Försvarsutskottets betänkande 2020/21:FöU6

Kompletterande bestämmelser till EU:s cybersäkerhetsakt

Sammanfattning

Utskottet föreslår att riksdagen antar regeringens förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt och ett förslag till ändring i samma lag.

I propositionen föreslår regeringen den nya lagen för att komplettera EU:s cybersäkerhetsakt, bl.a. när det gäller en nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Den nya lagen föreslås träda i kraft den 28 juni 2021.

En följdmotion har väckts med anledning av propositionen. Utskottet föreslår att riksdagen avslår följdmotionen och ett antal motionsyrkanden som väckts under allmänna motionstiden.

I betänkandet finns nio reservationer (M, SD, C, KD, L).

Behandlade förslag

Proposition 2020/21:186 Kompletterande bestämmelser till EU:s cybersäkerhetsakt.
Ett yrkande i en följdmotion.
Elva yrkanden i motioner från allmänna motionstiden 2020/21.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

1. Kompletterande bestämmelser till EU:s cybersäkerhetsakt

Riksdagen antar regeringens förslag till

1. lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt med den ändringen att ordet ”överenstämmelse” i rubriken närmast före 3 § och i 8 § 1 ska bytas ut mot ”överensstämmelse”,

2. lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Därmed bifaller riksdagen proposition 2020/21:186 punkterna 1 och 2.

2. Tillsynsansvaret över regelverket för cybersäkerhetscertifiering

Riksdagen avslår motion
2020/21:4069 av Pål Jonson m.fl. (M, KD).

Reservation 1 (M, C, KD, L)

3. Cybersäkerhet och utbildning

Riksdagen avslår motion
2020/21:3207 av Jessika Roswall m.fl. (M) yrkande 3.

4. Svenska myndigheters informationssäkerhet

Riksdagen avslår motionerna
2020/21:3086 av Edward Riedl (M) och
2020/21:3479 av Maria Stockhaus m.fl. (M) yrkandena 11 och 12.

Reservation 2 (M)

5. Samverkan mellan stat och näringsliv

Riksdagen avslår motion
2020/21:3444 av Pål Jonson m.fl. (M) yrkande 3.

Reservation 3 (M)

6. En it-haverikommission

Riksdagen avslår motion
2020/21:2921 av Niels Paarup-Petersen m.fl. (C) yrkande 22.

Reservation 4 (C)

7. Yttrandefrihet

Riksdagen avslår motion
2020/21:877 av Roger Richthoff m.fl. (SD) yrkande 41.

Reservation 5 (SD)

8. Utredning om samhällsviktig it-infrastruktur

Riksdagen avslår motion
2020/21:2214 av Jimmy Ståhl m.fl. (SD) yrkande 3.

Reservation 6 (SD)

9. Säkerheten i it-infrastruktur

Riksdagen avslår motion
2020/21:2214 av Jimmy Ståhl m.fl. (SD) yrkande 6.

Reservation 7 (SD)

10. Desinformation

Riksdagen avslår motion
2020/21:2921 av Niels Paarup-Petersen m.fl. (C) yrkande 25.

Reservation 8 (C)

11. Bredbandsutbyggnad

Riksdagen avslår motion
2020/21:3169 av Mikael Larsson m.fl. (C) yrkande 10.

Reservation 9 (C)

Stockholm den 1 juni 2021

På försvarsutskottets vägnar

Pål Jonson

Följande ledamöter har deltagit i beslutet: Pål Jonson (M), Niklas Karlsson (S), Paula Holmqvist (S), Jan R Andersson (M), Roger Richthoff (SD), Mattias Ottosson (S), Daniel Bäckström (C), Hanna Gunnarsson (V), Jörgen Berglund (M), Sven-Olof Sällström (SD), Kalle Olsson (S), Mikael Oscarsson (KD), Allan Widman (L), Caroline Nordengrip (SD), Elisabeth Falkhaven (MP), Alexandra Anstrell (M) och ClasGöran Carlsson (S).

Redogörelse för ärendet

Ärendet och dess beredning

Den 17 april 2019 beslutade Europaparlamentet och rådet att anta förordningen (EU) 2019/881 om Enisa (Europeiska unionens säkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). EU:s cybersäkerhetsakt trädde i kraft den 27 juni 2019. Vissa bestämmelser om cybersäkerhetscertifiering som kräver kompletterande nationella bestämmelser ska tillämpas fr.o.m. den 28 juni 2021.

Regeringen beslutade den 31 oktober 2019 att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande bestämmelser som EU:s cybersäkerhetsakt ger anledning till och överväga om det finns anledning att införa ytterligare krav för att skydda verksamhet som är av betydelse för Sveriges säkerhet (dir. 2019:73).

Utredningen, som tog namnet Cybersäkerhetsutredningen (Fö 2019:01), överlämnade den 30 september 2020 delbetänkandet EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58).

Delbetänkandet har remissbehandlats.

Lagrådet har granskat regeringens förslag.

Bakgrund

Syftet med EU:s cybersäkerhetsakt är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen.

EU:s cybersäkerhetsakt reglerar dels Europeiska unionens cybersäkerhetsbyrå (Enisa), dels ett ramverk för cybersäkerhetscertifiering.

I fråga om Enisa regleras mål, uppgifter och organisatoriska frågor. Enisa ska främja spridningen av cybersäkerhetscertifiering i unionen, bl.a. genom att bidra till inrättandet och underhållandet av ramverket för cybersäkerhetscertifiering på unionsnivå. Bestämmelserna i den delen trädde i kraft den 27 juni 2019.

Europeiska kommissionen ska utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. Enisa ska med hjälp av expertråd och i nära samarbete med Europeiska gruppen för cybersäkerhetscertifiering (ECCG) lämna förslag på europeiska certifieringsordningar. Syftet är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att

undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering medför att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater.

Genom ramverket möjliggörs en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering, vilket skapar en digital inre marknad för IKT-produkter, IKT-tjänster och IKT-processer.

Propositionens huvudsakliga innehåll

I propositionen föreslås en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I den föreslagna lagen finns kompletterande bestämmelser till EU:s cybersäkerhetsakt bl.a. när det gäller en nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Den nya lagen föreslås träda i kraft den 28 juni 2021.

Utskottets överväganden

Kompletterande bestämmelser till EU:s cybersäkerhetsakt

Utskottets förslag i korthet

Riksdagen antar regeringens förslag till kompletterande bestämmelser till EU:s cybersäkerhetsakt och lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Propositionen

Regeringen föreslår en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

En nationell myndighet för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och den nya lagen. Regeringen anser att kostnader i den verksamheten bör bekostas av de tillverkare och leverantörer som ansöker om ett europeiskt cybersäkerhetscertifikat.

Vidare föreslås att den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Den nationella myndigheten för cybersäkerhetscertifiering ska enligt propositionen få besluta om de förelägganden som behövs för att EU:s cybersäkerhetsakt, den nya lagen och föreskrifter som har meddelats i anslutning till lagen ska följas. Enligt förslaget ska ett beslut om föreläggande få förenas med vite.

Regeringen föreslår vidare att den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i akten eller en europeisk ordning för cybersäkerhetscertifiering.

Av regeringens proposition framgår att den nationella myndigheten för cybersäkerhetscertifiering ska kunna besluta om sanktionsavgifter för vissa överträdelser av EU:s cybersäkerhetsakt.
Det ska, enligt propositionen vara obligatoriskt att besluta om sanktionsavgift vid överträdelser av regelverket. Det ska gälla strikt ansvar vid sådana överträdelser.

Den nationella myndigheten för cybersäkerhetscertifiering ska enligt förslaget besluta om sanktionsavgiften. En sanktionsavgift ska kunna bestämmas

till lägst 10 000 kronor och högst 15 000 000 kronor. Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Den nya lagen ska enligt propositionen ändras så att upplysningsbestämmelsen i lagen om EU-förordningen (EG) nr 765/2008 anger den lydelse av förordningens titel som träder i kraft den 16 juli 2021.

I propositionen framgår att ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Regeringen föreslår att beslut enligt EU:s cybersäkerhetsakt och den nya lagen av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Vidare föreslår regeringen att den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt inte får obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes. I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen.

Den nya lagen ska enligt propositionen träda i kraft den 28 juni 2021. Lagen om ändring i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska enligt förslaget träda i kraft den 16 juli 2021.

Utskottets ställningstagande

Utskottet välkomnar regeringens förslag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Regeringens förslag tillstyrks på de skäl som anges i propositionen.

Tillsynsansvaret över regelverket för cybersäkerhetscertifiering

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandet om tillsynsansvaret över regelverket för cybersäkerhetscertifiering.

Jämför reservation 1 (M, KD, C, L).

Propositionen

Regeringen bedömer, i likhet med utredningen Cybersäkerhetsutredningen (Fö 2019:01) att Försvarets materielverk (FMV) är den myndighet som är bäst lämpad och bör utses att utföra de uppgifter som åligger den nationella myndigheten för cybersäkerhetscertifiering.

Regeringen menar att FMV bedriver verksamhet som kräver bred och djup kunskap och teknisk kompetens inom ramen för verksamhet som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system (CSEC). Erfarenhet från certifieringsverksamhet och den tekniska kunskapen som FMV har är också en fördel vid uppbyggnaden av ett system för en effektiv tillsyn över regelverket för cybersäkerhetscertifiering. Till detta kommer att FMV bedöms ha goda förutsättningar att hantera den i vissa fall känsliga information som kommer att behöva tillgängliggöras både vid cybersäkerhetscertifiering på högsta assuransnivån och inom ramen för tillsynsverksamheten.

Motionen

Pål Jonson m.fl. (M, KD) föreslår i följdmotion 2020/21:4069 att Myndigheten för samhällsskydd och beredskap (MSB) ska ha tillsynsansvaret för EU:s cybersäkerhetsakt. Motionärerna menar på att FMV i dag inte är en uppbyggd organisation för att utöva tillsyn till skillnad från MSB som redan utför sådana uppdrag mot olika aktörer. MSB har således en vana att arbeta med tillsyn mot aktörer på ett bredare sätt än FMV. Dessutom betonar motionärerna att det är motsägelsefullt att FMV ska ha både certifierings- och tillsynsuppdraget.

Utskottets ställningstagande

Utskottet vill betona vikten av att man noga överväger vilken myndighet som är bäst lämpad att utföra de uppgifter som åligger den nationella myndigheten för cybersäkerhetscertifiering. Utskottet instämmer i regeringens bedömning att en viktig utgångspunkt vid inrättandet av denna myndighet är att, som utredningen och flera remissinstanser framhåller, beakta de krav på oberoende som EU:s cybersäkerhetsakt ställer.

Utskottet noterar att både utredningen och regeringen bedömer FMV som lämplig myndighet att ansvara över utfärdande av cybersäkerhetscertifikat och utövandet av tillsyn över regelverket. Utskottet har inte någon annan uppfattning än att FMV:s erfarenhet bl.a. från certifieringsverksamhet och den tekniska kunskapen utgör en fördel vid uppbyggnaden av ett system för en effektiv tillsyn över regelverket för cybersäkerhetscertifiering. Utskottet finner sammanfattningsvis inte skäl att göra någon annan bedömning än regeringen då det gäller ansvaret för tillsynsansvaret. Utskottet avstyrker därmed motionsyrkandet.

Cybersäkerhet och utbildning

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om cybersäkerhet och utbildning.

Motionen

I kommittémotion 2020/21:3207 av Jessica Roswall m.fl. (M) föreslår motionärerna tydligare satsningar på utbildning och kompetens genom stärkta samarbeten inom EU (yrkande 3).

Bakgrund

Tidigare behandling

Utskottet har behandlat cyberfrågor bl.a. i betänkandet Nationell strategi för samhällets informations- och cybersäkerhet (bet. 2017/18:FöU4). Utskottet ansåg i betänkandet, likt regeringen, att det är nödvändigt att främja kunskaps- och kompetensutvecklingen på informationssäkerhetsområdet i samhället och gav därför stöd åt regeringens intention att verka för att berörda myndigheter utvecklar arbetet med att genomföra och stödja kartläggningar och utredningar om sårbarheter och lämpliga säkerhetsåtgärder i samhället.

NIS-direktivet behandlades i utskottet och riksdagen beslutade mot bakgrund av utskottets betänkande 2017/18:FöU14 bl.a. om en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Utskottet ansåg i betänkandet att det är nödvändigt med samarbete både inom EU och internationellt för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös.

Därutöver har utskottet i betänkande 2019/20:FöU7 välkomnat regeringens arbete med att etablera ett nationellt cybersäkerhetscentrum.

I betänkande 2020/21:FöU4 uttryckte även utskottet att ett viktigt steg för att stärka den svenska cybersäkerheten var inrättandet av det nya cybersäkerhetscentret.

Pågående arbete

I budgetpropositionen för 2021 (prop. 2020/21:1 utg.omr. 6) i fråga om samhällets informations- och cybersäkerhet föreslog regeringen att sammanlagt 50 miljoner kronor tillförs 2021 för det samlade arbetet med att inrätta ett nationellt cybersäkerhetscenter. Samverkan inom ramen för cybersäkerhetscentret inleddes under 2020 och innebär enligt regeringen att Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot stärks. Samverkan inom ramen för cybersäkerhetscentret ska utvecklas stegvis 2021–2023 för att bl.a. föra dialog med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad samt erbjuda kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper. Regeringen beskriver också i budgetpropositionen för 2021 att den utökade samordning som etableringen av centret innebär kommer att utgöra en viktig komponent i utvecklingen av informations- och cybersäkerheten i Sverige. I oktober 2020 redovisade FRA, Försvarsmakten, MSB och Säpo sitt arbete med att inrätta det nationella cybersäkerhetscentret för försvarsutskottet.

För att stärka cybersäkerheten på EU-nivå, ska ett europeiskt kompetenscentrum för cybersäkerhet inrättas liksom ett nätverk av nationella samordningscentrum för cybersäkerhetsfrågor. Centrumet ska stärka kapaciteten, kunskapen och infrastrukturen inom cybersäkerhet i unionen genom att bl.a. utveckla infrastruktur och tjänster för näringsliv och forskning. Andra uppgifter blir att föra samman centrala berörda parter inom EU, inbegripet industrin, akademiska institutioner, forskningscentrum och övriga relevanta organisationer i det civila samhället, och skapa en kompetensgemenskap för cybersäkerhet i syfte att stärka och sprida cybersäkerhetskompetens i EU. I april 2021 gav rådet grönt ljus för att inrätta ett kompetenscentrum för cybersäkerhet som ska samla investeringar inom forskning, teknik och industriell utveckling som rör cybersäkerhet. Regeringen har uttryckt i fakta-PM 2018/19:FPM11 att kommissionens förslag till insatser på europeisk nivå inom cybersäkerhetsområdet kan skapa ett europeiskt mervärde genom samordning av den i dag fragmenterade expertisen och kompetensen i Europa.

Utskottets ställningstagande

Utskottet lägger stor vikt vid att Sveriges cyberförmåga stärks och att samhälles cybersäkerhet förbättras. Utskottet ser därför positivt på arbetet med att inrätta det nationella cybersäkerhetscentret, vilket kommer att innebära att Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot stärks.

Utskottet anser utöver det att samarbetet för cybersäkerheten på EU-nivå kommer att stärkas genom att det europeiska kompetenscentret för cybersäkerhet inrättas tillsammans med ett nätverk av de nationella samordningscentren för cybersäkerhetsfrågor. Utskottet noterar därvid särskilt att en viktig uppgift blir att föra samman centrala berörda parter inom EU, inbegripet indu-

strin, akademiska institutioner, forskningscentra och övriga relevanta organisationer i det civila samhället, och skapa en kompetensgemenskap för cybersäkerhet i syfte att stärka och sprida cybersäkerhetskompetens i EU.

Med anledning av det ovan anförda anser utskottet att det inte finns skäl att vidta några åtgärder med anledning av motion 2020/21:3207 (M). Motionsyrkandet avstyrks.

Svenska myndigheters informationssäkerhet

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om svenska myndigheters informationssäkerhet.

Jämför reservation 2 (M).

Motionerna

Edward Riedl (M) uttrycker i kommittémotion 2020/21:3086 att det under de senaste åren vid flertalet tillfällen framkommit att svenska myndigheters arbete med informationssäkerhet är bristfällig. Motionärerna föreslår därför att regeringen borde se över myndigheternas informationshantering för att så snabbt som möjligt stärka informationssäkerheten på statlig nivå.

I kommittémotion 2020/21:3479 av Maria Stockhaus m.fl. (M) uttrycker motionärerna att svenska myndigheters säkerhetsarbete generellt inte hållit jämna steg med digitaliseringen. Motionärerna föreslår därför att regeringen bör ta ledningen för att på ett operativt sätt stödja myndigheters säkerhetsarbete (yrkande 11).

Vidare föreslår motionärerna att det införs ett fortbildningskrav inom informationssäkerhet för personer på ledande platser inom den offentliga sektorn (yrkande 12).

Bakgrund

Tidigare behandling

Försvarsutskottet uttryckte i betänkande 2018/19:FöU7 och 2019/20:FöU7 en positiv syn på att regeringen inom ramen för den nationella cybersäkerhetsstrategin avser att verka för att öka tydligheten i myndighetsstyrningen och lyfta fram betydelsen av ett tillfredsställande informations- och cybersäkerhetsarbete internt på myndigheter samt att den avser att ta fram en nationell modell för systematiskt arbete och verka för att samverkan och informationsdelning kan stärkas på området.

I samband med Riksrevisionens rapport om informationssäkerhetsarbete på nio myndigheter (RiR 2016:8) och regeringens påföljande skrivelse underströk utskottet i betänkande 2016/17:FöU8, på samma sätt som Riksrevisionen gjort i sin rapport, att man i statsförvaltningen hanterar mycket information

som är skyddsvärd och att ett seriöst arbete med informationssäkerhet bör ha som mål att all skyddsvärd information ska vara tillgänglig, riktig, konfidentiell och spårbar.

Utskottet har tidigare lagt stor vikt vid att Försvarsmakten utvecklar sin förmåga att försvara Sverige mot kvalificerade angripare i cyberrymden och att informations- och cybersäkerheten i samhället utvecklas (se bl.a. bet. 2019/20:FöU1, 2019/20:FöU7).

Pågående arbete

Det nationella cybersäkerhetscentret ska enligt regeringen utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet. Vidare ska centret bl.a. erbjuda kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper. Cybersäkerhetscentret har även i uppgift att hålla i dialoger med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad.

Regeringen uppdrog 2019 åt MSB att genomföra riktade utbildningsinsatser till statliga myndigheter, kommuner och regioner för att höja nivån på informationssäkerhetsarbetet i offentlig sektor. MSB ska enligt uppdraget även vid behov särskilt utveckla stöd till mindre myndigheter. Uppdraget redovisades till Regeringskansliet (Justitiedepartementet) den 1 mars 2021.

Vidare uppdrog regeringen även 2019 åt MSB att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Uppföljningsstrukturen ska syfta till att aktörer i offentlig förvaltning regelbundet ska erbjudas att medverka i uppföljningen och få återkoppling som omfattar en bedömning om vilken nivå deras informationssäkerhetsarbete befinner sig på samt förslag på åtgärder som bör vidtas för att uppnå en högre nivå på informationssäkerhetsarbetet. Uppdraget redovisades till Regeringskansliet (Justitiedepartementet) den 1 mars 2021.

Regeringen gav den 12 april 2018 MSB i uppdrag att uppdatera och vidareutveckla det metodstöd på informationssäkerhetsområdet som är riktat mot kommuner samt att genomföra riktade utbildningsinsatser mot kommuner, regioner och länsstyrelser (Ju2018/02265/SSK). Uppdraget redovisades den 1 april 2019. MSB har inom ramen för uppdraget utvecklat flera olika typer av utbildningar och stöd för att möta behoven i kommuner, regioner och länsstyrelser, t.ex. både lärarledd utbildning och webbutbildningar.

I MSB:s årsredovisning för 2020 framgår att myndigheten under 2020 bl.a. har gett ut ett föreskriftspaket som omfattar informationssäkerhet, it-säkerhet och incidentrapportering för statliga myndigheter. Dessutom framgår av årsredovisningen att myndigheten har genomfört en digital informationssäkerhetskonferens för offentlig sektor, en Tänk säkert-kampanj riktad till allmänhet och små företag, utbildningsinsatser för offentlig sektor samt en pilotutbildning för myndighetschefer.

I budgetpropositionen för 2021 (prop. 2020/21:1 utg.omr. 6) framgår det att MSB under 2019 har bedrivit ett arbete med de nya uppgifter som myndigheten ålagts genom förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, särskilt inom ramen för det samarbetsforum för en effektiv och likvärdig tillsyn som myndigheten leder. Vidare framgår det att flertalet myndigheter med tillsynsansvar har påbörjat sitt tillsynsarbete i någon form och att flera myndigheter också har påbörjat arbetet med att ta fram egna föreskrifter samt att myndigheterna inom Samverkansgruppen för informationssäkerhet har fortsatt arbetet med den samlade informations- och cybersäkerhetshandlingsplanen.

Utskottets ställningstagande

Den digitala utvecklingen i såväl Sverige som i övriga världen går mycket fort och svenska statliga myndigheter bedriver sedan många år olika digitaliseringsarbeten. Arbetet med informations- och cybersäkerhet är därför något som bör vara ständigt pågående.

Utskottet konstaterar att samverkan mellan berörda myndigheter har inletts med anledning av det nationella cybersäkerhetscentret under 2020, vilket regeringen och myndigheterna har redogjort för i olika sammanhang. Utskottet ställer sig positivt till centrets uppdrag att bl.a. erbjuda kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper.

Utskottet noterar vidare att MSB fortlöpande arbetar med informationssäkerhetsarbetet i den offentliga förvaltningen genom att bl.a. utveckla utbildningar och stöd på informationssäkerhetsområdet som är riktat mot olika delar av offentlig sektor.

Med anledning av det arbete som bedrivs anser utskottet att det för tillfället inte finns skäl att vidta åtgärder för tillfället i fråga om myndigheters informations- och cybersäkerhetsarbete. Utskottet avstyrker motionsyrkandena.

Samverkan mellan stat och näringsliv

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande avseende samverkan mellan stat och näringsliv.

Jämför reservation 3 (M).

Motionen

I kommittémotion 2020/21:3444 av Pål Jonson m.fl. (M) föreslår motionärerna förstärkt samverkan mellan stat och näringsliv på cybersäkerhetsområdet (yrkande 3).

Bakgrund

Tidigare behandling

Utskottet har i betänkande 2019/20:FöU7 understrukit att näringslivets roll är viktig i sammanhanget krishantering då så många centrala delar som behövs för att ett samhälle ska kunna fungera är privatägda. Utskottet såg positivt på att t.ex. flera länsstyrelser genomfört totalförsvarsseminarier där kommuner, regioner, näringsliv och frivilligorganisationer inom länet deltagit.

I betänkande 2020/21:FöU7 och 2020/21:FöU4 uttryckte utskottet att näringslivet är av central betydelse för försörjningsberedskapen och att involveringen av det privata näringslivet i planeringsarbetet bör öka. Vidare betonade utskottet att en långsiktig samverkan mellan offentliga och privata aktörer på den centrala, regionala och lokala nivån bör etableras.

Pågående arbete

Som utskottet har redogjort för ovan, beslutade regeringen den 10 december 2020 om att inrätta ett nationellt cybersäkerhetscenter.

Centret kommer att ge ett utvecklat och samordnat stöd om hur olika verksamheter i privat och offentlig sektor kan skydda sig mot cyberattacker. Samverkan med privata och offentliga aktörer ska utgöra en central del av uppdraget. Centret ska även verka för kunskaps-, kompetens- och informationsutbyte och samverkan med offentliga och privata aktörer, exempelvis när det gäller detektion, sårbarheter, hot, risker, analys, verktyg och metoder samt internationellt samarbete.

I den nationella strategin för samhällets informations- och cybersäkerhet (Skr. 2016/:213) framgår att regeringen ska verka för att lärosäten, industriforskningsinstitut, näringsliv och offentlig sektor samverkar för att öka nyttiggörande och innovation inom informations- och cybersäkerhetsområdet, och för att informations- och cybersäkerhet ska beaktas i samtliga strategiska samverkansprogram. Den 1 juni 2016 presenterade regeringen fem strategiska samverkansprogram som ska bidra till att möta flera av de samhällsutmaningar Sverige står inför. Det femte samverkansprogrammet, Uppkopplad industri och nya material, är inriktat på att stimulera en bred digitalisering av svensk industri genom en kraftsamling i form av samarbete mellan olika aktörer. Syftet är att samverkan ska stärkas mellan etablerad industri, it- och telekomföretag, tjänsteföretag, innovativa unga företag i digitaliseringens framkant samt olika forskningsmiljöer.

Utskottets ställningstagande

Samverkan mellan stat och näringsliv inom cybersäkerhetsområdet är av stor vikt. Mycket av den samhällsviktiga verksamheten ägs och drivs av näringslivet. Det gäller på alla samhällsområden, såsom elförsörjning och telekommunikation, genomförande av transporter och hälso- och sjukvård. Utskottet in-

stämmer därför med motionärerna i att det är väsentligt att näringslivet involveras i arbetet med att stärka informations- och cybersäkerheten i Sverige och i det svenska samhället.

Utskottet noterar att det pågår arbeten på flera håll, genom inrättande av det nya nationella cybersäkerhetscentret och genom att olika samverkansprogram arbetar med frågan kring samverkan mellan stat och näringsliv och ser inte skäl till att vidta några åtgärder för tillfället. Motionsyrkandet avstyrks.

En it-haverikommission

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om en it-haverikommission. Jämför reservation 4 (C).

Motionen

I kommittémotion 2020/21:2921 av Niels Paarup-Petersen m.fl. (C) föreslår motionärerna att en ”it-haverikommission” skapas. Denna ska enligt motionärerna ansvara för att analysera incidenter, skapa rekommendationer och sprida råd, riktlinjer och information om nödvändiga förbättringar i system såväl över hela den offentliga sektorn som inom kritiska privata sektorer (yrkande 22).

Bakgrund

Pågående arbete

Inom ramen för det nya cybersäkerhetscentret ska de ansvariga myndigheterna bl.a. koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, förmedla råd och stöd avseende hot, sårbarheter och risker samt tillhandahålla lägesbilder och analyser avseende hot, sårbarheter och risker.

I regeringsbeslutet Fö2019/01330 framgår att det nationella cybersäkerhetscentret ska göra Sverige säkrare genom att höja den samlade förmågan att möta cyberhoten och öka förmågan att effektivt stödja offentliga och privata aktörer. Detta avser även bidra till en stärkt säkerhet i samhället i breda termer, vilket inkluderar exempelvis svensk konkurrenskraft och vårt nationella välstånd. Genom samverkan i cybersäkerhetscentret skapas också förutsättningar för att myndigheterna i utökad utsträckning ska kunna bistå Regeringskansliet i strategiska frågor rörande cybersäkerhet.

Utskottets ställningstagande

Utskottet konstaterar att regeringen genom en rad initiativ de senaste åren markerat en tydlig förändring av inriktningen på politiken för den digitala förvaltningen. Cybersäkerhetscentrets uppgift att koordinera arbetet med att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, förmedla råd och stöd avseende hot, sårbarheter och risker samt tillhandahålla lägesbilder och analyser avseende hot, sårbarheter och risker svarar enligt utskottet mot de krav som framställs i motionen. Utskottet ser därför inte skäl att vidta några åtgärder för tillfället. Motionsyrkandet avstyrks.

Yttrandefrihet

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om yttrandefrihet.
Jämför reservation 5 (SD).

Motionen

Roger Richthoff m.fl. (SD) föreslår i kommittémotion 2020/21:877 att det är av yttersta vikt att verksamhet inom cybersäkerhet bedrivs på ett sådant sätt att den yttrandefrihet som råder i Sverige beaktas (yrkande 41).

Bakgrund

Tidigare behandling

I försvarsutskottets utlåtande 2016/17:FöU2 om Europeiska kommissionens meddelande om en gemensam ram för att motverka hybridhoten, instämde utskottet i konstitutions- och justitieutskottets syn på vikten av att värna den personliga integriteten och den grundlagsreglerade informations- och yttrandefriheten.

Utskottet har i betänkande 2018/19:FöU7 behandlat frågan om den nya myndigheten för psykologiskt försvar. Utskottet uttryckte då att det psykologiska försvaret måste ta sin utgångspunkt i att bevara det öppna samhällets fria kunskaps- och informationsutbyte. Utskottet var positivt till att regeringen tillsatt en utredning inför inrättandet av en ny myndighet för psykologiskt försvar. Utskottet välkomnade även i betänkande 2018/19:FöU1 att myndigheten kunde komma på plats under innevarande mandatperiod.

Pågående arbete

I augusti 2018 tillsatte regeringen en utredning om en ny myndighet för psykologiskt försvar (dir. 2018:80). Utredningen antog namnet Psykförsvarsutredningen och redovisades 2020. Den 18 mars 2021 beslutade regeringen att fr.o.m. den 1 januari 2022 inrätta en myndighet för psykologiskt försvar.

Utredningen bedömde att det psykologiska försvaret bör ses som en självklar del av arbetet med att värna det öppna samhället, den fria åsiktsbildningen samt Sveriges frihet och oberoende. En viktig del i detta, enligt utredningen, bör vara att stärka den samlade förmågan att identifiera och möta otillbörlig informationspåverkan och annan spridning av vilseledande information riktad mot Sverige. Detta måste enligt utredningen ske med respekt för den grundlagsskyddade tryck- och yttrandefriheten.

Utskottets ställningstagande

Utskottet instämmer i vikten av att det psykologiska försvaret tar sin utgångspunkt i att bevara det öppna samhällets fria kunskaps- och informationsutbyte. Den nya myndigheten för psykologiskt försvar kommer i det sammanhanget att få en viktig uppgift i att värna dessa värden. Som utredningen anger vill även utskottet betona att arbetet med såväl det psykologiska försvaret som cybersäkerhetsarbetet ska ske med respekt för den grundlagsskyddade tryck- och yttrandefriheten. Utskottet anser inte att det finns skäl till att vidta några åtgärder för närvarande och avstyrker därför motionsyrkandet.

Utredning om samhällsviktig it-infrastruktur

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om en utredning avseende samhällsviktig it-infrastruktur.

Jämför reservation 6 (SD).

Motionen

Jimmy Ståhl m.fl. (SD) uttrycker i kommittémotion 2020/21:2214 att möjligheten till fri konkurrens behöver kunna begränsas när det gäller nationella säkerhetsintressen och att infrastruktur som har nationellt säkerhetsintresse inte bör kunna säljas ut. Motionärerna föreslår att en utredning ska tillsättas som har som mål att säkerställa samhällsviktig it-infrastruktur (yrkande 3).

Bakgrund

Tidigare behandling

I betänkande 2017/18:FöU4 behandlade utskottet regeringens skrivelse om en nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Utskottet såg positivt på skrivelsen och föreslog att riksdagen skulle lägga skrivelsen till handlingarna.

I betänkande 2018/19:FöU7 samt 2019/20:FöU7 uttryckte sig utskottet återigen positivt till den nationella strategi för samhällets informations- och cybersäkerhet.

Utskottet ansåg i betänkande 2019/20:FöU7 att den nationella strategin låg till grund för en generell förstärkning av informations- och cybersäkerheten och specifika åtgärder vid företagsuppköp för att kunna säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.

Pågående arbete

I proposition 2020/21:30 Totalförsvaret 2021–2025, uttrycker regeringen att det är viktigt att säkerhetskänslig verksamhet skyddas när den exponeras för utomstående. Regeringen framhåller att Säkerhetspolisen och andra myndigheter vid flera tillfällen har uppmärksammat att utländska aktörer gör strategiska uppköp av svenska skyddsvärda verksamheter. Utbrottet av covid-19 innebär härtill att många företag har det mycket svårt ekonomiskt, vilket kan göra företagen än mer sårbara för uppköp. Regeringen lyfter i propositionen att det behövs mekanismer som gör att uppköp som kan skada Sveriges säkerhet kan stoppas.

Vidare framgår i proposition 2020/21:30 att regeringen tillsatte en utredning under hösten 2019, bl.a. mot bakgrund av de påpekanden som svenska myndigheter gjort när det gäller förekomsten av strategiska utländska uppköp, med uppdrag att lämna förslag på hur ett svenskt system för granskning av utländska direktinvesteringar inom skyddsvärda områden kan utformas (dir. 2019:50). Utredningen ska redovisa sitt slutbetänkande senast i november 2021.

Genom en ändring i den nuvarande säkerhetsskyddsförordningen, infördes den 1 april 2018 krav på samråd med Säkerhetspolisen och Försvarsmakten inför viss utkontraktering av säkerhetskänslig verksamhet. Arbetet med en ny säkerhetsskyddslag och en ny säkerhetsskyddsförordning som stärker skyddet för Sveriges säkerhet har slutförts.

Den 1 januari 2021 infördes ytterligare åtgärder för en bättre kontroll av överlåtelser av säkerhetskänslig verksamhet. Åtgärderna innebär ett antal nya krav som riktas mot den som vill sälja eller på annat sätt överlåta säkerhetskänslig verksamhet.

De nya åtgärderna är kompletteringar av säkerhetsskyddslagen (2018:585). De nya reglerna innebär bl.a. att verksamhetsutövare som avser att överlåta säkerhetskänslig verksamhet eller viss egendom är skyldiga att genomföra en särskild säkerhetsskyddsbedömning och en lämplighetsprövning.

I regeringens vårändringsbudget för 2021 (prop. 2020/21:99) skriver regeringen att Telias återköpsprogram är avslutat liksom regeringens analys av möjligheterna att på sikt avyttra statens ägande i Telia. Regeringen föreslår att riksdagen återkallar bemyndigandet till regeringen att minska statens röst- och ägarandel i Telia Company AB. När det gäller möjligheterna att på sikt avyttra statens innehav i Telia redovisar regeringen att Försvarsmakten i ett yttrande till försvarsutskottet anfört att en eventuell avyttring, helt eller delvis, av statens ägarandel i Telia kan få allvarliga konsekvenser för verksamheter som är betydande för Sveriges säkerhet (yttr. 2018/19:FöU2y). Försvarsmakten har

genomfört en fördjupad analys av riskerna med en försäljning av Telia (Fö2019/01317). Försvarsmaktens slutsats är att statens ägarandel i Telia inte bör minskas. Regeringen har inte funnit skäl att ifrågasätta Försvarsmaktens slutsats och bedömer att det inte bör vara aktuellt att minska statens ägande i Telia från den nuvarande nivån.

Utskottet uttryckte i yttrande 2018/19:FöU2y att det var viktigt att beakta eventuella strategiska motiv som kan finnas bakom utländska investeringar i exempelvis svensk infrastruktur. Utskottet betonade även att en eventuell avyttring av statens andel i Telia Company AB behövde analyseras grundligt genom att beakta de risker som en avyttring kan innebära.

Utskottets ställningstagande

Utskottet instämmer i regeringens bedömning i proposition 2020/21:30 att det behövs fler mekanismer som gör att uppköp som kan skada Sveriges säkerhet kan förhindras.

Utskottet noterar att det genom kompletteringar av säkerhetsskyddslagen (2018:585) nyligen införts ytterligare bestämmelser för en bättre kontroll av överlåtelser av säkerhetskänslig verksamhet. Med hänvisning till detta och till att regeringen dessutom har tillsatt en utredning under hösten 2019, med uppdrag att lämna förslag på hur ett svenskt system för granskning av utländska direktinvesteringar inom skyddsvärda områden kan utformas, anser utskottet inte att det i dagsläget finns anledning för riksdagen att vidta några åtgärder. Utskottet avstyrker därmed motionsyrkandet.

Säkerheten i it-infrastruktur

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om säkerheten i it-infrastruktur.

Jämför reservation 7 (SD).

Motionen

Jimmy Ståhl m.fl. (SD) uttrycker i kommittémotion 2020/21:2214 att all kommunikation ska klassas som osäker. Säkerhetsrutinerna för viss it-infrastruktur behöver ses över (yrkande 6).

Bakgrund

Tidigare behandling

För att öka säkerheten i nätverk, produkter och system samt för att skapa en säker infrastruktur för elektronisk kommunikation, har utskottet i betänkande

2017/18:FöU4 uttryckt att är det nödvändigt att verka för att elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder och att aktörer inom allmän ordning, säkerhet, hälsa och försvar har tillgång till moderna, säkra och robusta kommunikationslösningar.

Utskottet gav i betänkandet även sitt stöd åt regeringens syn att säker elektronisk kommunikation och andra it-relaterade tjänster bör stärkas vid upphandling och att det är viktigt att de verksamheter som har behov av en hög nivå av driftssäkerhet inom kommunikationsnät och it-relaterade tjänster ställer krav på detta vid upphandling

Utskottet har vidare gett sitt stöd till regeringens planer på att verka för en nationell strategi och åtgärdsplan för att säkra kryptosystem genomförs.

Pågående arbete

I regeringens nationella strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213) framgår att några av strategins målsättningar är att elektroniska kommunikationer ska vara effektiva, säkra och robusta.

Enligt strategin kommer regeringen att verka för att elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder, att aktörer inom allmän ordning, säkerhet, hälsa och försvar har tillgång till moderna, säkra och robusta kommunikationslösningar, att myndigheternas kompetens när det gäller upphandling av nätverk, produkter och system stärks och att myndigheterna vid upphandlingar säkerställer att hänsyn tas till säkerhetsaspekter samt att PTS förutsättningar att verka för en hög nivå av nät- och informationssäkerhet inom sektorn för elektronisk kommunikation stärks.

Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska vidare motsvara behoven i samhället. Regeringen ska därför verka för att en nationell strategi och åtgärdsplan för säkra kryptosystem genomförs.

En del av det nya nationella cybercentrets uppdrag är att höja den nationella förmågan att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter som riskerar att skada Sveriges säkerhet.

I MSB:s årsredovisning 2020 framgår att myndighetens arbete inom cybersäkerhet och säkra kommunikationer bedöms ha bidragit till att stärka informations- och cybersäkerheten i Sverige. Inom området säkra kommunikationer har myndigheten bl.a. lanserat en uppdaterad version av Swedish Government Secure Intranet (SGSI) videotjänst, som möjliggör för samhällsviktiga aktörer att ha videokonferenser upp till nivån skyddsvärd.

Utskottets ställningstagande

Utskottet vill betona att det är mycket angeläget att skydda säkerheten i nätverk, produkter och system. Det arbete som görs för att skapa en säker it-infrastruktur i landet är därför välkommet. Inrättandet av det nya nationella cybercentret, för att höja den nationella förmågan att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter som riskerar att skada Sveriges

säkerhet, är en viktig del i denna utveckling och kommer att utgöra en viktig del i arbetet med att skydda samhällsviktig infrastruktur. Utskottet avstyrker motionsyrkandet.

Desinformation

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om desinformation.
Jämför reservation 8 (C).

Motionen

I kommittémotion 2020/21:2921 av Niels Paarup-Petersen m.fl. (C) föreslår motionärerna att kunskapen om och insatser mot s.k. deep fakes och andra teknologiska möjligheter med samhällsstörande konsekvenser bör stärkas inom säkerhetsapparaten (yrkande 25).

Bakgrund

Tidigare behandling

I betänkande 2017/18:FöU4 behandlade utskottet regeringens skrivelse om den nationella strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). I skrivelsen redogjorde regeringen för att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. Strategin ska ses som ett uttryck för regeringens övergripande prioriteringar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Utskottet såg i betänkandet positivt på regeringens nationella strategi som man ansåg kommer att bidra till att skapa långsiktiga förutsättningar för informations- och cybersäkerheten för hela det svenska samhället.

I betänkande 2017/18:FöU14 om informationssäkerhet för samhällsviktiga och digitala tjänster ställde sig utskottet bakom regeringens förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster i syfte att genomföra EU:s s.k. NIS-direktiv (dvs. direktivet om nät- och informationssäkerhet) i svensk rätt.

Utskottet har uttryckt i betänkande 2018/19FöU7 att arbetet med cybersäkerhet är ett ansvar för hela samhället och alla aktörer. I enlighet med den vedertagna ansvarsprincipen bör berörda aktörer, enligt utskottet, ansvara för att identifiera och hantera informationspåverkan inom sina respektive ansvarsområden.

Utskottet har i betänkande 2020/21:FöU4 uttryckt att desinformation och påverkansoperationer (valpåverkan inkluderat) är en självklar del av det psykologiska försvaret.

Pågående arbete

Som utskottet tidigare redogjort för beslutade regeringen den 18 mars 2021 att fr.o.m. den 1 januari 2022 inrätta en myndighet för psykologiskt försvar.

Den nya myndigheten ska bl.a. ha i uppgift att identifiera, analysera och kunna lämna stöd i bemötandet av otillbörlig informationspåverkan och annan vilseledande information som riktas mot Sverige eller svenska intressen. Myndigheten ska också bidra direkt till att stärka befolkningens motståndskraft när det gäller det psykologiska försvaret.

I regleringsbrevet till MSB 2021 framgår det att myndigheten ska ha en god förmåga att identifiera och möta informationspåverkan och annan spridning av vilseledande information riktad mot Sverige.

I MSB:s årsredovisning från 2020 beskriver myndigheten att man bl.a. har följt och analyserat informationspåverkan kopplat till hanteringen av pandemin, rapporterat till Regeringskansliet samt erbjudit stöd (i form av exempelvis utbildningar) till nationella och regionala aktörer i frågan. De åtgärder som MSB har vidtagit under 2020 bedöms ha bidragit till att öka medvetenhet, beredskap och förmåga i samhället att identifiera och möta informationspåverkan, framför allt vad gäller informationspåverkan rörande pandemin.

Utskottets ställningstagande

Digitaliseringen har gjort det enklare att med tekniska verktyg manipulera bilden av verkligheten. Teknisk manipulation och andra tillvägagångssätt för att sprida desinformation utgör ett återkommande hot mot samhället. Arbetet med att inrätta myndigheten för psykologiskt försvar med uppgift att bl.a. lämna stöd i då det gäller att bemöta otillbörlig informationspåverkan och annan vilseledande information som riktas mot Sverige utgör därför en viktig del i skapandet av en robusthet mot den typen av verksamhet.

Utskottet anser att resultatet det pågående arbetet bör avvaktas. Motionsyrkandet avstyrks.

Bredbandsutbyggnad

Utskottets förslag i korthet

Riksdagen avslår ett motionsyrkande om bredbandsutbyggnad.
Jämför reservation 9 (C).

Motionen

I kommittémotion 2020/21:3169 av Mikael Larsson m.fl. (C) yrkar motionärerna på att Försvarsmakten aktivt bör delta och medverka i planeringen av bredbandsutbyggnaden med berörda aktörer (yrkande 10). Motionärerna menar att säkerhetsskyddslagen i dag stoppar byggnation av mobilmaster på många platser i Sverige och att aktörer som bygger infrastruktur för mobilt

bredband upplever att byggtillstånd rutinmässigt nekas i områden där flyghinder gäller. Motionärerna uttrycker att det vid ett avslag på inrådan av Försvarsmakten måste gå att hitta acceptabla alternativa placeringar.

Bakgrund

Tidigare behandling

I utskottets betänkanden 2016/17:FöU6, 2017/18:FöU6, 2018/19:FöU9, 2019/20:FöU9 samt 2020/21:FöU4 underströk utskottet vikten av att Försvarsmakten får goda förutsättningar att öva inom ramen för sin verksamhet. Utskottet har betonat att det är angeläget att regeringen verkar för att säkra Försvarsmaktens tillgång till övningsområden.

Pågående arbete

I Försvarsmaktens regleringsbrev för 2020 framgår det att Försvarsmakten i sina yttranden i våg- och vindkraftsärenden ska utveckla förmågan till tidig dialog och samverkan med övriga samhället. I uppdraget för 2020 ingick även att Försvarsmakten skulle analysera jämförbara länders och grannländers erfarenheter av fungerande samexistens mellan försvarsmakt och kraftigt utbyggd vindkraft inom samma geografiska område och att de skulle återkomma med förslag på hur det svenska systemet kan förbättras i det avseendet.

I myndighetens årsredovisning 2020 framgår det att Försvarsmakten kontinuerligt arbetar med dessa frågor och att myndigheten genom samverkan med bl.a. Energimyndigheten mottagit rekommendationer som möjliggör prioriteringar och åtgärder i Försvarsmaktens arbete med våg- och vindkraft.

Försvarsmaktens arbete med internationella jämförelse vad avser samexistens mellan försvars- och vindkraftsintresset fortsätter under 2021.

Utskottets ställningstagande

För att Försvarsmakten ska kunna genomföra givna uppgifter krävs kontinuerlig övning och utbildning m.m. Försvarsmakten är i behov av lämpliga övningsområden och andra mark-, luft- och vattenområden för att skapa, utveckla och bibehålla denna förmåga. Detta har utskottet tidigare understrukit, bl.a. i sitt betänkande med anledning av regeringens proposition Totalförsvaret 2021–2025 (bet. 2020/21:FöU4, prop. 2020/21:30). Utskottet vidhåller denna uppfattning.

Samtidigt vill utskottet betona vikten av en kontinuerlig och öppen dialog mellan Försvarsmakten och andra aktörer som vill bedriva verksamhet som kan komma att påverka Försvarsmaktens övningsområden. Utskottet ser därför positivt på det arbete som Försvarsmakten gör i det här avseendet.

Mot bakgrund av ovanstående avstyrker utskottet motionsyrkandet.

Reservationer

1. Tillsynsansvaret över regelverket för cybersäkerhetscertifiering, punkt 2 (M, C, KD, L)

av Pål Jonson (M), Jan R Andersson (M), Daniel Bäckström (C), Jörgen Berglund (M), Mikael Oscarsson (KD), Allan Widman (L) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:4069 av Pål Jonson m.fl. (M, KD).

Ställningstagande

Vi anser att det är naturligt att Försvarets materielverk (FMV/CSEC) ska ha rollen som den ansvariga myndigheten för cybersäkerhetscertifiering. FMV har redan i dag kompetens på högsta assuransnivån. Dessutom finns det en koppling till den höga kompetens som finns inom säkerhetsskyddsområdet på FMV.

Vår bedömning skiljer sig dock i ett avseende från regeringens bedömning. Vi anser att tillsynsuppdraget bör ligga på MSB och inte på FMV. Det finns två skäl för detta. För det första pekar FMV själva i sitt remissvar på att det är motsägelsefullt att myndigheten ska ha både certifierings- och tillsynsuppdraget. Det skulle i praktiken nämligen innebära att de ska utöva tillsyn av sig själva. För det andra har inte FMV en uppbyggd organisation för att utöva tillsyn till skillnad från MSB som redan utför sådana uppdrag. MSB har således vana att arbeta med tillsyn mot en rad olika aktörer på ett väsentligt bredare sätt än FMV.

Avslutningsvis bör det beaktas att kompetens på informationssäkerhetsområdet utgör en kraftigt begränsande faktor. Därför är det naturligt att bygga vidare på den kompetens som finns inom MSB på detta område, snarare än att FMV ska bygga upp ett helt nytt tillsynsområde för sin verksamhet.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

2. Svenska myndigheters informationssäkerhet, punkt 4 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:3479 av Maria Stockhaus m.fl. (M) yrkandena 11 och 12 samt
bifaller delvis motion
2020/21:3086 av Edward Riedl (M).

Ställningstagande

Svenska myndigheters säkerhetsarbete har generellt inte hållit jämna steg med digitaliseringen och vi anser därför att det är av yttersta vikt att det finns en tydlig ledning i det arbetet. Regeringen bör ta ledningen för att på ett operativt sätt stödja myndigheters säkerhetsarbete. Vikten av att värna den personliga integriteten och andra intressen som skyddas av offentlighets- och sekretesslagen är stor, och statens egna myndigheters arbete med detta måste förbättras.

Den offentliga sektorns ansvar gentemot medborgarna att upprätthålla sekretess och den personliga integriteten är stort. Ska vi klara omställningen till ett digitalt samhälle krävs en tydlig kompetensförsörjning och utveckling av ledningen inom den offentliga sektorn. Digitaliseringen innebär ett allmänt krav på effektivisering och modernisering inom den svenska förvaltningen och i detta ryms en stärkt kunskap och medvetenhet om hur informationssäkerheten ska förbättras. Därför bör ett fortbildningskrav för personer på ledande platser inom den offentliga sektorn införas.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

3. Samverkan mellan stat och näringsliv, punkt 5 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion

2020/21:3444 av Pål Jonson m.fl. (M) yrkande 3.

Ställningstagande

En bra samverkan mellan stat och näringsliv är centralt om samhällets samlade resurser ska kunna användas effektivt för att stärka såväl krisberedskap som totalförsvar i Sverige. Stora delar av de samhällsviktiga resurserna och tillhörande kompetens ligger i dag hos det privata näringslivet. Detta gäller inte minst på cyberområdet.

Det är därför centralt att samverkan mellan offentlig och privat sektor fördjupas. En stor del av produktutveckling inom cybersäkerhetsområdet sker i dag inom det privata näringslivet. Den teknikkompetens som finns bland dessa företag är ofta väsentligt högre än den som finns på statliga myndigheter. För att uppnå en fungerande marknad som kan leverera adekvata lösningar och produkter, krävs det en långsiktig strategisk dialog mellan myndigheter och företag om teknikutvecklingstrender samt om hot, risker och sårbarheter i cybermiljön. Genom en sådan dialog kan svensk underrättelse- och säkerhetstjänst få en bättre överblick över hur tekniktrender på cybersäkerhetsområdet kommer att påverka behovet av säkerhetsskydd.

Regeringens nationella strategi för samhällets informations- och cybersäkerhet innehåller inga konkreta förslag på hur samverkan med näringslivet kan förbättras och hur samhällets cybersäkerhet som helhet kan dra nytta av den teknikkompetens som finns på området i Sverige. Till exempel skulle en utökad användning av näringslivets säkerhetsdelegation i cybersäkerhetsfrågor och/eller näringslivets totalförsvarsråd, som Försvarsberedningen föreslår, kunna främja en effektivare samverkan med näringslivet. Det finns en stor vilja hos flera aktörer inom näringslivet att i ökad utsträckning ta samhällsansvar genom att bidra till arbetet med att stärka totalförsvaret, inte minst inom cybersäkerhetsområdet. Vi anser att man måste ta vara på det samhällsengagemanget genom att skapa bättre samverkan mellan näringsliv, stat och samhälle i syfte att öka skyddet mot olika former av cyberhot.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

4. En it-haverikommission, punkt 6 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 6 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:2921 av Niels Paarup-Petersen m.fl. (C) yrkande 22.

Ställningstagande

Jag anser att sårbarheten i den digitala infrastrukturen är uppenbar genom ständigt återkommande lagbrott, läckor och avbrott. För att förbättra säkerheten bör inom den verksamhet som grundlagts genom bl.a. genomförande av NIS-direktivet, nya Säkerhetsskyddslagen och GDPR skapas en s.k. it-haverikommission. Förslagsvis som en vidareutveckling av CERT-SE i samband med utvecklingen av cybersäkerhetscentret. It-haverikommissionen ska ansvara för att analysera incidenter, skapa rekommendationer och sprida råd, riktlinjer och information om nödvändiga förbättringar i system såväl över offentlig sektor som inom kritiska privata sektorer. Avslutningsvis anser jag att en sådan it-haverikommission bör kunna utfärda tvingande åtgärder.

5. Yttrandefrihet, punkt 7 (SD)

av Roger Richthoff (SD), Sven-Olof Sällström (SD) och Caroline Nordengrip (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 7 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:877 av Roger Richthoff m.fl. (SD) yrkande 41.

Ställningstagande

Försvarsberedningen betonar vikten av att utveckla ett cyberförsvar. Våren 2019 påbörjade Försvarsmakten och KTH etableringen av ett centrum för cyberförsvar och informationssäkerhet. Centrumet kommer att utvecklas tillsammans med ytterligare myndigheter. Vi ser mycket positivt på detta då vi länge påtalat vikten av att skapa och vidareutbilda ett cyberförsvar. Vi anser att regeringen måste se till att verksamheten inom cyberförsvaret bedrivs på ett sådant sätt att yttrandefriheten i Sverige beaktas.

6. Utredning om samhällsviktig it-infrastruktur, punkt 8 (SD)

av Roger Richthoff (SD), Sven-Olof Sällström (SD) och Caroline Nordengrip (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 8 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:2214 av Jimmy Ståhl m.fl. (SD) yrkande 3.

Ställningstagande

Alla företag bör konkurrera på lika villkor och ges samma möjligheter att investera i exempelvis it-infrastruktur. Möjligheten till fri konkurrens behöver dock kunna begränsas med hänsyn till nationella säkerhetsintressen. Infrastruktur som har ett nationellt säkerhetsintresse bör därför inte kunna säljas ut. Vid en avyttring av statliga bolag som innehar infrastruktur av nationellt intresse ska dessa delar av bolaget delas upp och behållas i statlig kontroll. Vi anser att regeringen bör tillsätta en utredning som har till mål att säkerställa samhällsviktig it-infrastruktur.

7. Säkerheten i it-infrastruktur, punkt 9 (SD)

av Roger Richthoff (SD), Sven-Olof Sällström (SD) och Caroline Nordengrip (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 9 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:2214 av Jimmy Ståhl m.fl. (SD) yrkande 6.

Ställningstagande

En del infrastruktur är särskilt känslig för dataintrång eftersom det lagrar information om medborgare, militär och politisk ledning. Det finns nationer vars lagar kan utkräva särskild information från både egna medborgare och inhemska bolag, oavsett bolagens globala placering. Vi menar att beroende på personers befattningar eller bolagens arbetsområde, kan konsekvenserna bli stora för såväl enskilda individer som företag. Företag kan beroende på geografisk placering, tvingas bryta mot EU-rätt, GDPR eller nationella lagar, vilket kan ställa företag i svåra situationer. All kommunikation måste klassas som osäker, även om en anläggning är digitalt fysiskt åtskild ifrån omvärlden. Det uppstår extraordinära problem om nationer utstuderat använder sina egna bolag, sin befolkning eller auktoritet till att illegalt inhämta it-information utanför sin egen nationsgräns. Lösningen ligger i att försvåra och skapa hinder som är fysiska, digitala, juridiska, och diplomatiska. Viss svensk digital infrastruktur behöver vara säkerhetskrypterad, hårdvara och mjukvara bör placeras på rätt ställen och tillgång till särskilt känslig information ska ske genom särskild

behörighet. Vi anser att säkerhetsrutinerna för viss it-infrastruktur behöver ses över.

8. Desinformation, punkt 10 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 10 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:2921 av Niels Paarup-Petersen m.fl. (C) yrkande 25.

Ställningstagande

Samhället är i dag avsevärt mer digitaliserat än för bara ett år sedan. Närmast över en natt har Sverige tagit ett historiskt digitaliseringskliv. Näringslivet, föreningslivet, vardagen och välfärden blir allt mer digitalt. Jag anser att kunskapen om och insatser mot s.k. ”deep fakes” och andra teknologiska möjligheter med samhällsstörande konsekvenser bör stärkas inom säkerhetsapparaten.

9. Bredbandsutbyggnad, punkt 11 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 11 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2020/21:3169 av Mikael Larsson m.fl. (C) yrkande 10.

Ställningstagande

Alla aktörer måste bidra till en utbyggnad av bredband, anser jag. I dag stoppar säkerhetsskyddslagen byggnation av mobilmaster på många platser i Sverige och bland annat upplever aktörer som bygger infrastruktur för mobilt bredband att byggtillstånd rutinmässigt nekas i områden där flyghinder gäller. Detta kan förbättras genom fördjupad dialog mellan Försvarsmakten och de aktörer som bygger infrastruktur. Mobilitetsmålet måste kunna uppnås utan att det kommer i konflikt med rikets säkerhet. Vid avslag på inrådan av Försvarsmakten måste det gå att hitta acceptabla alternativa placeringar. Jag anser att regeringen bör

verka för att Försvarsmakten utvecklas i sin dialog med de aktörer som bygger infrastruktur för bredband.

BILAGA 1

Förteckning över behandlade förslag

Propositionen

Proposition 2020/21:186 Kompletterande bestämmelser till EU:s cybersäkerhetsakt:

1. Riksdagen antar regeringens förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Följdmotionen

2020/21:4069 av Pål Jonson m.fl. (M, KD):

Riksdagen ställer sig bakom det som anförs i motionen om att Myndigheten för samhällsskydd och beredskap ska ha tillsynsansvaret för EU:s cybersäkerhetsakt och tillkännager detta för regeringen.

Motioner från allmänna motionstiden 2020/21

2020/21:877 av Roger Richthoff m.fl. (SD):

41. Riksdagen ställer sig bakom det som anförs i motionen om cyberförsvar och tillkännager detta för regeringen.

2020/21:2214 av Jimmy Ståhl m.fl. (SD):

3. Riksdagen ställer sig bakom det som anförs i motionen om att bevara samhällsviktig it-infrastruktur och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om säkerhetsrutiner för viss it-infrastruktur och tillkännager detta för regeringen.

2020/21:2921 av Niels Paarup-Petersen m.fl. (C):

22. Riksdagen ställer sig bakom det som anförs i motionen om en it-haverikommission och tillkännager detta för regeringen.
25. Riksdagen ställer sig bakom det som anförs i motionen om teknologiska möjligheter med samhällsstörande konsekvenser och tillkännager detta för regeringen.

2020/21:3086 av Edward Riedl (M):

Riksdagen ställer sig bakom det som anförs i motionen om att se över offentlig förvaltnings arbete med informationssäkerhet och tillkännager detta för regeringen.

2020/21:3169 av Mikael Larsson m.fl. (C):

10. Riksdagen ställer sig bakom det som anförs i motionen om att Försvarsmakten aktivt bör delta och medverka i planeringen av bredbandsutbyggnaden med berörda aktörer och tillkännager detta för regeringen.

2020/21:3207 av Jessika Roswall m.fl. (M):

3. Riksdagen ställer sig bakom det som anförs i motionen om uppföljning inom EU-samarbetet efter utbildning av informations- och cybersäkerhet och tillkännager detta för regeringen.

2020/21:3444 av Pål Jonson m.fl. (M):

3. Riksdagen ställer sig bakom det som anförs i motionen om en förstärkt samverkan mellan staten och näringslivet på cybersäkerhetsområdet och tillkännager detta för regeringen.

2020/21:3479 av Maria Stockhaus m.fl. (M):

11. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta ledningen för att på ett operativt sätt stödja myndigheternas säkerhetsarbete och tillkännager detta för regeringen.
12. Riksdagen ställer sig bakom det som anförs i motionen om att införa ett fortbildningskrav inom informationssäkerhet för personer på ledande positioner i offentlig sektor och tillkännager detta för regeringen.

BILAGA 2

Regeringens lagförslag

1 Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna lag kompletterar 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).

Förordningen (EU) 2019/881 benämns i denna lag EU:s cybersäkerhetsakt.

Ord och uttryck i denna lag har samma betydelse som i EU:s cybersäkerhetsakt.

Nationell myndighet för cybersäkerhetscertifiering

2 § Den myndighet som regeringen bestämmer

1. är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt, och
2. utövar tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Ackreditering av organ för bedömning av överenstämmelse

3 § I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

Tillsynsbefogenheter

4 § Vid tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs har den nationella myndigheten för

cybersäkerhetscertifiering de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt.

5 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för tillsynen och för att EU:s cybersäkerhetsakt, genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

6 § Den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Vid handräckning tillämpas bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Om den nationella myndigheten för cybersäkerhetscertifiering begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.

7 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering.

Administrativa sanktionsavgifter

8 § Den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift av den som

1. har utfärdat en EU-försäkran om överenstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,
2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. har utfärdat en EU-försäkran om överensstämmelse eller innehar ett cybersäkerhetscertifikat och inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering,

6. överträder ett beslut om föreläggande enligt 5 § som innebär ett förbud, eller

7. använder ett europeiskt cybersäkerhetscertifikat som har återkallats enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

9 § En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

10 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppkommit till följd av överträdelsen,

2. om den som har begått överträdelsen tidigare begått en överträdelse, och

3. den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

11 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

12 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

13 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

14 § Sanktionsavgiften tillfaller staten.

15 § En sanktionsavgift ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

16 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Tystnadsplikt

17 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).

Avgifter

18 § Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana avgifter.

Ändring av beslut av privata organ för bedömning av överensstämmelse

19 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och
2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Överklagande

20 § Beslut enligt EU:s cybersäkerhetsakt och enligt denna lag av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 28 juni 2021.

2 Förslag till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs att 3 § lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska ha följande lydelse.

Lydelse enligt förslaget i 2.1	*Föreslagen lydelse*
3 §	
I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.	
I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering *och marknadskontroll i samband med saluföring av produkter* och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.	I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.	

Denna lag träder i kraft den 16 juli 2021.

Tryck: Elanders Sverige AB, Vällingby 2021