Stockholm 2025-01-13

Försvarsdepartementet
Rättssekretariatet

Er referens: Fö2024/01550
Vår referens: 25-001

Netnod fick oktober 8 från Försvarsdepartementet möjlighet att komma med synpunkter på *Remiss av betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)*.

Netnod inkommer härmed med följande synpunkter:

- Samspelet mellan säkerhetsskyddslag, CSL och LoM är ej väldefinierat för tillgänglighetsaspekter av speciellt digitala tjänster
  Netnod anser att samspelet mellan lagrummen måste förtydligas för tillgänglighetsaspekter av säkerhetskänslig verksamhet
- Allriskansatsen används som helhetsgrepp utan komplement
  Netnod anser att om en allriskansats ska användas så måste detta kompletteras med verktyg som gör att verksamheter hanterar risk som verksamheterna inte redan är medvetna om

Lagförslaget är en del av flera lagförslag som ämnar höja motståndskraften hos aktörer inom EU, men det är fortfarande oklart vilket effekt detta förslag och andra förslag ämnar uppnå och hur denna effekt ska mätas och utvärderas.

Patrik Fältström
CSO

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

Netnod AB
Greta Garbos väg 13
169 40 Solna

Bilaga 1 - Detaljerade kommentarer

1. Inledning

Utredningen (SOU 2024:64) har utrett pusselbiten CER-direktivet i svensk kontext, och kommit med förslag på hur CER ska implementeras i svensk rätt och samspela med andra lagrum, inklusive säkerhetsskyddslagen. Den föreslagna lagen kallas för "*lag om motståndskraft hos kritiska verksamhetsutövare"* och refereras till som LoM i detta remissvar. Vidare refererar CSL till den föreslagna lagen i SOU 2024:18, SäkL till Säkerhetsskyddslag (2018:585) och SäkF till Säkerhetsskyddsförordning (2021:955).

På ett högre plan anser Netnod, precis som i första delen av utredningen, att det är oklart vilken effekt denna lag skall uppnå, och hur denna effekt skall mätas och utvärderas över tid. LoM, precis som CSL, är omfattande regelverk som tar betydande resurser i anspråk att efterleva, och därmed måste dessa gå att motivera ur ett resursperspektiv, eller med andra ord, *hur vet vi att CSL och LoM är bästa tänkbara användning av samhällets begränsade resurser för att uppnå en högre motståndskraft och därmed cybersäkerhetsnivå?*

Netnod noterar att LoM tillskriver aktörer inom digital infrastruktur rättigheter snarare än skyldigheter, bland annat genom att vara undantagna från 3–6 kap av den föreslagna lagen.

2. LoM och Säkerhetsskyddslagen mfl

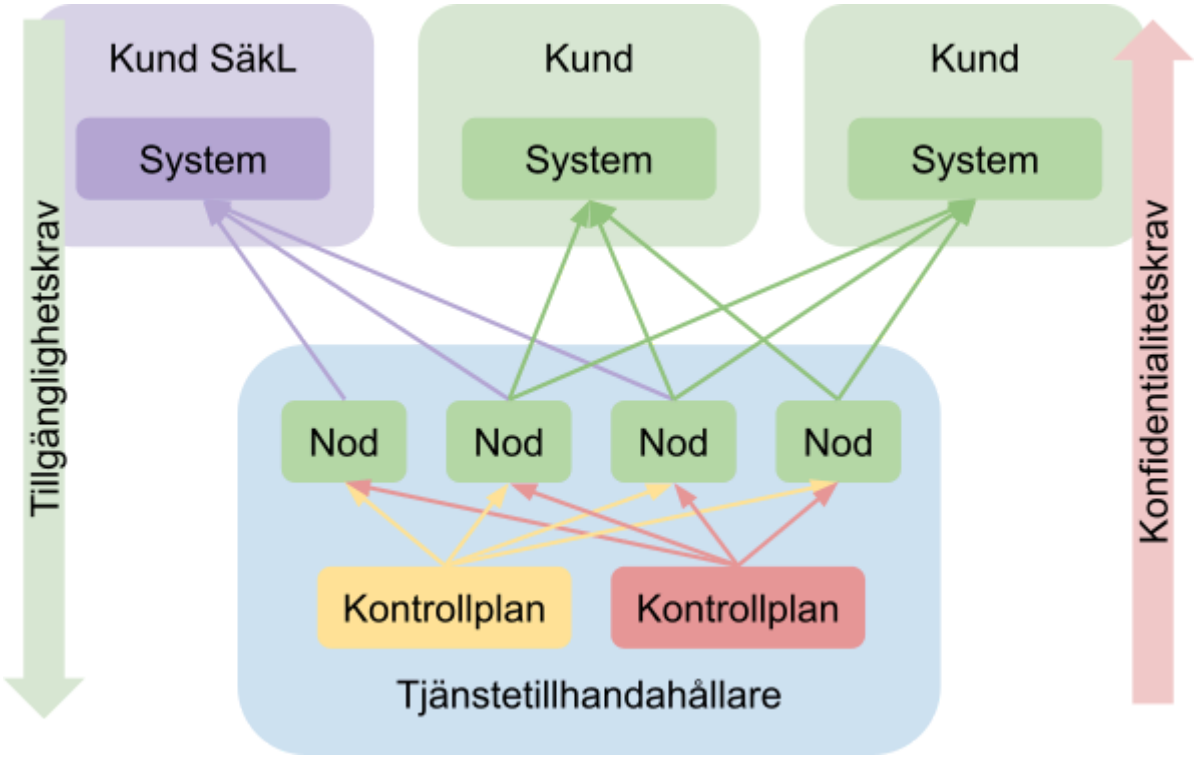
Utredningen går vidare på delbetänkandets linje om att Säkerhetsskyddslagen (SäkL) i allt väsentligt gäller framför både CSL och LoM, dvs att den del av en verksamhet som täcks av säkerhetsskyddslagen varken täcks av CSL eller LoM.

Netnod anser att betänkandet är väl avvägt för de fall som rör *konfidentialitet*, dvs *hantering av säkerhetsskyddsklassificerade uppgifter* (ett delområde för säkerhetsskyddet, se resonemang ss. 286-287 i SOU 2015:25 specifikt) då det är röjande av uppgifter som kan leda till skada för Sverige eller Sveriges intressen. Däremot uppstår oklarheter när det gäller *tillgänglighet* eller *i övrigt säkerhetskänslig verksamhet* (det andra delområdet för säkerhetsskyddet)*,* både i form av tillgänglighet och riktighet av information (som korrekt tid) och tillgänglighet av fysiska tjänster (som rent vatten), speciellt i frågan vilka nätverk och system (i enlighet med CSL-terminologi) som täcks av vilket lagrum.

Som exempel, Polismyndighetens säkerhetsskyddsföreskrifter (PMFS 2022:1) anger, i kontexten *konfidentialitet,* att system som behandlar *begränsat hemliga* och / eller *konfidentiella uppgifter* skall vara logiskt separerade (ex genom virtualisering) från system utan motsvarande krav, och system som hanterar *hemliga* och / eller *kvalificerat hemliga* uppgifter skall vara fysiskt separerade (ex genom separat hårdvara) från andra system. Detta leder naturligt till att de separerade systemen är de som faller under SäkL och därmed är undantagna från CSL (och kommande lagrum som CRA).

I kontexten *tillgänglighet* finns inte motsvarande vägledning, vilket gör att det blir en tolkningsfråga vilka nätverk och system som faller inom vilket lagrum. Detta blir särskilt

problematiskt i fråga om grossisttjänster, eller med andra ord, när samma tjänst tillhandahålls från en leverantör till flera kunder. Figur 1 illustrerar problematiken, där en (från leverantören sett) kund har säkerhetskänslig verksamhet vars krav *sipprar ner* i en tjänsteleverantörs tillhandahållande av grossisttjänster. Notera att i en översiktlig arkitekturskiss där information tillhandahålls uppåt, så sipprar tillgänglighetskrav *neråt* och konfidentialitetskrav *uppåt*, de är på så sätt varandras motsatser.



Figur 1: *Illustration över hur system som tillhandahåller grossisttjänster kan vara uppbyggda. Figurer illustrerar en tjänst (nederst i figuren) som tillhandahålls genom redundanta noder som i sin tur kan styras av redundanta kontrollplan, och kunder av olika typer som använder tjänsten. "Kund SäkL" illustrerar en SäkL kund som har säkerhetsskyddsavtal med tjänstetillhandahållaren, och "Kund" kunder som använder samma tjänst men som inte har säkerhetsskyddsavtal med "Tjänstetillhandahållare". Pilarna illustrerar den riktning information går, dvs kontrollplanens tillgänglighet påverkar noders tillgänglighet, som i sin tur påverkar tillgängligheten av den tjänst som kunden är beroende av.*

I figuren illustreras en tjänst som tillhandahålls genom redundanta noder, där olika kunder kan välja att ansluta sig till olika noder. I illustrativt syfte har en kund säkerhetsskyddsavtal med tjänstetillhandahållaren som avser leveransen av tjänsten, och resterande två kunder har ej säkerhetsskyddsavtal med tjänstetillhandahållaren. Det är samma tjänst, och samma verksamhet, som tillhandahåller samma funktion till flera kunder. Det förekommer inga uppgifter som är känsliga ur ett konfidentialitetsperspektiv i tjänstetillhandahållarens verksamhet.

SäkL använder analysnivån *verksamhet,* dvs SäkL pratar inte i huvudsak om system, nätverk, eller motsvarande utan om det som illustreras som "Tjänstetillhandahållare" i Figur 1 ur

perspektivet från Kund SäkL. CSL / NIS använder analysnivåerna *system* och *nätverk*, vilket illustreras av “Kontrollplan” och “Nod” i Figur 1.

Om tjänsten som tillhandahålls är tjänst som täcks av CSL, vilka delar av tjänsten (system och nätverk) hanteras under SäkL och vilka delar under CSL? I Figur 1 är den säkerhetskänsliga verksamheten hos “Kund SäkL” beroende av tre av fyra noder, har det någon påverkan på om den fjärde noden täcks av SäkL eller inte? Hur påverkas kontrollplanen?

Netnod ser här några möjliga slutsatser på frågan *“Vilka system och nätverk ska hanteras enligt CSL?”*:

- **I.** Inga, hela tjänsten täcks som helhet av SäkL genom säkerhetsskyddsavtal
- **II.** Enbart en av fyra noder täcks, den nod som inte tillhandahåller något enligt säkerhetsskyddsavtal hanteras under CSL
    - A. Alla delar som *kan* vara en del av den säkerhetskänsliga leveransen är säkerhetskänsliga
- **III.** En av fyra noder och ett kontrollplan hanteras enligt CSL
    - A. Tre noder och ett kontrollplan *kan* leverera hela den säkerhetskänsliga tjänsten med nedsatt redundans, därmed undantas de från CSL
- **IV.** En av fyra noder och två kontrollplan hanteras enligt CSL
    - A. Tre noder krävs för tillgänglighet av säkerhetskänslig tjänst enligt hur den säkerhetskänsliga verksamheten använder tjänsten, därför undantas dessa från CSL, och kontrollplanet täcks ej av SäkL då den ligger bakom leveransen
- **V.** Tre av fyra noder och ett kontrollplan hanteras enligt CSL
    - A. En nod och ett kontrollplan krävs för tillgänglighet med nedsatt redundans och möjlighet att konfigurera om parametrar för tjänsteleveransen
- **VI.** Tre av fyra noder och två kontrollplan hanteras enligt CSL
    - A. En nod krävs för att leverera tillgänglighet av säkerhetskänslig leverans med nedsatt redundans, dock kan denna inte konfigureras om utan kontrollplan
- **VII.** Alla komponenter av tjänsten hanteras enligt CSL

Motivering för tolkning **I.,** där alla komponenter täcks av SäkL, kan vara att det är orimligt att enbart delar av ett större system eller tjänst ska hanteras av CSL då komponenter i isolation inte är jämförbara med komponenter i en kontext. Det är helt enkelt orimligt att enbart delar av större system ska hanteras enligt CSL. Denna tolkning har som konsekvens att säkerhetskänslighet smittar brett nedåt, men är enklare att hantera för en leverantör då man inte behöver ta hänsyn till flera lagrum för en och samma tjänst. Detta gör att tjänstetillhandahållaren nog behöver säkerhetsskyddsavtal med sina leverantörer om det finns enskilda leveranser som påverkar tjänstens tillhandahållande.

Motivering för tolkning **VII.**, att hela tjänsten hanteras av CSL trots att dess tillgänglighet har påverkan på säkerhetskänslig verksamhet, kan vara att inga individuella delar av tjänsten har påverkan på tjänstens tillgänglighet då den är redundant byggd. Och därmed är tjänsten som helhet säkerhetskänslig men ingen av dess individuella delar, och därmed hanteras delarna

enligt CSL. Denna tolkning har som konsekvens att redundanta system inte sipprar tillgänglighetskrav i säkerhetskänslighetskontext nedåt i leverantörskedjan.

Tabell 1: *Förteckning över hur olika tolkningar påverkar hur komponenterna i systemet i Figur 1 hanteras av SäkL respektive CSL / LoM. Siffrorna visar på antal noder / kontrollplan för tolkningarna i löptexten, benämnda 1) - 7)*

	SäkL		**CSL / LoM**	
Tolkning	**Kontrollplan**	**Noder**	**Kontrollplan**	**Noder**
I.	2	4		
II.	2	3		1
III.	1	3	1	1
IV.		3	2	1
V.	1	1	1	3
VI.		1	2	3
VII.			2	4

Motivering för tolkningarna **II.-VI.** är att olika komponenter av tjänsten är säkerhetskänsliga ur perspektivet “Vilka delar av tjänsten måste *minst* fungera för att upprätthålla tillgänglighet enligt säkerhetsskyddsavtal?”. Ett svar på den frågan skulle kunna vara “En nod och ett kontrollplan krävs för att upprätthålla tillgänglighet enligt säkerhetsskyddsavtal, och därmed hanteras resterande noder och kontrollplan enligt CSL”, vilket illustreras av tolkningen **V.** i listan ovan.

Utredningarna (SOU 2024:18 och SOU 2024:64), SäkL, SäkF, kopplade föreskrifter, och utredningen *En ny säkerhetsskyddslag* (SOU 2015:25) ger i Netnods mening inte ett entydigt svar på ovan, utan lämnar det upp till tjänsteleverantören att göra denna bedömning.

Figur 1 är generisk, och kontrollplan och noder skulle kunna vara fysiska separata system, eller en del av samma större system, exempelvis ett kuberneteskluster. Figur 1 har två nivåer, en kontroll- / konfigurationsnivå och en nivå som tillhandahåller tjänst, men ofta har digitala tjänster fler nivåer, och Figur 1 visar därmed inte fullt ut den komplexitet som råder i verkligheten.

En ny säkerhetsskyddslag (SOU 2015:25) resonerar grundligt kring denna problematik, men operationaliserar den inte för redundanta, tekniskt varierande, eller system som tillhandahåller grossisttjänster, speciellt då beroenden sträcker sig över flera led och eventuellt över tid.

3. Allriskperspektivets ändamålsenlighet

Utredningen anammar den ansats som finns i direktiven på EU-nivå, vilket innebär att implementationen av LoM, och CSL, baseras på en allriskansats.

> *Åtgärderna ska vidtas på grundval av riskbedömningen, utgå från ett allriskperspektiv och vara proportionella i förhållande till risken.*
>
> (SOU 2024:64, s. 21)

Allriskansatser generellt saknar vetenskapligt stöd i termer av ändamålsenlighet och effekt, och beprövad erfarenhet ger att allriskansatser till risk och åtgärd i regel ej höjer den säkerhetsnivå som finns i en organisation och / eller verksamhet, utan snarare gör den säkerhetsnivå som finns synlig[1]. Detta genom att det är, för att använda Rumsfelds kända begrepp, *known knowns* som hanteras, då dessa är enklast att genomföra åtgärder för. LoM, och CSL, borde ha som ansats att lyfta fram *known unknowns*, och till viss del *unknown unknowns,* till ytan för att dessa ska kunna hanteras.

Netnod anser att LoM, och CSL, borde ställa krav på att vissa typer av scenarier skall kunna hanteras. Detta så att verksamhetsutövare har konkreta scenarier att utgå ifrån när de genomlyser sina egna verksamheter, i syfte att lyfta fram beroenden och förhållanden som inte är hanterade eller kända. Vidare anser Netnod att sådana scenarier bör övas och vara en del av Sverige större cybersäkerhetsstrategi.

Netnods erfarenhet gör gällande att förhållandevis få verksamheter är medvetna om sina digitala beroenden, oavsett om det rör sig om beroenden av fungerande Internetanslutning, externa certifikatskedjor, tredje-parts autentisering (allt från active directory i ett moln till BankID), DNS eller korrekt tid. Dessutom gör aktörer olika bedömningar av relevanta hot och risker genom allriskperspektiv, vilket leder till sämre möjligheter att se konsekvenser och göra konsekvensanalyser som visar på reell samhällspåverkan.

Stöd måste ges så att verksamheter tar reda på sina beroenden och hanterar dessa för att tillhandahålla tillräcklig förmåga.

Ett mindre diskuterat problem med allriskansatser är att de upplevs vara delegerbara enligt Netnods erfarenhet, vilket innebär att risk och åtgärd i kontext cyber ofta delegeras till IT-avdelningen i verksamheter. Detta leder till att risk och åtgärd inte nödvändigtvis har bäring på den samhällsviktiga leverans som verksamheten gör, och att den risk och åtgärd som hanteras är den som IT-avdelningen känner till och är mest bekväm med.

---

[1] Netnod har tidigare skrivit om detta i svar på *Fö2024/00785 - del 1*, *Fö2024/00785 - del 2*, och *Fö2024/00496 (SOU 2024:18, CSL)*. Dessa svar går att hitta på https://www.netnod.se/regular-page/public-policies-and-statements

4. Cybersäkerhet som kostnadsfråga

Utredningen tar inte tag i den strategiska kortsiktigheten rörande cybersäkerhet. Och speciellt föreslår utredningen inte någon ändring på nuvarande ordning av negativa incitament om man sköter sin cybersäkerhetsöverbyggnad dåligt. Netnod förordar att även positiva incitament skall användas för att balansera negativa incitament som böter och viten.

Exempel på möjliga positiva incitament är utbildningar, övningar, stöd med mera som incentiviserar och höjer kompetens och förmåga utan en strikt övre gräns.

Strategiskt leder negativa incitament (viten osv) till att aktörer med vinstpresumption skall optimera för att precis nå upp till den fastställda lägsta-nivån till minsta möjliga kostnad. Det är en trend som måste brytas. Som Netnod har argumenterat för tidigare; **cybersäkerhet får inte vara enbart en kostnadsfråga för inblandade aktörer**.

5. Sammanfattning

De förslag som utredningen lägger är steg i en god riktning, men den hanterar inte viss strukturell problematik (strategisk kortsiktighet, utvärderingskriterier, osv) och riskerar att vara resursineffektiv (allrisk som approach, osv) i det större perspektivet.

Netnod förordar att positiva incitament för en höjd förmåga måste komplettera de negativa incitament som finns i lagförslagen, att allriskapproachen ska kompletteras med i förhand tilldelade risker / hot / scenarier som ska hanteras och som går att öva på tillsammans i Sverige, och att tillgänglighetsaspekterna av leveranskedjor för säkerhetskänslig verksamhet utreds och tas fram gedigna vägledningar för.