028 blir 49 miljoner EUR.

Förslaget innehåller nya uppgifter för Enisa kopplat till byråns operativa arbete. Bl.a. föreslås upprättande av en ny stödfunktion för att bemöta utpressningsangrepp, s.k. ransomware, samt uppgifter att tillhandahålla verktyg för säker kommunikation och verktyg som kan användas vid bedömning av överenstämmelse med certifieringsordningar. I förslag på nya bestämmelser ska Enisa kunna ta ut avgifter för vissa tjänster och verktyg som byrån tillhandahåller. Därtill föreslås en ökad roll och nya funktioner inom sårbarhetshantering och hotunderrättelser. Vidare föreslås Enisa ingå som fast medlem i det nätverk för enheter för hantering av it-säkerhetsincidenter som inrättats enligt artikel 15 i NIS 2-direktivet (CSIRT-nätverket) samtidigt som byrån behåller sin sekretariatsroll inom nätverket. Enisa föreslås även få en tydligare roll avseende utvecklingen av en europeisk ram för cybersäkerhetskompetenser (ECSF). ECSF är ett ramverk med profiler för yrkesroller inom cybersäkerhet och utgör enligt kommissionens meddelande

[4] COM(2026) 16: Proposal Regulation Digital Networks Act (DNA).

om ”Cybersecurity Skills Academy” (COM(2023) 207) grunden för att bedöma EU:s kompetensförsörjningsbehov inom cybersäkerhet.

Det tidigare nätverket för nationella sambandspersoner (NLO-nätverk) finns inte med i det nya förslaget. Medlemsstaterna ska istället enligt förslagen utse minst två nationella sambandspersoner som ska fungera dels som kontaktyta för medlemsstaternas förfrågningar mot Enisa och dels arbeta med Enisas ordinarie verksamhet. I fråga om arbetet i Enisas styrelse föreslås kommissionens godkännande krävas vid större beslut. Därtill föreslås att styrelsen primärt ska utgöras av chefer, eller i andra hand högre beslutsfattare, från medlemsstaternas cybersäkerhetsmyndigheter.

Effektivare och tydligare processer i ramverket för cybersäkerhetscertifiering

Kommissionen föreslår ändringar i ramverket för cybersäkerhetscertifiering som syftar till att effektivisera och förtydliga processerna för framtagandet av certifieringsordningar. De föreslagna ändringarna innebär bl.a. nya bestämmelser om hur kommissionen ska beställa utkast till certifieringsordningar från Enisa och vilken information en sådan beställning måste innehålla. Därtill finns nya bestämmelser om hur ordningar ska tas fram och hur de ska förvaltas. När det gäller förvaltning föreslås en tydlig roll för Enisa att i samverkan med medlemsstater, unionsorgan och privat sektor besluta om hur ordningar ska förvaltas. Det föreslås också nya tidsbestämmelser om de ingående stegen i framtagande av certifieringsordningar inklusive att framtagandet av nya ordningar ska ta högst 12 månader. Vidare utökas de säkerhetsmål som certifieringsordningar ska eftersträva, bl.a. i syfte att harmonisera ordningarna med nya bestämmelser i EU:s cyberresiliensförordning och NIS 2-direktivet. I förslagen stärks också Enisas möjlighet att ta fram egna specifikationer som kan ligga till grund för nya certifieringsordningar, t.ex. om tillämpliga harmoniserade internationella eller europeiska standarder bedöms saknas. Det framgår även tydligare skrivningar vilka premierar europeiska framför nationella certifieringsordningar. Bl.a. föreslås kommissionen kunna be medlemsstater att upphäva en nationell certifieringsordning. Europeiska cybersäkerhetscertifieringsgruppen (ECCG), där medlemsstaternas certifieringsmyndigheter ingår, skulle dock i vissa fall kunna föreslå för kommissionen att beställa en ny certifieringsordning.

Därtill finns ett antal nya förslag i förhållande till ramverkets utformning i EU:s cybersäkerhetsakt av idag. Bland dessa finns att kommissionen aviserar en ny certifieringsordning för NIS 2-entiteters cybersäkerhet. Denna ska kunna användas för certifiering mot kraven på rikshanteringsåtgärder i NIS 2-direktivet, bl.a. för att entiteter med gränsöverskridande verksamhet ska kunna uppvisa efterlevnad av riskhanteringsåtgärderna i NIS 2-direktivet men också efterlevnad av andra unionsöverskridande eller sektoriella regelverk med säkerhetskrav. Den nya certifieringsordningen går i linje med att innehav av certifikat utfärdade från europeiska certifieringsordningar föreslås kunna innebära presumtion om regelefterlevnad av EU:s cyber- och digitala reglering i tillämpliga delar.

Vidare föreslås ett råd (European Cybersecurity Certification Assembly) inrättas för att på minst årlig basis samla relevanta intressenter för strategiska diskussioner om cybersäkerhetscertifiering inom unionen. Den intressentgrupp för cybersäkerhetscertifiering som etablerades i första cybersäkerhetsakten finns inte heller i det nya förslaget. Istället ska Enisa, utöver ovan nämnda råd, löpande samverka med relevant industri och andra parter inom ramen för ett brett externt samverkansmandat.

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

Kommissionen föreslår ett ramverk för att adressera icke-tekniska risker i IKT-leveranskedjor i högkritiska sektorer och andra kritiska sektorer enligt direktiv (EU) 2022/2555. Mekanismen som föreslås syftar till att identifiera viktiga IKT-tillgångar i kritiska IKT-leveranskedjor och föreslå lämpliga och proportionerliga åtgärder för de entiteter som framgår av bilaga I och II till direktiv (EU) 2022/2555.

Ramverket tar sin utgångspunkt i artikel 22 i NIS 2-direktivet om samordnade säkerhetsriskbedömningar för kritiska leveranskedjor och kompletterar denna med ytterligare bestämmelser om roller och processer för hur sådana bedömningar ska genomföras. Innebörden av förslagen är bl.a. att kommissionen, med utgångspunkt i bedömningar genomförda enligt artikel 22 i NIS 2-direktivet eller utifrån andra specificerade underlag, bl.a. ska kunna anta genomförandeakter om utnämning av tredjeländer som utgör cybersäkerhetsrisk och identifiera högriskleverantörer från sådana länder. Innan sådana genomförandeakter tas fram ska kommissionen också analysera om

landet i fråga har lagar eller bevisad praxis som kräver att företag rapporterar sårbarheter i mjuk- och hårdvara till nationella myndigheterna innan de uppmärksammats offentligt, om landet saknar effektiva rättsmedel och oberoende demokratisk kontroll som kan korrigera identifierade risker. Vidare ska bedömas huruvida hotaktörer som kontrolleras från landet bedriver skadlig cyberaktivitet samt om landet saknar förmåga eller vilja att samarbeta med kommissionen eller medlemsstaterna för att hantera identifierade risker. Ramverket innehåller också en interventionsmekanism för att, under särskilda omständigheter, kunna tillämpas på leverantörer på den inre marknaden som står under kontroll av tredjeländer eller leverantörer som utgör hög risk eller som kontrolleras av medborgare från ett sådant land.

För identifierade högriskleverantörer föreslås flera begränsningar som ska kunna införas 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. Enligt förslaget ska dock åtgärder som vidtas utifrån ramverket inte hindra medlemsstater från att anta eller bibehålla nationella bestämmelser för att säkerställa ett högre skydd. Därtill föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att delta i offentliga upphandlingar inom EU som rör tillhandahållande av komponenter för viktiga IKT-tillgångar, att ta del av EU-finansiering eller ingå i europeiskt standardiseringsarbete.

Av förslaget framgår särskilda bestämmelser rörande utfasning av utrustning från högriskleverantörer respektive förbud mot att installera ny utrustning från sådana leverantörer i mobilnät, fibernät och satellitnät för elektroniska kommunikationer. För mobilnät gäller att sådan utfasning ska ske inom 36 månader från publicering av en genomförandeakt där högriskleverantören i fråga definieras.

Leverantörer ska, innan de definieras som högriskleverantörer, enligt förslagen kunna höras. Vidare ska det gå att ansöka om undantag för att ingå i IKT-leveranskedjor hos NIS 2-entiteter eller för att deltaga i offentlig upphandling av komponenter som ingår i viktiga IKT-tillgångar. Därtill finns i förslaget bestämmelser om tillsyn och verkställighetsåtgärder. Sanktioner ska också kunna utfärdas mot NIS 2-entiteter vid överträdelser av sådana genomförandeaktörer som förbjuder nyttjande av komponenter från

högriskleverantörer inom viktiga IKT-tillgångar eller av krav på riskreducerande åtgärder enligt antagna genomförandeakter. Det föreslås vidare att den nationella myndigheten enligt CSA 2 ska kunna begära att en regleringsmyndighet enligt DNA-förslaget återkallar tillhandahållares radiospekrumtillstånd eller rätt att tillhandahålla elektroniska kommunikationsnät eller -tjänster. Detta föreslås gälla vid bristande efterlevnad av säkerhetskraven i CSA 2.

1.2.2 Ändringar i NIS 2-direktivet

Direktivets tillämpningsområde

Förslaget innebär bl.a. att tillämpningsområdet för NIS 2-direktivet utökas då nya aktörer inkluderas som NIS 2-entiteter. Det berör leverantörer av europeiska digitala identitetsplånböcker och europeiska företagsplånböcker, som föreslås klassificeras som väsentliga entiteter, oavsett storlek. Vidare föreslås alla operatörer av undervattensinfrastruktur för elektronisk kommunikation ingå i direktivets omfattning, såväl tillhandahållare av allmänna som icke-allmänna elektroniska kommunikationsnät. Även alla entiteter som ansvarar för strategisk infrastruktur med både civil och militär användning (dubbla användningsområden) ska omfattas av direktivets tillämpningsområde.

Förslaget innebär också att vissa aktörer inte längre ska omfattas av direktivet. Endast elproducenter med en produktionskapacitet på över en megawatt ska omfattas av direktivet, förutsatt att de i övrigt uppfyller storlekskravet i direktivet. Kravet om produktionskapacitet gäller även elproducenter som driver flera anläggningar vars sammanlagda produktionskapacitet överstiger en megawatt.

Kommissionen föreslår att en ny storlekskategori av företag inkluderas i direktivet, små midcapföretag, vilket omfattar företag som sysselsätter färre än 750 personer och har en årlig omsättning som inte överstiger 150 miljoner euro eller en årlig balansomslutning som inte överstiger 129 miljoner euro. Kommissionen föreslår vidare att entiteter som överstiger trösklarna för små midcap-företag ska klassificeras som väsentliga. Kommissionen föreslår även att den allmänna storleksregeln ska tillämpas på leverantörer av domännamnssystemstjänster (DNS-tjänsteleverantörer) vilket medför att mindre sådana aktörer inte längre kommer att omfattas av direktivet.

Förslaget innehåller också vissa förtydliganden i direktivets bilagor I och II avseende vårdgivare, elproducenter, vätgasverksamheter och aktörer inom kemisektorn, som har till syfte säkerställa rättssäkerhet och minska bördan för både verksamheter och nationella myndigheter.

Enisas och kommissionens uppgifter

Enisa ska enligt förslaget stödja medlemsstater i tillsynen av entiteter som tillhandahåller tjänster inom flera medlemsstater. Det innebär också att nationella tillsynsmyndigheter ska skicka in information till Enisa om bland annat de cybersäkerhetsrelaterade riskhanteringsåtgärder som den väsentliga eller viktiga entiteten har vidtagit. Enisa ska också genomföra analyser av gränsöverskridande cybersäkerhetskrav och lämna rekommendationer om tillsyn i samverkan mellan berörda medlemsstater. Vidare föreslås att kommissionen ska utvärdera behovet av genomförandeakter. I det fall kommissionen antar genomförandeakter får medlemsstaterna inte införa ytterligare nationella krav avseende de åtgärder som avses i artikel 21.2 i NIS 2-direktivet.

I förslaget anges även att kommissionen bör utveckla riktlinjer för NIS 2-entiteters krav på leverantörer avseende säkerhet i leveranskedjor. Syftet är att säkerställa rättslig tydlighet och förhindra att skyldigheter på ett otillbörligt sätt överförs till aktörer som inte omfattas av NIS 2-direktivet.

Nya krav på rapportering av utpressningsprogram

Förslaget innehåller krav på harmoniserad insamling av uppgifter om utpressningsprogram, s.k. ransomware-angrepp. NIS 2-entiteter ska enligt förslaget ange information om en incident har sitt ursprung i ett ransomware-angrepp samt hur entiteten hanterat incidenten, inklusive om något lösenbelopp begärts samt huruvida entiteten gjort någon sådan betalning.

1.3 Gällande svenska regler och förslagets effekt på dessa

Cybersäkerhetsakten är en förordning och därför direkt tillämplig i svensk rätt utan att den behövs genomföras i nationell lagstiftning. De ändringar som enligt förslaget ska göras i förordningen blir även de direkt tillämpliga. Viss kompletterande svensk lagstiftning kan eventuellt komma att behöva ses över, såsom lag (2021:553) med kompletterande bestämmelser till EU:s

cybersäkerhetsakt och förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Förslaget bedöms också påverka lagen (2022:482) om elektronisk kommunikation. Detta bland annat genom förslag om åtgärder mot högriskleverantörer i mobilnät, fasta nät och satellitnät för elektroniska kommunikationer.

Direktivförslaget bedöms påverka nationella regler som genomför NIS 2-direktivet i svensk rätt. Sverige har genomfört direktivet i huvudsak genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507). Även ändringar av myndigheters föreskrifter kan bli aktuella.

Vilka ytterligare ändringar i svensk lagstiftning som kan behöva göras är föremål för fortsatt analys.

1.4 Budgetära konsekvenser och konsekvensanalys

Enligt kommissionen skulle förslaget innebära att Enisas budget ökar med 81,5 procent till cirka 49 miljoner EUR från år 2028. Kommissionen har angett att detta ska finansieras genom omprioriteringar i den innevarande fleråriga budgetramen (MFF) och till viss del genom att Enisa kan ta ut nya avgifter bl.a. inom ramen för ECCF och för byråns verktyg för it-säkerhet. Huruvida detta träffar primärt näringslivets gränsytor mot Enisa, eller om det också kan innebära ekonomiska konsekvenser för offentlig sektor i Sverige, behöver analyseras vidare.

Inrättandet av ett europeiskt ramverk för säkerhet i IKT-leveranskedjor skulle innebära budgetmässiga åtaganden då det skulle ge nya uppgifter för de myndigheter som utövar tillsyn under den svenska NIS 2-regleringen då dessa också föreslås utöva tillsyn av bestämmelserna i det nya ramverket. Krav på att vidta riskreducerande åtgärder inom IKT-leveranskedjor eller krav på utfasning av, eller förbud mot, användning av vissa leverantörers komponenter inom viktiga IKT-tillgångar kommer också påverka svenska NIS 2-entiter.

2. Ståndpunkter

2.1 Preliminär svensk ståndpunkt

2.1.1 Budgetära konsekvenser

Regeringen anser att huruvida det finns utrymme att öka Enisas budget är något som bör beslutas inom ramen för förhandlingarna om EU:s långtidsbudget. Regeringen har en budgetrestriktiv hållning och anser att eventuella utgiftsökningar inom EU:s budget ska finansieras genom omprioriteringar inom befintliga ramar. Regeringen värnar även principen om en sund ekonomisk förvaltning.

2.1.2 Cybersäkerhetsakten

Enisas mandat

Det är positivt att kommissionen presenterat ändringar som omhändertar det faktum att Enisas roll utvecklats organiskt de senaste åren. Regeringen ser att Enisa i största möjliga utsträckning bör ha ett renodlat mandat fokuserat på stöd för implementering av EU-reglering, expertishjälp och vägledning samt att byråns roll inte bör överlappa med nationella eller andra EU-myndigheter. Vidare bör Enisas arbete i största möjliga mån vara horisontellt inriktat. Som huvudregel bör inte, utan särskilda skäl, verksamhet med fokus på särskilda sektorer eller andra verksamhetsmässiga delområden tillföras. Nya uppgifter för byrån bör följas av tydliga krav på informationsdelning och samverkan med nationella myndigheter, samt finansieras inom befintliga ekonomiska ramar.

Att förslaget utgår från att Enisa ska ha en självständig roll inom ramen för certifieringsramverket (ECCF), är också positivt och kan bidra till ökad effektivitet i Enisas verksamhet inom ramen för ECCF.

Nya uppgifter som föreslås för Enisa bör alltid föregås av analys av byråns kapacitet, befintliga resurser och huruvida Enisa är bäst lämpat att utföra uppgiften. I sammanhanget är det en nyckelfaktor att Enisas styrelse involveras i sådana överväganden och kan vägleda byrån genom att bidra till vilka prioriteringar som görs för byråns verksamhet. Vidare anser regeringen att det är centralt att eventuella ambitionshöjningar hanteras inom ramen för befintliga resurser.

Regeringen ställer sig 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). Regeringen behöver dock ytterligare analysera den föreslagna modellen där varje medlemsstat åläggs att bidra med två sekonderade nationella experter till Enisa som ska utgöra sambandspersoner.

Regeringen ser att de förslag som innebär att medlemsstaternas ges en stark, drivande roll via Enisas styrelse är positiva. CSA 2 bör inte precisera tjänstenivå eller yrkeskategori för medlemsstaternas delegater i Enisas styrelse. Sådana överväganden sköts bäst av medlemsstaterna själva.

Regeringen ämnar slå vakt om att Enisas roll inte blir övervägande operativ i förhållande till övriga uppgifter av stödjande karaktär. Det är centralt att EU-nivån inte duplicerar sådant som redan görs på nationell nivå och att arbetet bedrivs på ett kostnadseffektivt sätt. I sammanhanget krävs ytterligare analys av Enisas roll att ta fram vissa verktyg, inklusive sådana som byrån ska kunna ta ut avgifter för, men också förslaget att Enisa ska ingå i CSIRT-nätverket. Upprättandet av ett stödcenter inriktat på utpressningsprogram, s.k. ransomware, kan riskera att dels påverka Enisa i en operativ inriktning och dels förflytta byråns tonvikt från en horisontell ansats till att fokusera på särskilda delområden. Sverige bör dock ställa sig positivt till att kompetensramverket ECSF vidareutvecklas enligt förslaget i CSA 2, med beaktande av att ECSF bör utgöra ett efterfrågestyrt och flexibelt verktyg som är frivilligt för medlemsstaterna. Att ramverket utökas med ett certifieringsliknande förfarande där kompetenser ska attesteras kräver dock ytterligare överväganden.

Certifieringsramverket (ECCF)

Regeringen ser positivt på tydligare och mer transparenta bestämmelser rörande framtagande av certifieringsordningar och att ramverket effektiviseras i syfte att öka takten i framtagandet av certifieringsordningar. Nya tidsgränser behöver dock vara realistiska och får inte innebära att viktiga säkerhetsaspekter missas i framtagandet av ordningar. Regeringen ser positivt på att förslagen understryker Enisas självständiga roll och mandat för extern intressentsamverkan. När Intressentgruppen för certifiering samtidigt föreslås utgå krävs att Enisa agerar

självständigt inom ECCF samtidigt som byrån säkerställer adekvat samverkan med och faktainhämtning från experter både från medlemsstater och industri. Här bör det nya rådet för certifiering spela en roll avseende externa intressenters möjlighet till insyn och påverkan i ECCF. Detta gäller också vid förvaltning av certifieringsordningar, där både medlemsstater och industri har nyckelfunktioner. Regeringen avser även värna om att privata certifieringsorgan fortsatt kan utfärda certifikat enligt ECCF.

Regeringen ser positivt på förslag syftandes till att certifieringsordningar ska kunna omhänderta bestämmelser i reglering som tillkommit sedan cybersäkerhetsakten trädde i kraft 2019 då det kan förenkla regelefterlevnad. Samtidigt är det viktigt att certifiering som grundregel fortsatt är frivilligt. Regeringen bedömer att förslag rörande att certifieringsordningar ska kunna nyttjas som ett instrument för aktörer att uppnå och demonstrera regelefterlevnad kan bidra till minskad administrativ börda. Regeringen vill understryka att certifieringar utgör en delmängd i detta arbete, och att nationella tillsynsmyndigheter alltid har rätt att inleda tillsyn – och att ytterst finna att ett tillsynsobjekt inte efterlever tillämplig reglering – trots innehav av certifikat som utfärdats inom ECCF.

Regeringen tillstyrker att europeisk certifiering bör ha företräde framför nationella certifieringsordningar. Det är väsentligt att undvika fragmentering på den inre marknaden som det kan innebära om aktörer behöver förhålla sig till olika nationella system och tillvägagångssätt inom certifiering.

Regeringen välkomnar att de säkerhetsmål som certifieringsordningar ska ta i beaktande inte inkluderar geopolitiska, icke-tekniska krav då sådana krav inte bör ingå i tekniska certifieringsordningar. Samtidigt krävs mer analys av de utökade säkerhetsmålen som föreslås i CSA 2. Vidare anser regeringen att certifieringsordningar primärt bör bygga på internationell eller europeisk standardisering.

Ramverk för säkerhet i IKT-leveranskedjor

Regeringen ser att nya, unionsöverskridande regler avseende icke-tekniska risker i IKT-leveranskedjor i högkritiska och kritiska sektorer kan ge framåtdrift i EU:s samlade säkerhetsarbete under förutsättning att dessa är väl utformade och balanserade. Regeringen välkomnar därför kommissionens ambition om att få framdrift i och ökad harmonisering av medlemsstaternas säkerhetsarbete i

förhållande till icke-tekniska faktorer för IKT-leveranskedjor. Regeringen noterar att förslaget också omfattar vissa tekniska cybersäkerhetsåtgärder och anser även att det är viktigt att dessa harmoniserar med den horisontella regleringen i NIS 2- och CER-direktiven.

Regeringen noterar vidare att medlemsstaternas nationella regelverk för att åtgärda icke-tekniska risker i mobilnät är fragmenterade, och att rekommendationerna i EU:s verktygslåda för 5G-säkerhet inte genomförts fullt ut i flera EU-länder. Regeringen välkomnar därför kommissionens förslag som syftar till att säkerställa en harmoniserad ansats till icke-tekniska sårbarheter i 5G-nät. I nu gällande svensk lagstiftning är frågan om identifiering av och åtgärder mot högriskleverantörer i mobilnät en fråga för bedömning i relation till vilket hot sådana utgör mot Sveriges säkerhet. Målsättningen med den lagstiftningen överensstämmer i stora delar med CSA 2-förslaget. Vidare konstateras att förslagen om krav på utfasning av högriskleverantörer i fasta nät och satellitnät för elektroniska kommunikationer är långtgående och regeringen ser att närmare analys är nödvändig, i synnerhet i förhållande till vilka inverkningar de får för svenska företag. De föreslagna reglerna bedöms därutöver få konsekvenser för Sveriges nationella bestämmelser på området.

Vidare noterar regeringen att frågor om säkerhet i IKT-leveranskedjor tangerar frågor om nationell säkerhet som är medlemsstaters eget ansvar enligt fördraget om Europeiska unionen. Regeringen erinrar därför om att gemensamma åtgärder aldrig kan hindra medlemsstaterna från att vidta åtgärder för att säkerställa ett högre skydd än vad som krävs av EU-rätten i de fall det är nödvändigt av nationella säkerhetsskäl.

Riskbedömningar som föreslås ligga till grund för utpekande av länder och leverantörer med hög risk bör vara principbaserade och präglas av gedigen analys som medlemsstaterna deltar eller ges insyn i. Det är centralt att ramverket är proportionerligt och används i linje med EU:s åtaganden i handelsavtal samt inte nyttjas för omotiverad protektionism. Regeringen noterar att förslagen innehåller mekanismer för hur företag som pekas ut genom ramverket ska kunna höras innan kommissionens beslut fattas samt möjlighet för företagen att ansöka om undantag, vilket torde vara nödvändigt men kräver ytterligare analys.

2.1.3 NIS 2-direktivet

Sverige välkomnar kommissionens förslag till direktiv. Förslaget innehåller bestämmelser om ändringar i tillämpningsområdet för NIS 2-direktivet som väntas bidra till ökad regelefterlevnad och minska den administrativa bördan för berörda aktörer och tillsynsmyndigheter.

Regeringen ställer sig vidare positiv till att leverantörer av europeiska digitala identitetsplånböcker och företagsplånböcker omfattas av direktivet, då detta väntas stärka unionens samlade cyberresiliens. Det är dock viktigt att särskilja plånböckerna från varandra gällande kraven i direktivet, då den dimensionerande säkerhetsnivån skiljer sig mellan respektive plånbok, och detta är något regeringen kommer att verka för. Mot bakgrund av den rådande hotbilden mot undervattensinfrastruktur anser regeringen att relevanta operatörer av sådan infrastruktur bör omfattas av direktivet cybersäkerhetskrav.

Regeringen bedömer vidare att det krävs en noggrann analys av vilka aktörer som är relevanta att inkludera vad gäller strategisk infrastruktur med både civil och militär användning (dubbla användningsområden) för att säkerställa en väl avvägd reglering. Vidare bedömer regeringen att en väl avvägd reglering även behöver åstadkommas vad gäller det nationella utrymmet för ytterligare cybersäkerhetskrav i förhållande till sådana som kan finnas i genomförandeakter. Kommissionens förslag om Enisas utökade stöd till nationella myndigheter behöver samtidigt ses i ljuset av de förslag som presenteras i cybersäkerhetsakten avseende Enisas roll och mandat. Regeringen är i grunden positiv till byråns stödjande roll vid genomförande av regelverk. Förslaget om att fler uppgifter ska överföras till Enisa från nationella myndigheter behöver dock vägas noggrant mot risken att detta leder till onödig hög administrativ belastning, ökade kostnader och minskad kostnadseffektivitet.

Regeringen avser verka för att direktivet inte ska medföra en högre regelbörda för offentliga såväl som privata aktörer. Det pågår beredning inom Regeringskansliet om närmare ståndpunkter för direktivförslaget.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter gällande förslagen så som de nu presenterats är ännu inte kända, men flera medlemsstater har förmedlat preliminära

ståndpunkter i informella ståndpunktspapper. Några av huvuddragen i dessa redogörs för nedan.

Flera länder (bl.a. **Finland** och **Frankrike**) har välkomnat att EU:s cybersäkerhetsreglering förenklas och harmoniseras. Samtidigt har båda medlemsstater betonat att det, innan nya uppgifter tilldelas Enisa, krävs noggrann utvärdering och motivering av nya uppdrag samt att Enisas mandat bör vara fokuserat och komplettera (inte överlappa med) nationella myndigheters eller andra EU-organs roller.

Flera länder (bl.a. **Tyskland** och **Tjeckien**) har välkomnat en revidering av EU:s cybersäkerhetsakt men noterar att den borde föregåtts av en utvärdering av akten som skulle ha presenterats för medlemsstaterna redan under 2024. Att istället publicera utvärderingen tillsammans med förslaget har därför beskrivits som icke-ändamålsenligt.

Flera länder (bl.a. **Tyskland, Frankrike** och **Tjeckien**) har lyft att nya rättsakter sedan 2019 inneburit ett antal nya uppgifter för Enisa och att detta skett utan att åtföljas av en långsiktigt stabil ökning av Enisas resurser.

Ett antal medlemsstater (**Österrike, Belgien, Bulgarien, Kroatien, Tjeckien, Estland, Finland, Frankrike, Tyskland, Ungern, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Slovakien, Slovenien**) har gemensamt framfört önskan att Enisa får en roll som expertcentrum för cybersäkerhet som stödjer medlemsstaterna och fungerar som en kunskaps- och/informationsspridande, horisontell och tvärsektoriell myndighet samt en möjliggörare för EU-samarbete utan att bli en operativ entitet (såsom en CSIRT). Vidare nämns stärkt samarbete med europeiska standardiseringsorgan samt att Enisas styrelse får stärkt mandat att ge byrån vägledning och prioriteringar som viktiga frågor.

Flera medlemsstater **(**bl.a. **Spanien, Irland** och **Belgien)** har framfört att certifieringsramverket behöver förändras och att dess processer behöver förtydligas för att bli effektivt. De har bl.a. föreslagit ändringar i roller, i hur ECCG fungerar och kring hur certifieringsordningar tas fram och förvaltas.

Polen har argumenterat för att ändringarna i EU:s cybersäkerhetsakt bör användas för att göra Enisa till referensmyndighet för all cybersäkerhet och att Enisa bör involveras tidigt i processer som kan leda till lagstiftningsförslag.

2.3 Institutionernas ståndpunkter

Inga ståndpunkter är kända för närvarande.

2.4 Remissinstansernas och andra intressenters ståndpunkter

Förslagen har inte skickats ut på remiss.

3. Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Som rättslig grund har kommissionen angett artikel 114 i Fördraget om Europeiska unionens funktionssätt (EUF). Beslut fattas enligt ordinarie lagstiftningsförfarande, dvs. Europaparlamentet och rådet fattar beslut gemensamt.

3.2 Subsidiaritets- och proportionalitetsprinciperna

Eftersom de rättsakter som det föreslås ändringar i antogs på EU-nivå bedömer kommissionen att de bara kan ändras på EU-nivå. Kommissionen bedömer även att förslagen som lagts fram likväl upprätthåller subsidiaritetsprincipen.

Kommissionen bedömer vidare att initiativet till förslagen inte går längre än vad som är nödvändigt för att uppnå syftet med förenklingsåtgärderna utan att minska skyddet för hälsa, säkerhet och grundläggande rättigheter, samt att förslagen bevarar och optimerar de syften som de ändrade rättsakterna bygger på.

Regeringen delar preliminärt kommissionens bedömningar.

4. Övrigt

4.1 Fortsatt behandling av ärendet

Kommissionens förslag presenterades i rådet den 26 januari 2026. Förslagen förhandlas i rådet under våren 2026. Ordförandeskapet i rådet har kommunicerat en förväntan om att kunna avsluta förhandlingarna om Enisas mandat i CSA 2 under våren 2026. Förslagen väntas huvudsakligen diskuteras och förhandlas i den horisontella arbetsgruppen för cyberfrågor (HWP CI).

4.2 Fackuttryck och termer

CSIRT: enheter för hantering av it-säkerhetsincidenter (computer security incident response teams).

Cybersäkerhet: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

IKT: Informations- och kommunikationsteknik.

IKT-leveranskedjor: en summa av IKT-tjänster, IKT-produkter och IKT-processer som omfattar aktiviteter och aktörer som är inblandade i alla stadier innan en produkt blir tillgänglig eller en tjänst levereras på marknaden.

Kritiska entiteter: en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan i CER-direktivet.

Kritisk infrastruktur: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst.

Ransomware: utpressningsvirus och program som krypterar hela eller delar av en verksamhets information som lagras på drabbade informationssystem och gör informationen otillgänglig.