Säkerhetspolisen

REMISSVAR

Datum: 2024-05-27
Diarienummer: 2024-10857-2
Enhet: Rättsenheten

Mottagare:
Försvarsdepartementet
103 33 Stockholm

Referens:
Fö2024/00785

Ett nytt Nationellt cybersäkerhetscenter (Fö2024/00785)

Säkerhetspolisen har tagit del av delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning (Fö2024/00785).

Säkerhetspolisen delar utredningens uppfattning om att samverkan mellan myndigheter är av avgörande betydelse för att stärka den svenska cybersäkerheten.

Sammanfattningsvis är Säkerhetspolisen positiv till förslaget att samverkan inom Nationellt cybersäkerhetscenter (centret) sker under Försvaret radioanstalts (FRA) huvudansvar och att övriga centermyndigheter medverkar i och bidrar till centrets verksamhet på lika villkor. Emellertid är det inte tydligt vad ett sådant huvudansvar kommer att innebära när det gäller inriktningen av centrets operativa verksamhet. Det behöver även tydliggöras att FRA:s huvudansvar avser samordning av övriga centermyndigheters bidrag till centrets verksamhet men däremot inte styrning av myndigheternas respektive verksamhet inom cybersäkerhetsområdet. Förslagen i delbetänkandet saknar även nödvändig tydlighet när det gäller centrets uppdrag och därmed vad centermyndigheterna ska bidra med inom centret. Det finns även andra frågor i delbetänkandet som behöver klargöras.

Nedan följer Säkerhetspolisens synpunkter. I rubriksättningarna hänvisas till kapitel och rubriker i delbetänkandet.

5.1.1 En förordning om Nationellt cybersäkerhetscenter

Säkerhetspolisen är positiv till förslaget att centrets uppdrag och uppgifter regleras i en förordning om Nationellt cybersäkerhetscenter (föreslagen förordning/förordningen). Enligt Säkerhetspolisen är en förutsättning för att centret ska fungera effektivt att det har ett väl definierat uppdrag där det är tydligt för de samverkande myndigheterna vad de ska bidra med utifrån sina respektive verksamhetsområden. Bestämmelsen om centrets mål och uppdrag (2 § i föreslagen förordning) är emellertid bred och allmänt formulerad vilket dels kan leda till att centrets operativa uppdrag blir föremål för tolkning, dels kan innebära en risk för att centrets mål och uppdrag går utöver centermyndigheternas respektive verksamhetsområden.

Det framgår inte heller av bestämmelsen om centrets uppdrag är att ha *egen förmåga* att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter eller om centrets uppdrag är att stödja och stärka *andra myndigheters förmågor* i dessa avseenden. Om bestämmelsen innebär att centret ska ha en egen förmåga inom dessa områden vill Säkerhetspolisen framhålla att detta inte är möjligt i nuläget, då ett sådant uppdrag för centret skulle gå utanför centermyndigheternas verksamhetsområden.

I delbetänkandet föreslås att det bland centrets uppgifter, som ska anges i förordning, ska ingå att övergripande koordinera och delta i internationella samarbeten kopplade till centrets verksamhet. Det är för Säkerhetspolisen oklart om detta innebär att FRA, i egenskap av centrets huvudman, kommer att få inflytande över övriga centermyndigheters internationella samarbeten och i så fall på vilket sätt. Enligt Säkerhetspolisen behöver det tydliggöras i förordningen att FRA inte ska ha något sådant inflytande.

5.2 Ledning och styrning av NCSC

I delbetänkandet anges att FRA ska ges ett tydligt huvudansvar att leda samordningen, utvecklingen och genomförandet av centrets verksamhet. Säkerhetspolisen är positiv till att FRA får huvudansvaret för den samverkan som sker inom centret. Det framgår dock inte med tillräcklig tydlighet vad ett sådant huvudmannaskap kommer att innebära för inriktningen av centrets operativa verksamhet. Ett förtydligande kring detta är nödvändigt då de samverkande myndigheterna har olika verksamhetsområden och uppdrag. Det kan till exempel innebära att det finns motstående intressen vid myndigheternas hantering av en it-incident.

I delbetänkandet anges att FRA:s huvudansvar inte innebär att FRA tar över någon annan myndighets uppgifter eller verksamhetsområde i centret. Enligt Säkerhetspolisen behöver det tydligare komma till uttryck i förordningen. Det behöver även tydliggöras att FRA:s huvudansvar avser samordning av övriga centermyndigheters bidrag till centrets verksamhet men däremot inte styrning av myndigheternas respektive verksamhet inom cybersäkerhetsområdet.

5.3 Övriga centermyndigheters medverkan och bidrag

Säkerhetspolisen är positiv till förslaget att övriga centermyndigheter, utöver FRA, medverkar och bidrar till centrets verksamhet på lika villkor.

I delbetänkandet föreslås vidare att det i förordning om Nationellt cybersäkerhetscenter (7 § föreslagen förordning) ska anges att den verksamhet som centermyndigheterna bedriver som kan utföras inom ramen för centret ska utföras inom ramen för centret. Vidare anges att FRA, som huvudansvarig för centret och dess verksamhet, får en viktig roll att uppmärksamma och agera om centrets samtliga uppgifter och verksamheter inte täcks eller om denna princip inte respekteras.

Säkerhetspolisen anser att bestämmelsen ska tas bort och att det istället tydliggörs att det är centermyndigheternas verksamhet inom cybersäkerhetsområdet – med koppling till centrets mål och uppdrag – som bör utföras inom ramen för centret.

Det är inte heller klart hur FRA ska uppmärksamma och agera om principen inte respekteras. Myndigheterna som samverkar i centret är självständiga och den verksamhet som de bedriver inom centret faller inom respektive myndighets verksamhetsområde.

Säkerhetspolisen vill understryka att myndighetens arbete inom kontraspionage och uppföljning av statliga aktörers cyberförmåga och aktivitet även fortsatt med nödvändighet måste bedrivas utanför centret. Däremot kan Säkerhetspolisens arbete inom området generera information som under rätt förutsättningar kan delas och utgöra relevant underlag vid diskussion om samordning och koordinering av centermyndigheternas arbete inom centret.

5.3.1 Skyldighet att medverka och bidra

Säkerhetspolisen är positiv till förslaget att centermyndigheternas skyldighet att medverka i och bidra till centret inom ramen för sina verksamhetsområden ska regleras i varje myndighets instruktion. Enligt Säkerhetspolisen är det av avgörande betydelse att det framgår att myndighetens medverkan och bidrag till centret endast omfattar uppgifter *inom ramen för myndighetens*

verksamhetsområden. Det innebär att centermyndigheternas sammanlagda verksamhetsområden sätter den yttre ramen för den verksamhet som centret kan bedriva.

I delbetänkandet föreslås att det i förordning ska anges att centermyndigheterna ska bistå FRA med stöd till centergemensamma administrativa stödfunktioner (6 § andra stycket i föreslagen förordning). Då centret föreslås ingå i FRA:s organisation anser Säkerhetspolisen att det är lämpligt att FRA ensamt ansvarar för sådana stödfunktioner i centret. Dessutom görs i delbetänkandet bedömningen att FRA bör få en betydande del av de medel som tidigare har tilldelats övriga centermyndigheter för driften av centret och att dessa medel bland annat ska användas till gemensamma administrativa stödfunktioner (avsnitt 6.3). Säkerhetspolisen avstyrker därför förslaget i denna del.

5.3.3 CSIRT-funktionen CERT-SE

I delbetänkandet görs bedömningen att verksamheten i Sveriges nationella CSIRT-funktion (Computer Security Incident Response Team), CERT-SE, så snart som möjligt bör överföras från Myndigheten för samhällsskydd och beredskap (MSB) till FRA och centret. Vidare anges i delbetänkandet att de närmare rättsliga, organisatoriska och praktiska förutsättningarna för en sådan verksamhetsöverföring bör utredas i ett annat sammanhang. Enligt Säkerhetspolisens mening behöver konsekvenserna av en sådan överföring belysas, särskilt med beaktande av gällande EU-regleringar inom området.

En överföring av CSIRT-funktionen från MSB till FRA och centret behöver också utförligare samordnas med andra pågående utredningar inom cybersäkerhetsområdet, framförallt betänkandet om genomförande av NIS2-direktivet: *Nya regler om cybersäkerhet* (SOU 2024:18). I SOU 2024:18 framgår att bestämmelserna i NIS2-direktivet kommer att behöva införlivas i svensk lagstiftning innan det nya centret har inrättats. NIS2-direktivet kräver att ett antal funktioner ska finnas på plats på nationell nivå. Flera av dessa funktioner finns redan till följd av införlivandet av NIS1-direktivet, däribland CSIRT-funktion och olika samarbetsgrupperingar. Dessa funktioner har inordnats i MSB:s verksamhet. Andra funktioner kommer framöver att behöva utses med anledning av NIS2-direktivet, däribland en cyberkrishanteringsmyndighet. I SOU 2024:18 föreslås MSB få ansvar för CSIRT-funktionen och bli nationell cyberkrishanteringsmyndighet. I förevarande delbetänkande bedöms emellertid att CSIRT-funktionen ska flyttas från MSB till FRA och centret. Enligt Säkerhetspolisens mening behöver ett helhetsgrepp tas kring hur Sverige på bästa sätt integrerar och interagerar med EU i cyber- och informationssäkerhetsfrågor.

5.3.4 Andra myndigheter med tangerande uppdrag

I delbetänkandet bedöms att Myndigheten för psykologiskt försvar (MPF) bör bli en centermyndighet. Vidare anges att en nära operativ samverkan mellan MPF och centret bland annat kan bestå av utbyte av information och bedömningar i syfte att skapa lägesuppfattningar rörande allvarliga antagonistiska hot mot Sverige. Säkerhetspolisen noterar emellertid att det saknas en analys avseende konsekvenserna av MPF:s ingående i centret. Enligt Säkerhetspolisen behöver en sådan analys genomföras innan MPF eventuellt kan tas med som en samverkande centermyndighet. Bland annat behöver frågor som rör MPF:s uppdrag i relation till cyberområdet belysas.

5.4.1 Samverkan på strategisk nivå

I delbetänkandet föreslås att det i förordning ska anges att det ska finnas ett strategiskt samverkansråd vid centret där centermyndigheterna företräds av sina myndighetschefer (9 § föreslagen förordning). Säkerhetspolisen anser att det istället ska vara myndigheterna själva som

beslutar vilken befattningshavare som ska företräda respektive myndighet i ett sådant samverkansråd.

5.7 NCSC:s fortsatta utveckling

I delbetänkandet anges att centret med stor sannolikhet kommer att behöva ett eget Security Operations Center (SOC) som kan identifiera, analysera och motverka digitala hot. Säkerhetspolisen har svårigheter att överblicka vad ett sådant SOC-uppdrag för centret skulle omfatta. Det finns inte heller någon beskrivning av detta i delbetänkandet.

Övrigt

I nästa delbetänkande ska utredningen behandla bland annat frågor om informationsdelning. Säkerhetspolisen vill redan nu framhålla att det även fortsättningsvis behöver finnas ett särskilt samarbete med möjligheter till informationsdelning mellan Säkerhetspolisen och försvarsunderrättelsemyndigheterna.

Säkerhetspolisen noterar att ett antal betänkanden, promemorior och andra förslag som på olika sätt berör cybersäkerhetsområdet är under beredning i skrivande stund.[1] Förslagen är i vissa fall motstridiga vilket innebär att vägval i en viss fråga kommer att påverka även de övriga förslagen. Även i de fall förslagen inte är motstridiga påverkar de varandra och därmed styrningen och regleringen av cybersäkerhetsområdet. Enligt Säkerhetspolisens mening är det viktigt med ett helhetsgrepp och att samordning sker i den fortsatta beredningen av förslagen så att styrningen inom området blir konsekvent och effektiv.

Säkerhetspolisen noterar även att det saknas en 8 § i den föreslagna förordningen.

Remissvaret har beslutats av säkerhetspolischefen Charlotte von Essen. Verksjuristen Jessica Ovin har varit föredragande.

[1] Bland betänkanden, promemorior och andra förslag som berör cybersäkerhetsområdet och är under beredning kan följande nämnas: Försvarsberedningens delbetänkande *Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret* (Ds 2023:34), *Digital operativ motståndskraft för finanssektorn (DORA)* (Fi2024/00073), *Nya regler om cybersäkerhet* (SOU 2024:18*), En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur* (Fi2024/00185) och MSB:s förslag till en nationell plan för hantering av cybersäkerhetsincidenter och kriser. Även Underrättelseutredningens (Fö2023:04) kommande förslag kan komma att påverka verksamheten inom cybersäkerhetsområdet.