BESLUT

Datum	Diarienummer	Ärendetyp
2026-05-18	26FMV3242-2	1.3

Regeringskansliet
Försvarsdepartementet
103 33 Stockholm

Er referens	Ert datum	Er beteckning
Felix Nolte	2026-03-23	Fö2026/00576

Svar på remiss av Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS2-direktivet (EU 2022/2555)

Bakgrund

Försvarsdepartementet har remitterat Europeiska kommissionens (KOM) cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (CSA) samt riktade ändringar i NIS2-direktivet (NIS2D). Nedan följer FMV:s yttrande om de förslag som är av störst principiellt intresse för FMV.

Sammanfattning av de viktigaste synpunkterna

- FMV ifrågasätter utvidgningen till certifiering av NIS2D-entiteters cybersäkerhet. Det är tveksamt om någon kan gå i god för att en entitet uppfyller alla krav enligt NIS2D. [Art. 1]
- FMV emotsätter sig författningsreglerade avgifter för Enisa liksom utredningen och propositionen avseende genomförandet av cybersäkerhetsakten gjorde avseende avgifter till privata organ för bedömning av överensstämmelse (CAB:ar). Avgifter skulle verka hämmande på marknaden för CAB:ar och tillgången till svensk certifiering samt innebära fördröjningar av certifiering. Det skulle också verka hämmande för cybersäkerhet. [Art. 47]
- FMV stödjer ambitionen att effektivisera och förtydliga processerna för framtagandet av certifieringsordningar för cybersäkerhet Det får dock inte ske på bekostnad av kvalitet. Ordningarnas syfte att höja cybersäkerheten är det överordnade målet. FMV anser att ECCG-yttrande ska vara gemensamt för hela ECCG, precis som i dagens CSA. [Art. 74]
- FMV anser att tekniska specifikationer, oavsett hur och av vem de tas fram, behöver tas fram med samma öppenhet och noggrannhet som standarder. Den process som föreslås är inte tillnärmelsevis lika grundlig och bra. Specifikationer som krav för regelefterlevnad får inte vara hemliga för någon, varken för utvecklare, CAB:ar eller kunder. [Art. 85]
- Avskaffa ”bemyndigande” där det inte är absolut nödvändigt, t.ex. för ömsesidigt erkännande. [Art. 88 & 92]

FMV
Försvarets materielverk
115 88 Stockholm
Besöksadress: Banérgatan 62
Tel: 08-782 40 00
Fax: 08-667 57 99
registrator@fmv.se
www.fmv.se
Org.nr: 202100-0340
VAT nr: SE202100-0340-01

- FMV anser det mycket viktigt att befintlig beslutsprocedur i genomförandekommittén fortsätter gälla för att behålla möjligheten till blockerande minoritet. [Art. 118]
- FMV anser att Sverige inte bör acceptera fullharmonisering rörande NIS2D cybersäkerhetsåtgärder. Ett starkt skäl för detta är att många av de infrastrukturer som täcks av direktivet även har militära användningsområden och medlemsstaterna har exklusiv kompetens rörande nationell säkerhet. [NIS2D]

Ny cybersäkerhetsakt (CSA2)

Artikel 1 Innehåll och tillämpningsområde

KOM föreslår att CSA:s grundläggande tillämpningsområde utökas till NIS2-entiteters cybersäkerhet och aviserar att man kommer att begära en ny certifieringsordning för detta. Denna ska kunna användas för certifiering mot kraven på riskhanteringsåtgärder i NIS2D, bl.a. för att entiteter med gränsöverskridande verksamhet ska kunna uppvisa efterlevnad av riskhanterings-åtgärderna i NIS2D men också efterlevnad av andra unionsöverskridande eller sektoriella regelverk med säkerhetskrav.

FMV kan inte se hur någon ska kunna certifiera att en NIS2D-entitet efterlever alla relevanta säkerhetskrav i NIS2D. Kraven i sig är beroende av entiteternas egen riskanalys och det är oklart hur KOM:s kommande genomförandeförordning rörande säkerhetsåtgärder, som KOM föreslår kommer vara fullharmoniserande, kommer förhålla sig till detta. Nuvarande CSA klargör att en certifiering inte innebär ett intyg om säkerhet. Ett certifikat visar ”bara” att något evaluerats/certifierats på ett särskilt sätt av kompetent/ackrediterat organ vilket ”bara” visar assurans på viss nivå, inte säkerhet, vilket krävs för efterlevnad av cybersäkerhetskraven i NIS2D eller annan sektorslagstiftning med cybersäkerhetskrav. De nya förslagen går på tvärs med detta etablerade, och enda rimliga, synsätt. FMV menar att det behövs mer analys av vad KOM tänker sig ska certifieras och hur det ska ske.

Artikel 2 Definitioner

(30)
FMV anser att ”prior approval model” inte får innebära att en NCCA ska behöva göra om de bedömningar som CAB redan gjort. Att göra bedömningen obligatorisk innebär i princip att man, åtminstone delvis, tvingar fram ett statligt certifieringsorgan.

Sverige bör be att ”in the context of a specific certification process” byts ut mot en formulering som visar att det är det ackrediterade certifieringsorganets tänkta certifikat som avses.

(31)
FMV anser att ”general delegation model” inte får innebära att en NCCA ska behöva göra om de bedömningar som CAB redan gjort. Det ska endast innebära att certifieringsorganet kan utge certifikat på assuransnivå ”hög” utan ett ”prior approval” för varje certifikat.

Sverige bör påpeka att när man som Sverige valt att bara ha privata certifieringsorgan är det inte fråga om ”delegering”. Sverige kan föreslå att NCCA ges rätten att tillåta certifieringsorganen att utfärda certifikat med eller utan ”prior approval”.

Artikel 25 Styrelsens sammansättning

Det föreslås att styrelsen primärt ska utgöras av chefen, eller i andra hand högre beslutsfattare, från medlemsstaternas kompetenta myndigheter enligt NIS2D. FMV håller dock med regeringen som i sin faktapromemoria *Fakta-PM 2025/26:FPM78* till riksdagen menar att medlemsstaterna även fortsatt bör kunna bestämma helt själva vilka som ska utses till styrelsen.

Artikel 47 Avgifter

Artikel 47.2 [Avgifter för CAB:ar]

Europeiska unionens byrå för cybersäkerhet (Enisa) föreslås kunna ta ut vissa avgifter från de organ för bedömning av överensstämmelse (CAB:ar) som verkar inom ramen för certifierings-ordningarna för cybersäkerhet, dels för att delta i en certifieringsordning, dels per utfärdat certifikat.

FMV emotsätter avgifter för CAB:arnas deltagande i eller utfärdande av certifikat inom cybersäkerhetscertifieringsordningar. Sammanfattningsvis har svenska regeringen i avsnitt 6.3 i sin proposition (2020/21:186) till cybersäkerhetsakten och i utredningar explicit uttalat att det inte bör införas någon författningsreglerad avgiftsfinansiering för verksamhet som bedrivs av privata organ och som avser bedömning av överensstämmelse. Detta beslut grundar sig på en bedömning att avgifter skulle kunna skapa onödiga hinder för certifieringsprocessen och därmed försvåra uppfyllandet av cybersäkerhetsaktens mål. Liknande hinder skulle uppstå om motsvarande avgifter ska betalas till Enisa. Utredningar har också pekat på att avgifter skulle kunna leda till att organen för bedömning av överensstämmelse prioriterar lönsamma uppdrag framför sådana som är viktiga för samhället, vilket skulle kunna äventyra kvaliteten och oberoendet i bedömningsprocessen. Liknande fokusering på lönsamma uppdrag skulle kunna uppstå hos Enisa om de uppbär avgifter för viss verksamhet. Detta skulle kunna skapa andra prioriteringar än de som EU:s budget-myndighet förutsatt.

FMV menar också att avgifter inte ska införas i lagstiftningen eftersom dessa avgifter kan:

- **verka hämmande för tillgången till (CAB:ar)**:
  Införandet av avgifter skulle inte bara öka de direkta kostnaderna för företag, utan också den administrativa bördan. Företag skulle behöva hantera ytterligare processer för att betala avgifter, dokumentera betalningar och säkerställa att alla krav uppfylls. Om CAB:ar inte vill vara certifieringsorgan måste det antingen skapas statligt/statliga certifieringsorgan eller accepteras att motsvarande certifiering sker av certifieringsorgan i andra medlems-stater. Dessa aspekter bidrar starkt till svårigheterna med att få fram en CAB för den digitala identitetsplånboken.

  Företag bär redan kostnader för intern bedömning av överensstämmelse, såsom kostnader för testning, dokumentation och personal. Avgifter på externa organ för bedömning av överensstämmelse skulle alltså innebära dubbla kostnader, eftersom företag skulle tvingas betala både för sina egna interna processer och för externa bedömningar.

- **verka hämmande för tillgången till svenska certifieringar**: För små- och medelstora företag (SMF), som det kan vara fråga om på den svenska marknaden, skulle avgifter kunna bli en betydande börda. Avgifter skulle kunna göra certifieringsprocessen mindre

tillgänglig för mindre aktörer, särskilt SMF och nystartade företag, som redan har begränsade ekonomiska resurser. Detta skulle kunna leda till att endast större företag med tillräckliga resurser kan certifiera sina produkter, vilket i sin tur skulle motverka målet om en inkluderande och konkurrenskraftig inre marknad. EU:s cybersäkerhetsakt syftar till att säkerställa att alla företag, oavsett storlek, har möjlighet att certifiera sina produkter och tjänster. Avgifter skulle kunna underminera detta mål genom att skapa ekonomiska barriärer. Det ska dock sägas att även större företag har utmaningar i att hitta affärsmodeller för certifiering inom ramen för cybersäkerhetsakten.

- **innebära fördröjningar i certifieringsprocessen:** Avgifter skulle kunna leda till fördröjningar i certifieringsprocessen. Företag och organ skulle behöva hantera ytterligare administrativa steg, såsom fakturering, betalningsbekräftelser och eventuella tvister om avgiftsnivåer. Detta skulle kunna fördröja certifieringsprocessen och försvåra snabb introduktion av säkra produkter på marknaden. EU:s cybersäkerhetsakt syftar till att säkerställa att säkra produkter kan introduceras på marknaden så snabbt som möjligt. Fördröjningar i certifieringsprocessen skulle kunna motverka detta mål.

- **ge minskad transparens och förutsägbarhet:** Avgifter skulle kunna skapa osäkerhet och minskad transparens för företag, särskilt om avgiftsstrukturen är komplex eller svårförutsägbar. Företag skulle kunna ha svårt att förutse de totala kostnaderna för certifiering, vilket skulle kunna avskräcka dem från att delta i processen. Transparens och förutsägbarhet är avgörande för att företag ska kunna planera sina investeringar och säkerställa att de kan uppfylla kraven i cybersäkerhetsakten. Avgifter som är svåra att förutse skulle kunna underminera denna transparens.

  I Sverige betalar CAB:ar redan det nationella ackrediteringsorganet, NAB (i Sverige Swedac) för ackreditering och den nationella myndigheten för cybersäkerhetscertifiering, NCCA (i Sverige FMV) för s.k. bemyndigande och planerad tillsyn. I vissa länder, där certifieringsorganen är offentliga, är certifiering gratis. Medlemsstaterna ska själva kunna välja utifrån sina respektive avgiftsmodeller för genomförande.

- **verka hämmande för svensk cybersäkerhet:** Utredningar har också pekat på att avgifter skulle kunna leda till att organen för bedömning av överensstämmelse prioriterar lönsamma uppdrag framför sådana som är viktiga för samhället, vilket skulle kunna äventyra kvaliteten och oberoendet i bedömningsprocessen. Det kan vara viktigt för svenska kunder att evaluering och certifiering av cybersäkerhet utförs av svenska företag. Det är en fråga om tillit, särskilt vid statens (t.ex. försvarets) upphandlingar.

- **motverka EU:s mål om en enad digital marknad och ömsesidighet globalt:** EU:s cybersäkerhetsakt syftar till att skapa en enad digital marknad med höga säkerhets-standarder. Avgifter på organ för bedömning av överensstämmelse skulle kunna skapa fragmentering och olikheter mellan medlemsstaterna, eftersom avgiftsnivåer och strukturer skulle kunna variera mellan länder. Detta skulle kunna leda till att företag möter olika kostnader beroende på var de certifierar sina produkter, vilket skulle motverka målet om en enad och konkurrenskraftig inre marknad. KOM har betonat vikten av harmoniserade regler för att undvika sådana skillnader. Dessutom, inom motsvarande system för certifiering internationellt (CCRA) för IT-produkter (det enda område där vi så här långt har en certifieringsordning baserad på cybersäkerhetsakten) tas inga avgifter ut. Att

avgiftsbelägga i Sverige skulle därmed skapa en konkurrensnackdel visavi aktörer från tredjeländer.

Avgifter på organ för bedömning av överensstämmelse skulle kunna leda till ojämlik behandling av företag, särskilt om avgiftsnivåerna inte anpassas efter företagens storlek och ekonomiska förmåga. KOM har betonat att avgifter bör ta hänsyn till företagets storlek för att undvika orättvisa konkurrensförhållanden. Om avgifterna är proportionellt högre för mindre företag, skulle detta kunna skapa en konkurrensnackdel för SMF, vilket strider mot EU:s mål om en rättvis och inkluderande inre marknad.

Artikel 58 Kontaktpersoner från medlemsstater

I artikel 58 föreslås krav på att medlemsstater ska utse kontaktpersoner som utstationerade nationella experter vid Enisa och bestämmelser om deras roll vid byrån (artikel 58). FMV anser att kontaktpersoner som arbetar vid Enisa inte bör vara ett krav utan snarare en möjlighet som respektive medlemsstat själv beslutar kring. Det bör därför stå ”may” istället för ”shall”.

Artikel 73 Begäranden om en europeisk ordning för cybersäkerhetscertifiering

Artikel 73.2 [ECCG-begäran om en certifieringsordning]

Den nuvarande möjligheten för ECCG att rikta en begäran direkt till Enisa bör kvarstå.

Artikel 73.4 [KOM:s förberedelser för begäran av certifieringsordningar]

Det är bra att identifiera områden för certifieringsordningar och det allmänna syftet med ordningarna. Begäran bör dock inte föregripa arbetet från Enisa, intressenterna och den slutliga överenskommelsen och godkännandet från medlemsstaterna.

När det gäller tidsplaner har tidigare erfarenheter visat att KOM:s tidsplaner kan vara mycket optimistiska. Detta kan leda till den negativa effekten att man prioriterar hastigheten i framtagandet av ordningen framför dess kvalitet rörande cybersäkerhetsförbättringar.

Artikel 74 Utarbetande och antagande av europeiska ordningar för cybersäkerhetscertifiering

FMV stödjer ambitionen att effektivisera och förtydliga processerna för framtagandet av certifieringsordningar för cybersäkerhet. Det får dock inte ske på bekostnad av kvalitet. Ordningarnas syfte att höja cybersäkerheten är det överordnade målet.

Det föreslås nya tidsbestämmelser rörande stegen i framtagande av certifieringsordningar inklusive att framtagandet av nya ordningar ska ta högst tolv månader. FMV menar att tolv månader är för kort tid för att skapa en certifieringsordning med tillräcklig kvalitet som främjar cybersäkerhet. Jämför hur KOM vill kompromissa med säkerheten rörande den digitala identitetsplånboken för att möta uppsatta orimliga tidsfrister.

Artikel 74.2 [Tillfälliga arbetsgrupper]

Enisa föreslås fortsatt löpande samverka med relevant industri och andra parter, bl.a. genom tillfälliga arbetsgrupper (s.k. Ad Hoc Working Groups, AHWGs) dedikerade för detta.

FMV anser att det behövs en kontinuerlig dialog med relevanta intressenter under utvecklingen av certifieringsordningar. Att använda dessa tillfälliga arbetsgrupper är väl etablerat och är i grunden bra men FMV anser att man ska verka för att de ska vara mer öppna och inkluderande samt öppna för fler, åtminstone med observatörsstatus.

Artikel 74.5–6 [ECCG-medlemsyttranden]

I artikel 74.5 föreslås att innan Enisa översänder förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer till KOM ska byrån begära att medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering lämnar skriftliga yttranden om förslaget till certifieringsordning.

Att enskilda ECCG-delegaters ska lämna synpunkter istället för ett gemensamt yttrande är en förändring jämfört med dagens CSA. Dessa synpunkter kan Enisa få när som helst även utan denna reglering och FMV anser att ECCG-yttrande ska vara gemensamt för hela ECCG, precis som det regleras i dagens CSA. Ett skäl till det är att om de 27 ländernas åsikter skiljer sig åt kan det bli svårt för Enisa att jämka ihop det på 30 dagar. Det blir då svårt för Enisa att avgöra vad som är ”endorsed” givet att det inte ges något gemensamt ECCG-yttrande.

Art 77 Tekniska specifikationer i europeiska ordningar för cybersäkerhetscertifiering

I förslagen stärks Enisas möjlighet att ta fram egna tekniska specifikationer som kan ligga till grund för nya certifieringsordningar, t.ex. om tillämpliga harmoniserade internationella standarder eller europeiska standarder bedöms saknas.

FMV anser att ordningarna i första hand ska bygga på harmoniserade standarder, alternativt tekniska specifikationer som tas fram enligt Annex 2 i Standardiseringsförordningen 1025/2012. Undantag kan medges för assuransnivå ”hög” under förutsättning att vad som anges i skäl 76 i CSA iakttas (att det finns motiverade skäl och att dessa publiceras).

FMV anser att tekniska specifikationer, oavsett hur och av vem de tas fram, behöver tas fram med samma öppenhet och noggrannhet som standarder. Den process som beskrivs i denna förordning är inte tillnärmelsevis lika grundlig och bra. Ser man till att det finns en sådan process för Enisas utkast till specifikationer har man i princip skapat en process lika tung som standardisering varför man då lika gärna kan hänvisa endast till standarder. Avvikelser från detta skapar dåliga standarder som förvrider marknaden.

Otydlighet och exkludering avseende hur specifikationer tas fram bör sättas i relation till avtalet om Technical Barriers to Trade (TBT) inom WTO.

Artikel 77. 4 [Hemliga specifikationer]

I artikel 77.4 föreslås att ” I vederbörligen motiverade fall, särskilt om de tekniska specifikationerna innehåller information som skulle kunna äventyra säkerheten för certifierade IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, ska de distribueras endast till de intressenter som berörs av certifieringsordningens krav. Det ska inte hänvisas till sådana tekniska specifikationer i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.”

FMV emotsätter sig detta starkt. Pekar man mot specifikationer som krav för regelefterlevnad kan de inte vara hemliga för någon, varken för utvecklare, CAB:ar eller kunder.

Artikel 80 Säkerhetsmålen för europeiska ordningar för cybersäkerhetscertifiering

Det föreslås en utökning av de säkerhetsmål som certifieringsordningar ska eftersträva, bl.a. i syfte att harmonisera ordningarna med nya bestämmelser i EU:s cyberresiliensförordning (CRA) och NIS2D.

FMV stödjer att cybersäkerhetsmål (respektive cybersäkerhetskrav) i certifieringsordningarna i möjligaste mån mappar mot motsvarande mål och krav i EU:s sektorslagstiftning för cybersäkerhet. Certifiering kan dock ”bara” visa att vissa saker testats, på ett visst sätt av kompetent/ackrediterad personal som av NAB bedömts tillräckligt kompetent att utföra detta.

Nuvarande CSA klargör att en certifiering inte innebär ett intyg om säkerhet. Ett certifikat visar ”bara” att något evaluerats/certifierats på ett särskilt sätt av kompetent/ackrediterat organ vilket ”bara” visar assurans på viss nivå, inte säkerhet, vilket krävs för efterlevnad av cybersäkerhets-kraven i NIS2D eller sektorslagstiftning. De nya förslagen går på tvärs med detta etablerade (och enda rimliga) synsätt. FMV menar att det behövs mer analys av vad det är KOM tänker sig ska certifieras.

Artikel 81 Komponenter i europeiska ordningar för cybersäkerhetscertifiering

Artikel 81.3 d) [Verksamhet utanför EES]

Det föreslås att certifieringsordningar ska innehålla: ”Klargörande av vilka verksamheter för bedömning av överensstämmelse, såsom kalibrering, testning, certifiering och kontroll, för assuransnivå hög, eller för påvisande av regelefterlevnad och beviljande av presumtion om överensstämmelse, som är tillåtna utanför Europeiska ekonomiska samarbetsområdet (EES).”

FMV ifrågasätter om skälen till denna artikel, som anges i recit 104 (upphovsrätt och att inte omfattas av NIS2D), är helt giltiga. Om de vore giltiga, skulle samma skäl också kunna hindra ömsesidigt erkännande med tredje länder (om de framförde samma argument mot EU). Således, om denna artikel ska bevaras, bör de angivna skälen också gälla i en ömsesidig erkännandekontext, och begränsas till rent tekniska skäl.

Artikel 85 Utfärdande av europeiska cybersäkerhetscertifikat

Artikel 85.4 [Certifieringsaktiviteter vs tillsynsaktiviteter]

För FMV är det viktigt att allt som innebär att NCCA på något sätt överprövar CAB:arnas evalueringar/certifieringar rörande cybersäkerhet ska betraktas som certifieringsaktiviteter. Detta verkar, efter diskussioner i ECCG och motstridiga besked, även vara KOM:s inställning. Sverige bör dock säkerställa att det fortfarande blir så och att det är detta som är intentionen i förslaget här.

Eftersom vi i Sverige har valt att ha privata CAB:ar vill FMV inte hamna i en situation där NCCA (eller annan tillsynsmyndighet) tvingas överpröva evalueringar/certifieringar rörande cybersäkerhet. Det rimmar illa med vår roll som tillsynsorgan och det skapar oproportionellt dubbelarbete för såväl myndigheter som ackrediteringsorgan och CAB:ar. FMV förordar att vi endast kontrollerar att vederbörliga processer/formalia är uppfyllda, även om det är assuransnivå ”high”. På motsvarande sätt vill vi att regelverket tillåter oss att förlita oss på NAB:ens/Swedacs bedömningar kring cybersäkerhetskompetens etc. vid ackreditering och att FMV i vår roll som NCCA inte förväntas överpröva något i dessa delar vid ett bemyndigande. Återigen, FMV ska endast kontrollera att vederbörliga processer/formalia är uppfyllda.

Artikel 85.9 [Komponenter från högriskleverantörer]

Det föreslås i artikel 85.9 att för deras certifierade IKT-produkter, IKT-tjänster, IKT-processer eller hanterade säkerhetstjänster som identifierats, för hela eller delar av dem, som nyckeltillgångar enligt artikel 102, får innehavare av ett europeiskt cybersäkerhetscertifikat inte använda, installera eller på annat sätt integrera IKT-komponenter eller komponenter som inkluderar IKT-komponenter från högriskleverantörer i certifierade IKT-produkter, IKT-tjänster, IKT-processer eller hanterade säkerhetstjänster.

FMV stödjer ambitionen att högriskleverantörer inte används i certifierade produkter eller tjänster (eller NIS2D-entiteter). Det är emellertid svårt att se hur man ska kunna göra den bedömningen på ett inte alltför kostsamt sätt. Det är viktigt att medlemsstaterna får starkt inflytande i bedömningarna, t.ex. genom bibehållen beslutsprocedur i ECCC-kommittén som antar genomförandeakterna under CSA, om vilka som är högriskleverantörer och varför. Dessa bedömningar ska inte behöva göras av CAB:arna inom de olika certifieringsordningarna och inte heller av medlemsstaternas NCCA:er. Det ska finnas färdiga bedömningar att förhålla sig till.

Artikel 86 Nationella ordningar och certifikat för cybersäkerhetscertifiering

Artikel 86.5 [Företräde för EU:s certifieringsordningar]

Jämfört med nuvarande CSA föreslås tydligare skrivningar rörande företräde för europeiska certifieringsordningr framför nationella certordningar. Bland annat föreslås KOM kunna be medlemsstater att upphäva en nationell certifieringsordning. Enligt dagens CSA gäller redan att EU-ordningar ”släcker” nationella ordningar. Vissa medlemsstater har dock ansett att certifierings-objekt (exv. vissa IKT-produkter/IKT-tjänster) och/eller höga assuransnivåer rörande produkter/tjänster som inte redan täcks fortsatt bör kunna vara föremål för nationella ordningar.

FMV håller med om det senare bl.a. eftersom det går i linje med att vi kan ställa striktare krav i certifieringar och upphandlingar för t.ex. nationell säkerhet och säkerhetsskydd.

Artikel 88 Nationella myndigheter för cybersäkerhetscertifiering

Artikel 88.6. g) [Ytterligare eller specifika krav" för bemyndigande]

De "ytterligare eller specifika kraven" som det hänvisas till kan också, eller lika bra, kontrolleras vid ackrediteringen. Det nationella ackrediteringsorganet, NAB (i Sverige Swedac) har eller kan anskaffa nödvändig kompetens. Bemyndigande skapar fördröjningar och kostnader för alla inblandade, utan att bidra till särskilt mycket mer cybersäkerhet.

Artikel 92 Ytterligare harmonisering av befogenheterna för organen för bedömning av överensstämmelse

Se artikel 88.6 g) ovan.

En anledning till att behålla möjligheten till bemyndigande är för undantagsfall, t.ex. om det är nödvändigt för att uppfylla EU:s åtaganden rörande ömsesidigt erkännande, främst visavi CCRA.

Artikel 94 Ifrågasättande av kompetensen hos organen för bedömning av överensstämmelse

Artikel 94.2 [Avseende anmälan]

Notifiering/Anmälan baserar sig antingen på certifieringen (stödd av stipulerad dokumentation) från CB eller bemyndigandet (stödd av stipulerad dokumentation) från NAB.

Förslaget är rimligt så länge det handlar om att ge KOM information som NCCA redan har. KOM bör inte kunna tvinga NCCA att ha eller hämta in information den inte anser sig behöva det för sina NCCA-uppgifter.

Artikel 94.5 [Avseende rätten att överklaga]

Rätten att överklaga borde istället regleras i Artikel 96 tillsammans med övriga överklagande-möjligheter.

Rörande CSA är det dessutom felriktat att hänga upp det på notifieringen/anmälan eftersom denna inom CSA, till skillnad från övriga ackrediteringsvärlden, inte är en förutsättning för att få ge ut certifikat.

Artikel 95 Informations- och lagringsskyldighet för organ för bedömning av överensstämmelse

Artikel 95.3 [Konfidentialitet]

Ansökningar om ackrediteringar är konfidentiella p.g.a. affärssekretess. Beslut om ackreditering görs offentliga i NANDO och på Enisas webbplats.

Artikel 98–117 [Ramverk för en betrodd IKT-leveranskedja]

KOM föreslår ett nytt ramverk för att adressera icke-tekniska risker i IKT-leveranskedjor i högkritiska sektorer och andra kritiska sektorer enligt NIS2D Mekanismen som föreslås syfta 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 NIS 2-direktivet.

FMV ser ett potentiellt behov av att NIS2-entiteter analyserar sina leveranskedjor och vidtar åtgärder för att säkra dem. Frågan är dock om det är rimligt att tro att någon hela tiden kan ha sådan insyn och kontroll i sina leveranskedjor att det kan hanteras tillräckligt bra med tekniska säkerhetsåtgärder.

FMV kan, gällande kapitel IV Säkerhet i leveranskedjor, se positivt på att det skapas en förmåga att värna EU:s digitala suveränitet. Samtidigt kan detta instrument, när det används, komma att få långtgående konsekvenser för såväl samhällets funktionalitet som för medlemsstaternas ekonomier. FMV bedömer att det är mycket viktigt att medlemsstaterna ges skarpa mandat att på olika sätt kunna påverka när och hur detta instrument används.

Ramverket tar sin utgångspunkt i artikel 22 i NIS 2-direktivet om samordnade säkerhetsrisk-bedömningar 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 KOM, 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.

FMV anser att om KOM ges rätt att anta genomförandeakter på detta område blir det extra viktigt att behålla nuvarande kommittologiförfarande (ref. till artikel 5.4 i kommittologiförordningen och därmed möjlighet till blockerande minoritet, jfr. nedan om art. 118).

Det som rör nationell säkerhet är undantaget och detsamma gäller förmodligen rörande produkter för dubbla användningsområden (”dual use”). Annars bör Sverige verka för att det blir undantaget så att vi har egen rådighet i frågan. Enligt förslaget ska åtgärder som vidtas utifrån ramverket inte hindra medlemsstater från att anta eller bibehålla nationella bestämmelser för att säkerställa ett högre skydd, vilket FMV stödjer.

Det föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att delta i offentliga upphandlingar inom EU som rör tillhandahållande av komponenter för viktiga IKT-tillgångar. FMV anser att en medlemsstat alltid själv ska kunna upphandla det den anser sig behöva för nationell säkerhet, säkerhetsskydd, etc. även rörande produkter för dubbla användningsområden.

Det föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att ta del av EU-finansiering, vilket FMV i princip stödjer.

Därtill föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att delta i europeiskt standardiseringsarbete. FMV förespråkar i princip att hela välden är inblandad i all standardisering, både för att nyttja allas kompetens och för att få sälja på allas marknader. Det är också i den globala prövningen av cybersäkerhetskrav som det kan säkerställas att det görs en så omfattande analys som möjligt och att det som standardiseras används överallt.

Artikel 118 Kommittéförfarande

I artikel 118.2 föreslås beslutsproceduren i artikel 5 i kommittologiförordningen. I dagens CSA gör man en referens till endast artikel 5.4. Det nya förslaget innebär att KOM ändrar till normalförfarandet där det krävs en kvalificerad majoritet av medlemsstaterna emot KOM:s förslag till genomförandeakt för att stoppa det. Detta ger medlemsstaterna betydligt mindre inflytande än idag (då det räcker med blockerande minoritet) trots att man lagt till en rad genomförandeakter som rör förhållandevis genomgripande saker som kan påverka hur medlemsstaterna valt att arbeta.

FMV förordar kraftigt att befintlig beslutsprocedur fortsätter gälla.

EU-kommissionens befogenheter att anta genomförandeakter

KOM föreslås få nya möjligheter att anta genomförandeakter jämfört med idag.

- 81.5: gemensamma principer och standardbestämmelser för komponenter i en certifieringsordning

Kan vara bra i princip, för tydlighet och harmonisering. Dock kan mer analys och bevakning behövas så att det inte blir för stelbent givet att det i framtiden kan bli fråga om många olika typer av saker som ska certifieras.

- 85.5: specificerar förfaranden för modeller med förhandsgodkännande eller allmän delegering

Att specificera processerna kan vara bra men FMV vill inte att man denna väg kan tvinga fram överprövningar av de evalueringar/certifieringar som CAB:ar redan gjort. Det skapar dubbelarbete och merkostnader för alla berörda. Ett NCCA ska dessutom inte kunna tvingas ägna sig åt tekniska utvärderingar. Det skulle i princip innebära att man (åtminstone delvis) tvingar fram ett statligt certifieringsorgan.

- 87.1: internationellt erkännande av europeiska cybersäkerhetscertifikat

Det finns inget ömsesidigt erkännande idag mellan EUCC-certifikat och CCRA-certifikat, däremot hur systemen ska kunna samspela. FMV förordar initialt att vi emotsätter oss genomförandeakter på detta område.

- 92.8: förfarandena, inbegripet för gränsöverskridande samarbete, för auktorisering av organ för bedömning av överensstämmelse

  Att specificera processerna kan vara bra. Men man skulle kunna lägga till något om att dessa genomförandeakter inte ska påverka nationell suveränitet rörande vår offentligrätt eller förvaltningsrätt, t.ex. inte göra gränsöverskridande samarbete tvingande.

- 100.2: beteckna tredjelande som ett land som utgör ett cybersäkerhetsproblem för IKT-leveranskedjorna

  Genomförandeförordningar skapar harmoniserade bedömningar men medlemsstaterna kan ha väldigt olika uppfattningar om vilka länder som utgör problem. Att låta KOM anta genomförandeförordningar innebär att man avhänder sig medlemsstaterna möjligheten att göra dessa bedömningar själva. Det är därför extra viktigt att behålla nuvarande kommittologi-procedur i denna fråga.

NIS2-direktivet

Fullharmonisering rörande säkerhetsåtgärder

Ändringarna rörande Enisas och KOMs uppgifter rör inte certifieringsramverket direkt. Dock föreslås att i det fall KOM antar genomförandeakter får medlemsstaterna inte införa ytterligare nationella krav avseende de åtgärder som avses i artikel 21.2 i NIS 2-direktivet (s.k. fullharmonisering).

FMV anser att Sverige inte bör acceptera fullharmonisering rörande NIS2-direktivets cyber-säkerhetsåtgärder. Ett starkt skäl för detta är att många av de infrastrukturer som täcks av direktivet även har militära användningsområden och medlemsstaterna har exklusiv kompetens rörande nationell säkerhet. Medlemsstaterna måste kunna avgöra själva om de behöver ställa högre cybersäkerhetskrav än den miniminivå som kan vara bra att reglera på EU-nivå. Vissa av medlemsstaterna har också en starkare hotbild både för militära hot och hybridhot än andra medlemsstater.

I remissvar (25FMV7305-3) till Myndigheten för samhällsskydd och beredskap, numera Myndigheten för civilt försvar (MCF), avseende förslag till nya föreskrifter enligt ny cybersäkerhetslag hänvisade FMV till att KOM har mandat att anta genomförandeakter avseende dylika cybersäkerhetsåtgärder. Om förslaget går igenom, dvs att dessa cybersäkerhetsåtgärder inte får gå utöver de som stipuleras i kommande genomförandeförordning, blir det viktigt att bevaka dels att genomförandeåtgärderna ger utrymme för den nationella lagstiftning vi vill ha på området, dels att MCF (eller FRA/NCSC om ärendet går vidare till dem) beaktar denna fullharmonisering om och när de antar föreskrifterna. Detta kan också avse ländernas rätt att införa krav på olika typer av certifieringar som kommer finnas baserade på CSA.

Ärendet

I den slutliga handläggningen har jurist Karin Adamsson och rådgivare Jörgen Samuelsson deltagit. Jörgen Samuelsson har varit föredragande.

Försvarets materielverk

Håkan Lombrink
Tf Chefsjurist

Sändlista

Regeringskansliet (Försvarsdepartementet)

Kopia till

Christina Knutsson Hamrén (Försvarsdepartementet)
Lednings- och ekonomistaben
Juridik- och säkerhetsstaben
Arkiv