DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

Stockholm 2024-05-28

Försvarsdepartementet
Rättssekretariatet

Er referens: Fö2024/00496
Vår referens: 24-002

Netnod fick den sjätte mars från Försvarsdepartementet möjlighet att komma med synpunkter på ett förslag på Remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Netnod inkommer härmed med följande huvudsynpunkter:

- I varken EU-direktivet eller utredningen presenteras en tydlig och klar mätbar förväntad effekt av direktiv och lagförslag
  Netnod anser att alla större reformer måste följas av tydliga mätbara mål som möjliggör för att objektivt mäta om mål uppnåtts
- EU-direktiv och lagförslag använder ex-ante formuleringar i lagtext som minskar det organisatoriska handlingsutrymmet för lösningar
  Netnod anser att reformen borde ta sikte på de ansvarsfrågor som uppstår i en digitaliserad värld där tjänster byggs i lager
- EU-direktiv och lagförslag förordar ett allriskperspektiv
  Netnod anser att enbart en delmängd de aktörer som täcks av lagstiftningen har den kompetens och de resurser som krävs för att effektivt arbeta med allriskansatser

Det är positivt att cybersäkerhet är högt upp på politiska agendor, men det är problematiskt att de lösningar som föreslås, främst från EU-håll, inte tar hänsyn till hur digital teknologi tas fram, byggs, och underhålls.

DocuSigned by:
Karin Ahl
D7E0380DC2044DE...

Karin Ahl
VD

Tel: +46 70-280 12 65
Email: karin@netnod.se

Netnod AB
Greta Garbos väg 13
169 40 Solna

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

Bilaga 1 - Detaljerade kommentarer

1. Övergripande

Netnod anser att det är positivt att cybersäkerhetsfrågor står högt på politiska agendor, både på EU-nivå och på nationell nivå. Dock anser Netnod att direktivet, och därmed lagförslaget, inte föreslår en optimal lösning för att uppnå syftet med direktivet, dvs en höjd cybersäkerhetsnivå i unionen och därmed en effektivare inre marknad.

Det är värt att kommentera att det inte finns någon utvärdering som belägger att NIS(1) operationellt har höjt cybersäkerhetsnivån i unionen. Se vidare kommentarer nedan. Netnod ser det som problematiskt att så pass stora reformer som NIS(1) inte grundligt utvärderas innan de förändras och / eller byggs vidare på. Speciellt med argumentation att NIS(1) påstås vara framgångsrik.

Netnod kommenterar med detta remissvar inte enbart den svenska implementationen av EU-direktivet NIS2, utan kommenterar i kontext av hur regelverk *för att uppnå en hög nivå av cybersäkerhet i unionen* borde utformas.

I denna text används dessa termer som följer: NIS(1)-direktivet avser Direktiv (EU) 2016/1148, NIS(1)-lagen/lagstiftningen de lagar, förordningar och föreskrifter som finns i kontext av *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*, NIS2-direktivet avser Direktiv (EU) 2022/2555, och NIS2-lagen/lagstiftningen avser de förslag som nu är på remiss, och NIS utan numrering regelfloran som helhet.

2. Digitalisering och tvärfunktionalitet

I termer av tvärfunktionell förvaltning så anser Netnod att det lagda lagförslaget, precis som flera andra lagförslag Netnod har kommenterat på under åren[1], försöker tvinga in funktioner och tjänster som byggts i en digital lagerbaserad värld i en vertikal form. Som exempel på detta finns PTS remissvar[2] på denna remiss, som argumenterar för att PTS har särskild kompetens för att reglera LEK-sektorn[3] “som har speciella förutsättningar” (PTS remissvar, s. 9). Netnod är av uppfattningen att dessa speciella förutsättningar egentligen är den digitaliserade arkitekturmodell som nu ligger till bas för i princip all digitalisering, men som varit basen för elektroniska kommunikationer än längre, den modell som IVA beskriver som

[1] Se https://www.netnod.se/public-policies-and-statements generellt för Netnods åsikter, och specifikt svaren för “Fi2023/01693 Frågor om dagens och framtidens utmaningar på konnektivitetsområdet”, “Cyber Resilience Act”, “Fi2023/01681 En telesamverkansgrupp för fredstida kriser och höjd beredskap”, “Ju2020/04335 Kommunikationstjänsten SGSI”, “PTS dnr 20-7032 Föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur”, och “Ju2017/03997 Informationssäkerhet för samhällsviktiga och digitala tjänster”.
[2] Se https://www.regeringen.se/contentassets/968c4517fe2f49f3aa2b2284bf28316b/pts.pdf
[3] Sektorn under lag om elektronisk kommunikation, en sektor som domineras av funktioner och tjänster som erbjuds i grossistform i lagerbaserade lösningar.

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

lasagnemodellen[4] där tjänster i praktiken levereras i lager från grossistleverantörer till slutanvändare.

I fallet elektroniska kommunikationer rör det sig om lager som svartfiber, ethernet och IPv6, och i fallet digitalisering om lager som operativsystem / plattform, autentisering, tjänst och kommunikation / Internet.

Netnod anser att den offentliga förvaltningen borde organisera sig och förvalta efter det sätt som teknik byggs på idag, dvs en tvärfunktionell förvaltning där de "speciella förutsättningar" som sektorn för elektronisk kommunikation har snarare är en norm än ett undantagsfall. I en sådan förvaltning är ansvarsområden inte vertikala, utan horisontella, och den myndighet som har ansvar för kommunikation specificerar den, och den myndighet som har ansvar / översyn för autentisering bidrar till den specifikationen, osv.

Detta leder till att det inte är ett problem att lyda under flertalet föreskrifter / standarder för en verksamhetsutövare, då regelbördan internt bara är applicerbar på vissa delar av verksamheten. Exempelvis att standardfloran för autentisering har sitt tillämpningsområde och att standardfloran för kommunikation sitt tillämpningsområde. Utredningen föreslår istället en vertikalt fokuserad lösning där en aktör kan hamna under flera vertikala regelfloror, exempelvis två skilda föreskriftsserier under olika regleringsmyndigheter som till och med skulle vara motstridiga i termer av krav på autentisering.

Som exempel behöver alla organisationer ha fungerande (digital) autentisering, allt från vattenkraftverk till kommunkontor till banker, och då är det resursineffektivt om alla ska ta fram eller upphandla sin egen lösning.

Kommunikation och autentisering används som exempel ovan, det finns fler funktioner som i stort sett alla aktörer måste ha, men som aktörer nästan i regel hittar på egna lösningar för.

3. Lagnamnsförslaget avspeglar inte det lagen rör

Den nya lag som utredningen föreslår kallas för "Lag för cybersäkerhet" men rör enbart en delmängd av cybersäkerhetsområdet, och specifikt tar den fokus på vad som brukar kallas för ledningssystem för informationssäkerhet, så kallade LIS, och kan inte anses beröra cybersäkerhet i dess helhet.

> *11 § Språket i offentlig verksamhet ska vara vårdat, enkelt och begripligt.*
>
> (Språklag 2009:600, 11 §)

Netnod anser inte att det är vårdat att påstå att cybersäkerhet enbart handlar om ledningssystem och incidentrapportering.

[4] Se *Digitalisering för ökad konkurrenskraft (IVA 2019)* och *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur (FOI 2020)*

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

Lagens namn borde förslagsvis korrekt avspegla området den reglerar, exempelvis genom namn som “Lag om ledningssystem för cybersäkerhet [för vissa verksamheter]”.

En “Lag för cybersäkerhet” borde, förutom att reglera ledningssystem, **minst** reglera offentliga entiteters förhållningssätt till standarder, standardiseringsprocesser och deltagande i sådana (eftersom standarder idag står för tvärfunktionell koordinering), reglera tvärfunktionellt ansvar i den digitala lasagnemodell vi de facto har idag[5], och speciellt diskutera ansvarsutkrävning i en cyberkontext där tjänster byggs på grossisttjänster i lager.

4. Ex-ante och ex-post i en cybersäkerhetsvärld

Lite förenklat kan man säga att reglering i huvudsak finns i två former, ex-ante och ex-post. Där ex-ante (“före händelsen”) reglering styr beteenden för att främja funktion, och ex-post (“efter händelsen”) reglering som styr ansvarsprocesser efter att någon form av skada / händelse (misstänks) skett.

Övergripande har EU fört argumentationen att en perfekt värld kräver bara ex-post-lagstiftning, dvs lagstiftning som reglerar aktörers ansvarsförhållande gentemot varandra när skada uppstår. Exempelvis EU-direktiv 2018/1972, dvs LEK-direktivet på EU-nivå, innehåller en omfattande argumentation om varför ex-ante lagstiftning bara ska användas i undantagsfall. NIS2 och dess nationella implementation är nästan uteslutande ex-ante, det vill säga reglerar beteende i och utanför organisation utan att skada har skett, vilket strider mot dessa principer.

Netnod är även oroade över att den homogenisering av ledningssystem som de föreslagna regeländringarna leder till på sikt kommer leda till en homogenisering av praktiska cybersäkerhetslösningar. En sådan lösningshomogenisering innebär därmed en lägre diversitet bland lösningar på marknaden, och därmed en större chans att liknande sårbarheter kan utnyttjas i flera system och tjänster. Detta skulle därmed kunna leda till en negativ effekt på den operationella cybersäkerhetsnivån i unionen.

Cybersäkerhetslagstiftning måste skapa incitament för diversitet av lösningar. Netnod anser att fokus måste flyttas från processer till utfall, med ramverk där aktörer hålls till svars för skada som uppstår vid bortfall av tjänst.

Det finns också i det föreslagna regelverket en risk att så kallad regression mot medelvärdet (“regression towards the mean”) sker, att aktörer som är inte är så bra blir lite bättre, och att aktörer som är duktiga blir sämre, detta då förslaget motiverar aktörer att använda liknande ledningssystem.

[5] Se bland annat *Digitalisering för ökad konkurrenskraft (IVA 2019)* och *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur (FOI 2020)*.

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

5. Små aktörer gör viktiga saker

Direktivet tar fasta på att små aktörer gör viktiga saker, bland annat genom att storlekskraven undantas på vissa typer av verksamheter (ex elektroniska kommunikationsnät och DNS-tjänster). Detta är sunt ur perspektivet att inte bara stora utan även små aktörer gör viktiga saker, speciellt i vår digitaliserade lagnemodellsbyggda värld där små aktörer kan tillhandahålla speciella lösningar i lager som skalar väldigt väl och utnyttjas av större aktörer.

Det är däremot inte sunt ur perspektivet att små aktörer åläggs att göra saker på ett sådant sätt som man normalt bara gör i stora organisationer. Vissa manövrar som förespråkas i direktivet och lagen kräver att verksamheten är processtyrd, eller åtminstone utgör sig för att vara processtyrd när tillsynsmyndigheten är på plats. Det är få små organisationer som är processtyrda och det är en styrningsform som är lämplig först när en organisation når en betydande storlek.

Se även kommentarer och tankar nedan kring allriskperspektiv som belyser problematik med liknande ursprung.

6. Allriskperspektiv i en större kontext

Den grundläggande filosofin i utredningen och NIS2-direktivet är att (cyber)säkerhet baserad på en allriskansats är bättre än riktade och spetsade risker. Denna ansats saknar vetenskaplig grund. Den beprövade erfarenheten i sammanhanget poängterar att allriskperspektiv är mer resurskrävande och kräver mer kompetens att hantera än smalare riskperspektiv.

> *Vi menar att allriskperspektivet, som präglar den fredstida krisberedskapen, är alltför omfattande och därmed svårgripbart. Det är besvärligt att ta beslut om hur begränsade resurser ska användas för att hantera hela det spektrum av risker som allriskperspektivet omfattar (trafikolyckor, bränder, solstormar, pandemier med mera). I synnerhet gäller detta aktörer som förfogar över begränsade resurser för analys och förmågeutveckling.*
>
> *(Risk i svensk beredskap, FOI, s. 11)*[6]

Även *Oxford Handbook of Regulation* (2010) lyfter fram subjektiviteten som framkommer vid riskbedömning. Visserligen listas flertalet för- och nackdelar, men överlag är argumentationen att riskhantering lätt blir en bedömningssport i samband med tillsynsverksamhet, speciellt då frågor om proportionalitet ligger på bordet.

Netnod gör samma bedömning som FOI, att ett alltför brett allriskperspektiv riskerar leda till ineffektiv, och ibland felaktig, resursanvändning på systemnivå, vilket går stick i stäv med den föreslagna lagens syfte. Netnods bedömning är att en majoritet av de organisationer

[6] *Risk i svensk beredskap,* FOI, https://www.foi.se/rest-api/report/FOI-R--5285--SE, men se även *Det civila försvarets utgångspunkt i krisberedskapen*, FOI, https://www.foi.se/rest-api/report/FOI-R--4431--SE

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

som täcks av den föreslagna lagstiftningen hade gynnats av att få exempel på explicita hot, risker och händelser att hantera och förbereda sig för då de saknar främst resurser, men även kompetens, att själva göra dessa avvägningar på den nivå som motsvarar den konsekvens utpekade hot och risker hade gett.

I sammanhanget finns även att delade risker och hot ger en kontext att utföra övningar inom, exempelvis om ett civilförsvarsområde har en gemensam pool av risker och hot som ska hanteras. Enligt Netnod är övningar en av nyckelingredienserna för förmågehöjning inom cybersäkerhet.

7. Incitament för faktisk förmågehöjning saknas

Netnod anser att det är möjligt att tolka och följa de föreslagna regeländringarna på ett sådant sätt att verksamheter inte uppnår någon reell förmågehöjning, speciellt för organisationer som redan idag är resursbegränsade och / eller små.

Likväl kan organisationer, speciellt små, som har hög cybersäkerhetsförmåga inte uppfylla de föreslagna kraven på organisatorisk överbyggnad, och därmed bli föremål för eventuellt vite.

Med andra ord, det är möjligt att uppfylla kraven som ställs i de föreslagna regeländringarna på ett sådant sätt att den operativa nivån av cybersäkerhet inte höjs, likväl är det möjligt att ha en hög operativ cybersäkerhetsnivå utan att uppfylla kraven i de föreslagna regeländringarna.

Då vites- och bötesparagraferna syftar på de föreslagna reglerna (och inte operationell förmåga) menar Netnod att det inte nödvändigtvis är i de täckta organisationernas direkta ekonomiska intresse att höja sin cybersäkerhetsnivå, utan att snarare syftar det direkta ekonomiska intresset att säkerställa nödvändig överbyggnad, eller ledningssystem, för cybersäkerhet.

Netnod menar att syftet med lagen enligt dess syftesparagraf, *att uppnå en hög cybersäkerhetsnivå*, därmed inte uppfylls. På så sätt riskerar Cybersäkerhetslagen bli en papperstiger[7].

8. Tillsynens art och dess påföljder

Netnod noterar, precis som andra remissinstanser, att tillsynens art skiljer sig från NIS(1) till NIS2. Av särskild vikt är att tillsynsmyndigheter inte längre kan ingripa med sanktioner mot organisationer som *inte* bedriver ett systematiskt- och riskbaserat

[7] Se liknande resonemang i Michels, J. D., & Walden, I. (2020). Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?. *European Law Review,* och Ferguson, D. D. S. (2023). The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. *International Cybersecurity Law Review*, *4*(4), 371-386.

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

informationssäkerhetsarbete. Däremot kan sanktioner användas mot organisationer som inte vidtar sina egna föreslagna åtgärder.

> *Det innebär att tillsynsmyndigheten ska utöva tillsyn över att verksamhetsutövare uppfyller kraven på riskhanteringsåtgärder, incidentrapportering och anmälan.*
>
> *(SOU 2024:18, s. 225)*

Detta antar Netnod kan vara för att det går att ha en hög nivå av operationell cybersäkerhet utan att denna bedrivs systematiskt och riskbaserat. Exempelvis kan en organisation med hög teknisk kompetens helt sköta sin operationella cybersäkerhet i linjeverksamheten, dvs utan att uppnå de rekvisit som finns för ett systematiskt och riskbaserat arbete så som det målas upp i både nuvarande NIS(1)-lagstiftningen och den föreslagna NIS2-lagstiftningen.

Netnod ser det som positivt att det föreslagna lagförslaget i den här frågan närmar sig formuleringar i Säkerhetsskyddslagen, det vill säga fokus på åtgärder och effekt.

I en förlängning anser Netnod att framtida utformning av tillsyn behöver ta höjd för de sätt och metoder som används för att bygga digitala tjänster. Att kunna utforma tillsyn för en lagerbaserad och tvärfunktionell digital värld är en del av en fungerande tvärfunktionell förvaltning.

Rörande påföljder finns det i EU-direktivet två huvudsakliga sanktioner om en tillsyn leder till åtgärd; 1) *civilrättsliga påföljder* (som böter), 2) *straffrättsliga påföljder* för person i ledande befattning (som misskött sig etc). Utredningen föreslår att punkt 2) helt utgår då straffrättsliga påföljder inte kan tilldelas icke-fysiska personer.

Netnod håller med om bedömningen, men ser en större problematik i den avsaknad av harmonisering som finns gällande ansvarsutkrävande i frågor inom unionen. Både specifika frågor som straffrättsliga påföljder för personer i ledande befattning, men också mer generella frågor som tjänstemannaansvar.

9. Regelverket i sin kontext

Det är för oss aktörer som lyder under flertalet regelverk med säkerhetsfokus problematiskt att detta förslag presenteras utan föreslagna ändringar i och anpassningar till säkerhetsskyddslagstiftningen och med ett förslag på lagtext för CER. Detta gör att det är svårt att förhålla sig till helhetslösningen och de effekter som kan ske på ett högre plan.

Speciellt är Netnod oroade över hur NIS2 och Säkerhetsskyddslagen ska samspela, detta då i fallet med NIS(1) och Säkerhetsskyddslagen så är ansatserna vitt skilda (allrisk- och konsekvensperspektiv). Netnod ser positivt på att utredningen presenterar en minskning av kraven på ledningssystem kontra nuvarande lagstiftning, och att fokus i tillsynsfrågor hamnar på (säkerhets-) åtgärder.

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

I sammanhanget är det också relevant att påpeka att för många aktörer kommer man hamna i en situation där Säkerhetsskyddslagen täcker en del av en verksamhet, men att NIS2 täcker resterande verksamhet då den *smittar* hela verksamheten. Säkerhetskyddsanalyser riskerar då att bli en bedömning av vilken del av verksamheten som man inte vill ska lyda under NIS, speciellt eftersom gällande lagstiftning för NIS jämfört med Säkerhetsskyddslagen är tungrodd. Det är med andra ord enklare att se sig täckt av Säkerhetsskyddslagen än NIS, vilket kan få en del kontraproduktiva systemeffekter då det kan finnas organisationer vill se sig som mer säkerhetsskyddskänsliga än de egentligen är för att undvika NIS.

Netnod önskar att utredningen tar tillvara på hur dagens digitala tjänster byggs och underhålls, och specifikt undersöker hur tvärfunktionell förvaltning ska fungera i en säkerhetskontext i en digitaliserad värld.

10. Utvärdering av reformen

I Netnods mening har inte NIS(1) utvärderats grundligt nog, varken i termer av dess faktiska effekt, eller i termer av vilken effekt som hade uppnåtts utan denna lagstiftning och reform. Notera att man på EU-nivå inte kommer fram till att operationella effekter har skett, utan konstaterar med ord som *katalysator*, *attitydförändring*, och *lagstiftningsåtgärder* att vissa saker har skett[8]. Detsamma gäller för den utvärdering som gjorts av den svenska implementationen av NIS(1)[9], som tydligt fokuserar på attityd och inställning, och inte heller gör någon ansats till att sammanfatta eller beskriva samhällseffekter eller någon förändring av cybersäkerhetsnivå.

Den aktuella utredningen gör inte några betydande ansatser till att föreslå en utvärderingsmodell för reformen. Detta måste göras innan reformen träder i kraft så att det inte längre fram går att flytta målstolparna för att få reformen att verka eller inte verka framgångsrik. Enligt Riksrevisionens rapport "På skakig grund"[10] bör "*reformernas förväntade effekter och mål samt kostnader redovisas tydligt och företrädesvis kvantitativt i de propositioner där reformförslagen läggs fram*" (s. 5), dvs utvärderingskriterierna ska vara fastställda och mätbara.

Enligt EU-direktivet ska reformen utvärderas 2027. Det som ska utvärderas då är *rimligtvis* om reformen har lett till en höjning av cybersäkerhetsnivån i unionen, och vad som ska mätas borde specificeras redan nu.

11. Sammanfattning

Det är positivt att cybersäkerhet diskuteras och att lösningar föreslås. Men det är resurseffektivare för samhället att ta ett tvärfunktionellt angreppssätt på cybersäkerhet som fenomen så att samhället som helhet kan undvika krav på processtyrning som inte passar

[8] Se bland annat inledande motiveringar i NIS2-direktivet, Direktiv (EU) 2022/2555.
[9] Se *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet*, Myndigheten för samhällsskydd och beredskap, slutrapport 2022-12-20
[10] *På skakig grund - beslutsunderlag inför stora reformer (RiR 2022:15)*

DocuSign Envelope ID: 7EA66CB1-FE55-4952-A55C-D8103902C11E

alla organisationer, krävande allriskperspektiv som mindre organisationer inte mäktar med, och istället fokusera på mätbara effekter av cybersäkerhetsarbetet.

En tvärfunktionell förvaltning gör att det blir naturligt att från myndighetshåll tilldela spetsiga hot och risker inom funktionsområden, exempelvis genom att ställa upp krav på att autentiseringsfunktioner ska kunna hantera explicita hot och risker som kommunikationsbortfall. Detta underlättar för övningar och samarbete organisationer emellan, vilket sannolikt kommer leda till en höjning av cybersäkerhetsnivån.

På strategisk sikt behövs även tydliga incitament för att vara riktigt duktig på cybersäkerhet. Idag är, och med denna reform förblir, cybersäkerhet en kostnadsfråga som handlar om att nå upp till en miniminivå av ledningssystem för att undvika vite.