Stockholm 2026-05-15

Myndigheten för Civilt Försvar

Er referens: MCF 2026-04554
Vår referens: 26-025

Netnod fick från Myndigheten för Civilt Försvar möjlighet att komma med synpunkter på *Förslag till nya föreskrifter om säkerhetsåtgärder och utbildning enligt cybersäkerhetslag (2025:1506)*.

Netnod framför härmed följande synpunkter:

- Att lagen enligt förslaget ska gälla *hela verksamheten* riskerar att sudda ut gränser mellan tekniska lager och ansvarsförhållanden, vilket är oförenligt med den distribuerade Internetinfrastrukturen och gällande arkitekturer för digitalisering.
  Netnod föreslår att lagen i stället kopplas till de delar av verksamheten som är relevanta för de nätverk, informationssystem och tjänster som faktiskt omfattas av lagen.
- Kravet att *säkerställa* att leverantörer uppfyller kraven är orealistiskt, då ingen aktör normalt har full kontroll över hela leveranskedjan i en digital kontext, speciellt då kunden är betydligt mindre än leverantören.
  Netnod föreslår att formuleringen ändras till att verksamhetsutövaren ska "verka för" att relevanta krav uppfylls inom de delar verksamhetsutövaren faktiskt kan påverka.

Vi förespråkar att föreskrifter och annan reglering bör vara teknikneutral och funktionsorienterad, med fokus på verifierbar funktion och faktisk leveransförmåga (robusthet), snarare än att styra hur verksamhetsutövare organiserar sina interna processer eller leverantörskedjor. Krav i lagstiftning bör inte ställas om de inte, med vetenskaplig grund och beprövad erfarenhet, **alltid** leder till avsett utfall – i detta fall höjd förmåga.

Fredrik Lindeberg, PhD
Chief Information Security Officer

Tel: +46-76 511 32 72
Email: flindeberg@netnod.se

Netnod AB
Greta Garbos väg 13
169 40 Solna

Bilaga 1 - Detaljerade kommentarer

Välkommen ambition med problematiskt utfall

Netnod välkomnar ambitionen att stärka Sveriges cybersäkerhet och robustheten i samhällsviktig digital infrastruktur. Netnod anser dock att reglering och tillsyn måste utformas i överensstämmelse med Internets och den digitala infrastrukturens tekniska, organisatoriska och marknadsmässiga funktionssätt.

Netnod har i tidigare remissvar och policyunderlag återkommande framhållit vikten av att reglering av Internet och digital infrastruktur utgår från Internetarkitekturens grundläggande egenskaper, inklusive decentralisering, teknikneutralitet, lagerseparation och ansvarsfördelning mellan oberoende aktörer. Se till exempel:

- Netnod synpunkter 2025 på ett förslag på Förordning om digitala nät (Digital Networks Act, DNA)
- Netnod synpunkter 2016 på EU-Kommissionens förslag till moderniserat regelverk för elektroniska kommunikationer

Internet och digital infrastruktur utgör distribuerade system bestående av många oberoende aktörer, tekniska lager och ömsesidiga beroenden. Robusthet och resiliens uppnås ofta genom diversitet, redundans, federation och alternativa kommunikationsvägar mellan oberoende aktörer snarare än genom centraliserad kontroll eller vertikal integration. Detta gäller särskilt inom digital infrastruktur och elektroniska kommunikationsnät där fysisk infrastruktur, transmission, IP-nät och tjänstelager ofta tillhandahålls av olika aktörer med olika ansvar och olika möjligheter att påverka funktion och säkerhet.

Mot denna bakgrund ser Netnod en risk att föreskriftsförslaget i flera delar utgår från en modell där cybersäkerhet huvudsakligen antas kunna uppnås genom central styrning och kontroll inom en organisation och dess leverantörskedja. Detta riskerar att skapa otydliga ansvarsförhållanden och tillsynsförväntningar som inte motsvarar den faktiska ansvarsfördelningen i Internetinfrastruktur och elektroniska kommunikationsnät.

I konsekvensutredningen anges exempelvis att:

> *Till skillnad från den tidigare NIS-regleringen gäller cybersäkerhetslagen hela verksamheten hos berörda organisationer...*
>
> (s.3, Konsekvensutredning för MCF 2026-04554)

Netnod anser att denna typ av formulering riskerar att sudda ut viktiga gränser mellan olika tekniska lager, olika verksamhetsdelar och olika ansvarsförhållanden. För Internetinfrastruktur är det centralt att ansvar knyts till den funktion och det lager en aktör faktiskt kontrollerar. En aktör kan exempelvis ansvara för transmission eller fysisk infrastruktur utan att samtidigt kontrollera IP-routing, DNS, molntjänster eller de tjänster som använder infrastrukturen, och detta även om samma organisation bedriver någon av dessa.

Netnod vill även uppmärksamma formuleringar där verksamhetsutövare förutsätts kunna säkerställa funktion eller cybersäkerhet genom externa leverantörskedjor.

Föreskriftsförslaget anger exempelvis att:

> *Verksamhetsutövaren ska säkerställa att de krav som ställs på verksamhetsutövaren i denna författning uppfylls av leverantören…*

samt att verksamhetsutövaren ska hantera:

> *risker i verksamhetsutövarens digitala leveranskedjor…*

Netnod delar uppfattningen att risker i leverantörskedjor behöver analyseras och hanteras. Det är något Netnod dock anser måste utgå från de förväntningar på leverans som finns på organisationen, och inte som dagens alltmer dominerande ex-ante-reglering som söker regelefterlevnad utan att nödvändigtvis leda till överlevnad.

Samtidigt är det viktigt att regleringen utformas med förståelse för att Internet och elektroniska kommunikationer bygger på federerade beroenden mellan autonoma aktörer och separata tekniska lager där ingen aktör normalt har full kontroll över hela kedjan. En verksamhetsutövare kan normalt ställa krav, följa upp leverantörer, skapa redundans och välja alternativa lösningar, men kan inte ensam säkerställa funktion eller cybersäkerhet genom hela Internetekosystemet.

Netnod anser därför att regleringen i större utsträckning bör fokusera på verifierbar funktion och faktisk leveransförmåga snarare än detaljerade antaganden om hur verksamhetsutövare organiserar sina interna processer eller leverantörskedjor. Det centrala bör vara om verksamhetsutövaren faktiskt kan upprätthålla funktion, hantera incidenter, återställa tjänster och upprätthålla erforderlig robusthet. Hur detta uppnås bör i huvudsak vara upp till respektive verksamhetsutövare.

Olika verksamhetsutövare kan uppnå motsvarande eller högre nivå av robusthet genom olika tekniska och organisatoriska lösningar. En aktör kan välja få leverantörer med höga SLA-nivåer och centraliserad styrning medan en annan aktör kan uppnå hög robusthet genom flera oberoende operatörer, routingdiversitet, multihoming och alternativa transmissionsvägar. Båda modellerna kan vara ändamålsenliga beroende på verksamhetens förutsättningar och riskbild.

Samma problematik, att regleringen inte tar höjd för arkitekturens logik, återfinns kring IT- och OT-system i föreskriftsförslaget. Historiskt har dessa typer av system skiljts åt genom distinkta definitioner, men gränsen är idag otydlig. Cyberfysiska system, till exempel medicinskåp, alkolås, journalsystem på plattor, upplåsning av jourbilar och inpasseringssystem, finns numera även utanför den traditionella OT-världen. Även om särbehandling i vissa fall är meningsfull, likt Lag (2022:482) om elektronisk kommunikation som skiljer mellan nummerbaserade och nummeroberoende kommunikationstjänster

baserat på arkitektur, är det centralt att hanteringen av IT- och OT-system istället utgår från systemens förmåga att upprätthålla funktion, hantera incidenter och möjliggöra återställning. Att enbart skilja systemen baserat på daterad terminologi är inte en meningsfull ansats för framtiden.

Samma problematik återfinns i reglerna om segmentering (Segmentering, 4 kap. Tekniska och driftrelaterade säkerhetsåtgärder, 10 §). Exempelvis så säger paragrafen att gästnät (punkt 1) inte får vara på Internet om det också tillhandahålls externa tjänster på Internet (punkt 3), eftersom de då är i samma logiska segment.

Segmentering är i praktiken en teknik som bäst används tillsammans med andra tekniker, men som inte nödvändigtvis är en förutsättning för att uppnå god säkerhet. Detta är problematiskt eftersom det ställer specifika tekniska krav istället för att fokusera på det önskade utfallet.

Krav på åtgärder får inte vara tvingande tekniska lösningar utan ska vara funktionsbaserade och syfta till att uppnå ett verifierbart utfall i form av robusthet och resiliens. Behovet av den föreslagna åtgärden bör utredas i stället för att ställas som ett absolut krav.

Netnod vill i detta sammanhang understryka att robusthet i Internetinfrastruktur historiskt ofta har uppnåtts genom decentralisering, diversitet och oberoende felmoder snarare än genom centraliserad kontroll. Reglering och tillsyn bör därför vara teknikneutral och funktionsorienterad snarare än indirekt styrande mot vissa organisations- eller leveransmodeller. En reglering som alltför starkt utgår från specifika styrnings- eller leveransmodeller riskerar att minska teknikneutralitet och innovationsutrymme utan att nödvändigtvis förbättra faktisk resiliens.

Netnod anser även att vissa formuleringar bör omarbetas för att bättre spegla faktiska ansvarsförhållanden i Internetinfrastruktur och digitala leveranskedjor. Formuleringen, visserligen i konsekvensutredningen:

> *Till skillnad från den tidigare NIS-regleringen gäller cybersäkerhetslagen hela verksamheten hos berörda organisationer...*

riskerar att bli alltför långtgående och otydlig, särskilt för verksamhetsutövare vars verksamhet består av flera tekniska och organisatoriska delar med olika funktioner, ansvar och beroenden. Netnod föreslår därför att formuleringen, och motsvarande framtida användning, istället tydliggör kopplingen till de funktioner, system och tjänster som faktiskt omfattas av cybersäkerhetslagen, exempelvis:

> *Cybersäkerhetslagen gäller de delar av verksamheten som är relevanta för de nätverk, informationssystem och tjänster som föreskrifterna avser.*

Netnod anser på motsvarande sätt att termen “säkerställa” i formuleringen:

> *Verksamhetsutövaren ska säkerställa att de krav som ställs på verksamhetsutövaren i denna författning uppfylls av leverantören utom i de delar kravet i sin helhet uppfylls av verksamhetsutövaren.*
>
> (4 kap. Tekniska och driftrelaterade säkerhetsåtgärder, 1 §)

riskerar att feltolkas som att verksamhetsutövaren förväntas ha faktisk rådighet över externa aktörer och deras underleverantörer. Netnod föreslår därför att formuleringen istället utformas exempelvis som:

> *Verksamhetsutövaren ska genom avtal, uppföljning och riskhantering verka för att relevanta krav på cybersäkerhet uppfylls av leverantörer inom de delar verksamhetsutövaren faktiskt kan påverka.*

En sådan formulering skulle tydligare koppla skyldigheten till möjligheten att påverka samtidigt som ett tydligt ansvar för riskhantering och uppföljning bibehålls.

Netnod anser avslutningsvis att föreskrifterna och tillhörande vägledning bör knyta ansvar och tillsyn till den funktion en aktör faktiskt levererar, det lager den kontrollerar och den påverkan den kan utöva. Denna tydlighet speglar Internetarkitekturens grundläggande principer och stärker därmed möjligheten att uppnå verklig robusthet och resiliens i Sveriges digitala infrastruktur, eftersom all digitalisering på sikt kommer att följa Internetarkitekturen.