

Remissyttrande
Fö2024/00496

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Remissyttrande angående delbetänkandet ”Nya regler om cybersäkerhet” (SOU 2024:18)

Sammanfattning

Lantmännen har beretts möjlighet att yttra sig angående rubricerad remiss och har följande att anföra.

Utredningen har haft en mycket svår uppgift att analysera ett omfattande direktiv på mycket kort tid och med svåra förutsättningar. Lantmännen finner det dock olyckligt att utredningen inte valt att bygga på den redan väl etablerade grund som nuvarande NIS-lagstiftning lagt, utan snarare valt att bygga om den nu föreslagna cybersäkerhetslagen från grunden. Detta ger enligt Lantmännen både tillsynsmyndigheter och verksamhetsutövare en betydligt mer komplicerad och tidskrävande uppgift att analysera lagen samt att försöka efterleva den och bedriva tillsyn. Befintliga analyser och etablerade rutiner måste helt enkelt avvecklas och ersättas med nya.

Lantmännens yttrande summeras i följande punkter:

1. Endast MSB bör ges föreskriftsrätt
2. Endast nödvändiga system bör omfattas – inte hela verksamhetsutövaren
3. NIS 2 och synergier med beredskapssystemet och totalförsvaret
4. Förtydliga syftet med cybersäkerhetslagen
5. Sårbarhetskanningar
6. Direktivets sektorsavgränsningar behöver förtydligas
7. Riskhanteringsåtgärder måste vara lämpliga
8. Förenkla incidentrapporteringen
9. Etablera en gemensam systemplattform för myndighetskontakter

1. Endast MSB bör ges föreskriftsrätt

Lantmännen instämmer med MSB:s och Livsmedelsverkets remissvar om att den föreslagna föreskriftsrätten bör ses över.

Med NIS 2 breddas antalet sektorer som omfattas av direktivet och antalet verksamhetsutövare kommer att öka betydligt. Eftersom små verksamhetsutövare ej omfattas av NIS 2 så kommer en stor del av verksamhetsutövarna att ha närvaro i flera europeiska länder och inom flera olika sektorer. Att ha en enda myndighet med föreskriftsrätt minskar den administrativa bördan för verksamheter som annars skulle

behöva följa olika föreskrifter från flera tillsynsmyndigheter. Detta förenklar processen för efterlevnad och gör det lättare för verksamheter att implementera nödvändiga säkerhetsåtgärder utan att behöva navigera genom en komplex regelverksstruktur.

Genom att centralisera föreskrifträtten till Myndigheten för samhällsskydd och beredskap (MSB) säkerställs en enhetlig och samordnad strategi för cybersäkerhet över alla sektorer. Detta förhindrar fragmentering och inkonsekvens i regleringen, vilket är särskilt viktigt i en så tvärssektoriell fråga som cybersäkerhet. En central myndighet kan utveckla standardiserade regler som gäller över hela linjen, vilket förenklar efterlevnad och tillsyn. Föreskrifterna som tagits fram under den nuvarande NIS-lagen visar att det mycket väl går att ha enhetliga föreskrifter avseende säkerhetsåtgärder (riskhanteringsåtgärder) för flera sektorer. MSB:s föreskrifter (MSBFS 2018:8), Livsmedelsverkets föreskrifter (LIVSFS 2022:2) samt Energimyndighetens föreskrifter (STEMFS 2021:3) är exempel på detta.

En centraliserad föreskrifträtt gör det möjligt för MSB att snabbt reagera på nya hot och förändringar i cybersäkerhetslandskapet. Med en enda myndighet ansvarig för att utfärda föreskrifter kan regler och riktlinjer snabbt uppdateras och anpassas efter aktuella behov.

Genom att koncentrera föreskrifträtten till MSB kan resurser användas mer effektivt. Istället för att varje sektorsspecifik myndighet ska utveckla och underhålla sina egna föreskrifter, kan MSB använda sina resurser för att skapa omfattande och robusta regler som täcker flera sektorer. Detta leder till bättre resursfördelning och minskade kostnader för både myndigheter och verksamheter.

2. Endast nödvändiga system bör omfattas – inte hela verksamhetsutövaren

NIS 2-direktivet syftar, som Lantmännen tolkar direktivet, till att skydda de nätverk och system som är nödvändiga för att verksamhetsutövarna i de olika sektorerna ska kunna förse Sverige och EU:s inre marknad med verksamhetsutövarnas varor och tjänster. För detta syfte är inte alla nätverk och informationssystem lika värda. Fokus i cybersäkerhetslagen bör tydligt ligga på att säkerställa att de nätverk och informationssystem som är nödvändiga för att verksamhetsutövarna ska kunna tillhandahålla dessa varor och tjänster är robusta och säkra.

Identifieringen av vilka system som är nödvändiga kan förslagsvis ske genom en analys, likt beskrivet i Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (STEMFS 2021:3):

”Dessa föreskrifter avser en leverantörs nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster.

”För att identifiera vilka nätverk och informationssystem som leverantören använder för att tillhandahålla samhällsviktiga tjänster ska leverantören analysera sina nätverk och informationssystem”

Liknande tillvägagångssätt används även i Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten (LIVSFS 2022:2):

"... som kan påverka säkerheten i de nätverk och informationssystem som används för tillhandahållandet av den samhällsviktiga tjänsten."

Sammanfattningsvis instämmer Lantmännen med Livsmedelsverkets invändning av förslaget att verksamhetsutövaren i sin helhet ska omfattas av cybersäkerhetslagen. Detta skulle vara ytterst kostnadsdrivande och öka komplexiteten för både tillsyn och efterlevnad. Istället bör lagen tydligt avgränsas till de delar av verksamheten och de system som påverkar säkerheten i de tjänster som omfattas enligt direktivets bilagor. Detta möjliggör ett mer fokuserat och kostnadseffektivt säkerhetsarbete, vilket Lantmännen menar är i linje med NIS 2-direktivets intentioner.

Lantmännen rekommenderar även att lagstiftaren undersöker hur tolkningen av begreppet entitet skett i andra medlemsländer som kommit långt i sitt arbete med implementationen av NIS 2-direktivet, så att det i högsta möjliga mån finns samsyn.

3. NIS 2 och synergier med beredskapssystemet och totalförsvaret

Cybersäkerhetslagen är omfattande och sammanfaller mycket väl i tid med Sveriges återuppbyggnad av beredskapssystemet och totalförsvaret. Av den anledningen instämmer Lantmännen med de synpunkter som framförs av MSB och Livsmedelsverket i deras respektive remissvar angående behovet av en grundlig analys av hur NIS 2-direktivet, i kombination med CER-direktivet och den kommande lagstiftningen kring dessa direktiv, relaterar till det beredskapssystem som byggs i Sverige. Vi delar uppfattningen att en sådan analys saknas i utredningen. För Sveriges totalförsvaret vore det positivt om utredningen och den efterföljande implementationen av cybersäkerhetslagen tog hänsyn till fler aspekter av denna återuppbyggnad, för att på sikt undvika en situation där det behövs drastiska ändringar av cybersäkerhetslagen.

Livsmedelsverket lyfter fram att beroende på vilken hotbild cybersäkerhetslagen dimensioneras för, kommer dess effekter att kunna harmonisera med totalförsvarets uppbyggnad. De viktiga samhällsfunktioner som har identifierats av MSB kan till stor del inrymmas i de sektorer som lagen omfattar.

Vidare framhåller Livsmedelsverket att även om cybersäkerhetslagen dimensioneras för en fredstida hotbild, bidrar den till ökad robusthet inom cybersäkerhet för de sektorer som omfattas. Denna robusthet kommer att vara värdefull både i fredstid och vid höjd beredskap eller krig. Lantmännen anser, i likhet med Livsmedelsverket, att lagstiftaren bör förtydliga vilken roll cybersäkerhetslagen ska fylla i relation till det svenska beredskapssystemet. En sådan klarläggning är avgörande för att säkerställa att lagen integreras effektivt med nationella strategier och krisberedskapsplaner.

Vi uppmanar därför att lagstiftaren tar till sig dessa synpunkter och utför en noggrann analys av hur cybersäkerhetslagen ska samverka med beredskapssystemet. Detta är nödvändigt för att undvika fragmentering och för att säkerställa att lagen bidrar till en

sammanhållen och effektiv cybersäkerhetsstruktur som kan hantera både fredstida och icke fredstida hot.

4. Förtydliga syftet med cybersäkerhetslagen

Lantmännen instämmer med Livsmedelsverkets uppmaning att förtydliga syftet med cybersäkerhetslagen. Ett klart och tydligt syfte är avgörande för att verksamhetsutövare ska förstå vilka aspekter av säkerhetsarbetet som ska prioriteras och hur de ska bidra till att uppnå lagens mål. Detta förtydligande kommer att underlätta för både verksamhetsutövare och tillsynsmyndigheter i deras arbete med att implementera och övervaka säkerhetsåtgärder.

5. Sårbarhetskanningar

Många verksamheter utför redan regelbundna sårbarhetsskanningar som en del av deras interna säkerhetsprotokoll. Att tillsynsmyndigheten också utför dessa skanningar kan leda till onödigt dubblering av arbete, där samma sårbarheter identifieras flera gånger utan att tillföra något nytt värde. Det vore mer effektivt och förenligt med praxis att tillsynsmyndigheten istället ges rätt att granska verksamhetens interna skanningsprocesser, systemstöd för sårbarhetsskanning, och resultat.

Sårbarhetsscanningar kan oavsiktligt störa verksamhetens nätverk och system. Även om skanningarna är avsedda att vara icke-invasiva, finns det alltid en risk att de kan orsaka driftstörningar, prestandaproblem eller till och med systemfel. Detta kan påverka verksamhetens kontinuitet och leda till oplanerade störningar, kostnader och förluster.

Sårbarhetsskanningar som utförs av en tillsynsmyndighet innebär även integritets- och sekretessrisker. Verksamhetsutövarers nätverk och informationssystem innehåller ofta känslig information som inte bara rör företagets verksamhet utan även dess kunder och partners. Att ge en extern part tillgång till dessa system kan leda till att konfidentiell information exponeras eller utsätts för risk.

6. Direktivets sektorsavgränsningar behöver förtydligas

Lantmännen instämmer med Livsmedelsverkets uppmaning att förtydliga direktivets sektorsavgränsningar, särskilt inom livsmedelssektorn. Vi delar uppfattningen att begreppet livsmedelsföretag (food business) bör tydliggöras. När det gäller begreppet industriell produktion och bearbetning, är vi eniga med Livsmedelsverket om att även dessa begrepp behöver klargöras. Det är viktigt att precisera vad som avses med dessa termer för att undvika förvirring och säkerställa att rätt verksamheter omfattas av cybersäkerhetslagen.

7. Riskhanteringsåtgärder måste vara lämpliga

Lantmännen instämmer i Livsmedelsverkets remissvar om att en riskhanteringsåtgärd kan vara proportionell men olämplig. Lantmännen anser att det är helt nödvändigt att en riskhanteringsåtgärds lämplighet också bedöms innan den införs.

8. Förenkla incidentrapporteringen

Komplex incidentrapportering riskerar att fördröja rapporteringen. Lantmännen instämmer med Livsmedelsverkets oro kring överlappande incidentrapportering och anser att detta måste hanteras för att undvika onödigt dubbelrapportering.

Förslaget innebär att flera verksamhetsutövare inom samma koncern kan omfattas av incidentrapporteringsbestämmelserna, vilket kan leda till att en enskild incident måste rapporteras flera gånger om delade IT-resurser påverkas. För koncerner som potentiellt kan behöva rapportera samma incident i flera länder innebär det en betydande administrativ börda om samma incident även måste rapporteras enskilt för varje verksamhetsutövare – inom varje sektor.

Det är relevant för CSIRT och tillsynsmyndigheten att få information om alla påverkade verksamhetsutövare, men detta bör kunna göras utan att samma incident behöver rapporteras upprepade gånger.

9. Etablera en gemensam systemplattform för myndighetskontakter

Lantmännen instämmer med MSB:s och Livsmedelsverkets remissvar avseende en gemensam plattform för registrering av verksamhetsutövare och tillstyrker MSB:s förslag i sin helhet:

”4. Säkerställ att anmälan, på samma sätt som incidentrapportering, görs på ett samlat sätt centralt till den gemensamma kontaktpunkten som stöd för totalförsvaret och för vidare distribution till berörd tillsynsmyndighet.”

Lantmännen instämmer även med Livsmedelsverkets skepsis om två månader är tillräckligt för att ge verksamhetsutövare tid att bedöma huruvida de omfattas av lagen samt genomföra anmälan.

Om Lantmännen

Lantmännen är ett lantbrukskooperativ och norra Europas ledande aktör inom lantbruk, maskin, bioenergi och livsmedel. Vi ägs av 18 000 svenska lantbrukare, har 12 000 anställda, har verksamheter i ett 20-tal länder och omsätter cirka 70 miljarder kr på årsbasis. Med basen i spannmål förädlar vi åkermarkens resurser för ett livskraftigt lantbruk. Några av våra mest kända varumärken inom livsmedel är AXA, Kungsörnen, Scan, Korvbrödsbagarn, GoGreen, FINN CRISP och Bonjour.

Vårt företag är grundat på kunskap och värderingar som har funnits i generationer hos våra ägare. Genom forskning, utveckling och verksamhet i hela värdekedjan tar vi tillsammans ansvar från jord till bord.

Lantmännen är såväl Sveriges största lantbruksföretag som Sveriges största livsmedelsföretag och har verksamheter i hela livsmedelsvärdekedjan, t ex hela vägen från framtagandet av nya växtsorter genom sin världsledande växtförädling till färdiga egna livsmedelsprodukter som säljs i butik.

Läs gärna mer på www.lantmannen.se

Med vänlig hälsning
Lantmännen

Johannes Eriksson
Koncernsäkerhetschef & CISO
E-post: johannes.eriksson@lantmannen.com