REMISSVAR

Datum	Diarienummer	Ärendetyp
2024-05-24	24FMV2092-2	1.3
	Dokumentnummer	Sida
		1(10)

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Er referens	Ert datum	Er beteckning
Klara Lidman Kittel	2024-03-06	Fö2024/00496

Svar på remissen Nya regler om cybersäkerhet (SOU 2024:18)

Sammanfattning

Försvarsdepartementet har den 3 mars 2024 (Fö2024/00496) remitterat delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18). Försvarets materielverk (FMV) har tagit del av betänkandet och lämnar i detta remissvar synpunkter på utredningens förslag.

FMV delar utredningens bedömning att det i många avseenden kan vara sektors- och tillsynsmyndigheterna som bäst kan bedöma vilka föreskrifter som är lämpliga (effektiva och proportionerliga) inom sin sektor och dess marknad. FMV delar också utredningens förslag att det i lagen är tydligt att skyldighet att lämna uppgifter inte gäller uppgifter som är säkerhetsskyddsklassificerade.

Dock är det FMV:s uppfattning att det bör övervägas att stödet till myndigheter med ansvar för föreskrifter och tillsyn utökas utöver vad som föreslås i utredningen. Ett sådant stöd kan utformas i enlighet med vad som beskrivs närmare i FMV:s rapport till regeringen ”Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt” (23FMV2840-8).

FMV framhåller att utredningen inte har belyst att det är en mycket stor utmaning för de föreslagna förskrifts- och tillsynsmyndigheterna att var och en etablera och upprätthålla den kompetens som är nödvändig för att utforma sektorsanpassade riskhanteringsåtgärder och ett systematiskt riskbaserat informationssäkerhetsarbete.

Sammanfattningsvis har FMV synpunkter som omfattar avsnitten:

- Alternativt förslag
- Certifiering
- Tillsynsmyndigheter i Sverige
- Föreskrifter
- Tillsynsmyndighetens undersökningsbefogenheter
- Tillfälligt upphävande av auktorisation eller certifiering

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

Avsnitt 5.2.11 Alternativt förslag

Myndigheten för samhällsskydd och beredskap (MSB), Säkerhetspolisen, Transportstyrelsen och Integritetsmyndigheten (IMY) har framfört till utredningen att det bör finnas en gemensam föreskrift med grundkrav som gäller för samtliga sektorer i syfte att konkretisera de riskhanteringsåtgärder som anges i cybersäkerhetslagen. Enligt myndigheterna är det ingen större skillnad på grundkraven som kan ställas rörande nätverks- och informationssystem oavsett sektor.

Dessa grundkrav skulle i en sådan lösning kunna kompletteras av tillsynsmyndigheterna som också skulle ha föreskriftsrätt för respektive tillsynsområde. Detta skulle kunna utformas på motsvarande sätt som i säkerhetsskyddsregleringen där Säkerhetspolisen och Försvarsmakten får meddela föreskrifter om bland annat säkerhetsskyddsåtgärder och övriga tillsynsmyndigheter får meddela kompletterande föreskrifter inom sitt tillsynsområde.

Till utredningen har från MSB föreslagits att hela den offentliga sektorn, dvs. samtliga statliga myndigheter, regioner och kommuner som utgångspunkt borde omfattas av cybersäkerhetslagen för att säkerställa ett allriskperspektiv. NIS-direktivets krav skulle enligt en sådan modell utgöra en lämplig ”bottenplatta", som i förekommande fall kan kompletteras av säkerhetsskyddsregleringens bestämmelser.

Utredningen har därför övervägt om ansvaret för att ge ut föreskrifter bör flyttas från tillsynsmyndigheterna till MSB. Detta skulle innebära att det beslutas om en gemensam föreskrift som gäller för samtliga sektorer vilket skulle ge en enhetlig reglering vilket i sin tur skulle underlätta och effektivisera organiseringen av cybersäkerheten för verksamhetsutövare som bedriver verksamhet i flera sektorer.

FMV har förståelse för utredningens uppfattning att tidsramen begränsar utrymmet för att inom utredningen utreda att tillämpningsområdet utökas avseende bl.a. överföring av föreskriftsrätt till en annan myndighet och frågan om etablerandet av en ”bottenplatta” som skulle kunna utgöra grund även för säkerhetsskyddslagstiftningen.

FMV anser emellertid att frågan om hur regelverk för cybersäkerhet organiseras och styrs inom staten för att undvika regelfragmentering och ojämn tillämpning är mycket angelägen och omgående behöver utredas vidare. I ett sådant utredningsarbete bör FMV:s rapport avseende uppdragsredovisning till regeringen i form av ”Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt” (23FMV2840-8)[1] beaktas.

[1] FMV:s svar på regeringsuppdrag avseende att föreslå hur nationella behov kan tillgodoses vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetakt (Fö2021/00796, 2023-05-11).

Avsnitt 7.4 Certifiering

I direktiven till utredningen anges att NIS2-direktivet skärper kraven på väsentliga och viktiga entiteter vad gäller riskhanteringsåtgärder, i nuvarande lagstiftning benämnda som säkerhetsåtgärder och rapporteringsskyldigheter. Medlemsstaterna ska säkerställa att entiteterna vidtar tekniska, operationella och organisatoriska åtgärder för att hantera risker för säkerheten i nätverks- och informationssystem. Direktivet fastställer vissa minimikrav på åtgärder som entiteterna ska vidta. Kraven omfattar bl.a. rutiner för riskanalys och säkerhet i informationssystem.

Enligt direktivet får medlemsstaterna bestämma att entiteter som ett led i riskhanteringen ska använda särskilda certifierade produkter i nätverks- och informationssystem.
Enligt direktiven ska utredaren analysera hur ändamålsenlighet och proportionalitet i sådana föreskrifter kan beaktas samt hur de ska meddelas.

Utredningen har, utöver att redovisa tillämpliga författningsbestämmelser, inte närmare analyserat om cybersäkerhetsnivån nationellt är otillräcklig och därför kan aktualisera ett behov av att införa nationella krav på certifiering av IKT[2]-produkter och -tjänster på det nu aktuella området, oaktat Europeiska kommissionens framtida ställningstagande i frågan om delegerade akter.

FMV kan notera att det av flera nationella offentliga utredningar och myndighetsrapporter framkommer att det mer allmänt föreligger mer eller mindre allvarliga säkerhetsbrister i informations- och nätverkssystem hos många offentliga och enskilda verksamhetsutövare, också på NIS2-området, vilket har möjliggjort och möjliggör cyberangrepp med allvarliga konsekvenser som följd. Av nämnda utredningar och rapporter, och i belysning av omvärldsutvecklingen, kan slutsatsen dras att det föreligger ett angeläget behov av att med olika tillgängliga åtgärder stärka skyddet av informations- och nätverkssystem inom NIS2-direktivets tillämpningsområde. Cybersäkerhetsutredningen[3] framhöll att certifiering av IKT-produkter och IKT-tjänster är en av flera åtgärder som bör vidas för att öka säkerheten i informations- och nätverkssystem.

FMV anser att syftet med och tillämpning av artikel 24.1 i NIS2-direktivet inte kan anses förutsätta att kommissionen, som utredningens slutsats får förstås, först konstaterar att cybersäkerhetsnivån är otillräcklig och att en konsekvensanalys föreligger.

FMV anser att förslag på åtgärder som syftar till att stärka säkerheten i informations- och nätverkssystem bör grundas på att det föreligger brister i denna säkerhet alternativt att det finns skäl att ytterligare förstärka säkerheten för att motverka eventuella framtida hot, sårbarheter och risker. Det är verksamhetsutövarens ansvar att bedöma hot, sårbarheter och risker i informations- och nätverkssystem och vilka säkerhetsåtgärder som ska införas. Det är samtidigt en stor utmaning för varje verksamhetsutövare att göra en hotbilds-, sårbarhets- och riskbedömning till grund för behov av säkerhetsåtgärder och att såväl etablera som upprätthålla tillräcklig kompetens inom cybersäkerhet, attackvägar, säkerhetsåtgärder, certifiering, m.m.

---

[2] Informations- och kommunikationsteknik.
[3] SOU 2020:58/SOU 2021:63.

FMV kan notera att i NIS2-direktivet anges bl.a. att *"…för att påvisa efterlevnaden av riskhanteringsåtgärder för cybersäkerhet, och i frånvaro av lämpliga europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881, bör…medlemsstaterna främja användningen av relevanta europeiska och internationella standarder bland väsentliga och viktiga entiteter, eller så får de ålägga entiteter att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer"*. Det kan i detta sammanhang noteras att inom ramen för förordning (EU) 2019/881[4] har en frivillig europeisk certifieringsordning (EUCC[5]) för IKT-produkter antagits under 2024 och som börjar tillämpas fullt ut 2025 samt att en motsvarande ordning för molntjänster (EUCS[6]) är under framtagande och bedöms kunna tillämpas 2025/26.

Även en certifieringsordning för 5G är under framtagande. Vidare pågår diskussioner om att utveckla fler europeiska cybersäkerhetscertifieringsordningar i enlighet med Cybersäkerhetsakten (jfr. " Union Rolling Work Programme for European cybersecurity certification" - URWP). URWP pekar främst på e-plånböcker (jfr. eIDAS-förordningen), hanterade säkerhetstjänster (jfr. nedan om utvidgningen av Cybersäkerhetsakten) samt produkter med digitala element (jfr. Cyberresiliensakten, CRA) om inte dessa produkter kan certifieras redan inom de andra certifieringsordningarna.

Vidare undersöker Enisa[7] hur uppfyllande av cybersäkerhetskrav rörande artificiell intelligens (inom vissa särskilt undersökta sektorer) ska kunna visas med stöd av cybersäkerhetscertifiering (jfr. AI-akten).

FMV delar inte utredningens slutsats att det är rimligt att avvakta kommissionens beslut om behov av certifieringskrav eftersom sådana krav ska införas först om cybersäkerhetsnivån bedöms vara otillräcklig och ska dessutom föregås av bland annat en konsekvensanalys. Det finns ett antal EU-regleringar på cyberområdet som framhåller certifiering av IKT-produkter och -tjänster som ett sätt att visa uppfyllnad av vissa närmare angivna krav på cybersäkerhet. Samtidigt bör det noteras att det är flera olika faktorer som påverkar hur nationella behov för ökad cybersäkerhet kan identifieras och omsättas till säkerhetskrav som kan bedömas och prövas med stöd av olika certifieringsordningar inom det europeiska ramverket för cybersäkerhetscertifiering.

Myndigheten anser att frågan om ett behov av krav på certifiering av IKT-produkter, - tjänster eller -processer som används av väsentliga eller viktiga verksamhetsutövare inom tillämpningsområdet för NIS2 (den föreslagna cybersäkerhetslagen), i första hand bör analyseras i ett nationellt sammanhang och om behov bedöms föreligga så kan frågan därefter även prövas mot bakgrund av om kommissionen finner behov av att anta delegerade akter på området. Det är först när kommissionen antar delegerade akter och som också omfattar ett nationellt behov som det saknas skäl för att införa en nationell reglering på området.

---

[4] Cybersäkerhetsakten.
[5] European Cybersecurity Certification Scheme.
[6] European Cybersecurity Certification Scheme for Cloud Services.
[7] European Union Agency for Cybersecurity.

Krav på certifiering nationellt förutsätter dock en mycket god förmåga, samt tillräckligt med resurser, för att analysera behoven och påverka certifieringsordningarna och standarderna så att de möter sådana behov. Dessa krav behöver analyseras för alla berörda sektorer, varför det behöver göras tydligt vilka myndigheter som bör ha ansvar, leda och/eller samverka i detta arbete. Detta beskrivs närmare i FMV:s rapport (uppdragsredovisning) till regeringen ”Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt” (23FMV2840-8).

FMV vill framhålla att när det gäller frågan om att analysera hur ändamålsenlighet och proportionalitet i eventuella föreskrifter om krav på certifierade produkter och tjänster inom NIS2 tillämpningsområdet samt hur de ska meddelas, kan det noteras att dessa frågor till del behandlades av Cybersäkerhetsutredningen (SOU 2021:63) och att den utredningen gjorde bedömningen att den aktuella lagstiftningen medger att berörda myndigheter i form av föreskrifter kan ställa krav på användning av certifierade produkter och tjänster inom berört ansvarsområde, även om några sådana krav det vid den tidpunkten ännu inte hade införts.

I avvaktan på att kommissionen indikerar att frågan om delegerade akter är aktuell anser FMV att frågan om nationella krav på certifiering enligt europeiska certifieringsordningar inom ramen för den föreslagna cybersäkerhetslagen bör bli föremål för en djupare analys i det fortsatta lagstiftningsarbetet och som ett led i angelägna åtgärder för att stärka säkerheten i informations- och nätverkssystem hos verksamhetsutövare som omfattas av NIS2.

Avsnitt 8.4.2 Tillsynsmyndigheter i Sverige och avsnitt 8.4.5 Föreskrifter

Utredningen har övervägt om ansvaret för att ge ut föreskrifter bör flyttas från tillsynsmyndigheterna till MSB. Detta skulle innebära att det beslutas om en gemensam föreskrift som gäller för samtliga sektorer vilket skulle ge en enhetlig reglering och underlätta för verksamhetsutövare som bedriver verksamhet i flera sektorer.

Utredningen gör bedömningen att den myndighet som har tillsynsansvar och/eller föreskriftsrätt inom en sektor har typiskt sett bäst kunskaper om sektorn (och den privata marknad som därmed eventuellt är aktuell) i fråga och därmed bäst förutsättningar att veta vilken tillsyn som är möjlig, lämplig och effektiv. Utredningen anser även att det är tillsynsmyndigheterna som bäst kan bedöma vilka föreskrifter som är lämpliga (effektiva men proportionerliga) inom sin sektor och dess marknad. Därför bör sektorsmyndigheterna på relevant nivå representera sin sektor vid utformningen av EU-regleringen på området. Detta avser typiskt sett att bistå regeringen vid EU-förhandlingar i rådet eller att inom kommittéväsendet bistå regeringen eller själva representera Sverige vid framtagandet av delegerad eller genomförande lagstiftning.

För att motverka risken för fragmentering av föreskrifter och ojämn tillämpning av tillsyn föreslår utredningen att MSB även fortsättningsvis ska leda ett samarbetsforum där tillsynsmyndigheterna ingår, samt föreslås ges uppdraget att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete.

FMV:s delar utredningens bedömning att det i många avseenden kan vara sektors- och tillsynsmyndigheterna som bäst kan bedöma vilka föreskrifter som är lämpliga (effektiva och proportionerliga) inom sin sektor och dess marknad.

Dock framhåller FMV att det är en mycket stor utmaning för de föreslagna förskrifts- och tillsynsmyndigheterna att var och en etablera och upprätthålla den kompetens som är nödvändig för att utforma sektorsanpassade riskhanteringsåtgärder och ett systematiskt riskbaserat informationssäkerhetsarbete. Denna kompetens omfattar bl.a. kunskap om IKT, cybersäkerhet, risker för sårbarheter och attacker, effektiva säkerhetsåtgärder, effektiva kontrollmetoder och certifiering samt förmågan att för egna sektorns intressen påverka relevanta standarder och certifieringsordningar. Denna kompetens behöver även etableras och kontinuerligt finnas tillgänglig hos de olika tillsynsmyndigheterna för att de över tiden och för det stora antalet verksamhetsutövare ska kunna genomföra en sådan tillsyn som leder till den cybersäkerhet som är syftet med NIS2.

FMV ser att ett samarbetsforum för tillsynsmyndigheterna, och den vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete som ska utvecklas, riskerar att bli otillräckligt ur ett kompetens- och resurssättningsperspektiv.

FMV ser en likaledes påtaglig risk för att föreskrifter och tillsyn med den föreslagna modellen blir fragmenterad och ojämnt tillämpad samt att kompetensen inom området sprids på allt för många ansvariga myndigheter vilket även kan medföra en kompetensbrist inom området. vilket även framkommit i utvärderingar av det nuvarande NIS-direktivets genomförande och tillämpning.

Myndighetens uppfattning är att det behövs ett utvecklat stöd till föreskrifts- och tillsynsmyndigheterna utöver vad som föreslås i utredningen. Ett sådant stöd bör utformas i enlighet med vad som beskrivs närmare i FMV:s rapport (uppdragsredovisning) till regeringen ”Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt” (23FMV2840-8).

En sådan funktion kan utgöra ett samlat expertstöd till förskrifts- och tillsynsmyndigheter angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov av riskhanteringsåtgärderna som anges i artikel 21. Sådana riskhanteringsåtgärder behöver omsättas i mer detaljerade krav på t.ex. säkerhetsegenskaperna hos IKT-produkter, krypteringslösningar, arkitektur, drift, inhyrda tjänster (exempelvis molntjänster), AI, Internet of Things, underhåll, övervakning och lämpliga kontrollmetoder (inkl. certifiering) samt därtill relaterade standarder. FMV ser det som mindre rimligt att alla dessa olika kompetenser och förmågor kan etableras med tillräcklig expertis och i tillräcklig mängd separat hos var och en av de 11 myndigheter som ges ansvar för föreskrifter och tillsyn.

En stödfunktion som den som föreslås kan samverka med sektorsmyndigheterna och tillsammans med dessa bevaka eller proaktivt delta i eller påverka utvecklingen i relevanta standardiseringsorgan och certifieringsordningar.

Avsnitt 8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Utredningen föreslår att tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare. Enligt utredningen avses med oberoende organ exempelvis ett företag som genomför säkerhetsrevisioner. Organet ska vara oberoende i förhållande till tillsynsmyndigheten och den verksamhetsutövare vars verksamhet ska granskas. Organet ska ha den sakkunskap som krävs för säkerhetsrevisionen. Det är upp till tillsynsmyndigheten att bedöma om lämpliga organ som ska utföra säkerhetsrevisionen bör pekas ut i samband med åläggandet eller om det kan överlåtas till verksamhetsutövaren.

Om det, som framgår av utredningen (s. 237), är upp till tillsynsmyndigheten att avgöra vad som är ett oberoende organ så kan det ju leda till olika kvalitet i hur säkerhetsrevisioner genomförs. Ställer man krav på att ett sådant oberoende organ ska vara ackrediterat, dvs att ett företag eller en organisation får ett opartiskt och nationellt accepterat godkännande av att ha kompetens, system och rutiner för att utföra säkerhetsrevision, så blir det ju mer enhetligt än att vara utlämnad till tillsynsmyndighetens godtyckliga bedömning avseende vad som är ett oberoende organ (exempelvis i ett tillsynsärende).

FMV anser att sådana oberoende organ ska uppfylla fastställda krav på kompetens och organisation samt dessutom vara ackrediterade och behöriga att genomföra sådana säkerhetsrevisioner. Exempelvis ackrediterar SWEDAC[8] företag som erbjuder stöd och granskning av implementering av ledningssystem och standarder. Regeringen bör därför ge en myndighet uppgiften att verka för att sådana kriterier med tillhörande certifieringsordning, och som också adresserar svenska behov, utvecklas inom cybersäkerhetsaktens certifieringsramverk. Om en sådan certifieringsordning för företag som kan göra säkerhetsrevisioner etableras, kan företag med kompetens att göra säkerhetsrevisioner alltså certifieras (godkännas) och ställas under tillsyn inom ramen för cybersäkerhetsaktens regelverk.

Avsnitt 9.5.5 Tillfälligt upphävande av auktorisation eller certifiering

Av NIS-direktivet (skäl 133) framgår att för att de sanktioner som är tillämpliga på överträdelser av efterlevnadskontrollåtgärder i direktivet ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att, under vissa närmare angivna förutsättningar, tillfälligt upphäva eller begära tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls av en väsentlig entitet samt begära införande av ett tillfälligt förbud för en fysisk person som har ledningsansvar på nivån för verkställande direktör eller juridiskt ombud att utöva ledande funktioner.

---

[8] Swedish Board for Accreditation and Conformity Assessment - Styrelsen för ackreditering och teknisk kontroll

Sådana tillfälliga upphävanden eller förbud bör dock endast tillämpas som sista utväg, dvs. först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i direktivet har uttömts och endast fram till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka de tillfälliga upphävandena eller förbuden tillämpades. Vidare anges att införandet av sådana tillfälliga upphävanden eller förbud bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

Den angivna regleringen kommer till uttryck i artikel 32.5 a) i direktivet där det anges att medlemsstaterna ska säkerställa att de behöriga myndigheterna har befogenhet att tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten.

Kravet på medlemsstaterna att vidta åtgärder i enlighet med artikel 32.5 a) väcker frågan om hur en lämplig författningsreglering kan åstadkommas för att möta kraven i direktivet och samtidigt beakta regleringen i det europeiska ramverket för cybersäkerhetscertifiering[9] och tillämpliga europeiska certifieringsordningar (genomförandeförordningar). Exempelvis föreslås ett europeiskt certifikat för en molntjänst eller för de föreslagna hanterade säkerhetstjänsterna grundas på att vissa närmare angivna krav på kompetens- och säkerhetsfunktioner är uppfyllda.

Förordning EU 2019/881 och tillämpliga europeiska certifieringsordningar (genomförandeförordningar), utgör en lagkonstruktion som i sammanhanget kan anses utgöra *lex specialis* och som därför får anses uttömmande föreskriva förutsättningarna för utfärdande av certifikat och bemyndigande och när ett eventuellt återkallande av dessa ska vara möjligt.

När det gäller hanterade säkerhetstjänster, som tillhandahålls av specialiserade företag, ska noteras att de är avgörande för förebyggande, upptäckt och hantering av samt återhämtning från cybersäkerhetsincidenter. Exempel på sådana tjänster är upptäckt av eller hantering av incidenter, penetrationstestning, säkerhetsrevisioner eller rådgivning, dvs. sådana åtgärder för att stärka cybersäkerheten och som även anges i NIS2-direktivet. Medlemsländerna vill nu stärka EU:s cyberresiliens genom att även kunna anta europeiska ordningar för certifiering för hanterade säkerhetstjänster, varför en ändring i denna del av förordning (EU) 2019/881 är under absolut slutfas i sin slutliga behandling

NIS2-direktivet möjliggör för den utsedda myndigheten, dvs. enligt förslaget MSB, att besluta att sådana företag som certifierats med stöd av förordning (EU) 2019/881 och som tillhandhåller bl.a. angivna tjänster och berörda certifieringsorgan ska omfattas av NIS2 tillämpningsområde. Det ska dock noteras att prövningen av och beslut om certifiering av angivna företag sker enligt formerna och kraven som är angivna i det europeiska ramverket för cybersäkerhetscertifiering av självständiga ackrediterade organ för bedömning av överenstämmelse (evaluering- och certifieringsorgan) och att bemyndigande för ett sådant organ att utfärda certifikat på viss angiven assuransnivå kan komma att meddelas av den nationella myndigheten för cybersäkerhetscertifiering (FMV).

---

[9] Förordning EU 2019/881.

Det kan även noteras att de genomförandeförordningar som utfärdas inom ramen för det europeiska ramverket för cybersäkerhetscertifiering innefattar bestämmelser om krav för utfärdande av ett certifikat och även när ett certifikat får återkallas, dvs. när det brister i förutsättningarna för certifikatets fortsatta giltighet. Motsvarande gäller även för beslut om bemyndigande av ett certifieringsorgan (företag) att få utfärda ett certifikat på viss angiven nivå. Enligt det angivna ramverket är det således certifieringsorganet och/eller den nationella myndigheten för cybersäkerhetscertifiering som, när författningsenliga förutsättningar föreligger, ansvarar för utfärdande respektive återkallande av nu angivna certifikat. Som utredningen anför ska prövningen av så väl tillfälligt upphävande som återställande av ett certifikat ske enligt andra bedömningskriterier än de som återfinns i NIS2-direktivet.

FMV delar därför utredningens bedömning att det inte ska införas en möjlighet att med stöd av den föreslagna cybersäkerhetslagen tillfälligt upphäva en väsentlig verksamhetsutövares auktorisation (bemyndigande) eller certifiering på tillämpningsområdet för förordning (EU) 2019/881.

FMV anser dock att det kan komma att uppstå en situation, där en tillsynsmyndighet inom ramen för tillämpningen av den föreslagna cybersäkerhetslagen bedömer att det hos en aktör som omfattas av den lagen, även kan ifrågasättas om kraven och förutsättningar för ett giltigt certifikat eller bemyndigande fortsatt är uppfyllda. I detta sammanhang menar FMV att bedömning kan ske att frågan bör komma till det angivna certifieringsorganets och/eller den nationella myndighetens (FMV) kännedom för vidare åtgärd, dvs. ett eventuellt tillfälligt återkallande eller annan form av ingripande med stöd av genomförandeförordningen och lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Artikel 32.5 a) i NIS2-direktivet möjliggör att det i den nationella lagstiftningen införs en reglering som ger de behöriga myndigheterna befogenhet att begära att ett certifierings- eller auktorisationsorgan, eller en domstol enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten. För det fall en tillsynsmyndighet på NIS2-området bedömer att det finns skäl anta att det finns brister i förutsättningarna för ett fortsatt giltigt certifikat för en IKT-produkt eller -tjänst som är certifierad enligt det angivna ramverket, kan den myndigheten uppmärksamma certifieringsorganet och/eller den nationella myndigheten för cybersäkerhetscertifiering på förhållandena och därvid även aktualisera att organet eller den myndigheten vidtar lämpliga åtgärder, som t.ex. kan innefatta ett tillfälligt upphävande av certifikatets giltighet.

FMV anser sammanfattningsvis att ett direkt ingripande mot certifikat eller bemyndigande som beslutats enligt förordning (EU) 2019/881 endast bör ske i enlighet med vad som anges i denna förordning och av utsedda certifieringsorgan och/eller den nationella myndigheten för cybersäkerhetscertifiering (FMV).

I den slutliga handläggningen har rådgivare Thomas Wallander, rådgivare Jörgen Samuelsson, jurist Karin Adamsson, senior rådgivare cybersäkerhet Dag Ströman, säkerhetsskyddskoordinator Kjell Jönsson, chef för avdelningen Cybersäkerhet och certifiering John Billow och informationssäkerhetschef Thomas Palfelt deltagit. Thomas Palfelt har varit föredragande.

Försvarets materielverk

Anders Sjöborg
Chefsjurist, Juridik- och säkerhetsstaben

Sändlista
Försvarsdepartementet

Kopia till
Försvarsmakten
FMV Lednings- och ekonomistaben
FMV Juridik och säkerhetsstaben
Arkiv