Stockholm 2024-05-24

Försvarsdepartementet
Enheten för cyber- och hybridfrågor

Er referens: Fö2024/00785
Vår referens: 24-003

Netnod fick den 26 april från Försvarsdepartementet möjlighet att komma med synpunkter på ett förslag på *Ett nytt Nationellt cybersäkerhetscenter*.

Netnod inkommer härmed med följande synpunkter:

- Sekretess eller motsvarande för delad information måste utredas grundligt i kommande delutredning för att undvika att privata aktörer får incitament att *inte* dela information
  Netnod anser att nästa del av utredningen bör komma fram till att information delad med cybersäkerhetscentret ska täckas av liknande sekretessregler som information delad i NTSG
- Utredningen förordar ett allriskperspektiv som riskerar bli urvattnat
  Netnod anser att allriskperspektiv inte är ändamålsenligt, och att man istället ska använda sig av specifika och väldefinierade risker och hot
- Utredningen diskuterar inte risker kring strategisk kortsiktighet och dagens regressiva incitament hanteras inte
  Netnod anser att incitament för informationsdelning och annat deltagande måste utredas, cybersäkerhet får inte vara enbart en kostnadsfråga för inblandade aktörer

Netnod är positiva till förslagen generellt, och speciellt att centret ej är tillsynsmyndighet eller regleringsmyndighet eller placerad hos sådan.

Patrik Fältström
Säkerhetsskyddschef

Tel: +46-706059051
Email: paf@netnod.se

Netnod AB
Greta Garbos väg 13
169 40 Solna

Bilaga 1 - Detaljerade kommentarer

1. Netnod Kommentarer

Netnod är övergripande positiva till förslaget. Det är en förbättring för privat sektor med en huvudman för NCSC jämfört med den nuvarande situationen där det finns en otydlighet i vilken organisation som är ansvarig för NCSC.

Utredningen föreslår ett tydligare mandat, genom handlingar som att regeringen tillsätter chef och att även personal-, arbetsgivar- och budgetansvar diskuteras i kommande betänkande, är ett steg i rätt riktning.

Netnod är också positiva till att delbetänkandet föreslår att centret (dvs FRA) **ej** är tillsynsmyndighet eller regleringsmyndighet. Detta undanröjer en del av de hinder som finns för informationsdelning mellan privat sektor och offentlig sektor.

Informationsdelning
Nästa delbetänkande kommer att behandla informationsdelning, och här vill Netnod poängtera att det är av yttersta vikt att information delad med NCSC kan hanteras som skyddsvärd enligt offentlighet- och sekretesslagen samtidigt som den kan delas mellan de aktörer som har behov av den, vilket kan inkludera fler spelare än de i NCSC ingående myndigheterna. Netnod anser detta bör hanteras liknande den förändring som gjordes i 44 kap, 4 § offentlighets- och sekretesslagen genom Regeringens proposition 2023/24:60.

Informationsdelningssystemet måste dessutom fungera på så sätt att information av värde för andra aktörer delas utan fördröjning så att inte bara lägesbild kan skapas utan även uppdateringar av lägesuppfattning.

Allriskperspektiv
Beredskaps- och säkerhetslogiken i Sverige före 90-talet var inte baserad på ett allriskperspektiv, utan var baserat på betydligt spetsigare perspektiv där specifika hot skulle mötas och hanteras. Detta hade som konsekvens att det var förhållandevis oproblematiskt att konstruera scenarier och öva dessa inom relevanta säkerhetsperspektiv.

Netnod är oroade över att delbetänkandet inte tillräckligt djupt reflekterar kring konsekvensen av att förorda ett allriskperspektiv jämfört med alternativet, att arbeta med ett antal spetsigare perspektiv. Problem kan till exempel uppstå genom att ingående aktörer, när man ska enas om risk- och sårbarheter ur ett allriskperspektiv, inte blir tillräckligt spetsiga. Var och en kan enbart göra bra bedömningar om risker och hot som man förstår, och en förhandling kan leda till att enbart urvattnade hypotetiska risker hanteras. Dessutom kan dessa övergripande risker, till skillnad från spetsiga, vara svåra att realisera i övningar och bedömningar som leder till förmågehöjande åtgärder.

Det kan mycket väl vara så att det centret har tillräcklig kompetens att på ett meningsfullt sätt arbeta med ett allriskperspektiv, men Netnod ställer sig tveksamt till att allriskperspektiv, av anledningar ovan, bör användas av inblandade aktörer.

Strategisk kortsiktighet
Övergången till ett allriskperspektiv kan underlätta för en positiv utveckling på kort sikt, men det blir svårare att se långsiktiga vinster. Detta då allriskperspektiv hittills har lett till att de risker och hot som tagits fram delvis har kunnat ignoreras. Allriskperspektiv gör att det blir svårare att och omständigare att framarbeta relevanta övningar, speciellt mellan aktörer som har gjort olika bedömningar av relevanta hot och risker genom allriskperspektiv[1]. Detta i sin tur leder till sämre möjligheter att se konsekvenser och göra konsekvensanalyser som visar på reell samhällspåverkan. Utan sådana konkreta analysresultat blir riskerna och hoten lättare att ignorera. Vi förespråkar därför istället att specifika och väldefinierade risker och hot används.

Incitament måste finnas för att aktörer ska arbeta långsiktigt med cybersäkerhet, så att cybersäkerhet inte bara är och förblir en kortsiktig kostnadsfråga, som det mer än gärna tummas på i fredstid. Netnod har flera gånger påpekat att negativa incitament för inrapportering i form av böter vid avsaknad av inrapportering inte hjälper. Vi står fast vid att att positiva incitament behövs för att balansera den kombination av negativa incitament vi ser idag, t.ex.:

- Det är komplicerat att rapportera in cyberincidenter
- Risk att information som delas blir del av ett tillsynsärende
- En avsaknad av återrapportering från de som tar emot rapporter
- Böter i det fall man inte rapporterar och blir påkommen

Netnod har bla sagt detta i sitt remissvar på *En telesamverkansgrupp för fredstida kriser och höjd beredskap (Fi2023/01681)*[2].

[1] Se bland annat *Risk i svensk beredskap,* FOI, https://www.foi.se/rest-api/report/FOI-R--5285--SE, för utveckling av motsvarande resonemang.
[2] Netnod svar på Fi2023/01681, https://www.regeringen.se/contentassets/fb0cf3ec2f9a440ebbba89904280213b/netnod.pdf