Myndigheten för samhällsskydd och beredskap

Remissvar

Datum
2024-05-24

Ärendenr
MSB2024-06366

Ert datum
2024-05-01

Er referens
Fö2024/00785

Avdelningen för cybersäkerhet och säkra kommunikationer
Johan Turell

Regeringskansliet
Försvarsdepartementet

Delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning.

Myndigheten har fått tillfälle att lämna synpunkter på ovan nämnt delbetänkande.

Sammanfattning

MSB instämmer i att det nationella cybersäkerhetscentrets (NCSC) former för ledning, organisering och styrning behöver utvecklas för att uppnå målet att stärka Sveriges förmåga på cybersäkerhetsområdet.

MSB ser positivt på att de myndigheter som deltar i NCSC:s verksamhet föreslås medverka och samverka utifrån samma grundförutsättningar. Att Myndigheten för psykologiskt försvar (MPF) föreslås bli en del av NSCS:s verksamhet kommer även det att stärka det nationella cybersäkerhetsarbetet.

MSB menar dock att utredningen i sitt delbetänkande inte har beaktat de förhållanden som följer av områdets komplexitet och EU-rätten i tillräcklig omfattning. MSB konstaterar att flera centrala förslag lämnas utan tillräcklig motivering och närmare analys av alternativ.

Förslaget som behandlar placeringen av CERT-SE och uppgiften som CSIRT-enhet är otydligt anser MSB, och detta gör det svårt att fullt ut ta ställning till centrala delar av utredningen.

Rollen och uppgifterna som den nationella cyberkrishanteringsmyndigheten ska ha överensstämmer i hög grad med de uppgifter och den förmåga som redan finns i dag hos MSB. För att inte försena genomförandet av NIS2-direktivet ytterligare är det centralt att MSB även fortsättningsvis ges rollen som nationell CSIRT-enhet, cyberkrishanterings-myndighet och NIS-kontaktpunkt. MSB bedömer att det går att på ett resurseffektivt sätt förena dessa roller hos MSB med en stark samordning och integrering av verksamhet i NCSC. MSB utvecklar detta resonemang i en bilaga till detta remissvar.

Synpunkter av principiell karaktär

Centrala förslag lämnas utan tillräcklig motivering och analys

I delbetänkandet presenteras ett flertal förslag med stor påverkan på cybersäkerhets-området, exempelvis att verksamheten i NCSC ska avgränsas till vad som benämns

”betydande incidenter” i NIS2-direktivet[1] samt att FRA ska vara cyberkrishanterings-myndighet och CSIRT-enhet. En grundläggande princip om att allt arbete som kan genomföras i NCSC ska genomföras i NCSC ställs även upp. Utredningen betonar även tydligt samverkan som grundprincip.

MSB är medveten om att det har varit ett komplext uppdrag som har bedrivits under knappa tidsförhållanden. På grund av komplexiteten i frågorna hade det dock varit önskvärt att centrala förslag och principer motiverades i större utsträckning, där även olika alternativa lösningar vägts mot varandra.

Placering av CERT-SE och uppgiften som CSIRT-enhet

MSB uppfattar en otydlighet när det gäller förslagen kring placering av funktionen CERT-SE och uppgiften som CSIRT-enhet. Här kan noteras att i sammanfattningen konstateras att utredningens bedömning är att

> …ett effektivt utförande av NCSC:s uppgifter förutsätter att verksamheten i den nationella CSIRT:en (Computer Emergency Response Team) förs över från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt och NCSC.

Samtidigt anger utredningen att de närmare förutsättningarna för denna överföring bör utredas i ett annat sammanhang och att verksamheterna så länge ska integreras så nära som möjligt. Förslaget konkretiseras i avsnitt 3.4.4. där det konstateras att

> …de närmare rättsliga, organisatoriska och praktiska förutsättningarna för en verksamhetsöverföring, bland annat hur en sådan skulle påverka MSB:s krishanterings-, informationssäkerhets- och cybersäkerhetsarbete och särskilt de ansvarsområden som följer av NIS-direktiven, bör dock utredas närmare i ett annat sammanhang.

Slutligen konstaterar utredningen i avsnitt 6.6 att några EU-rättsliga konsekvenser inte följer av förslaget eftersom utredningen i nuläget inte föreslår någon överföring. Det är således en rad grundläggande frågor som kräver fortsatt utredning och det är därför enligt MSB:s bedömning svårt att nu ta ställning till förslagets genomförbarhet.

EU-rättsliga konsekvenser

Cybersäkerhetsområdet är av stor strategisk vikt för EU. Nuvarande och kommande EU-reglering[2] medför att cybersäkerhetsområdet kommer att vara ett av de mest EU-reglerade områdena, något som minskar den nationella handlingsfriheten.

Utredningen presenterar inte någon analys av de EU-rättsliga konsekvenserna av förslagen, trots att utredningen både använder begrepp som ”betydande incident” från NIS2-

[1]EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

[2] För en sammanställning, se MSB EU förändrar cybersäkerhetsområdet Årsrapport it-incidentrapportering 2023, sid 33 – 43.

direktivet och förordar en annan fördelning av EU-uppgifter än den utredning som tar fram förslag på hur NIS2- och CER-direktivet ska genomföras i Sverige.[3]

MSB instämmer i utredningens bedömning att de EU-rättsliga konsekvenserna behöver utredas innan en förändring sker, och önskar särskilt peka på de utmaningar som myndigheten i en särskild skrivelse identifierat vid en överföring av CERT-SE från MSB till FRA.[4]

MSB anser att det hade varit värdefullt med ett fördjupat resonemang om hur nationella initiativ på cybersäkerhetsområdet kan genomföras på ett sätt som kompletterar Sveriges åtaganden enligt EU-rätten.[5]

Övriga synpunkter på delbetänkandet

MSB (avsnitt 3.3.4)

MSB noterar att beskrivningen av MSB:s uppgifter inte är fullständig. Utredningen hade vunnit på, framför allt, en mer detaljerad beskrivning av CSIRT-enhetens uppgifter och förmågor, exempelvis en beskrivning av operativ samverkan i Sverige med aktörer utanför NCSC och internationellt. I princip all den verksamhet som CERT-SE bedriver, särskilt när funktionen utför de uppgifter som MSB har i rollen som ”CSIRT-enhet” enligt NIS-direktivet, är författningsstyrd. Genom NIS2-direktivet och annan kommande EU-reglering (såsom Cyberresiliensakten[6] och Nätverkskoderna[7]) blir den författningsreglerade styrningen ännu mer omfattande och detaljerad.

Mål och utgångspunkter (avsnitt 5.1)

MSB instämmer i flertalet av de mål som utredningen ställer upp, såsom utvecklad och kravställd samverkan, ett allriskperspektiv, samt att näringslivets förmågor bättre tas tillvara. MSB är också positiv till att cybersäkerhetsarbetet konsolideras för att på så sätt skapa goda möjligheter till synergier och resurseffektivitet. Flera av målen svarar även mot de utmaningar som Riksrevisionen lyft i sin granskning.[8]

En förordning om Nationellt cybersäkerhetscenter (avsnitt 5.1.1)

MSB instämmer i att det kan finnas anledning att reglera verksamheten i NCSC via förordning för att få en tydligare styrning jämfört med en lösning med överenskommelser.

---

[3] Utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (Fö 2023:01).
[4] Se närmare om sådana EU-rättsliga konsekvenser i bilaga 1 sid 9 – 18.
[5] För mer information se Bilaga 1 sid 19. Se närmare om konsekvenser av en överföring av CERT-SE från MSB till FRA i Bilaga sid 9 och framåt.
[6] European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)).
[7] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 11.3.2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.
[8] Regeringens styrning av samhällets informations- och cybersäkerhet − både brådskande och viktig (RiR 2023:8).

För att detta ska bli framgångsrikt behöver dock mål och uppgifter vara tydliga. Begrepp som ”förebygga”, ”upptäcka” och ”hantera” betyder olika saker för olika organisationer och behöver därför definieras och preciseras.

Det är dock svårt att se hur förordningsförslaget bidrar till ökad tydlighet när uppgifter och mål inte har detaljerats ytterligare jämfört med skrivningarna i den överenskommelse som styr NCSC:s arbete idag. Det finns heller inte någon redogörelse i delbetänkandet för hur utredningen ser på uppgifternas innehåll. Problematiken med otydlighet förstärks genom att förordningsförslagets lista över NCSC:s uppgifter inte heller görs uttömmande.

Utredningen problematiserar det i uppdragsbeskrivningen använda begreppet *större* it-incidenter och dess betydelse samt föreslår att detta ersätts med NIS2-begreppet *betydande* it-incidenter[9]. MSB delar utredningens bedömning av att begreppet större it-incidenter är otydligt. Att istället välja att knyta verksamheten hos NCSC tilll begreppet ”betydande it-incident” enligt NIS2-direktivet får dock en rad följdverkningar som utredningen inte har analyserat.

En händelse ska behandlas som en ”incident” i NIS2-direktivets bemärkelse om den:

1. uppfyller definitionen av begreppet ”incident” i NIS2-direktivet,
2. inträffar hos en väsentlig eller viktig verksamhetsutövare och
3. inte samtidigt utgör en säkerhetsskyddsincident.

I NIS2-direktivets mening är ”betydande incident” en delmängd av ”incident”, och båda begreppen definieras formellt. Mot den bakgrunden är följden av utredningens förslag att *endast* subklassen av incidenter som utgör betydande incidenter, men som inte utgör säkerhetsskyddsincidenter, ska hanteras i NCSC. MSB menar därför att utredningens förslag innebär att:

1. NCSC inte kommer ha någon särskild uppgift när en it-relaterad säkerhetsskydds-incident inträffar.
2. De i centret ingående myndigheterna ska samarbeta mer för att hantera sådana incidenter som NCSC ges i uppgift att koncentrera sig på (”medel allvarliga” incidenter). I många fall kommer de allvarligaste it-incidenterna att utgöra säkerhetsskyddsincidenter, och hanteringen av sådana incidenter ingår inte, enligt utredningens förslag, i NCSC:s uppdrag.
3. It-incidenter som inte omfattas av Cybersäkerhetslagen inte hanteras i NCSC, detta eftersom det inte ingår i NCSC:s uppdrag att hantera allvarliga oönskade it-relaterade händelser som inträffar hos verksamhetsutövare som inte ingår i Cybersäkerhetslagens tillämpningsområde.

I NCSC:s befintliga uppdragsbeskrivning avgränsas inte centrets verksamhet till att endast hantera och förebygga incidenter inom ramen för en särskild reglering. Det framgår också av avsnitt 5.3.2 i delbetänkandet att utredningen menar att den inriktningen ska kvarstå.

MSB vill även rikta uppmärksamhet mot att EU-kommissionen har rätt att i kommande genomförandeakter ytterligare precisera begreppet ”betydande incident” med syfte att närmare inrikta och harmonisera incidentrapportering i unionen. Centrets verksamhetsram

[9] NIS2-begreppet är dock egentligen ”betydande incidenter”.

kommer därmed med utredningens förslag att i centrala aspekter definieras av en utomstående entitet (EU-kommissionen).

Skyldighet att medverka och bidra (avsnitt 5.3.1)

MSB delar utredningens förslag att centermyndigheternas skyldighet att medverka i och bidra till cybersäkerhetscentret ska regleras i varje myndighets instruktion och samordnas i det strategiska rådet.

För att kunna skapa önskade synergieffekter är det dock inte tillräckligt att enbart allmänt ålägga myndigheterna att samverka inom sina respektive uppdrag, utan det krävs ett arbete med att jämka samman och förtydliga kopplingarna mellan centret och centermyndigheternas respektive uppdragsbeskrivningar. Långtgående tolkningsmöjligheter vad som vid varje givet tillfälle ”kan” göras av andra myndigheter försvårar enligt MSB:s bedömning möjligheterna att planera och resurssätta den gemensamma verksamheten i NCSC.

Därför ser MSB, till skillnad från utredningen, ett behov av att snarast utvärdera centrets och de deltagande myndigheternas rättsliga handlingsutrymme, vilket också Riksrevisionen påpekat. Utan det kommer den formulering som valts i myndigheternas instruktioner inte att leda till den utveckling som önskats under de senaste sex åren.

EU-reglering i förhållande till den svenska säkerhetsskyddslagstiftningen (5.3.2)

Utredningen hanterar inte frågan om vilka gränsytor som finns i centret mellan EU:s regelverk och den svenska säkerhetsskyddslagstiftningen. Skrivningarna i avsnitt 5.3.2 antyder att användningen av begreppet ”betydande incident” ger en möjlighet att koppla samman EU:s regelverk och den svenska säkerhetsskyddslagstiftningen, och därmed ge en lämplig grund för myndigheter med operativa uppgifter med koppling till nationell säkerhet att bidra till NCSC:s verksamhet. MSB delar inte denna bedömning eftersom begreppet ”betydande incident”är definierat i NIS2-direktivet och endast gäller sådana incidenter inom direktivets tillämpningsområde som inte samtidigt utgör säkerhetsskyddsincidenter.[10]

CSIRT-funktionen CERT-SE (avsnitt 5.3.3)

I avsnittet problematiseras kring överlappningar och oklara gränssnitt mellan funktionen CERT-SE och NCSC. Utredningen konstaterar att om verksamheten inom ramen för det formella uppdraget som CSIRT-enhet enligt NIS2-direktivet utökas ytterligare så kommer fler överlappningar att uppstå. De exempel som utredaren ger på en utökad verksamhet är dock uppgifter som MSB som CSIRT-enhet redan utför idag. Överlapp mellan myndigheters uppdrag och NCSC:s uppdrag bör istället ses som positivt eftersom det ger förutsättningar för synergier när MSB som CSIRT-enhet bedriver sin verksamhet inom ramen för NCSC.

Det framgår inte vilka praktiska, resursekonomiska och säkerhetsrelaterade skäl som talar för att verksamheterna förs samman jämfört med den huvudregel utredningen redan har föreslagit, dvs att verksamhet som *kan* genomföras i NCSC *ska* genomföras i NCSC.

[10] Nationell säkerhet är undantaget från NIS2-direktivets tillämpningsområde enligt artikel 2 p 6, se även SOU 2024:18 s 154 ff.

MSB delar, enligt ovan, utredningens syn om att samarbetet i operativa frågor mellan myndigheterna i NCSC bör koncentreras till allvarliga it-incidenter. MSB konstaterar att en sådan inriktning dock medför att uppgiften som CSIRT-enhet utifrån NIS2-direktivet inte fullt ut kan utföras inom ramen för NCSC. Skälet till det är att CSIRT-enheten enligt resonemanget ovan inte kan avgränsas till betydande incidenter.[11] CSIRT-enheten ska hantera och ge stöd vid incidenter som inträffar hos väsentliga eller viktiga verksamhetsutövare, oavsett om de är betydande eller inte.

Det kommer att finnas tusentals väsentliga och viktiga verksamhetsutövare som omfattas av NIS2-direktivet i Sverige.[12] CSIRT-enheten ska skyndsamt bistå dessa verksamhetsutövare när de begär stöd. Det finns en risk att NCSC, om CERT-SE med uppdraget som CSIRT-enhet flyttas till FRA, begränsas i sina möjligheter att fokusera på allvarliga it-incidenter.

I Bilaga 1 redovisar MSB ytterligare konsekvenser som skulle följa av en överföring av CERT-SE.

Vidare konstaterar MSB att utredningen om genomförande av NIS2- och CER-direktiven redan har utrett hur myndighetsrollerna som följer av NIS2-direktivet bör fördelas bland svenska statliga myndigheter. I regeringens inriktning till det arbetet ingår också att se över hur NIS2- och CER[13]-direktiven kan implementeras på ett samordnat sätt som ger synergieffekter. NCSC-utredningens förslag innebär att den ordning som den utredningen föreslår åsidosätts, med en mindre sammanhållen implementering som följd.

Slutligen föreslår NCSC-utredningen att FRA ska bli nationell cyberkrishanterings-myndighet utifrån NIS2-direktivet. Utredningen redogör inte för skälen till sin bedömning. Under utredningens arbete med frågan har MSB haft ett samtidigt regeringsuppdrag i vilket det har ingått att analysera vilken roll och uppgifter en nationell cyberkrishanteringsmyndighet ska ha i det svenska systemet utifrån NIS2-direktivets art. 9 och vissa ytterligare medskick ifrån regeringen. MSB redovisade den 15 maj regeringsuppdraget att ta fram underlag och förslag till en nationell plan för hantering av cybersäkerhetsincidenter och kriser. I uppdraget ingick att utreda vilken roll och uppgifter cyberkrishanteringsmyndigheten ska ha. MSB:s slutsatser blev att den rollen och de uppgifterna i hög grad överenstämmer med den roll, de uppgifter och den förmåga som MSB redan har. I uppdragsredovisningen har MSB pekat på risker i termer av dubbelarbete och oklar ansvarsfördelning som uppstår om någon annan myndighet får uppdraget.[14]

[11] Enligt NIS2-direktivet art. 11, p. 3c har CSIRT-enheten i uppgift att vidta åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahålla stöd till de berörda väsentliga och viktiga entiteterna.
[12] Se uppskattningar gjorda i SOU 2024:18 kapitel 12.
[13] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.
[14] Se Bilaga 2: Sveriges cyberkrishanteringsplan - förslag till nationell plan för hantering av cybersäkerhetsincidenter och kriser, sid. 21-23, 36-55, 58-64, 77-86, 98-110, 126-129 och 132-144.

Deconfliction (avsnitt 5.4.3)

Utredningen föreslår att NCSC bör få i uppdrag att utarbeta former för ”deconfliction” i verksamheten där både skyddsintresset och underrättelseintresset bör vara adekvat representerat.

MSB instämmer i att hanteringen av målkonflikter när det gäller hur information ska användas, för underrättelsesyfte eller skyddssyfte, är en central fråga. MSB vill lyfta fram att för den nationella CSIRT:en är det viktigt att ha högt förtroende att kunna hantera skyddsvärd information på ett säkert sätt och samtidigt kunna i så stor omfattning som möjligt dela information med berörda intressenter i Sverige och de internationella CSIRT-nätverken. Det gäller särskilt information om sårbarheter, en hantering som i stora delar kommer att vara författningsreglerad i samband med genomförandet av NIS2-direktivet och därefter Cyberresiliensakten. Centret behöver därför förhålla sig till en rad regleringar vid utarbetande av en process för hantering av målkonflikter eller deconfliction.[15] MSB ser gärna ett fördjupat resonemang kring hur NIS2-direktivets och Cyberresiliensaktens regler ska ses i förhållande till de uppgifter som åligger FRA enligt myndighetens instruktion[16] att stödja Försvarsmaktens cyberförsvarsförmåga. Vid en flytt av CERT-SE till en underättelsemyndighet skulle det vara extra viktigt.[17]

Ikraftträdande (avsnitt 7)

MSB bedömer att ett genomförande av förslagen till den 1 september 2024 kommer att ytterligare försena Sveriges genomförande av NIS2-direktivet, särskilt när det gäller CSIRT-enhetens förmågeutveckling och den nationella cyberkrishanteringsmyndighetens etablering.

I detta ärende har generaldirektör Charlotte Petri Gornitzka beslutat. Johan Turell har varit föredragande. I den slutliga handläggningen har också verksamhetsstrategen Helena Andersson, avdelningschefen Åke Holmgren och rättschefen Anna Asp deltagit.

Charlotte Petri Gornitzka Johan Turell

Bilagor

Bilaga 1: Konsekvenser av överföring av cybersäkerhetsverksamhet från MSB till NCSC-SE/FRA

Bilaga 2: Sveriges cyberkrishanteringsplan – förslag till nationell plan för hantering av cybersäkerhetsincidenter och kriser

[15] Art 12 NIS2-direktivet, se även artikel 14-18 i Cyberresiliensakten .
[16] 3 e § förordning (2007:937) med instruktion för Försvarets radioanstalt
[17] Se bland annat Bilaga 1 Konsekvenser av överföring av cybersäkerhetsverksamhet från MSB till NCSC-SE/FRA sid 11-12.