GENERALDIREKTÖREN

2024-05-07

Dnr 2024/01320
Saknr 1.1.3

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

Livsmedelsverkets yttrande över remiss från Försvarsdepartementet angående Delbetänkandet 2024:18, Nya regler om cybersäkerhet

Er referens: Fö2024/00496

Sammanfattning

Livsmedelsverket har tagit del av delbetänkandet om nya cybersäkerhetsregler, SOU 2024:18 och lämnar i detta remissyttrande ett antal synpunkter.

Livsmedelsverket konstaterar att utredningen genomförts under kort tid och att arbetet är komplext. Vidare välkomnar Livsmedelsverket att en ny lagstiftning, cybersäkerhetslagen, utformas.

Livsmedelsverket tillstyrker den förordning om tillsynsmyndigheter för sektorerna dricksvatten, avloppsvatten samt produktion, distribution och bearbetning av livsmedel som utredningen föreslagit.

Nedan finns Livsmedelsverkets huvudsakliga synpunkter sammanfattade.

Förtydliga syftet med cybersäkerhetslagen
Livsmedelsverket anser att syftet för den föreslagna lagen behöver förtydligas. Det är inte tydligt om lagen har samma syfte som direktivet– att med cybersäkerhet främja den inre marknaden – eller om cybersäkerhetslagen avser att bemöta en hotbild som omfattar fredstida kris och krig, dvs. höjd beredskap.

Statliga myndigheters och kommuners omfattning i sin helhet är inte en direktivsnära lagstiftning
Utredningen föreslår att statliga myndigheter (med några undantag), kommuner och regioner ska omfattas av cybersäkerhetslagen. Livsmedelsverket anser att detta

Postadress
Box 622
751 26 Uppsala

Besöksadress
Dag Hammarskjölds väg 56 A
Leveransadress
Dag Hammarskjölds väg 56 C
752 37 Uppsala

Telefon
018-17 55 00
Telefax
018-10 58 48

E-post
livsmedelsverket@slv.se
Internet
www.livsmedelsverket.se

Organisationsnummer
202100-1850
VAT-nummer
SE202100185001
Innehar F-skattebevis

innebär en utökning av direktivet. NIS2-direktivet avser att i huvudsak omfatta de myndigheter som kan påverka rörlighet och handeln i unionen. En utökad omfattning på så sätt som föreslås bör föregås av en fördjupad konsekvensanalys då den kan vara förknippad med höga kostnader för de som omfattas.

För att undvika en vanlig typ av överlappande tillsynsansvar i kommunal verksamhet föreslår Livsmedelsverket även att tillsynsobjektet ska vara kommunala myndigheter istället för kommunen som juridisk person.

Att hela verksamhetsutövaren omfattas får långtgående konsekvenser
Livsmedelsverket är tveksamma till ändamålsenligheten i utredningens förslag att en verksamhetsutövare ska omfattas i sin helhet och anser att ett förtydligande av hur lagförslaget ska tillämpas på verksamhetsutövaren behövs. I de fall den omfattade tjänsten, dvs den sektor som är beskriven i bilaga 1, utgör en delmängd av verksamhetsutövarens leverans anser Livsmedelsverket att riskanalyser och riskhanteringsåtgärder enligt lagförslaget ska tillämpas på den tjänsten. Om tillämpningen av lagen inte förtydligas kan detta komma att leda till en oavsiktlig omfattning hos verksamhetsutövare. Livsmedelsverket anser att cybersäkerhetslagen ska tillämpas på den samhällsviktiga tjänsten samt den verksamhet och de nätverk och informationssystem som kan påverka säkerheten i den.

Att verksamhetsutövare ska omfattas i sin helhet kommer för vissa verksamheter, däribland kommuner, kommer att innebära att de blir föremål för tillsyn av flera tillsynsmyndigheter. Livsmedelsverket är tveksamma till nyttan med att flera tillsynsmyndigheter tilldelas ansvar för tillsyn för samma verksamheter och anser att cybersäkerhetslagens tillämpning bör anpassas så att tillsynsansvaret blir tydligt och avgränsat.

Föreskriftsrätten bör ses över för att undvika överlappande reglering
Utredningen föreslår att varje tillsynsmyndighet ska ha föreskriftsrätt för systematiskt cybersäkerhetsarbete. Livsmedelsverket avstyrker att sådan föreskriftsrätt ska ges till varje tillsynsmyndighet, i synnerhet då ett överlappande tillsynsansvar för samma verksamhetsutövare kommer att förekomma med utredningens föreslag.

Direktivets sektorsavgränsningar behöver förtydligas
Utredningen föreslår i sitt delbetänkande inga ytterligare förtydligande kring de sektorsavgränsningar som finns i NIS2-direktivets bilagor. Livsmedelsverket menar att lagstiftningen behöver förtydliga sektorerna ytterligare för att verksamhetsutövare ska kunna avgöra om de omfattas. Livsmedelsverket anser att en vägledning kring omfattning inte är tillräcklig i detta fall då påföljder av

överträdelser kan vara allvarliga för verksamhetsutövarna. En tydlighet i bindande reglering är därför nödvändig.

Direktivets bestämmelse om ledningens ansvar bör inkluderas i cybersäkerhetslagen

I utredningens förslag har direktivets explicita skrivelse om ledningens ansvar för beslut om riskhanteringsåtgärder inte tagits med. Detta med hänvisning till att ledningen implicit är ansvarig. Livsmedelsverket avstyrker detta ställningstagande och anser att ett explicit krav på ledningens ansvar är av central betydelse för ett framgångsrikt cybersäkerhetsarbete.

Riskhanteringsåtgärder ska vara lämpliga

Utredningen har gjort ställningstagandet att det räcker med att en riskhanteringsåtgärd är proportionell varvid direktivets skrivelse ”lämplig” har uteslutits ur förslaget. Livsmedelsverket avstyrker detta ställningstagande och framhåller att en riskhanteringsåtgärd kan vara proportionell men olämplig. Livsmedelsverket anser att det är helt nödvändigt att en riskhanteringsåtgärds lämplighet också bedöms innan den införs.

Bestämmelser kring incidentrapportering bör ses över

Utredningen har i förslaget bortsett från direktivets intention att tidiga varningar ska ske ”utan onödigt dröjsmål”, Utredningen föreslår att en tidsfrist på 24 timmar är tillräcklig. Livsmedelsverket är tveksamma till utredningens förslag och anser att en tidig varning bör ske inom 6 timmar, dock med förbehåll att en sådan varning ska vara begränsad till information som är nödvändigt för CSIRT:ens lägesbedömning och som kan vara till nytta för andra verksamhetsutövare.

Sammanfattning av övriga synpunkter på förslaget

Utöver de synpunkter som redovisats ovan har Livsmedelsverket även synpunkter som är av mer kortfattad karaktär, dessa redovisas ytterligare i dokumentet under rubriken ”Övriga synpunkter”. Sammanfattningsvis rör dessa synpunkter följande:

- Livsmedelsverket är tveksamt till att en bedömning av uppsåt eller oaktsamhet ska ske vid ingripande åtgärder och förordar att ett strikt ansvar ska föreligga (jfr. 5 kap 3 §cybersäkerhetslagen).
- Vad som avses med ”uppförandekoder och certifieringsmekanismer” behöver förtydligas (jfr 5 kap 4 § cybersäkerhetslagen)
- Nödvändighet att reglera dubbelbestraffning avseende Allmänna dataskyddsförordningen bör ses över (jfr. 5 kap 17 § cybersäkerhetslagen)
- Konsekvenser av CSIRT:ens uppgift att samla in och analysera forensiska uppgifter bör analyseras närmare (29 § förordning cybersäkerhet)

- Livsmedelsverket avstyrker ett distribuerat system för verksamhetsutövares anmälan och förordar en gemensam plattform för registreringsuppgifter (14 § cybersäkerhet förordning)
- Livsmedelsverket är tveksamt till skrivelsen ”en riskanalys” och anser att fler riskanalyser kan vara nödvändiga (3 kap 1 § cybersäkerhetslagen)
- Regleringen avseende säkerhetsskanningar och dess resultat bör förtydligas (4 kap 9 § cybersäkerhetslagen)
- Användning av ordet ”förvärv” bör förtydligas eller ändras (3 kap 1 § cybersäkerhetslagen)
- Livsmedelsverket är tveksamt till att 14 dagar är en lämplig tidsfrist för ändrade uppgifter i anmälan (2 kap 2 § cybersäkerhetslagen)
- Begreppet ”huvudsakligt etableringsställe” behöver förtydligas (3 § cybersäkerhet förordning)
- Livsmedelsverket är tveksamt till att begränsningen ”när så är lämpligt” har uteslutits avseende information till kunder i händelse av incidenter (3 kap 3 § cybersäkerhetslagen)

Generella synpunkter

NIS2 i kombination med CER-direktivet och kommande lagstiftning kring det direktivet behöver analyseras i relation till det beredskapssystem som byggs i Sverige. I utredningen finns ingen sådan analys. Beroende på vilken hotbild som cybersäkerhetslagen dimensioneras för kommer dess effekter att kunna harmonisera med totalförsvarets uppbyggnad. De viktiga samhällsfunktioner som är identifierade av MSB[1] kan i mångt och mycket inrymmas i de sektorer som lagen omfattar, och med den utökade omfattning utredningen föreslår med statliga myndigheter, kommuner och regioners omfattning kan cybersäkerhetslagen omfatta stora delar av civilsamhället. Även om cybersäkerhetslagen dimensioneras för en fredstida hotbild för att minska fragmenteringen av den inre marknaden får den effekten att det byggs större robusthet avseende cybersäkerhet för de sektorer som omfattas, en robusthet som kommer att vara till nytta såväl som i fredstid som vid höjd beredskap och krig. Livsmedelsverket anser dock att lagstiftaren bör förtydliga vilken roll cybersäkerhetslagen ska fylla i relation till det svenska beredskapssystemet.

Relationen mellan NIS2-direktivet och säkerhetsskyddslagen behöver också analyseras i större utsträckning. Utredningsdirektivet gav utredningen i uppgift att föreslå ändringar för att uppnå en mer sammanhållen systematik mellan regelverken. Då säkerhetsskyddslagen har ett antagonistiskt perspektiv medan NIS2, och därmed cybersäkerhetslagen, har ett allriskperspektiv bör dessa olika lagstiftningar kunna komplettera varandra. Dock kan tillsynssystemet för säkerhetsskyddslagen i vissa fall försvåra tillsynen för cybersäkerhetslagen då det för vissa sektorer blir olika tillsynsmyndigheter för de olika regelverken. Enligt dagens reglering kan en verksamhetsutövare omfattas av både NIS-lagen och säkerhetsskyddslagen. Detta har medfört svårigheter för Livsmedelsverket vid tillsyn då Livsmedelsverket inte har tillsynsansvar för säkerhetsskyddslagen. I en vidare analys bör övervägas om det finns samhälleliga vinster att tillsynsansvaret för säkerhetsskyddslagen och cybersäkerhetslagen ska tilldelas en och samma myndighet. Oavsett detta instämmer Livsmedelsverket med MSB:s remissvar[2] att cybersäkerhetslagen kan fungera väl som en bottenplatta även för säkerhetskänslig verksamhet.

[1] Lista med viktiga samhällsfunktioner, MSB1844
[2] MSB:s Remissvar delbetänkandet 2024:18 Nya regler om cybersäkerhet

Synpunkter på förslagen

Förtydliga syftet med cybersäkerhetslagen

Livsmedelsverket anser att utredningens förslag till syftesformulering i cybersäkerhetslagen behöver förtydligas så att det framgår vad lagstiftaren vill åstadkomma med en hög cybersäkerhetsnivå.

Standarder för ledningssystem för informationssäkerhet beskriver hur arbete och ambitioner om säkerhet måste sättas in i en kontext som gör det möjligt att förstå varför resurser ska läggas på säkerhet och vilka aspekter av säkerheten som ska prioriteras. Vanligtvis formaliseras detta i en informationssäkerhetspolicy som beskriver hur en viss säkerhetsnivå ska bidra till vad det är organisationen vill uppnå, dvs. hur säkerhet ska bidra till en organisations övergripande mål och syfte.

Ett tydligt syfte kommer att underlätta säkerhetsarbetet för verksamhetsutövare som omfattas av lagen eftersom det hjälper dem att förstå vilka aspekter av säkerhetsarbetet som ska prioriteras för att följa lagen. Verksamhetsutövare behöver förstå om syftet med lagen följer direktivet och är att förbättra EU:s inre marknad, eller om det finns ett annat syfte kopplat exempelvis till Sveriges förmåga att hantera kris och krig. Båda syftena kan vara rimliga och lämpliga, men lagen behöver tydligt visa vad som avses. Syftet bör därmed ge en uppfattning om vilken hotbild som riskhanteringsåtgärderna ska bemöta.

Syftet kommer även att vara nödvändigt för att tillåta tillsynsmyndigheterna att göra korrekta bedömningar av verksamhetsutövares säkerhetsarbete och prioriterade åtgärder. I tillägg blir ett förtydligat syfte helt nödvändigt när en bedömning om huruvida en verksamhetsutövare bör omfattas ska göras. Utredningen föreslår att enskilda verksamhetsutövare ska kunna ansöka om att undantas från att omfattas. En bedömning ska göras "med hänsyn till … lagens syfte"[3]. Så som lagens syfte är formulerat är det svårt att avgöra vad som ska fungera som grund för en sådan bedömning.

Statliga myndigheters och kommuners omfattning i sin helhet är inte en direktivsnära lagstiftning

Offentlig förvaltning enligt direktivet

NIS2-direktivets syfte att uppnå en hög cybersäkerhetsnivå för att förbättra den inre marknaden framgår i artikel 1. För detta syfte framhålls i skälssats 37 att det bör omfatta infrastruktur som ”tillhandahållare av tjänster” har ett allt större beroende

[3] Delbetänkandet,4§ förordning om cybersäkerhet

till, däribland vissa aspekter av offentlig förvaltning.[4] Utredningen framhåller dock att samtliga myndigheter i Sverige (med några undantag) ska omfattas av lagen. Detta innebär inte en direktivsnära lagstiftning. Livsmedelsverket menar till skillnad från utredningen att myndigheterna kan bedöma om den egna verksamheten träffas av det fjärde kriteriet i direktivets definition av ”offentlig förvaltningsentitet”.

I artikel 6.35 förtydligas innebörden av "offentlig förvaltningsentitet" i en definition och direktivet ställer upp fyra kriterier som ska uppfyllas. Däribland att en sådan entitet ska ha "befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital." Det finns en tydlig koppling till en väl fungerande inre marknad, dvs. de verksamhetsutövare som direktivet syftar till att omfatta är sådana vars frånfall skulle påverka marknadens funktion.

Utredningen menar att det sista kriteriet (f) om befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital är svårt att förstå och framhåller att det inte möjligt eller ändamålsenligt att bedöma vilka av Sveriges myndigheter som har befogenhet att fatta sådana beslut. Istället föreslår utredningen att samtliga statliga myndigheter ska omfattas, med hänvisning till NIS2-direktivets syfte. Utredningen hänvisar dock inte till syftet så som det uttrycks i direktivets artikel 1, utan ett annat syfte hämtat från skälssatserna[5] om att införa enhetliga storlekskriterier för vilka som ska omfattas.

Cybersäkerhetslagen föreslås allmänt ställa krav på verksamhetsutövare att själva avgöra om de omfattas av lagen. Det bör på motsvarande sätt vara möjligt även för myndigheter att tolka det fjärde kriteriet i direktivets definition och själva avgöra huruvida deras verksamhet kan fatta beslut som påverkar gränsöverskridande rörlighet för personer, varor, tjänster och kapital.

Om kommuner som verksamhetsutövare

Livsmedelsverket anser till skillnad från utredningen att verksamhetsutövaren i en kommunal kontext bör vara den kommunala nämnd som levererar en tjänst som tas upp i direktivets bilagor. Detta underlättar sannolikt nämndernas regelefterlevnad och det kommer att göra tillsynsmyndighetens arbete mera tydligt och avgränsat

[4] Europaparlamentets och rådets direktiv (EU) 2022/2555, skälssats 37
[5] Delbetänkandet SOU 2024:18, s. 130

och sammantaget leda till bättre förutsättningar att höja kommuners cybersäkerhetsnivå.

Livsmedelsverket instämmer i SKR:s invändning om att kommunen som juridisk person inte samlat ska betraktas som en verksamhetsutövare.[6] När fullmäktige lämnat uppdrag åt en viss nämnd anses det i detta uppdrag ligga en befogenhet för den nämnden att företräda kommunen i rättegång som gäller den verksamheten, vilket i praktiken liknar motsvarande reglering i 27 § myndighetsförordningen (2007:515).[7]

Om verksamhetsutövaren anses vara den aktuella kommunala nämnden begränsas också problematiken med ett överlappande tillsynsansvar med flera involverade tillsynsmyndigheter, eftersom kommuner har ansvar för bland annat vårdtjänster och va-tjänster, men mera sällan förlägger dessa ansvarsområden i samma nämnd.

Tillsynsansvaret kan förvisso fortfarande bli otydligt avseende delade resurser hos verksamhetsutövaren. Det är inte ovanligt att samtliga kommunala verksamheter använder en gemensam IT-avdelning eller att kommunen har en gemensam övergripande säkerhetsorganisation. I tillägg kan vissa tekniska lösningar användas av flera olika delar av verksamheten. Inom ramen för dagens NIS-reglering har den kommunala dricksvattenverksamheten själva avgjort vilka nätverk och informationssystem samt vilka verksamheter som kan påverka säkerheten i den samhällsviktiga tjänsten. Tillsynen har utformats därefter. Det kan dock behöva regleras hur tillsynsansvar över sådana situationer där delade resurser används ska ske.

Att hela verksamhetsutövaren omfattas får långtgående konsekvenser

Livsmedelsverket avstyrker förslaget att verksamhetsutövaren i sin helhet ska omfattas om det innebär att verksamheter hos verksamhetsutövaren som inte omfattas av bilagorna ska stå under tillsyn. Om detta inte är intentionen anser Livsmedelsverket att cybersäkerhetslagen behöver förtydligas avseende tillämpning hos en verksamhetsutövare.

Att cybersäkerhetslagen tillämpas på en verksamhetsutövare i sin helhet skulle leda till en mycket omfattande tillsyn som inte bedöms bli effektiv och ändamålsenlig (se ovan Om kommuner som verksamhetsutövare). Däremot tillstyrker Livsmedelsverket att

[6] Delbetänkandet SOU 2024:18, sid. 135
[7] Madell & Lundin, Kommunallagen (22 jan. 2024, JUNO), kommentaren till 6 kap. 15 §. Se även Kammarrätten i Jönköpings dom 2019-12-18, mål.nr. 2122-19.

cybersäkerhetslagen bör tillämpas på de delar av verksamheten som kan påverka säkerheten i den tjänst som avses enligt direktivets bilagor.

NIS-lagens utformning möjliggör för verksamhetsutövaren att använda tekniska åtgärder för att effektivt förhindra att nätverk och informationssystem som används i andra tjänster kan påverka säkerheten i den omfattade tjänsten. Ett sådant förhållningssätt möjliggör även att olika nivåer av säkerhet kan införas i olika delar av en teknisk miljö baserat på risk och gällande krav.

Att underhålla samma nivå av säkerhet i de system som används för leverans av tjänsten som för kringliggande administrativa system som inte påverkar säkerheten i den samhällsviktiga tjänsten kan vara kostsamt och kan i värsta fall leda till en sämre säkerhet i de tjänster som direktivet avser omfatta. Möjlighet att använda tekniska säkerhetsåtgärder för att separera känsliga nätverk och informationssystem som kräver en högre nivå av säkerhet innebär en kostnadseffektiv metod för att uppnå det mål och syfte som NIS2-direktivet sätter upp.

Sektorn produktion, bearbetning och distribution av livsmedel i NIS2-direktivet är avgränsad för att inte omfatta konsumentledet, dvs. ambitionen är inte att försäljning av livsmedel i butik ska omfattas. Det är dock inte ovanligt att större verksamhetsutövare i livsmedelssektorn levererar tjänster såväl inom produktion, bearbetning och produktion som direkt till konsument. Att omfatta hela verksamhetsutövaren utan en tydlig beskrivning av tillämpning av förslaget innebär således i praktiken att ytterligare tjänster som faller utanför NIS2-direktivets avgränsning omfattas. Detta innebär ett stort avsteg från direktivets intention att enbart omfatta de tjänster som avgränsats i bilagorna.

På ett liknande sätt kan en verksamhetsutövare vars omsättning, balansomslutning och/eller personalstyrka överstiger de angivna tröskelvärdena komma att omfattas baserat på att de levererar en tjänst som inryms i avgränsningarna i direktivets bilagor, även om tjänsten enbart utgör en väldigt liten del av deras totala verksamhet. Exempelvis kan ett klädföretag som även distribuerar vissa livsmedel till sina butiker komma att omfattas på grund av att deras totala omsättning, balansomslutning och/eller personalstyrka överstiger tröskelvärdena. Livsmedelsverket anser att detta inte är NIS2-direktivets intention, utan istället utgör en oavsiktlig omfattning.

Livsmedelsverket gör bedömningen att myndighetens egen verksamhet bör komma att omfattas av lagen i och med att verket bör kunna leva upp till samtliga delar av direktivets definition på ”offentlig förvaltningsentitet.” I egenskap av omfattad verksamhetsutövare bör vår egen regelefterlevnad underlättas av ett förtydligande

kring tillämpningsområdet då myndighetens verksamhet är bred och tillhandahåller en mångfald av olika tjänster.

Föreskriftsrätten bör ses över för att undvika överlappande reglering

Livsmedelsverket avstyrker utredningens förslag att den myndighet som har tillsynsansvar också får meddela föreskrifter avseende säkerhetsåtgärder (riskhanteringsåtgärder), systematiskt informationssäkerhetsarbete samt utbildning för sin sektor.[8] Livsmedelsverket anser istället att MSB bör ges rätten att meddela föreskrifter om systematiskt informationssäkerhetsarbete för samtliga sektorer, med fokus på systematik och en definition av det, samt föreskrifter om utbildning.

Livsmedelsverket anser även att tillsynsmyndigheterna ska ges tillfälle att yttra sig om dessa föreskrifter samt att tillsynsmyndigheten ska få möjlighet att vidta åtgärder vid bristande efterlevnad.

Livsmedelsverket tillstyrker utredningens förslag om att kompletterande föreskrifter avseende riskhanteringsåtgärder (säkerhetsåtgärder) bör meddelas av tillsynsmyndigheten för den tjänst som tillsynsmyndigheten har tillsynsansvar för.

Livsmedelsverket är tveksamma till den struktur för föreskriftsrätt som föreslås i betänkandet eftersom det innebär att en verksamhetsutövare kommer att omfattas av föreskrifter från fler olika tillsynsmyndigheter.

Enligt förslaget skulle en verksamhetsutövare som har flera olika verksamheter, till exempel sektorerna dricksvattenproduktion, avloppshantering, avfallshantering och energiproduktion kunna träffas av föreskrifter som berör systematiskt informationssäkerhetsarbete, utbildning och riskhanteringsåtgärder från minst tre olika tillsynsmyndigheter. Om dessa sektorer verkar under ett och samma ledningsorgan vilket beslutar om säkerhetsåtgärder i förhållande till risk på någon detaljnivå blir situationen problematisk.

Nuvarande NIS-lag ger MSB rätten att meddela föreskrifter avseende det systematiska informationssäkerhetsarbetet. Med en liknande struktur för det nya förslaget skulle överlappande föreskrifter för en och samma styrning i högre grad kunna undvikas, liksom merarbetet av att varje tillsynsmyndighet meddelar egna föreskrifter med i stort sett samma innehåll som de övriga tillsynsmyndigheterna.

[8] Delbetänkandet, 35§ förordningen

Direktivets sektorsavgränsningar behöver förtydligas

Livsmedelsverket tillstyrker ansvarsfördelningen att myndigheten tilldelas tillsynsansvar för sektorerna dricksvatten, avloppsvatten samt produktion, bearbetning och distribution av livsmedel, men önskar ett ytterligare förtydligande av sektorernas avgränsning jämfört med utredningens förslag.

Avloppsvatten
Avgränsningen för avloppssektorn är inte helt tydlig vilket kan leda till svårigheter för en verksamhetsutövare att bedöma om de omfattas av cybersäkerhetslagen eller inte.

Lagstiftaren behöver tydliggöra vad "icke-väsentlig del av sin allmänna verksamhet" betyder och i vilka termer detta ska mätas. För exempelvis en gruvverksamhet kan hantering av industrispillvatten utgöra en mindre del av gruvföretagets allmänna verksamhet sett till finansiell omsättning. I praktiken kan dock verksamheten vara helt väsentlig för att gruvdriften ska få fortgå. Ett avbrott i hanteringen av industrispillvatten skulle kunna innebära att verksamheten i övrigt inte kan fortlöpa.

Produktion, bearbetning och distribution av livsmedel
Liknande otydligheter förekommer i sektorn för livsmedel. Livsmedelsverket anser i likhet med utredningen att begreppet livsmedelsföretag (food business) bör avse en form av verksamhet som omfattar aktiviteter som hänger samman med något stadium/några stadier i produktions-, bearbetnings- och distributionskedjan för livsmedel.

Utredningen kommer till slutsatsen att endast fysiska och juridiska personer ska betraktas som verksamhetsutövare. Däribland fysiska och juridiska personer som är livsmedelsföretagare (food business operators). Ett livsmedelsföretag (food business) är inte en fysisk eller juridisk person, utan snarast en form av verksamhet, och kan således inte vara att betrakta som en verksamhetsutövare i direktivets mening. Med bakgrund av detta blir det motsägelsefullt att omfatta verksamhetsutövaren (den juridiska personen) inom livsmedelssektorn i sin helhet.

Industriell produktion och bearbetning
Begreppet industriell produktion och bearbetning har inte definierats genom direktiven eller livsmedelslagstiftningen, och dess närmare innebörd berörs inte i direktiven. Primärproduktionen betraktas i allmänhet inte som industriell produktion även om vissa verksamheter har nått en hög grad av mekanisering, hög specialisering och bedrivs i stor skala.

- Är exempelvis en storskalig mjölkgård, utrustad med mjölkningsrobotar industriell?
- Är exempelvis ett stort slakteri (ej fjäderfä) industriellt, trots att de flesta moment i slakten utförs manuellt, i princip helt utan inslag av automatisering?

Livsmedelslagstiftningen är som utgångspunkt tillämplig ”från jord till bord”, dvs. i alla led/stadier i den s.k. livsmedelskedjan (i alla ”stages of production, processing and distribution[9]”). Vid tillämpningen av livsmedelslagstiftningen finns det i princip aldrig skäl för att fundera över vad begreppet produktion avser.

Begreppet produktion nämns först i livsmedelslagstiftningens definition av begreppet ”stages of production, processing and distribution”[10] (som det första stadiet i kedjan). Bör primärproduktion således förstås kunna omfattas av direktiven (”industrial production and processing”). I livsmedelslagstiftningen används begreppet produktion [11] nästan uteslutande i primärproduktionssammanhang.

Begreppet produktion används ofta med en tämligen vid innebörd, som synonym till skapande eller tillverkning. Mot bakgrund av att även bearbetning nämns bör det dock vara möjligt att åtskilja produktion och bearbetning från varandra.

Om begreppet produktion ska avse primärproduktion anser Livsmedelsverket att innebörden av begreppet bearbetning behöver förtydligas. Begreppet bearbetning har i livsmedelslagstiftningen en snäv definition[12] som skulle kunna utesluta en väsentlig andel av verksamheter i livsmedelssektorn som skulle kunna omfattas av cybersäkerhetslagen.

Sammantaget är ett förtydligande av vilka delar av livsmedelskedjan som ska omfattas av den föreslagna lagen nödvändig eftersom avgränsningen i direktivets bilaga öppnar för tolkningar.

[9] Förordning EG nr 178/2002 ’stages of production, processing and distribution’ means any stage, including import, from and including the primary production of a food, up to and including its storage, transport, sale or supply to the final consumer and, where relevant, the importation, production, manufacture, storage, transport, distribution, sale and supply of feed;
[10] Ibid.
[11] Förordning EG nr 178/2002
[12] Förordning EG nr 852/2004: "processing" means any action that substantially alters the initial product, including heating, smoking, curing, maturing, drying, marinating, extraction, extrusion or a combination of those processes;

Direktivets bestämmelse om ledningens ansvar bör inkluderas i cybersäkerhetslagen

Livsmedelsverket anser att en bestämmelse kring ledningens engagemang och ansvar ska inkluderas i lagen. Livsmedelsverket avstyrker förslaget att bestämmelsen om ledningens beslut om riskhanteringsåtgärder inte inkluderas i lagen. Istället ska en sådan bestämmelse inkluderas och formuleras så att det blir tydligt hur och på vilken nivå ett ledningsorgan ska godkänna riskhanteringsåtgärder.

Utredningen föreslår att inte inkludera NIS2-direktivets artikel 20 om styrning i sin helhet. Den centrala bestämmelsen om att ledningsorgan ska godkänna och övervaka riskhanteringsåtgärder för cybersäkerhet finns inte med i utredningens förslag till cybersäkerhetslagen.

Ett mindre framgångsrikt informationssäkerhetsarbete har ofta sin grund i bristande styrning och ledarskap. MSB:s undersökning Infosäkkollen från både 2021 och 2023 visar på brister i styrning hos de deltagande organisationerna. Efter undersökningen 2023 uttryckte MSB i sammanfattningen att ”resultatet inom arbetsområdet för Ledningens styrning och kontroll visar på en avsaknad av engagemang från organisationernas ledningar. Medan ett visst skydd kan uppnås utan aktiv inriktning och uppföljning av ledningen så är MSB:s bedömning att förutsättningarna för att bedriva ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete saknas utan ledningens löpande engagemang. För att kunna arbeta systematiskt över tid måste säkerhetsarbetet prioriteras och tilldelas resurser.”[13]

Genom att inkludera ett krav på ledningens engagemang i lagtexten förtydligas på vilken nivå i en organisation ansvar för säkerhet förväntas tas. Utredningen föreslår långtgående möjligheter till ingripanden vid överträdelser där en tillsynsmyndighet till och med ska kunna förbjuda en person att utöva ett ledningsuppdrag. På detta vis indikeras ledningens betydelse, även om sanktionen inte ska kunna riktas mot offentlig verksamhet. Inkludering av ett explicit krav på ledningens engagemang i säkerhetsarbetet kommer att ytterligare förtydliga ledningens betydelse och underlätta för tillsynsmyndigheterna vid bedömning.

Riskhanteringsåtgärder ska vara lämpliga

Livsmedelsverket anser att lagen ska ställa krav på att riskhanteringsåtgärder ska vara såväl proportionella som lämpliga i förhållande till risken de avser hantera. Därmed avstyrks utredningens förslag om att riskhanteringsåtgärder som

[13] Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen : Resultatredovisning av Infosäkkollen och It-säkkollen

identifierats enbart ska bedömas mot proportionalitet vilket utelämnar direktivets ordalydelse ”proportionella och lämpliga”[14].

Åtgärder som syftar till att höja säkerhetsnivån i en verksamhet behöver vara såväl lämpliga som proportionella i förhållande till den risk de avser hantera. Formuleringen om att åtgärder ska vara lämpliga och proportionella finns i direktivet och återkommer i andra etablerade standarder inom säkerhetsområdet.[15] Utredningen framför dock att det inte tillför något att ange att åtgärderna ska vara lämpliga och föreslår istället att åtgärder enbart behöver vara proportionella i förhållande till risken.[16] En frånvaro av kravställning på lämpliga åtgärder kommer att försvåra regelefterlevnaden, det kan leda till införande av direkt olämpliga åtgärder och kan i tillägg försvåra tillsynsmyndigheternas arbete.

Eftersom införande av riskhanterande åtgärder kan vara kostsamt behöver verksamheten sätta kostnaden för åtgärden i proportion till den uppskattade kostnaden för konsekvenserna av att risken realiseras, dvs. åtgärderna behöver på detta sätt vara proportionella för att inte i praktiken innebära en förlust för verksamheten. Det är dock centralt att de åtgärder som införs hanterar risken på effektivt sätt, dvs. de behöver vara anpassade till att hantera riskerna och deras konsekvenser utan att orsaka nya risker eller försvåra för verksamheten att utföra sin uppgift. En viss teknisk åtgärd kan exempelvis fungera väl i en miljö med traditionella IT-system, men ha förödande konsekvenser för driftssäkerheten i en miljö med industriella styrsystem. En åtgärd måste också vara väl anpassad för att kunna förvaltas och fungera i verksamheten den ska skydda.

För att avgöra om en åtgärd är proportionell i förhållande till risken behöver såväl åtgärden som risken göras mätbar. Det mått som finns att tillgå är kostnad - kostnad för införande och förvaltning av åtgärden samt kostnad för att hantera konsekvenserna av ett realiserat hot. Detta mått fångar dock inte upp huruvida åtgärden är lämplig för den verksamhet och tekniska miljö den ska införas i. I praktiken kan en direkt olämplig åtgärd innebära en kostnad som fortfarande är proportionell i förhållande till risken.

Vid en tillsyn kommer tillsynsmyndigheten att behöva bedöma de åtgärder en verksamhetsutövare vidtagit för att hantera sina risker. Detta är en bedömning som kräver erfarenhet och en kunskap om vad som är generellt vedertaget för hur olika typer av risker bör hanteras i olika typer av miljöer och verksamheter. Om åtgärder enbart ska vara proportionella i förhållande till risken kommer tillsynsmyndigheten

[14] Direktivet (EU) 2022/2555 (NIS2), Artikel 21 punkten 1
[15] se exempelvis ISO/IEC 27001:2023 6.1.3 a
[16] Delbetänkandet SOU 2024:18, s. 192

inte att kunna ingripa om det framkommer att mindre lämpliga eller olämpliga åtgärder används.

Bestämmelser kring incidentrapportering bör ses över

Tidsfristen för första varning kan förkortas
Livsmedelsverket avstyrker att skrivelsen ”utan onödigt dröjsmål” för den första tidiga varningen har uteslutits i utredningens förslag. Livsmedelsverket anser också att tidsfristen kan förkortas till 6 timmar efter att verksamhetsutövaren fått kännedom om incidenten. 6 timmar är i paritet med nuvarande NIS-lag och MSB:s föreskrifter om incidentrapportering för statliga myndigheter (MSBFS 2020:8)

En skyndsam initial informationsdelning kan vara av särskild relevans till exempel vid spridning av skadlig kod då andra verksamhetsutövare kan ha nytta av sådan information. För att möjliggöra en sådan tidig varning och inte belasta verksamhetsutövare med stora rapporteringsformulär måste en tidig varning implementeras med en för verksamhetsutövaren enkel och effektiv process. För verksamhetsutövare som ingår i en koncern med delade IT-resurser kan en sådan enkel och effektiv process bli än mer nödvändig.

Överlappande incidentrapportering bör analyseras
Livsmedelsverket ställer sig frågande till eventuell överlappande incidentrapportering och anser att detta behöver hanteras så att verksamhetsutövare inte behöver rapportera samma incident fler gånger än nödvändigt.

Förslagets omfattning innebär att flera verksamhetsutövare i en och samma koncern kan omfattas och därmed blir föremål för bestämmelser om incidentrapporter. Det är inte ovanligt att företag i en koncern använder delade IT-resurser och det kan innebära att en övergripande incident får påverkan på flera anmälda juridiska personer. Det kan givetvis vara relevant för CSIRT och tillsynsmyndigheten att få tillgång till uppgifter om vilka verksamhetsutövare som påverkas, men en rapportering av samma uppgift kring en enskild incident flera gånger bör undvikas.

Ändring av ordet varning till notifiering
Livsmedelsverket instämmer i MSB:s påpekande av att ordet varning bör ersättas med notifiering.[17]

[17] MSB:s Remissvar delbetänkandet 2024:18 Nya regler om cybersäkerhet

Övriga synpunkter på förslaget

Nedan följer ett antal mindre observationer kring förslaget som ändå är relevanta för lagstiftaren att ta hänsyn till vid utformning av den färdiga cybersäkerhetslagen.

Omständigheter vid ingripande, uppsåt eller strikt ansvar
Livsmedelsverket motsätter sig förslaget att vid ett ingripande bedöma om en överträdelse begåtts med uppsåt eller oaktsamhet[18]. Livsmedelsverket anser att nu gällande utgångspunkt avseende strikt ansvar införs även i cybersäkerhetslagen.

Begreppet uppsåt är ett komplext juridiskt begrepp, där det finns olika typer och det kan omfatta olika nivåer och synes ha olika förklaring inom olika rättsområden. Detta riskerar att skapa oklarheter och försvåra tillsynsmyndigheternas bedömningar.

Avseende uppförandekoder och certifieringsmekanismer
Livsmedelsverket anser att det är nödvändigt med ett förtydligande av vad som menas med de förmildrande omständigheterna om verksamhetsutövaren "följt godkända uppförandekoder eller godkända certifieringsmekanismer" (Cybersäkerhetslagen, 5 kap 4 §) om dessa ska kunna beaktas.

Det finns inget ytterligare förtydligande avseende vad uppförandekoder eller certifieringsmekanismer är eller hur de ska bedömas som godkända.

Avseende reglering av dubbel bestraffning
I utredningens förslag till lag om cybersäkerhet anges i 5 kap § 17 att tillsynsmyndigheten inte får besluta om sanktionsavgift om överträdelsen i fråga har lett till att verksamhetsutövaren påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen. Livsmedelsverket är tveksamma till huruvida det är nödvändigt att specifikt identifiera detta hinder för att besluta om sanktionsavgift med tanke på etablerade bestämmelser kring dubbel bestraffning.

Avseende CSIRT-enhetens uppgifter
Utredningen föreslår i förordningens 29 § ett antal uppgifter som CSIRT-enheten ska utföra, däribland att "samla in och analysera forensiska uppgifter". En sådan uppgift utförs vanligtvis vid och efter en cybersäkerhetsincident där det föreligger en misstanke om brott. Livsmedelsverket är tveksamt till huruvida det bör vara CSIRT-enhetens uppgift att utföra en sådan uppgift då det snarare kan behöva falla inom en brottsutredande myndighets ansvarsområde. Spårbarheten och kontrollkedjan ("chain of custody") är av stor vikt vid denna typ av insamling av bevis.

[18] Delbetänkandet, 5 kap §3 lag om cybersäkerhet

Avseende insamling av registreringsuppgifter
Utredningen förslår att tillsynsmyndigheterna ska få i uppgift att samla in registreringsuppgifter på omfattade verksamhetsutövare som anmäler sig till dem. Dessa ska sedan göras tillgängliga för den gemensamma kontaktpunkten. Livsmedelsverket instämmer i MSB:s remissvar avseende en gemensam plattform för registrering av verksamhetsutövare[19]. Det förefaller naturligt att uppgiften att tillhandahålla en sådan plattform ges till den gemensamma kontaktpunkten eftersom denna ska rapportera uppgifterna till Kommissionen. Det bör även finnas fördelar kopplat till verksamhetsutövarnas incidentrapportering eftersom registreringsuppgifterna kan användas för att på ett bättre sätt koppla en incidentrapport till en anmäld verksamhetsutövare.

Vidare föreslår utredningen att ett register över verksamhetsutövare ska lämnas in till den gemensamma kontaktpunkten två månader efter att lagen trätt i kraft och sedan i vart fall vartannat år[20]. Den gemensamma kontaktpunkten ska sedan lämna uppgifter vidare till kommissionen och samarbetsgruppen. Livsmedelsverket är tveksamma till om två månader är tillräckligt för att ge verksamhetsutövare tid att bedöma huruvida de omfattas av lagen samt genomföra anmälan.

Avseende 'en' riskanalys
Utredningen föreslår i cybersäkerhetslagens 3 kap, 1 § att riskhanteringsåtgärder "ska utgå ifrån ett allriskperspektiv och en riskanalys". Formuleringen "en riskanalys" har i nuvarande NIS-lag varit problematisk och olika tillsynsmyndigheter har gjort olika tolkningar av vad ”en riskanalys” i praktiken betyder för en verksamhets säkerhetsarbete.

Livsmedelsverket är tveksamma till formuleringen ”en” och anser att även fler riskanalyser bör vara möjliga och ofta nödvändiga för att en verksamhetsutövare ska anses efterleva regelverket.

Avseende säkerhetsskanningar
Utredningen föreslår i cybersäkerhetslagens 4 kap, § 9 att tillsynsmyndigheten ska få låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av lagen. Det ges inga ytterligare förtydliganden kring vilka begränsningar sådana skanningar ska ha, hur de ska utföras eller vilka delar av en teknisk miljö de får utföras på. Livsmedelsverket tillstyrker att en sådan skanning alltid ska ske i samarbete med verksamhetsutövaren men anser att bestämmelsen behöver förtydligas och att det kan vara lämpligt att meddela tydliggörande föreskrifter, som

[19] MSB:s Remissvar delbetänkandet 2024:18 Nya regler om cybersäkerhet
[20] Delbetänkandet, förordningen 14 §

även reglerar hur ett resultat av en sådan säkerhetsskanning ska hanteras, kopplade till bestämmelsen.

Avseende förvärv av informationssystem
I förslaget till cybersäkerhetslagens 3 kap § 1 listas områden som en verksamhetsutövares riskhanteringsåtgärder ska omfatta, däribland "säkerhet vid förvärv, utveckling och underhåll av nätverks och informationssystem." MSB har till utredningen föreslagit att "förvärv" i sammanhanget ska ersättas med "anskaffning" för att visa hur kraven även gäller när ett informationssystem används men inte köpts, exempelvis vid en utkontraktering. Livsmedelsverket tillstyrker MSB:s förslag. Utredningen utgår strikt ifrån den svenska översättningen av direktivet för sin tolkning och hävdar att det innebär en utökning av direktivet om kraven ska gälla vid anskaffning av informationssystem. Termen "acquisition" som används i den engelska texten översätts mer korrekt till "anskaffning" eftersom ordet betyder att skaffa sig tillgång till något i en bredare bemärkelse än att enbart köpa det. ISO/IEC gör även denna mer korrekta översättning och använder ordet "anskaffning" för "acquisition" i standarden ISO/IEC 27001.[21]

Avseende anmälan av ändrade uppgifter
Utredningen föreslår i cybersäkerhetslagens 2 kap § 2 att ålägga verksamhetsutövare att anmäla förändrade uppgifter i registreringen inom 14 dagar. Enligt kap 5, § 1 ska tillsynsmyndigheten ingripa vid överträdelser av den paragrafen. Livsmedelsverket anser att formuleringen bör ändras så att förändrade uppgifter ska anmälas utan onödigt dröjsmål. Det kan komma att bli problematiskt för verksamhetsutövare att förhålla sig till en fast tidsgräns på enbart 14 dagar och tillsynen av efterlevnad och ingripanden kommer att vara svåra att genomföra då det kan finnas tolkningar kring när i tiden en viss uppgift i praktiken fastställts.

Avseende huvudsakligt etableringsställe
Utredningen föreslår i förordningens § 3 att "plats för cybersäkerhetsverksamhet" ska beaktas vid avgörande av huvudsakligt etableringsställe. Livsmedelsverket anser att formuleringen bör ändras till "huvudsaklig plats för cybersäkerhetsverksamhet" då det inte är ovanligt att sådan verksamhet förekommer på flera olika platser för en och samma verksamhetsutövare.

[21] SVENSK STANDARD SS-EN ISO/IEC 27001:2023, Bilaga A. Även

Information till kunder om betydande incident
Utredningen föreslår i cybersäkerhetslagens 3 kapitel 3 § att kunder ska informeras vid en allvarlig incident. Direktivets skrivelse (artikel 23) om att detta ska ske ”när så är lämpligt” har tagits bort i utredningens förslag. Livsmedelsverket anser att skrivningen ”när så är lämpligt” bör införlivas i cybersäkerhetslagen då det kan finnas situationer när kunder inte behöver informeras.

Konsekvenser

Utredningen föreslår i sin konsekvensanalys att befintliga tillsynsmyndigheter ska få ökade anslag med 2 miljoner kronor per år för löpande kostnader.[22] Livsmedelsverket anser att den analys som genomförts inte speglar de verkliga kostnaderna men också att läget varit svårbedömt då ansvarsförhållandena inte varit tydliga. Till exempel beror en kostnad hos tillsynsmyndigheten, utom personalkostnader, på hur tillsynsmyndigheten klassar information som delges under en tillsyn och om specifika IT-verktyg krävs för tillsynen. Vidare leder otydligheter i sektorsavgränsningarna till svårigheter att bedöma antalet tillsynsobjekt. Om cybersäkerhetslagen ska komma att omfatta verksamhetsutövare i sin helhet kan det även få konsekvenser för tillsynens omfattning, samma gäller om samtliga kommuner ska omfattas eller inte. Det anslag som ges sätter ambitionsnivån för tillsynsverksamheten och därmed påverkar den även robustheten i samhället avseende cybersäkerhet. Livsmedelsverket anser att den ekonomiska konsekvensen av förslaget behöver en djupare analys.

Beslut i detta ärende har fattats av generaldirektör Annica Sohlström. I den slutliga handläggningen medverkade avdelningscheferna Helena Brunnkvist, Eiríkur Einarsson, Kristina Granelli, Daniel Karlsson, Kristina Ohlsson, Eva Corp och Mattias Åsander. Föredragande var Katarina Sunnegårdh och Anders Lindström.

Annica Sohlström

Katarina Sunnegårdh

[22] Delbetänkande SOU 2024:18, Konsekvensanalysen, avsnitt 12.6.7