

Försvarsdepartementet

fo.remissvar@regeringskansliet.se
carolina.hofgren@regeringskansliet.se

Svar avseende remiss av Ett nytt Nationellt cybersäkerhetscenter – del 1

TechSverige lämnar på eget initiativ ett remissvar avseende rubricerat delbetänkande (dnr Fö2024/00785).

TechSverige är en bransch- och arbetsgivarorganisation för företag inom techsektorn med drygt 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i förbundsgruppen Almega och i Svenskt Näringsliv.

TechSverige välkomnar att det föreslås en ökad samlad förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter. Som framgår nedan, är det dock ett svårt uppdrag att genomföra som hittills inte har fått den uppmärksamhet det förtjänar under flera mandatperioder.

Statens roll

Kompetensfrågorna kommer att vara avgörande och statens viktigaste bidrag till höjd informations- och cybersäkerhet är förmodligen att vidta åtgärder för att minska kompetensbristen. Även ändamålsenliga resurser av andra slag behövs för det statliga arbetet ska få genomslag. Det är förmodligen också så att den kritik som har föranlett utredningsuppdraget beror på högt ställda förväntningar, utan att tillräckliga resurser, förberedelser och ledarskap har funnits på plats. Inom informations- och cybersäkerhetsarbetet går dessa problem långt bak i tiden.

Allmänt om förslagen

Även om TechSverige har välkomnat både Nationell cybersäkerhetscenters (NCS) arbete och regeringens engagemang i informationssäkerhetsfrågorna blir det svårt att ställa sig bakom förslaget att flytta centret till Försvarets radioanstalt (FRA).

I ljuset av genomförandet av NIS2-direktivet, de allmänna förutsättningarna för ett brett informationssäkerhetsarbete i samhället och redan gällande lagar och regler vore det rimligare att placera centret (eller motsvarande funktioner) vid Myndigheten för samhällsskydd och beredskap (MSB). Nedan utvecklas detta något och TechSverige avser återkomma till frågorna i remissvaret avseende delbetänkande Nya regler om cybersäkerhet (SOU 2024:18), dnr Fö2024/00496.

Som framgår nedan, är det remitterade underlaget under alla omständigheter inte tillräckligt som beslutsunderlag.

Kort om remissen

TechSverige noterar att inga näringslivsorganisationer har tagits upp på remisslistan. Informations- och cybersäkerhetsfrågor är mycket högt uppe på dagordningen för många aktörer i samhället – inte minst i näringslivet. Hur staten organiserar detta arbete är en fråga som angår långt fler än de elva statliga myndigheter som upptas på remisslistan. Som jämförelse remitterades delbetänkandet om genomförandet av NIS2-direktivet (som delvis berör samma frågor) till hela 213 remissinstanser.

Allmänt om bakgrunden till utredningen

I uppdraget till utredaren står det att "verksamheten inom NCSC har inte nått den effekt som krävs för att centret fullt ut ska uppnå sitt syfte". Även om TechSverige har hört till dem som har önskat mer av Nationellt cybersäkerhetscenter (NCSC) så speglar det uttalandet förmodligen orimliga förväntningar. Den dåvarande regeringen fattade beslutet om NCSC i december 2020, beslutet om uppdraget till utredaren fattades i oktober 2023.

Observationen är snarare att NCSC har kommit längre än förväntat på tre år. Det har förvisso gjorts genom att bygga på existerande samarbeten och forum, liksom att börja med områden och aktörer som redan låg långt fram i arbetet.

Samarbetsformen och andra förutsättningar för centret som den tidigare regeringen gav var otillräckliga. Att givet detta, ifrågasätta NCSC:s resultat på den korta tiden och dessutom föregripa vad utredaren borde komma fram till (jfr DN Debatt, 23 april 2023), kommer nog inte vara till fördel för Sveriges samlade behov inom informations- och cybersäkerhet.

Även utredaren till föreliggande rapport fick ett svårt uppdrag att utföra på kort tid. Med detta sagt, så finns det behov av tydligare former för verksamheten och framför allt en större hänsyn till det sammanhang som NCSC ska verka i.

Synpunkter på valda förslag

TechSverige avstyrker förslaget att FRA ska ha huvudansvar för att leda samordning, utveckling och genomförande av centrets verksamhet.

Huvudskälet till att avstyrka förslaget är att denna fråga inte kan avgöras isolerat till NCSC:s verksamhet utan måste bestämmas i ett mycket bredare sammanhang. TechSverige avser utveckla synpunkter på detta i remissvaret avseende delbetänkande Nya regler om cybersäkerhet (SOU 2024:18), dnr Fö2024/00496.

Utöver frågan om huvudmannskapet, presenteras några andra förslag rörande centrets verksamhet, reglering, ingående myndigheter m.m. Dessa förslag kan verka rimliga, men behöver också prövas när en mer gedigen utredning förhoppningsvis görs om framtiden, sammanhanget och formerna för NCSC (eller något motsvarande).

TechSverige avstyrker förslaget att verksamheten i den nationella CSIRT:en förs över från MSB till FRA och NCSC.

Ställningstagandet blir en följd av TechSveriges syn att hela frågan kräver mer av utredning och hänsyn till redan rådande förutsättningar för ett brett arbete med informations- och cybersäkerhet. Förslaget föregriper det remitterade NIS2-betänkandet.

I sak framförs inte någon djupare analys till grund för skälen, förutsättningarna eller vad konsekvenserna skulle bli. Detta tillkortakommande vidgår även utredaren (s. 44).

Det framstår som principiellt tveksamt att flytta verksamhet som bl.a. regleras av inre marknadsdirektiv från EU till en underrättelsemyndighet. Konsekvenserna av detta är i dagsläget svåra att överblicka.

FRA:s grunduppdrag som signalspaningsmyndighet av dessutom utomordentlig vikt för Sveriges säkerhet. Grunduppdraget kan förväntas öka i omfattning i och med det försämrade säkerhetsläget samtidigt som även det breda arbetet med

informationssäkerhet i samhället också förväntas öka. Att förena ett underrättelseuppdrag, med stora krav på sekretess m.m., och ett uppdrag där myndighet behöver nå långt ut till många aktörer förefaller svårgörligt. Det är och förmodligen inte heller ändamålsenligt för endera uppdraget.

TechSverige är dock positiv till ambitionen, oavsett huvudmannaskap, att förbättra samarbetet med näringslivet.

Cybersäkerhetscentret bör stärka och fördjupa samverkan med näringslivet och andra intressenter. NCSC bör därför få i uppdrag att utreda relevanta målgruppers förväntningar och behov, liksom hur intressenterna kan bidra till centrets verksamhet och mål. Hur detta ska samordnas med andra gränssnitt mot näringslivet berörs dock inte nämnvärt.

TechSverige anser att konsekvensbeskrivningen är otillfredsställande.

Konsekvensbeskrivningarna är begränsade och korta, men också anmärkningsvärda. Utredaren tycks bl.a. mena att förslagen innebär "färre administrativa och praktiska problem och att begränsade resurser – inte minst personal – utnyttjas bättre" och att det i sin tur "ökar cybersäkerheten i samhället och stora kostnader kopplade till cyberhot och incidenter undviks". Det är naturligtvis ett önskvärt resultat, men möjligen otillräckligt analyserat och baseras också på en övertro om vad en enskild aktör kan åstadkomma inom det breda informations- och cybersäkerhetsarbetet.

* * *

Avslutningsvis vill TechSverige framhålla att regeringens engagemang i frågorna om informations- och cybersäkerhet är mycket välkommet.

Utredaren redogör för delar av den kritik som har riktats mot NCSC och dess arbete från bl.a. näringslivet. TechSverige noterar dock att det också finns ett stort engagemang bland TechSveriges medlemmar och allmänt i näringslivet för att öka det privat–offentliga samarbetet i dessa angelägna frågor.

Det arbete som NCSC har gjort hittills kommer också att behövas framgent. Alla har att vinna på en mer samordnad och samlande politik på området. TechSverige har goda förhoppningar om att regeringen kan åstadkomma det med ett bredare, och i vissa avseenden, mer förutsättningslöst sätt att ta sig an frågorna.

En informationssäkerhetspolitik vore välkommen.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Fredrik Sand
näringspolitisk expert