Svar på uppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter

16 december 2019

FRA FÖRSVARSMAKTEN MSB Myndigheten för samhällsskydd och beredskap Säkerhetspolisen

Innehåll

Uppdraget

Regeringen har uppdragit åt Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020 (se bilaga 1).

Uppdraget ska gemensamt redovisas till Regeringskansliet (Försvarsdepartementet och Justitiedepartementet) senast den 16 december 2019.

Målbild för ett nationellt cybersäkerhetscenter

De fyra myndigheterna samverkar sedan många år kring frågor som rör cybersäkerhet i olika sammanhang.

Efter att ha gemensamt konstaterat att information, kunskap och erfarenheter kan nyttjas än mer effektivt genom en fördjupad myndighetssamverkan inom cybersäkerhetsområdet beslutade myndigheterna i december 2018 att intensifiera diskussionerna sinsemellan. Målsättningen var att konkretisera vilka förmågor som behövs för att skapa en sammanhängande helhet av myndigheternas verksamhet på cybersäkerhetsområdet och hur privat-offentlig samverkan kan utvecklas. Även organisatoriska aspekter skulle beröras.

I och med att ett nationellt cybersäkerhetscenter aviserades i regeringsförklaringen i januari 2019, kom den fördjupade samverkan att prioritera frågor som relaterar till en sådan funktion. Myndigheterna var tidigt överens om att ett framtida nationellt cybersäkerhetscenter ska höja den nationella förmågan genom samordnat agerande, informationsdelning och kunskapsöverföring.

Myndigheterna är överens om följande målsättningar för ett nationellt cybersäkerhetscenter:

Samordning av förmågor som förebygger, upptäcker och hanterar cyberangrepp och andra it-incidenter gör Sverige säkrare inom cyberområdet.
Centrets arbete är begränsat till informationssäkerhet på cyberarenan, det vill säga cybersäkerhet. Ett nationellt cybersäkerhetscenter bedöms inte ha möjligheten att lösa hela nationens cybersäkerhet utan dimensioneras för att öka skyddet för skyddsvärd verksamhet mot antagonistiska hot. Dock kommer kunskap som genereras i centret i största möjliga utsträckning delas generöst till olika aktörer.

Antagonistiska hot kan för centrets del beskrivas som företrädesvis, men inte uteslutande, statsunderstödda aktörer som drivs av nationella intressen och bedriver kvalificerade cyberoperationer mot Sverige och svenska intressen i syfte att komma över, förvanska eller förstöra information som har betydelse för Sveriges säkerhet och välstånd.

Myndigheterna agerar sömlöst, vilket ökar respektive myndighets operativa förmåga att effektivt stödja offentliga och privata aktörer.
En av de främsta fördelarna med ett nationellt cybersäkerhetscenter är att de i centret ingående myndigheterna kan och bör dela information och kunskap så att respektive myndighet kan lösa sitt uppdrag på ett effektivare sätt. Därmed stärks också Sveriges förmåga. Det betyder således att ett nationellt cybersäkerhetscenter inte övertar de ingående myndigheternas uppgifter, mandat eller förmåga. Genom

det gemensamma arbetet i centret kommer expert- och föreskrivande myndigheter att ensa det nationella cybersäkerhetsarbetet och därmed minska dagens fragmentering.

Det svenska cyberförsvaret stärks.
En god nationell cybersäkerhetsnivå är en förutsättning för att Sverige ska kunna försvara sig mot antagonistiska hot på cyberarenan. Arbete som bedrivs vid ett nationellt cybersäkerhetscenter kommer således stärka det svenska cyberförsvaret.

FRA, Försvarsmakten, MSB och Säkerhetspolisen tog under våren fram ett gemensamt förslag på vilka leveranser som skulle kunna göras inom ramen för ett nationellt cybersäkerhetscenter i sin initiala form samt på längre sikt. Myndigheterna arbetade även fram ett förslag på hur centret stegvis kan bemannas. Detta arbete har varit grunden i det fortsatta arbetet med att förbereda ett inrättande av ett nationellt cybersäkerhetscenter.

För att ytterligare tydliggöra avsikten med pågående samarbete tecknade de fyra myndigheterna i oktober 2019 en överenskommelse om fördjupad myndighetssamverkan om cybersäkerhet. Överenskommelsen reglerar på ett övergripande sätt hur de deltagande myndigheternas samverkan ska ske i ett initialt skede samt avsikten att samlokalisering av relevant verksamhet ska genomföras från och med år 2020.

Av överenskommelsen framgår att den fördjupade samverkan ska utgå från myndigheternas respektive roller och mandat och i övrigt bedrivas inom ramen för de författningar som gäller för respektive myndighet. Överenskommelsen upprättades i samråd med Polismyndigheten, Post- och Telestyrelsen (PTS) och Försvarets materielverk (FMV).

Överenskommelsen utgör en naturlig utgångspunkt i arbetet att inrätta ett nationellt cybersäkerhetscenter såsom aviserades i 2019 års regeringsförklaring.

Samverkan inom ramen för uppdraget

Arbetet med att besvara regeringens uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter grundar sig således i det utvecklingsarbete som FRA, Försvarsmakten, MSB och Säkerhetspolisen inledde i december 2018 och som formaliserades i och med upprättandet av överenskommelsen om fördjupad myndighetssamverkan om cybersäkerhet.

Med hänsyn till att ett av centrets syften är att stödja aktörer inom offentlig och privat sektor, har samverkansfrågor utgjort en central del i arbetet med uppdraget. Det har handlat om nära samverkan med Polismyndigheten, FMV och PTS men även att skapa förutsättningar för en regelbunden dialog med näringslivet samt Sveriges kommuner och regioner.

För att inhämta synpunkter och påbörja en dialog genomförde myndigheterna en samverkanskonferens där representanter från näringslivet och utpekade samverkansorganisationer deltog. Deltagarna i konferensen bidrog med värdefulla synpunkter och underlag till utvecklingsarbetet.

Inrättande och stegvis uppbyggnad av ett nationellt cybersäkerhetscenter 2020-2025

Verksamheten vid det nationella cybersäkerhetscentret förväntas bidra till höjd nationell förmåga genom ett samordnat agerande, informationsdelning och kunskapsöverföring. Centret förväntas fullt utbyggt leda till:

- Kortare ledtider från detektion till åtgärd.
- Bättre analysresultat med ett större utbyte av information.
- Ökad tydlighet i budskap och rekommendationer.
- Ökad tillgänglighet till de ingående myndigheterna för såväl privata som offentliga målgrupper.
- Stärkt privat-offentlig samverkan.
- Ett ensat nationellt cybersäkerhetsarbete samt harmonisering av föreskrifter och skyddsåtgärder.
- Effektivare användning av statens resurser.

Det arbete som sker i centret förstärker myndigheternas förmåga att lösa sina respektive uppgifter. Varje myndighet bidrar till centrets verksamhet efter egen förmåga och budget.

Myndigheterna bedömer att behovet av stöd i cybersäkerhetsfrågor är mycket hög i såväl den offentliga som privata sektorn, men i varierande grad och omfattning.

Målgrupper i den offentliga sektorn vid fullt utbyggt center:

- Bevakningsansvariga myndigheter.
- Tillsynsmyndigheter inom säkerhetsskydd och NIS-regleringen.
- Övriga statliga myndigheter.
- Kommuner och landsting.
- Sveriges Kommuner och Regioner (SKR) och andra motsvarande organisationer.

Målgrupper i den privata sektorn vid fullt utbyggt center:

- Företag inom prioriterade sektorer utifrån samhällets funktionalitet och totalförsvar, exempelvis inom sektorerna energi och telekommunikation.
- Verksamheter som berörs av NIS-regleringen.
- Företag med stor betydelse för export och nationell ekonomi.
- Cybersäkerhets- och kryptoindustri samt konsultföretag.
- Leverantörer inom säkerhetsskydd.
- Försvarsindustri.
- Näringslivets säkerhetsdelegation, Säkerhets och försvarsföretagen (SOFF) och andra motsvarande organisationer.

Myndigheterna bedömer att ett nationellt cybersäkerhetscenter inte kommer att ha möjlighet att tillgodose stöd till samtliga av dessa målgrupper i ett inrättande- och uppbyggnadsskede. Verksamheten i cybersäkerhetscentret kommer att stegvis byggas upp för att tillhandahålla ändamålsenligt stöd till både offentlig sektor och näringsliv.

Uppgifter och verksamhet

Centret stärker de ingående myndigheternas (och därmed samhällets) samlade förmåga att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter. Genom arbetet i centret skapas förutsättningar att nyttja begränsade resurser mer effektivt.

Vid inrättandet ska centret ha följande övergripande uppgifter:

- Sammanställa analyser och lägesbilder avseende hot, sårbarheter och risker.
- Sprida information mellan ingående myndigheter och andra aktörer.
- Koordinera arbetet vid it-incidenter och cyberangrepp.

Centret kommer att stödja det förebyggande arbetet för de mest skyddsvärda verksamheterna. Samverkan med privata och offentliga aktörer kommer utgöra en central del i centrets uppgifter och verksamhet. Under 2020 kommer arbetet i centret att fokusera på en gemensam lägesbild om hot och sårbarheter på cybersäkerhetsområdet, samt gemensamma och regelbundet uppdaterade rekommendationer och riktlinjer rörande grundläggande it-säkerhetsåtgärder – särskilt åtgärder som skyddar mot it-angrepp. Dessutom kommer ett arbetssätt för informationsdelning och koordinering av åtgärder vid it-incidenter att tas fram. Leveranser under 2020 är avsedda att komma till bred nationell nytta genom att de kan tillämpas av alla berörda aktörer, men centret skapar även möjligheter att arbeta med anpassade insatser i syfte att förebygga cyberangrepp för det mest skyddsvärda verksamheterna.

Från och med 2021 fortsätter utvecklingsarbetet med processer, metod och teknik i syfte att stärka såväl kvalitet som kvantitet i de externa leveranserna, med särskilt fokus på detektion och analys, informationsdelning i gemensamma system och extern samverkan. Vidare finns verksamheter som på sikt, helt eller delvis, skulle kunna ingå i eller samlokaliseras med centret för att underlätta samverkan eller för att mer effektivt använda statens resurser. Exempel på sådana verksamheter är en nationell funktion för incidenthantering, sensorverksamhet och en nationell modell för systematiskt informationssäkerhetsarbete.

Genom utvecklingen av verksamheten kommer omfattningen och ambitionen i centrets leveranser att öka. Det kan handla om följande:

- Erbjuda anpassade och aggregerade lägesbilder och analyser avseende hot, sårbarheter och risker.
- På ett mer effektivt sätt samordna hantering av inträffade händelser, exempelvis arbete vid it-incidenter, och riktade och samordnade varningar.
- Stärka samordning av förebyggande skyddsåtgärder och pågående ärenden, exempelvis tekniska säkerhetsanalyser och kartläggning av verksamheters beredskap vid it-incidenter.
- Främja ett utökat informationsutbyte med privata och offentliga aktörer, exempelvis avseende detektion, sårbarheter, hot, risker, analys, verktyg och metoder, genom att utgöra en plattform för samverkan.
- Gemensamma, kompetenshöjande insatser för ingående myndigheter och identifierade målgrupper, exempelvis övningar och utbildningar.
- Centret skapar möjligheter att utveckla ett gemensamt arbetssätt för ansvariga myndigheters hantering av it-incidenter.

Genom att utgöra en plattform för samverkan kommer centret att kunna främja ett utökat informationsutbyte med privata och offentliga aktörer exempelvis avseende detektion, sårbarheter, hot, risker, analys, verktyg och metoder. Privata och offentliga aktörer ska uppleva att det nationella cybersäkerhetsarbetet är mer samordnat.

Verksamheten i centret kommer att byggas upp under en femårsperiod för att kunna ge full effekt 2025. Utvecklingen av centret kommer att utvärderas löpande för att säkerställa att tänkt effekt uppnås.

Organisation och styrning

I överenskommelsen som FRA, Försvarsmakten, MSB och Säkerhetspolisen upprättade i oktober 2019 beskrivs hur ledning och styrning av det nationella cybersäkerhetscentret ska fungera fram till dess att centret formellt inrättas under 2020. Sammanfattningsvis innebär det att de beslut som behöver fattas inför inrättandet tas av en styrgrupp bestående av cheferna för de myndigheter som bidrar med resurser i centret. Även Polismyndigheten ingår således i styrgruppen. För att vidareutveckla den inriktning som styrgruppen ger, har en arbetsgrupp tillsatts.

Organisation och styrning måste vara anpassad efter att centret bygger på en fördjupad myndighetssamverkan och det gemensamma ansvar som detta innebär. Deltagande myndigheter kommer därför att dela på ansvar avseende exempelvis avtal, service samt teknisk och administrativ infrastruktur. Tills vidare fördelas ansvar utifrån förmåga och möjlighet att hantera frågan. På längre sikt kommer ansvarsfördelningen att formaliseras i överenskommelser.

Centret ska på övergripande nivå styras av en strategisk styrgrupp bestående av högsta chefen, eller den som chef utser, för de myndigheter som bidrar med personalresurser till centret. Den strategiska styrgruppen ska fatta de beslut som behövs för att inrikta och långsiktigt utveckla verksamheten.

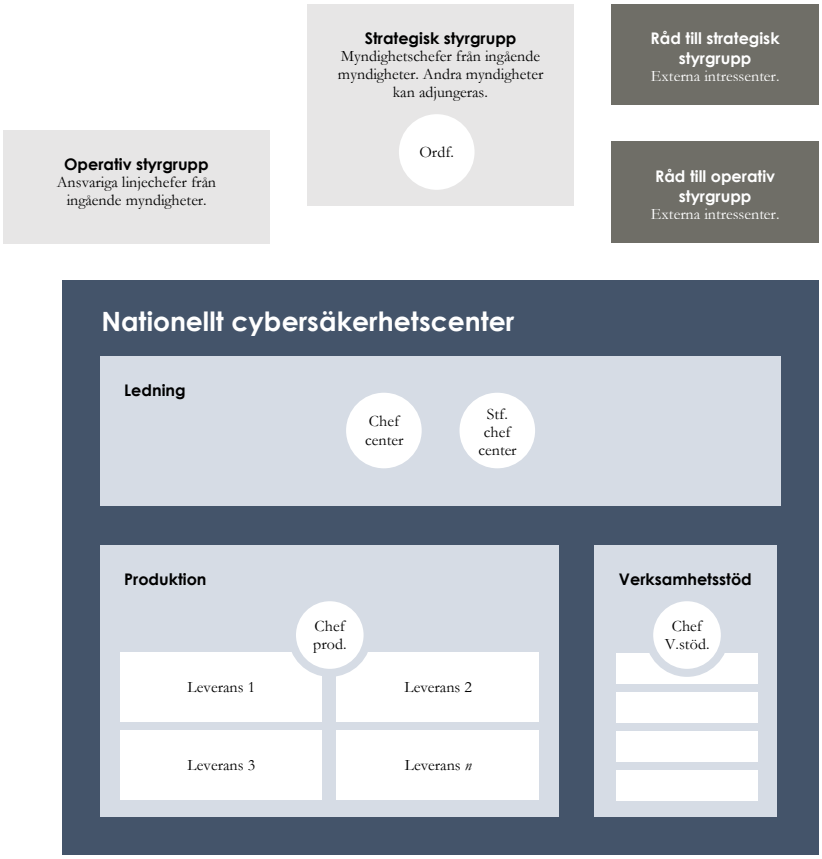
För styrning på kort- och medellång sikt ska det finnas en operativ styrgrupp bestående av representanter från linjeverksamheter som berörs av centrets verksamhet från respektive myndighet. Den operativa styrgruppen ska skapa förutsättningar för centrets chef att utveckla verksamheten.

Som stöd ska den strategiska och operativa styrgruppen ha varsitt råd som består av representanter från offentlig och privat sektor.

Det löpande arbetet i cybersäkerhetscentret ska ledas av en chef och en ställföreträdande chef. Chefen ska utses för ett tidsbegränsat chefsförordnande av den strategiska styrgruppen efter ett ansökningsförfarande. Chef och ställföreträdande chef ska i första hand rekryteras från de ingående myndigheterna. Cheferna bör över tid representera olika deltagande myndigheter. Chefen för centret övertar inte arbetsgivaransvaret för myndigheternas respektive medarbetare som är placerade vid centret eller som på annat sätt deltar i centrets arbete. Chefen för centret leder centrets produktion. Centrets produkter fastställs i konsensus mellan de deltagande myndigheterna – i första hand genom att myndigheternas personal i centret tilldelats tillräckliga beslutsmandat. Chefen för centret ska också rådgöra med den operativa styrgruppen i syfte att säkerställa att centrets verksamhet följer verksamhet hos hemmamyndigheterna.

Beroende av centrets fortsatta utveckling kan organisation och styrning av cybersäkerhetscentret komma att behöva förändras och anpassas efterhand. Detta

kommer löpande att utvärderas.



Figur 1. Övergripande organisation av det nationella cybersäkerhetscentret vid inrättandet 2020.

Lokaler och infrastruktur

En för verksamheten anpassad lokal för samlokalisering behöver vara dimensionerande för vad centret kan leverera på kort och lång sikt. Samlokalisering är en förutsättning för att det nationella cybersäkerhetscentret ska kunna agera samordnat, snabbt och sömlöst.

På kort sikt finns ett behov av lokaler som är dimensionerade för cirka 20-30 personer. På längre sikt bedöms en gemensam lokal behöva erbjuda plats för cirka 250 personer. Det inkluderar att arbetsplatser görs tillgängliga för olika typer av samverkanspersoner från andra myndigheter, näringslivet och andra aktörer. För att underlätta samverkan med näringsliv och andra verksamheter behöver den gemensamma lokalen även inrymma bland annat reception, mötesrum och konferenslokal.

Det gemensamma arbetet kommer starta första kvartalet 2020 i MSB:s lokaler i Solna. Denna tillfälliga gemensamma lokal bidrar till att myndigheterna kan leverera enligt plan under 2020.

Arbetet i centret ställer krav på etablering av gemensamma system för informationsdelning och säker tillgång till respektive myndighets interna system.

Säkerhetsskydd av lokaler och system samt säkerhetsprövning av personal ska svara mot den verksamhet som utförs i centret. En permanent lokal behöver därför anpassas till en

verksamhet som hanterar information som är placerad i upp till och med säkerhetsskyddsklass hemlig.

Kostnadsberäkningar

Inrättandet av det nationella cybersäkerhetscentret kommer att medföra merkostnader för ingående myndigheter avseende personal, lokaler och infrastruktur. Inledningsvis rör det sig främst om kostnader för etablering av gemensamma lokaler och nödvändig infrastruktur. Under 2020 bedöms tillkommande kostnader kunna rymmas inom existerande ekonomiska ramar. Samtliga ingående myndigheter står för sina egna kostnader. Nedan redovisas samlade tillkommande kostnader för administrativ personal, lokaler och infrastruktur och rörliga kostnader (exempelvis konsultarvoden, resor, samverkan, kompetensutveckling, teknikutveckling och licenser).

	2021	2022	2023	2024	2025
Stödpersonal	6	15	21	26	28
Lokaler och infrastruktur	35	45	45	45	45
Rörliga kostnader	30	40	50	50	50
Summa	71	100	116	121	123

Tabell 1. Tillkommande kostnader för nationellt cybersäkerhetscenter exklusive myndigheternas egen personal (operativ personal) 2021-2025 (mkr).

Under 2020 kommer bemanningen av centret att byggas upp till sammanlagt cirka 25 årsarbetskrafter från ingående myndigheter där majoriteten kommer från FRA och MSB. FRA och MSB kommer från 2021 och framåt kraftigt öka antalet medarbetare som är en del av centrets verksamhet, följt av Säkerhetspolisen. Även Försvarsmakten kommer att successivt öka antalet medarbetare. 2022 når bemanningen i centret cirka 125 årsarbetskrafter varav cirka en femtedel beräknas vara från övriga aktörer. 2025 beräknas centret att bemannas av totalt cirka 250 årsarbetskrafter varav cirka 200 från FRA, Försvarsmakten, MSB och Säkerhetspolisen. Två tredjedelar av bemanningen kommer vid det laget från FRA och MSB.

Från 2021 och framåt bedöms förmågeutvecklingen accelerera och då finns behov av resursförstärkning och nyrekryteringar till ingående myndigheter för att säkerställa en långsiktig utveckling av centrets verksamhet i den omfattning som krävs för att stärka Sveriges säkerhet. Den totala tillkommande kostnaden, inklusive kostnader för nyrekryteringar av operativ personal, för centret vid 2025 är uppskattas till cirka 300 miljoner per år. Myndigheterna avser att återkomma med ytterligare detaljer i kommande budgetunderlag.

Ytterligare ingående myndigheter i centret samt övrig myndighetssamverkan

Centret kommer möjliggöra en samordnad samverkan mellan de i centret ingående myndigheterna och andra myndigheter med kopplingar till cybersäkerhetsområdet. Samverkan utformas med hänsyn till behov, befintliga strukturer och samverkansforum såsom Samverkansgruppen för informationssäkerhet (SAMFI). Samverkansformerna kommer att vidareutvecklas för att centret på effektivaste sätt ska kunna nå olika grupper av myndigheter. Prioriteringen av dessa baseras på ingående myndigheters förutsättningar och behov.

Polismyndigheten, FMV och PTS är redan idag delaktiga i det arbete som sker för att förbereda etablering av centret. Bland annat genom att de kan representeras i såväl styrgrupp som arbetsgrupp.

Polismyndigheten hanterar ett stort antal it-incidenter och it-relaterade brott. För att säkerställa ett effektivt informationsutbyte med centret avser Polismyndigheten, under de förutsättningar som nu är kända, att redan vid inrättandet år 2020 placera personal i centret. Företrädesvis i form av 1-2 sambandspersoner eller liknande funktion.

En ökad effektivitet av Sveriges samlade hantering av it-incidenter kan leda till att flera it-incidenter där brott kan misstänkas upptäcks. Vissa av dessa brott ska då utredas av Polismyndigheten. Detta kan framöver leda till ett ökat resursbehov hos Polismyndigheten.

PTS avser att delta i cybersäkerhetscentrets verksamhet med bland annat kunskap, information och relationer. PTS är tillsynsmyndighet för bland annat elektronisk kommunikation, NIS (digital infrastruktur, digitala tjänster), betrodda tjänster och nationella toppdomäner – sektorer som är viktiga ur ett cybersäkerhetsperspektiv. PTS tar fram regler, bedriver tillsyn och tar emot incidentrapporter i samtliga tillsynsområden, t.ex. avseende driftsäkerhet, informationssäkerhet och säkerhetsskydd. PTS har även lång erfarenhet av privat-offentlig samverkan genom att genomföra robusthetshöjande åtgärder och samverkan för ökad krishanteringsförmåga i sektorerna, bland annat genom övningar och utbildningar med privata aktörer. PTS har etablerade kontaktvägar, relationer till och forum med aktörer i dessa sektorer, som används för delning av säkerhetsrelaterad information. Därutöver har PTS etablerade internationella samarbeten.

PTS deltar redan idag i den fördjupade myndighetssamverkan, där ett flertal personer med olika kompetenser i begränsad omfattning deltar i olika arbetsgrupper. PTS avser att fortsätta och fördjupa denna samverkan inom ramen för cybersäkerhetscentrets verksamhet. Ett utökat deltagande i centrets verksamhet, till exempel mer omfattande arbete i olika arbetsgrupper eller där personal placeras i centret företrädesvis genom en sambandsperson eller liknande funktion kräver dock en ökad resurstilldelning.

FMV avser att delta i det nationella cybersäkerhetscentrets verksamhet vad avser industrisäkerhet inom ramen för privat-offentlig samverkan och här bidra med kunskap, erfarenhet, information och ett stort kontaktnät såväl nationellt som internationellt. Vad avser industrisäkerhet och krav på skydd av säkerhetsskyddsklassificerade informationstillgångar så är FMV den myndighet i Sverige som överlag tecknar flest säkerhetsskyddsavtal såväl nationellt som internationellt och där myndigheten har lång erfarenhet av att på ett strukturerat sätt normera, kravställa och kontrollera säkerhetsskydd hos leverantörer i försvarsindustrin. FMV har sedan många år varit delaktig i olika arbetsgrupper i internationella forum för industrisäkerhet och certifieringar där man gemensamt bedriver arbete avseende att ta fram ramverk inom cybersäkerhet. Denna typ av ramverk ser FMV att man med fördel kan utarbeta inom ramen för privat-offentlig samverkan i verksamheten för ett nationellt cybersäkerhetscenter. FMV ser också möjlighet att delta i samverkan gällande att ensa hot- och lägesbild inom cybersäkerhet och hur detta förs i dialog med de privata aktörerna där behovet är stort avseende att erhålla denna typ av underlag för sin verksamhet. FMV:s erfarenhet är att det finns en stark önskan, åtminstone i försvarsindustrin, avseende att myndigheterna ställer ensade krav inom ramen för ett säkerhetsskyddsavtal där FMV anser att en sådan ensad kravbild med

fördel utarbetas på sikt inom ramen för det nationella cybersäkerhetscentret där FMV kan bidraga med kunskap och erfarenhet.

Beroende på hur centret utvecklas behöver annan etablerad myndighetssamverkan och samverkan med andra offentliga aktörer löpande ses över för att renodla arbetssätt och undvika dubbelarbete. Det är viktigt samverkan med externa aktörer inom ramen för centret karaktäriseras av transparens avseende vilka frågor som avhandlas och hur.

Näringslivets behov av stöd och bidrag till centrets verksamhet

Det nationella cybersäkerhetscentret kommer att tillhandahålla både privata och offentliga aktörer en ändamålsenlig mötesplats för extern samverkan rörande cybersäkerhet i sina permanenta lokaler. Mötesplatsen utgörs både av lämpliga lokaler och tekniska lösningar som möjliggör gemensamma projekt eller annan form av samverkan med näringslivet och andra aktörer. Inom ramen för centret blir det enklare för verksamheter som behöver stöd att på ett samlat sätt få tillgång till samtliga ingående myndigheters kunskap och kompetens. Centret underlättar även för ingående myndigheter att på ett mer effektivt sätt nå ut till och stödja industri och näringsliv i cybersäkerhetsfrågor, inte bara direkt utan även genom att branschorganisationer, konsulter och cybersäkerhetsindustrin. Förutom att sprida information från cybersäkerhetscentret, kan organisationer genom ett partnerskap med centret även ansvara för att samla in och förmedla behov och stöd till centret.

Den samverkan som skett inom ramen för arbetet med regeringsuppdraget har gett en tydlig bild av att det finns ett stort intresse hos näringslivet att bidra med information och förmåga till centret och i gengäld få tillgång till information om sårbarheter, hotbilder och rekommenderade åtgärder. Aktörerna lyfte fram vikten av att nyttja existerande samverkansforum som Forum för informationsdelning (FIDI) samt att informationsdelning både förutsätter förtroende för hur informationen hanteras och leder till resultat i form av återkopplingar.

Det fortsatta arbetet kommer att ske i nära samverkan med näringslivet och ta sin utgångspunkt i både existerande privat-offentlig samverkan, exempelvis befintliga FIDI-nätverk inom it-drift och kritisk infrastruktur, samt den dialog med näringslivet och andra aktörer som sker inom ramen för arbetet med att utveckla centret.

Konsekvensbeskrivning

Försvarets radioanstalt

FRA ser flera möjligheter att, tillsammans med de andra myndigheterna, stärka och få större utväxling av de insatser FRA idag gör på cybersäkerhetsområdet inom ramen för ett cybersäkerhetscenter. FRA:s signalspaning på cyberarenan är en förutsättning för att Sverige ska kunna följa de kvalificerade aktörerna bakom antagonistiska cyberhot mot Sverige. Denna information och kunskap omvandlar FRA till direkt och indirekt skydd till gagn för de mest skyddsvärda verksamheterna i Sverige, men som även kan komma andra målgrupper till del i ett cybersäkerhetscenter.

En framgångsfaktor för FRA har varit organisatorisk och fysisk samgruppering av underrättelse- och cybersäkerhetsverksamheterna i en och samma avdelning. Med verksamhet som bedrivs delvis i ett center kan kopplingen mellan uppdragen försvagas om inte tillräckliga förutsättningar ges för att bedriva effektivt gemensamt arbete, exempelvis

tekniskt, juridiskt och säkerhetsmässigt acceptabla lösningar att dela sekretessbelagd information.

Utöver den ökning av medarbetare som redovisas ovan och de nu kända förutsättningarna bedömer FRA att det finns ett behov av komplettering av administrativa och tekniska stödfunktioner vid FRA om cirka 10 årsarbetskrafter.

Försvarsmakten

Försvarsmaktens bidrag till och verksamhet i centret anknyter framför allt till Försvarsmaktens uppgifter rörande säkerhetsskydd och cybersäkerhet. Försvarsmakten ser centret som en möjlighet att stärka myndighetens förmåga att lösa dessa uppgifter samtidigt som den ömsesidiga spridningen av myndigheternas kunskaper och kompetens inom området underlättas.

Försvarsmaktens resurser för säkerhetsskydd och cybersäkerhet är dimensionerade för lösandet av myndighetens huvuduppgifter samt det särskilda ansvar myndigheten har för försvarssektorn. Resurserna utgör därmed en integrerad delfunktion i Försvarsmaktens totala förmåga att genomföra militära operationer. Det innebär att Försvarsmakten inte avdelar hela verksamheter ur nuvarande organisation till centret. Istället tillförs en särskild resurs med samverkanspersonal och analytiker som nyrekryteras och successivt ökar till cirka 10 årsarbetskrafter från och med utgången av 2022. Denna personal kommer att samgrupperas i centret med övriga myndigheters resurser.

Under 2020 bedöms Försvarsmaktens kostnader för inrättandet av centret kunna finansieras inom befintliga ramar. Detta kommer att ske genom en omprioritering av planerad verksamhet.

Från och med 2021 anser Försvarsmakten att det utöver fördelningen av de gemensamma kostnaderna som redovisas i tabell 1 kommer att behövas ett resurstillskott till myndigheten för att etablera och vidmakthålla den samverkan och den verksamhet som förutses i centret. Medlen tillförs successivt och kommer från 2022 att uppgå till cirka 20 miljoner kronor per år Kostnaderna fördelar sig på personal och framdragning av infrastruktur för Försvarsmaktsspecifika system.

Myndigheten för samhällsskydd och beredskap

MSB ser att den nära samverkan som är tänkt att ske i centret kommer att bidra till att myndighetens breda arbete med att stärka samhällets informations- och cybersäkerhet får ökad effekt. Det handlar inledningsvis om arbetet med grundläggande cybersäkerhet i organisationer, lägesbild, och stöd vid it-incidenthantering.

MSB:s styrkor ligger i både det förebyggande och operativa cybersäkerhetsarbetet. MSB ger råd och stöd om förebyggande arbete samt hanterar it-incidenter och cyberrelaterade kriser i samhället bland annat genom den nationella funktionen CERT-SE. Myndigheten är mottagare av unik information genom incidentrapportering från statliga myndigheter och leverantörer av samhällsviktiga tjänster enligt NIS-regleringen. Slutligen bedriver MSB en omfattande nationell och internationell samverkan inte minst med näringslivet genom ett flertal privat-offentliga forum.

Etableringen av centret sker inledningsvis i MSB:s lokaler och detta kommer att innebära viss anpassning av lokaler och övrig verksamhet på kort sikt. Då myndigheten har ambitionen att placera ett större antal medarbetare vid centret kommer MSB både att behöva nyrekrytera och omprioritera planerad verksamhet. Den långsiktiga utvecklingen

kommer inte att kunna finansieras utan ökade anslag, något som MSB avser att återkomma till i kommande budgetunderlag. Utöver den ökning av medarbetare som redovisas ovan och de nu kända förutsättningarna bedömer MSB att det finns ett behov av komplettering av administrativa och tekniska stödfunktioner vid MSB om cirka 5 årsarbetskrafter.

Säkerhetspolisen
Säkerhetspolisens bidrag till cybersäkerhetscentret kommer fram för allt att komma från myndighetens säkerhetsskyddverksamhet, företrädesvis i form av resurser för analys. Samtidigt som centret kommer att skapa förutsättningar för att agera mer samordnat och effektivt, innebär tillskapandet av centret också att resurser som idag läggs på nuvarande säkerhetsskyddsuppdrag måste omprioriteras till förmån för centrets verksamhet.

Under 2020 bedöms kostnader för inrättandet av centret kunna finansieras inom Säkerhetspolisens befintliga ramar. Dock kommer planerad verksamhet att behöva omprioriteras för att tillgängliggöra resurser.

Från och med 2021 kommer utvecklingen av centret inte att kunna finansieras utan ökade anslag för nyrekryteringar. För att kunna hantera det samlade behovet av analys på säkerhetsskyddsområdet behöver Säkerhetspolisen resursförstärkningar. Exempelvis kommer myndighetens resurser inte vara tillräckliga för att både kunna bidra till centrets analysverksamhet och ta fram de dimensionerande hotbeskrivningar som Säkerhetspolisen är ålagd genom säkerhetsskyddslag och förordning.

Övriga behov eller hinder

Den fördjupade samverkan som sker inom centret förutsätter att det finns både tekniska och rättsliga förutsättningar för informationsdelning av sekretessreglerad och säkerhetsskyddsklassificerad information liksom behandling av personuppgifter. Därtill måste arbetet bedrivas med fullgott säkerhetsskydd. Inför inrättandet av centret kommer myndigheterna därför att genomföra närmare utredningar rörande bland annat personalsäkerhet, fysiskt skydd, informationssäkerhet, informationsdelning och sekretess. I det fall arbetet med att utveckla centrets verksamhet visar på att det rättsliga regelverket utgör ett hinder kan det bli aktuellt för myndigheterna att påtala behov av regelförändringar.

Regeringen

2019-09-26
Fö2019/01000/SUND

Försvarsdepartementet

Försvarets radioanstalt
Box 301
161 26 Bromma

Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter

Regeringens beslut

Regeringen uppdrar åt Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020.

Bakgrund

Sveriges säkerhet och välstånd vilar i stor utsträckning på digitala grunder. Det är av vikt att digitaliseringens möjligheter tillvaratas samtidigt som de risker den leder till måste hanteras. Cyberhoten mot Sverige och svenska intressen är omfattande. Genom teknikutveckling och digitalisering blir hoten och sårbarheterna fler vilket gör att vi måste stärka Sveriges säkerhet. I 2019 års regeringsförklaring aviserades att regeringen avser att upprätta ett nationellt center för att öka informations- och cybersäkerheten.

Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt Säkerhetspolisen bedriver inom ramen för sina uppgifter verksamheter som är centrala för att skydda Sverige mot cyberhot. Enligt den handlingsplan som bland annat dessa myndigheter redovisade den 1 mars 2019 (Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022, Ju2019/00885/SSK) har de myndigheter som omfattas av detta uppdrag inlett ett fördjupat samarbete på informations- och cybersäkerhetsområdet. Det samarbetet utgör en naturlig utgångspunkt för regeringens inrättande av ett nationellt cybersäkerhetscenter.

Telefonväxel: 08-405 10 00
Fax: 08-723 11 89
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 9
E-post: fo.registrator@regeringskansliet.se

Närmare om uppdraget

Det nationella cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Vidare ska centret ge ett utvecklat och samordnat stöd om hur olika aktörer i privat och offentlig sektor kan skydda sig mot cyberattacker där en central del kan vara gemensamma analyser och lägesbilder om hot, sårbarheter och risker. Centret ska också kunna understödja Regeringskansliet i frågor kring cybersäkerhet. Verksamheten ska bidra till att förbättra skyddet mot antagonistiska hot och minska de digitala sårbarheterna.

Myndigheternas förslag till ett nationellt cybersäkerhetscenter ska utgå från alla berörda myndigheters befintliga uppdrag och rymmas inom givna ekonomiska ramar. Myndigheterna ska inom ramen för uppdraget samråda med och inhämta synpunkter från Polismyndigheten, Försvarets Materielverk och Post- och telestyrelsen samt andra berörda myndigheter och inleda kontakter för att upprätta en regelbunden dialog med näringslivet och Sveriges kommuner och landsting. Fler aktörer ska kunna bidra till verksamheten på sikt.

Myndigheterna bör i uppdraget förhålla sig till andra pågående nationella och internationella initiativ på informations- och cybersäkerhetsområdet.

Myndigheterna ska senast den 16 december 2019 gemensamt redovisa uppdraget till Regeringskansliet (Försvarsdepartementet och Justitiedepartementet). Av redovisningen ska framgå:

- Bedömning av och förslag på vilka uppgifter som vid inrättandet bör ingå i ett nationellt cybersäkerhetscenter samt förslag till organisation och styrning av verksamheten i centret. Förslagen ska innehålla en analys av ekonomiska och personella konsekvenser.
- Bedömning av och förslag på vilka ytterligare uppgifter eller verksamheter inom ramen för befintlig myndighetsstruktur och befintliga myndighetsuppdrag som, på kort respektive längre sikt, skulle kunna vara ändamålsenliga och kostnadseffektiva att bedriva inom centret. Förslagen ska innehålla en analys av konsekvenser för organisation och styrning av verksamheten i centret samt kostnadsberäkningar.

- Förslag om ytterligare myndigheter bör ingå i centret samt förslag till strukturer för samverkan med berörda myndigheter som inte kommer att ingå i centret.
- Hur näringslivets behov av stöd kan tillgodoses samt hur näringslivet kan bidra till centrets verksamhet med beaktande av näringslivets skiftande behov och roller.
- Eventuella övriga behov eller hinder som har identifierats.

På regeringens vägnar

Peter Hultqvist

Fredrik Norberg

Likalydande till

Försvarsmakten
Myndigheten för samhällsskydd och beredskap
Säkerhetspolisen

Kopia till

Statsrådsberedningen/UTR
Justitiedepartementet/SSK, L6, L4, PO, KH
Utrikesdepartementet/ES
Försvarsdepartementet/MFI, MFU, RS, SI
Finansdepartementet/ESA, SFÖ, K, BA
Näringsdepartementet/EIN, BI
Infrastrukturdepartementet/D, DF
Försvarets materielverk
Polismyndigheten
Post- och telestyrelsen
Sveriges kommuner och landsting
Säkerhets- och försvarsföretagen (SOFF)
Svenskt näringsliv
Teknikföretagen
Verket för innovationssystem