Stockholm 2026-04-22

Finansdepartementet

Er referens: Fi2026/00065
Vår referens: 26-010

Netnod fick den 26 januari från Finansdepartementet möjlighet att komma med synpunkter på ett förslag på betänkandet *Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)*.

Netnod inkommer härmed med följande synpunkter:

- Stöd till företag är inte ändamålsenligt utformat.
  Netnod anser att marknadskontrollsmyndigheterna ska ge vägledning, råd och utbildning, men att inget ekonomiskt stöd skall ges direkt till leverantörer, utan om ekonomiskt stöd ges ska det utformas så att det är (slut)kunderna som erhåller stöd som sedan sipprar till leverantörer genom marknadsuppgörelser
- Sekretessen för incidentrapporter och där kopplad information är för bred.
  Netnod anser att sekretessen enbart ska gälla ekonomiska och tekniska förehavanden, och absolut inte får täcka *åtgärder* som rekommenderas eller togs i samband med en incident

Netnod lämnar återstående delar av förslaget utan direkt kommentar, men vill samtidigt påpeka att förhandsregleringsdelarna av förslaget (inkluderat text på EU-nivå) inte nödvändigtvis är ändamålsenliga för en höjd cybersäkerhetsnivå i unionen.

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

Inledning

Netnod välkomnar generellt initiativ som syftar till att höja cybersäkerhetsnivån i unionen, vilket *Kompletterande bestämmelser till EU:s cyberresiliensförordning* avser att göra. Vi vill dock betona vår generella åsikt att lagstiftning i en digital kontext, där tjänster byggs i lager (lasagnemodellen), borde fokusera på *ex-post* ansvarsfrågor snarare än *ex-ante* processreglering. Våra detaljerade kommentarer, som följer, adresserar två områden där den föreslagna lagstiftningen riskerar att bli kontraproduktiv eller ineffektiv.

Stöd till leverantörer är kontraproduktivt för en fungerande marknad

Netnod anser att förslaget gällande ekonomiskt stöd till leverantörer är felaktigt utformat och riskerar att snedvrida marknaden. Marknadskontrollsmyndigheterna bör istället fokusera på att erbjuda vägledning, råd och utbildning. Ett direkt ekonomiskt stöd till leverantörer är inte det mest ändamålsenliga sättet att höja säkerhetsnivån.

Istället, om statligt ekonomiskt stöd ska ges, bör det utformas så att det går till *slutkunderna*. Kunderna kan sedan via marknadsuppgörelser premiera de leverantörer som kan erbjuda högre cybersäkerhet, vilket skapar en naturlig och marknadsdriven incitamentstruktur för leverantörer att förbättra sina produkter och tjänster.

För bred sekretess riskerar att hindra lärande och samverkan

Sekretess för information kopplad till incidentrapportering är för bred i det föreslagna betänkandet. **Även andra remissinstanser har påpekat att spridning av information om sårbarheter och incidenter är en av de viktigaste aspekterna för att förebygga framtida incidenter och förbättra den gemensamma cybersäkerheten.**

Netnod anser att sekretessen strikt ska begränsas till ekonomiska och tekniska förehavanden. Däremot får sekretessen absolut inte gälla de *åtgärder* som rekommenderades eller togs i samband med en incident.

En för bred sekretess, särskilt förslaget om strikt tystnadsplikt och en 40-årig sekretess med omvänt skaderekvisit, riskerar att hämma samverkan och informationsspridning, och därmed leda till försämrad cyberresiliens, vilket går emot förordningens mål. Den föreslagna 40-årsgränsen är närmast en evighet på internet och skulle leda till att vi inte fritt kan diskutera sårbarheter i teknik som används.

Det omfattande hemlighållandet av detaljer om cyberincidenter kan leda till en *försämrad riskuppfattning* i samhället i stort. Det allmänna intresset av offentliggörande av dylika uppgifter ibland måste anses vara påkallat, även om det innebär negativa ekonomiska konsekvenser för enskilda verksamheter, i de fall detta vägs upp av större positiva konsekvenser för det övriga samhällets cybersäkerhet.

Dessutom skapar den föreslagna strikta tystnadsplikten osäkerhet kring vilken information som får spridas, vilket hämmar det viktiga informella informationsutbytet som bär upp cybersäkerhetssamverkan. Eftersom tystnadsplikten inskränker meddelarfriheten riskerar det att leda till att offentliganställda väljer att inte dela information som är nödvändig för samhällets cyberresiliens.

Att dela information om **vidtagna åtgärder** är avgörande för att uppnå kollektivt lärande och därmed en faktiskt högre cybersäkerhetsförmåga i unionen. Lagstiftning som CRA, liksom NIS2, riskerar att vara resursineffektiv och kan uppfyllas utan att nödvändigtvis uppnå en operationellt högre cybersäkerhetsnivå om inte lärdomar sprids effektivt.

Sammanfattning

Netnods primära synpunkter rör utformningen av ekonomiskt stöd och omfattningen av sekretessen för incidentrelaterad information. För att uppnå den avsedda effekten – en högre cybersäkerhet – måste lagstiftningen vara ändamålsenlig och ta hänsyn till marknadsdynamik. Direkt ekonomiskt stöd till leverantörer är inte en lämplig lösning, och en för bred sekretess av åtgärder som vidtagits i samband med incidenter riskerar att hämma det kollektiva lärandet som är nödvändigt för att bygga ett robustare digitalt samhälle. Lagstiftningens utformning bör säkerställa att ingripanden i enskildas intressen faktiskt leder till det avsedda resultatet, vilket vi anser är oklart i dessa två specifika delar av förslaget.