Se sändlista

Ert tjänsteställe, handläggare
Regeringskansliet, Försvarsdepartementet

Ert datum
2021-09-22

Er beteckning
Fö2021/00796

Vårt tjänsteställe, handläggare
HKV LEDS CIO, Linda Avad
073-852 11 53, linda.avad@mil.se

Vårt föregående datum

Vår föregående beteckning

Yttrande över slutbetänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Allmänt

Försvarsmakten delar flera av utredningens grundläggande bedömningar och är i huvudsak positiv till utredningens författningsförslag. Försvarsmakten vill i sammanhanget dock peka på att den allvarligaste bristen inom informationssäkerhetsområdet inte är avsaknad av författningsreglerade krav och rekommendationer utan att befintliga krav och rekommendationer inte efterlevs i tillräckligt hög utsträckning. Detta har uppmärksammats av regeringen i propositionen Ett starkare skydd för Sveriges säkerhet (prop. 2020/21:194). Det är därför positivt att utredningen bedömer att effekterna av de ändringar i säkerhetsskyddslagen (2018:585) som gjorts till följd av propositionen behöver utvärderas innan det övervägs vidare om informationssystem som behandlar vissa säkerhetsskyddsklassificerade uppgifter, eller andra informationssystem där obehörig åtkomst kan medföra en skada för Sveriges säkerhet, ska godkännas av en utpekad central myndighet (kapitel 13). Behovet av utvärdering gör sig enligt Försvarsmaktens uppfattning generellt gällande även i fråga om införande av andra krav, och även i förhållande till effekterna av den nya säkerhetsskyddsförordningen (2021:955).

Försvarsmakten vill inledningsvis framföra att det vore önskvärt om det i dessa sammanhang mer vedertagna begreppet *kriterier*, i stället för krav, används i det fortsatta lagstiftningsarbetet. Försvarsmakten vill därutöver framföra följande synpunkter.

Författningsförslag (kapitel 1)

Ett utvidgat samrådsförfarande

Försvarsmakten har ingen erinran mot förslaget i 3 a kap. 1 och 2 §§ säkerhetsskyddslagen om ett utvidgat samrådsförfarande med Säkerhetspolisen och Försvarsmakten, under förutsättning att Försvarsmakten tillförs ökade resurser och att förslaget att ta bort kravet på skriftlighet medför en ökad flexibilitet och en minskad byråkrati. Det är av största vikt att förslaget inte medför längre handläggningstider. Försvarsmaktens uppfattning om vilka konsekvenser som förslaget medför för myndigheten framgår nedan under Konsekvensbeskrivning.

Det kan dock ifrågasättas om uttrycket samrådsmyndighet bör användas (de föreslagna 3 a kap. 2, 3 och 5 §§ och 7 kap. 2 a och 9 §§ säkerhetsskyddslagen samt 3 kap. 1 § säkerhetsskyddsförordningen). Uttrycket har nyligen fasats ut ur säkerhetsskyddslagstiftningen (se prop. 2020/21:194 och säkerhetsskydds-förordningen). Dessutom ska befintliga samråd enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen i de flesta fall ske med en tillsynsmyndighet. Mot den bakgrunden kan det framstå som förvirrande att återinföra uttrycket samrådsmyndighet, enbart för det nu aktuella samrådet. Under alla förhållanden är förslaget i 3 kap. 1 § säkerhetsskyddsförordningen att Säkerhetspolisen och Försvarsmakten ska vara samrådsmyndigheter inom sina respektive tillsyns-områden inte anpassat till den nya tillsynsstrukturen som följer av prop. 2020/21:194; det finns fler tillsynsmyndigheter än Säkerhetspolisen och Försvarsmakten.

Det bör därför i stället i säkerhetsskyddslagen föreskrivas att samrådet ska ske med den myndighet som regeringen bestämmer, utan att ange uttrycket samrådsmyndighet. Det bör därutöver i säkerhetsskyddsförordningen föreskrivas att samrådet ska ske med Säkerhetspolisen eller, om verksamhetsutövaren hör till Försvarsmaktens eller Försvarets materielverks tillsynsområde, med Försvarsmakten.

Vidare ser Försvarsmakten visserligen praktiska fördelar med en ordning där Säkerhetspolisen och Försvarsmakten har rätt att besluta om sanktionsavgifter (den föreslagna 7 kap. 2 § säkerhetsskyddslagen). Det kan dock ifrågasättas om inte sådana beslut lämpligen bör fattas av en tillsynsmyndighet (jfr. 6 kap. 1 § säkerhetsskyddslagen).

Därutöver kan det övervägas om det i 3 a kap. 1 § andra stycket säkerhets-skyddslagen kan förtydligas att verksamhetsutövaren *i vissa fall* ska samråda enligt 2 §. Av de föreslagna 3 a kap. 1 och 2 §§ säkerhetsskyddslagen följer nämligen motsatsvis att samrådsskyldigheten inte gäller för informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig och andra informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som

endast är ringa. Samrådsskyldigheten gäller inte heller om verksamhetsutövaren bedömer att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt.

Kravet på verksamhetsutövares godkännande

Eftersom de föreslagna kraven på en särskild säkerhetsskyddsbedömning, lämplighetsprövning och samråd i 3 a kap. 1 och 2 §§ säkerhetsskyddslagen omfattar såväl informationssystem som ska tas i drift som väsentliga förändringar av sådana system bör kravet på verksamhetsutövares godkännande i 3 a kap. 4 § säkerhetsskyddslagen gälla även informationssystem som i väsentliga avseenden förändras. Paragrafen skulle kunna kompletteras i detta avseende, t.ex. enligt följande.

”Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift, *eller i väsentliga avseenden förändras,* förrän det har godkänts från säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.”

Tillsynsmyndigheters rätt att få tillgång till informationssystem

Försvarsmakten vill särskilt tillstyrka förslaget i 6 kap. 3 § säkerhetsskyddslagen om att tillsynsmyndigheter ska ha rätt att få tillgång till informationssystem som används i verksamhet som omfattas av tillsynen. Förslaget bedöms möjliggöra en effektivare tillsyn och därmed ge verksamhetsutövarna ökade förutsättningar att efterleva befintliga krav. Det kan dock övervägas om det i det fortsatta lagstiftningsarbetet – i allmänmotiven och i författningskommentaren till paragrafen – bör förtydligas att rätten till tillgång till informationssystemen endast avser de delar av systemen som berörs av tillsynen och syftar till att utvärdera systemens säkerhet och sårbarheter.

Certifiering av nätverks- och informationssystem (kapitel 12)

Försvarsmakten delar utredningens bedömning att en certifieringsordning för IKT-produkter, IKT-tjänster och IKT-processer i nätverks- och informationssystem i säkerhetskänslig verksamhet inte bör införas. Nätverks- och informationssystem i säkerhetskänslig verksamhet består i huvudsak av kommersiella produkter. De icke-kommersiella produkterna utgörs vanligen dels av säkra kryptografiska funktioner som granskas och godkänns av Försvarsmakten med stöd av säkerhetsskyddslagstiftningen, dels av ett fåtal så kallade högassuransprodukter som i nätverks- och informationssystem inom Försvarsmaktens tillsynsområde granskas och godkänns av Försvarsmakten. Det är för tidigt att säga vilken påverkan som framtida certifieringar inom ramen för det europeiska ramverket för cybersäkerhetscertifiering kan få för möjligheten att stärka säkerheten i nätverks- och informationssystem generellt. Detsamma gäller också säkerhetskänslig verksamhet. Enligt cybersäkerhetsakten är dess syfte bland annat att höja cybersäkerhetsnivån i den europeiska unionen och bidra till ökad tillgång till produkter och tjänster som kan möta kvalificerade angrepp.

Utvecklingen och effekterna av det europeiska ramverket bör beaktas och utvärderas innan en nationell särskilt anpassad ordning för certifiering i säkerhetskänslig verksamhet övervägs ytterligare. Skulle en sådan ordning bedömas lämplig kan tillsynsmyndigheterna, som utredningen påtalat, föreskriva om det med stöd av säkerhetsskyddslagstiftningen.

Försvarsmakten tillstyrker att Försvarets materielverk får ett uppdrag i samråd med bl.a. Försvarsmakten. Uppdraget behöver dock omformuleras. Försvarsmaktens invändning mot det föreslagna uppdraget är att det tar sikte på nätverks- och informationssystem i säkerhetskänslig verksamhet, när fokus i stället bör ligga på nätverks- och informationssystem i andra verksamheter. Uppdraget bör därför ta sikte på arbetet *inom ramen för det europeiska ramverket för cybersäkerhetscertifiering*. Försvarsmakten är beredd att delta i dialog tillsammans med Försvarets materielverk om hur uppdraget kan formuleras.

Som utredningen pekat på finns det betydande möjligheter att dra nytta av det europeiska ramverket för cybersäkerhetscertifiering för nationella ändamål när det gäller att stärka informations- och cybersäkerheten generellt i samhället, men även i säkerhetskänslig verksamhet. Certifiering av IKT-produkter, IKT-tjänster och IKT-processer kan vara en åtgärd som medför ökad säkerhet i Sveriges nätverks- och informationssystem. En förutsättning för detta är dock, som utredningen påpekat, att sådana produkter, tjänster och processer svarar mot de nationella behoven. Det är därför av yttersta vikt att de nationella behoven och kravställningarna identifieras och beaktas när de gemensamma certifieringsordningarna inom ramen för det europeiska ramverket för cybersäkerhetscertifiering tas fram. Det är på det arbetet, och inte specifikt på nätverks- och informationssystem i säkerhetskänslig verksamhet, som fokus nu bör ligga.

Försvarsmakten delar utredningens bedömning att det behöver tas fram en struktur för att nationella behov och krav kan bevakas vid framtagandet av skyddsprofiler inom ramen för det europeiska ramverket för cybersäkerhets-certifiering och har inte något emot att Försvarets materielverk får i uppdrag att ta fram en sådan struktur.

För att de nationella behoven ska kunna identifieras och den nationella kravställningen ska kunna bli relevant krävs det, som utredningen konstaterat, därutöver ett aktivt deltagande från övriga berörda aktörer, t.ex. de myndigheter som deltar i det nationella cybersäkerhetscentret och den svenska industrin. Då säkerhet inom säkerhetskänslig verksamhet ofta är beroende av säkerhets-egenskaper hos kommersiella produkter och tjänster som skulle kunna verifieras inom det europeiska ramverket för cybersäkerhetscertifiering, bör behov från de säkerhetskänsliga verksamheterna ingå bland de krav som Sverige bör verka för att inarbeta i cybersäkerhetsaktens certifieringsordningar. Det är därför av största vikt att Försvarsmakten och Säkerhetspolisen ges en aktiv roll i arbetet med den nationella kravställningen.

Den av Försvarsmakten föreslagna ramen för regeringsuppdraget kan således skapa förutsättningar för att Sverige ska kunna bevaka de nationella intressena i arbetet inom det europeiska ramverket för cybersäkerhetscertifiering, vilket är angeläget. Om arbetet faller väl ut och gemensamma certifieringsordningar tas fram som svarar mot de nationella behoven, samt att tillgången till certifierade produkter på marknaden blir tillräckligt hög, kommer användningen av certifierade produkter, tjänster och processer att öka. Det skulle öka säkerheten i svenska nätverks- och informationssystem, såväl generellt som i säkerhetskänslig verksamhet. Försvarsmakten vill samtidigt framhålla att certifiering endast är en del av säkerhetsarbetet och att en övertro på certifiering kan ge negativa effekter. Från ett nationellt perspektiv är det vidare viktigt att fritt kunna välja produkter då ett oberoende certifieringsorgan endast kan ta begränsad hänsyn till säkerhetspolitiska bedömningar.

Sammantaget skulle ett regeringsuppdrag som tar sikte på arbetet inom ramen för det europeiska ramverket för cybersäkerhetscertifiering på sikt öka säkerheten i Sveriges nätverks- och informationssystem.

Det kan slutligen påpekas att den av utredningen föreslagna tidsplanen med en redovisning den 1 januari 2023 inte framstår som genomförbar. Försvarsmakten uppskattar att uppdragets genomförande kräver i vart fall 12 månader.

Försvarsmaktens uppfattning om vilka konsekvenser som förslaget medför för myndigheten framgår nedan under Konsekvensbeskrivning.

Konsekvensbeskrivning (kapitel 17)

Av utredningens förslag om ett utvidgat samrådsförfarande med Säkerhetspolisen och Försvarsmakten framgår inte några uppskattningar över antalet samrådsärenden eller omfattningen av dessa. Det är därför svårt för Försvarsmakten att bedöma vilka konsekvenser som förslaget får för myndigheten. Det kan dock konstateras att samrådsförfarandet medför att till del nya – och sannolikt omfattande – arbetsuppgifter påförs myndigheten, t.ex. i fråga om förelägganden. Mot den bakgrunden bedömer Försvarsmakten att förslaget kräver ökade resurser för myndigheten. Utan ökade resurser finns en risk för långa handläggningstider i samrådsärendena, vilket skulle påverka verksamhetsutövarnas möjlighet att bedriva säkerhetskänslig verksamhet och kunna få negativ inverkan på Sveriges säkerhet.

Ett lyckat resultat av det föreslagna uppdraget till Försvarets materielverk förutsätter att de aktörer som Försvarets materielverk ska samråda med, däribland Försvarsmakten, har resurser och möjlighet att delta aktivt i arbetet. Av samma skäl som utredningen bedömt att Försvarets materielverk behöver tillskjutas ekonomiska resurser för uppdraget bör även Försvarsmakten få ökade anslag.

— o 0 o —

I beredningen av ärendet har deltagit it-säkerhetsstrateg Fredrik Börjesson, kryptostrateg Pia Gruvö, informationssäkerhetsspecialist Hrafn Steiner, verksamhetsutvecklare Christina Löfgren, stabschef Jakob Gille, kommendörkaptener Per Brink och Tomas Hedström, utvecklingsledare David Olgart, sektionschef Tobias Rogell och systemingenjör Martin Skogman.

Detta remissyttrande har beslutats av ställföreträdande chef för juridiska avdelningen Kerstin Bynander. I den slutliga handläggningen har dessutom tillförordnad sektionschef Helene Arango Magnusson och cybersäkerhetsspecialist Linda Avad deltagit samt, som föredragande, försvarsjurist Halszka Onoszko.

Kerstin Bynander

Halszka Onoszko

Sändlista
Försvarsdepartementet fo.registrator@regeringskansliet.se

För kännedom
HKV LEDS (CIO, JUR, PERS, TF, STAB)
INS
MUST
PROD