Branschorganisationen
för dagligvaruhandeln

Ärendenummer: Fö2024/00496
Inskickat: 2024-05-24
Ansvarig tjänsteman: Ulrika Dahlin

Från:
Svensk Dagligvaruhandel

Till:
Försvarsdepartementet

Remiss avseende Nya regler för cybersäkerhet

Svensk Dagligvaruhandel är branschorganisationen för dagligvaruhandeln i Sverige. Våra medlemsföretag är Axfood AB, City Gross AB, Coop Sverige AB, ICA Sverige AB, Lidl Sverige KB och Livsmedelshandlarna. Tillsammans står vi för drygt 95 % av dagligvaruhandeln i Sverige, med butiker över hela landet. Dagligvaruhandeln sysselsätter runt 95 000 personer, varav en tredjedel är unga (15–24 år).

Svensk Dagligvaruhandels remissvar

Svensk Dagligvaruhandel har tagit del av förslaget till delbetänkandet 2024:18 Nya regler om cybersäkerhet.

Vi ser positivt på att regeringen tar cybersäkerhet på stort allvar och vi delar uppfattningen att cybersäkerhet är ett område där det finns stora utmaningar idag. Alla aktörer, såväl privata som offentliga, har ett ansvar och arbete att göra för att bidra till att upprätthålla en hög motståndskraft mot cyberrelaterade hot mot samhällsviktiga tjänster.

I detta remissvar tar vi utgångspunkt i uppdraget till utredningen avseende *”Utgångspunkten från regeringen var att förslagen utformas så att **regelbördan och administrationen minimeras** för berörda verksamhetsutövare”* samt *”Innebär inte några skyldigheter utöver vad som följer av direktivet”*. Vi ser inte att dessa delar till fullo uppfyllts i delbetänkandet 2024:18 Nya regler om cybersäkerhet och vi kommer också nedan ge exempel på detta. Utredningens förslag driver administration snarare än skapar riskminimering. I nuläget bedömer företagen en utökning om en till tre FTE vardera för att hantera administrationen.

Överlag ser vi en utmaning med att utredningen inte är konkret utan att flera förtydliganden avses specificeras i föreskrifter och kompletteringar från Myndigheten för samhällsskydd och beredskap (MSB) och utpekade

Besöksadress: Regeringsgatan 60
Postadress: 103 29 Stockholm, Sverige
info@svdh.se

tillsynsmyndigheter. Vi menar att det finns många obesvarade frågor i utredningen som bör förtydligas redan i lagtexten för att undvika en godtycklig och/eller överlappande implementation. Till detta kommer implementationen av CER-direktivet också få konsekvenser för medlemsföretagens omfattning av NIS-direktivet som inte kommer vara utredda förrän till hösten.

Vi förstår och respekterar bristen på tid som utredningen haft men beklagar också att det inneburit avsaknad av näringslivsrepresentanter i expertgruppen. Vi ser därmed konsekvenser för näringslivet och inte minst dagligvaruhandeln som vi väljer att lyfta i detta remissvar. Svensk Dagligvaruhandeln avstyrker därför utredningens förslag gällande syfte med den nya cybersäkerhetslagen, avsaknaden av lämplighetsprincipen, utredningens tolkning om att hela verksamheten ska omfattas, formuleringen kring myndigheternas möjlighet till säkerhetsskanningar, formuleringen kring föreskriftsrätten samt att NIS2-direktivets bestämmelse om ledningens ansvar bör inkluderas i cybersäkerhetslagen. Svensk Dagligvaruhandel tillstyrker däremot föreslagen förändring till minst 24 h för incidentrapportering. Slutligen lämnar vi övergripande synpunkter vad gäller såväl definitionen av livsmedelsföretag samt belyser den svenska regleringen ur ett internationellt perspektiv för dagligvaruhandelns behov.

Syfte – lagens första paragraf

I förslaget till lag om cybersäkerhet (kap 1 §1) förslås följande formulering ”Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.” Vi anser, i likhet med Livsmedelsverket, att syftet med lagen varken är fullständigt, fokuserat eller i linje med syftet med EU-direktivet.[1]
Som syftet är formulerat i dagens lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster bedömer vi ligger mer i linje med NIS2-direktivets syfte och syftet i föreslagen lag bör därmed justeras i enlighet med direktivet.

Förslag: Syftet med den föreslagna lagen behöver förtydligas och bör justeras i enlighet med direktivet.

Avsaknad av lämplighetsprincipen och konsekvenser att detta

Vi styrker utredningens tolkning att proportionalitet ska bedömas i relation till risk. Vi, i likhet med Livsmedelsverket, avstyrker att utredningen utelämnar lämplighet och likställer det med proportionalitet. Vår uppfattning är att utredningen därmed missar viktiga delar avseende bedömningen av säkerhetsåtgärder. NIS2-direktivet

[1] Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148 (4) var att bygga upp cybersäkerhetskapaciteten i hela unionen, begränsa hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

(Art. 21 (1) andra stycket) beskriver lämpligheten enligt följande: ”Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna […]”. Begrepp som ”senaste” (state-of-the-art[2]) och genomförandekostnad har använts tidigare i europeisk lagstiftning, i synnerhet GDPR och här finns det befintliga tolkningar från olika europeiska organ så som ENISA och EDPB. Att inte använda dessa i svensk lagstiftning förfaller sig inte som en förenkling och tar bort möjligheten att tillgå dessa tolkningar och vägledningar.

Vi är i synnerhet bekymrade över att avsaknaden av lämplighetskriterium kan innebär stora utmaningar för mindre mogna teknologiområden såsom cyberfysiska system (Operational Technology) som också omfattas av direktivet. Användning av enbart proportionalitetskriteriet skulle kunna innebära krav på åtgärder som finns men inte är tekniskt lämpliga att införa för cyberfysiska system eller inte är ”state-of-the-art” enligt betydelsen i ENISA, då höga skyddsbehov i proportion till risk inte kan tillgodoses med det som är tillgängligt som ”state-of-the-art”. Det är därmed vår uppfattning att cybersäkerhetslagen även behöver införa begreppet ”lämpligt” och använda det på motsvarande sätt som i GDPR och NIS2-direktivet. Detta är också något som Livsmedelsverket lyfter i sitt remissvar.

Förslag: Det är nödvändigt att inkludera NIS2-direktivets skrivelse om ”lämplighet” vid sidan om ”proportionalitet” för utvärdering av riskhanteringsåtgärder.

Att hela verksamheten ska omfattas är en övertolkning av EU-direktivet

Utredningen föreslår att “hela verksamheten” ska omfattas av direktivet. Vi ser, i likhet med Livsmedelsverket, omfattande praktiska konsekvenser som enligt vår uppfattning dessutom går emot regeringens uppdrag att säkerställa ”så låga administrativa och andra kostnader som möjligt för entiteterna”.

Att hela verksamheten omfattas skulle ha omfattande praktiska konsekvenser för ett företag i dagligvaruhandeln. I NIS2-direktivet görs ett medvetet val att enbart partihandel ska omfattas, vilket därmed exkluderar butiker. Genom omfattning av hela verksamheten, som beroende på organisationsstrukturer eller associering, skulle nätverk- och informationssystem för detaljhandel ändå komma att omfattas för de företag där dessa verksamheter bedrivs av samma juridiska person. Även nätverks- och informationssystem för andra delar av en verksamhet som bedriver partihandel skulle genom lagförslagets definition av ”hela verksamheten” omfattas. Detta får till konsekvens att lagens omfattning skiljer sig markant mellan våra medlemsföretag baserat på hur deras organisationsstruktur för närvarande ser ut. För vissa medlemsföretag skulle därmed även andra verksamheter som butik, marknad, kundhantering och dylikt omfattas trots att deras nätverks- och informationssystem inte utgör eller påverkar den verksamhet lagen har för avsikt att

[2] What is "state of the art" in IT security? — ENISA (europa.eu)

reglera. Dessa företag skulle drabbas av onödig administration för att utföra och underhålla omfattande riskanalys(er) för hela verksamheten för delar av verksamheten som inte avses i direktivet.

Utöver den praktiska konsekvensen ser vi också ett antal logiska och innehållsmässiga slutsatser som är inkonsekventa och leder till osäkerhet rörande omfattningen av hela verksamheten. Utredningen anför att det inte finns något stöd i NIS2-direktivet som medger att inte hela verksamheten skulle omfattas. Det ska anmärkas att enligt vår uppfattning är en uttömmande avgränsning praktiskt omöjligt och teoretisk tvivelaktig och det är därför tvivelaktigt att anföra detta som argument. Vår uppfattning är att det likaväl saknas ett uttryckligt yttrande om att hela verksamheten ska omfattas[3].

Som sitt huvudargument hänvisar utredning till skäl 16. Vår uppfattning är att skäl 16 huvudsakligen avser frågan om en entitets (verksamhet) storlek, och att en entitet som inte är medelstor i sig själv, på grund av samband med sina partner eller anknutna entiteter (verksamheter) bör uppfattas som medelstor i sin helhet, och därmed faller under NIS2-direktivet, och inte hur vidare en entitet (verksamhet) är avgränsningsbar inom sig själv. Vi ser också relevans i intentionen ”För att undvika att entiteter […] betraktas som väsentliga eller viktiga entiteter när detta vore oproportionellt [..]” då syftet förefaller vara begränsande. Medlemsstaterna är vidare uppmanade i skäl 16 att ta hänsyn till hur” [en] entitet är oberoende av sin partner eller de anknutna företagen med **avseende på de nätverks- och informationssystem** som entiteten använder” (vår fetmarkering). Om man använder resonemanget inom en entitet (verksamhet) verkar det rimligt att om delar av nätverk eller informationssystem är oberoende för olika delar av verksamheten så behöver de inte omfattas. Som exempel skulle ett oberoende (d v s möjlighet att avgränsa) i praktiken kunna innebära att en applikation (och den underliggande infrastruktur såsom hårdvara, operativsystem och middleware) som är eller kan göras oberoende av andra applikationer, som berör den reglerade verksamheten, inte bör omfattas. Att därmed tillämpa skäl 16 som motivering till att hela verksamheten ska omfattas är svårt att följa.

Av skäl 21 [4] i direktivet framgår en intention att hela verksamheten inte nödvändigtvisbör omfattas. Enligt skäl 21 kan kommissionen tillhandahålla vägledning för tillämpningsområden och proportionalitet när entiteter *”samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv”.* Då direktivet använder ordet entitet behöver

[3] Att utredningen introducerade detta genom induktion betraktas som vetenskapligt tvivelaktigt enligt gängse vetenskapsfilosofi.

[4] Kommissionen kan tillhandahålla vägledning för att bistå medlemsstaterna med att genomföra bestämmelserna i detta direktiv om tillämpningsområde och med att utvärdera proportionaliteten i de åtgärder som ska vidtas i enlighet med direktivet, särskilt vad gäller entiteter med komplexa affärsmodeller eller driftsmiljöer, varvid en entitet samtidigt kan uppfylla kriterierna för både väsentliga och viktiga entiteter eller samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv.

verksamheten här tolkas som aktiviteter som verksamheten bedriver. Direktivet är därmed explicit i frågan om att det kan förekomma verksamhetsområden som är undantagna från direktivet. Därmed förefaller tolkningen att hela verksamhet (i NIS2-direktivets mening av entitet) omfattas inte som nödvändig och därmed orimlig.

Vidare anför utredningen att *”det framstår också med hänsyn till att nätverks- och informationssystem många gånger är sammankopplade inom hela verksamhet samt att incidenter inom en del kan påverka annan del att det skulle leda till gränsdragningsproblem att försöka dela upp verksamheten.”* Denna tolkning innehåller en logisk inkonsekvens. Nästan alla nätverk och system är idag sammankopplade genom internet och detta går även över organisatoriska gränser. Detta innebär att **om** (vilket vi ifrågasätter) argumentets logik är korrekt, medför det att cybersäkerhetslagen behöver omfatta alla verksamheter som är kopplade till ett system som används av en verksamhet som omfattas av NIS2-direktivet, vilket i förlängningen innebär att varje verksamhet som faller under NIS2-direktivet ”smittar” sina leverantörer som i sin tur ”smittar” sina kunder. (Detta skulle gå emot själva cybersäkerhetslagen och NIS2-direktivet då leverantörskedjan enbart i första led bedöms omfattas och med det följer att en avgränsning där tillåts). Vidare skulle utredningens logik i förlängningen innebära att **många** verksamheter omfattas om kriteriet för samkoppling eller påverkan av incidenter skulle vara relevant. I praktiken kan dock nätverks- och informationssystem separeras från varandra genom tekniska implementationer. Indikationer för detta kan finnas i olika delar av lagen om elektronisk kommunikation som definierar användare (Kapitel 1 §7) som separata entiteter som är uppkopplade till nätverk som tillhandahåller säkerhet (Kapitel 8 §1) och kan genom det separera dessa användare. Vi ser även att företags nätverk vanligtvis tillämpar, enligt gängse standard (ISO 27002 8.22), fysisk och logisk separation för att avskilja delar av sina nätverk och informationssystem. Utöver det har vi tydlig evidens i Payment Card Industry Data Security Standard (PCI DSS), som gäller som en av de mest restriktiva säkerhetsstandarderna, att en avgränsning med hänsyn till säkerhet av Card Data Environment (CDE) är nödvändig och lämplig för att särskilja säkerhetsbehov. Och till sist kan vi nämna att även Common Criteria, som omnämns i Sverige i samband med säkerhetsskydd och nätverks- och informationssäkerhet[5], har en definition av ett ”security target” för att säkerställa lämplig avgränsning och med detta indikera att det inte bara är möjligt men även nödvändigt för att behärska komplexiteten. Därmed verkar en mera rimlig slutsats vara att även företagsnätverk internt är avgränsningsbara. Av detta följer att en avgränsning inom en verksamhet är möjligt genom fysisk och/eller logisk separation, genom säkerhetsåtgärder. Därmed behöver inte hela verksamheten omfattas och lagen bör i stället förtydliga behov av avgränsningar.

Förslag: Utredningen bör förtydligas och ta tydlig ställning för att hela verksamheten inte bör omfattas då det inte är förenligt med andra svenska lagar samt gängse

[5] SOU 2021:63, Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem

standardisering. Utredningen bör istället föreslå att en avgränsning genom en omfattningsbeskrivning (motsvarande ISO 27001 eller PCI DSS 4.0) ska göras.

Vi föreslår också ett möte med utredningen och utpekad sektorsmyndighet där vi tillsammans får förklara hur vår bransch är uppbyggd och organiserad och hur den påverkas beroende på utredningens definitionsval. Vi tror också att ett sådant möte skulle vara till nytta för utredningen vad avser den konsekvensanalys som måste genomföras för dagligvaruhandeln. Detta för att säkerställa att lagstiftningen går att kontrollera för utpekade myndigheter och går att efterleva på ett administrativt rimligt och konkurrensneutralt vis för branschen.

Oklarheter avseende tillsynsmyndigheten möjligheter att genomföra säkerhetsskanningar

NIS2-direktivets artikel 11 specificerar CSIRT-enheternas ansvar och befogenheter. Bland dessa ingår enligt artikel 11.3 a *”övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, **på begäran, tillhandahållande av stöd** till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem”.* Vidare specificeras i artikel 11.3 e att CSIRT ska *”tillhandahållande, **på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning** av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan”.* Slutligen anges i artikel 11. 3 h att *”CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters **allmänt tillgängliga nätverks- och informationssystem**. Sådan skanning får utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar”* (vår fetmarkering).

Syftet med detta är uttalat främjande och underlättande av samordnad delgivning av information om sårbarheter.

I NIS2-direktivet artikel 32.2 d och 33.2 c framgår att myndigheter när de utför sina tillsynsuppgifter har befogenhet att underställa väsentliga respektive viktiga entiteter *”säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten”*.

Den svenska utredningen skriver i författningskommentarerna om förslag till lag om cybersäkerhet 4 kap 9 § att *”en säkerhetsskanning får inte ha någon negativ inverkan på hur nätverks- och informationssystem fungerar och ska ske i samarbete [med] verksamhetsutövaren [sic]”*. Tyvärr lämnas inte vidare hänvisningar till föreskrifter eller närmare information om hur tillsynsmyndigheternas befogenheter avseende säkerhetsskanningar ska avgränsas.

Vi anser till att börja med att NIS2-direktivets och utredningens begrepp ”säkerhetsskanning” eller den engelska variantens ”security scan” behöver

förtydligas. Inom informations- och cybersäkerhet finns det vedertagna begreppet ”sårbarhetsskanning” eller ”vulnerability scanning” som avser skanning som utförs för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem. Det framgår dock inte av lagtexten om utredningen anser dessa begrepp vara synonyma. Vi ser detta som ytterligare ett exempel på det som MSB lyfter i sitt remissvar till utredningen om att lagen bör använda vedertagna begrepp och normalt språkbruk inom området.

Förslag: Utredningen behöver förtydliga vad begreppet ”säkerhetsskanning” anses omfatta. Om det är ”sårbarhetsskanning” som avses bör detta begrepp tillämpas i stället för ”säkerhetsskanning”.

Vi anser vidare att utredningen tydligare bör specificera tillsynsmyndigheternas mandat avseende genomförande av ”säkerhetsskanningar” så att det framgår att tillsynsmyndigheternas mandat likställs med CSIRT-enheternas mandat att utföra icke-inkräktande skanning av allmänt tillgängliga nätverks- och informationssystem, vilket exempelvis har förtydligats i den tyska implementationen av direktivet. Även Livsmedelsverket lyfter i sitt remissvar att bestämmelserna kring säkerhetsskanningar bör förtydligas.

Det finns dock ett antal utmaningar med sårbarhetsskanningar som vi vill göra utredningen uppmärksammade på:

1. Sårbarhetsskanningar riskerar alltid att påverka prestanda och tillgängligheten av ett företags nätverks- och informationssystem eftersom de konsumerar prestandakraft som inte sällan leder till försämrad prestanda, avbrott och systemkrascher. Därför behöver sårbarhetsskanningar planeras noggrant för att genomföras vid tidpunkter då det som regel är låg belastning nätverks- och informationssystemen. Det kan också vara så att vissa resurser av detta skäl behöver exkluderas från sårbarhetsskanningar. Detta gäller bland annat industriella informations- och styrsystem eller IoT-system som MSB som samlingsnamn benämner ”cyberfysiska system”[6].

2. Sårbarhetsskanningar ger sällan en komplett bild över sårbarheterna i en organisations nätverks- och informationssystem. För att visa en fullständig bild behöver det genomföras så kallad autentiserad skanning där de verktyg som används ges *priviligierad* behörighet till de system som omfattas av skanningen. Detta innebär att det samtidigt öppnar upp för en vidare behörighet till resurser som bör skyddas genom att brandväggsregler och nätverkssegmentering åsidosätts. I praktiken innebär detta att öppna upp för nya attackvektorer in i den skannade organisationens IT-miljö. Vem tar ansvar för risken det medför att dessa verktyg har höga behörigheter till

[6] Se MSB:s vägledning ”Grundläggande säkerhet i cyberfysiska system”, MSB1880 från december 2021.

organisationens nätverks- och informationssystem eller konsekvenser av ett intrång detta kan ge upphov till? Det bör därför vara uteslutet att tillsynsmyndighet ska ges befogenhet att utföra autentiserad skanning för att identifiera sårbarheter i organisationens samtliga nätverks- och informationssystem. Vad avser skanning av externt tillgängliga nätverks- och informationssystem är det dessutom så att de allra flesta företag har skydd mot bland annat överbelastningsattacker som är designade till att stoppa externa verktyg från att skanna av verksamhetsutövarens resurser. Om dessa ska tas bort för tillsynsmyndighetens möjlighet att utföra skanning kräver det att tillsynsmyndighetens skanningsverktyg godkänns som säkra i verksamhetsutövarens skyddsprodukter. Detta är alltså även vid extern icke-inkräktande skanning ett avsteg från de säkerhetsmekanismer som satts på plats för att skydda verksamhetsutövarens resurser.

3. Sårbarhetsskanningar – särskilt icke-inkräktande skanning – ger i regel upphov till mängder med resultat som utgörs av falsklarm och falska positiva svar som är mycket tids- och resurskrävande att utreda. Exempelvis tar analyserna inte hänsyn till vilka systemversioner som är sårbara eller vilka kompenserande säkerhetsåtgärder som organisationen har infört. För företag som har publika gästnätverk där våra kunder kan koppla upp sig är det heller inte ovanligt att icke-inkräktande sårbarhetsskanningar från ett externt perspektiv visar sårbarheter hos enheter som är uppkopplade på organisationens publika gästnätverk och därmed inte tillhör verksamhetsutövaren vilket kan vara tidsödande att skilja från resurser som ingår i organisationens egna nätverks- och informationssystem. Dessutom bör myndigheterna överväga om sådan skanning är förenlig med den europeiska dataskyddsförordningen (GDPR) då den innebär ett inte obetydligt integritetsintrång gentemot privata individer snarare än mot de verksamhetsutövares resurser som är underställda lagen.

4. Frågan om rapporternas konfidentialitet. En sårbarhetsskanning som genomförs på ett korrekt sätt visar i regel upp den samlade bilden över sårbarheter och osäker konfiguration i en organisations nätverks- och informationssystem. Det är information som behöver hanteras ytterst konfidentiellt och absolut inte får delas med utomstående då dessa kan användas för att planera attacker mot en aktörs IT-miljö. Vi önskar därför att lagen förtydligar att dessa rapporter ska klassificeras som kvalificerat hemliga eller hemliga i enlighet med säkerhetsskyddslagen 2 kap § 5 (och skyddas som sådana) samt att dessa rapporter därmed behöver förtydligas som sekretesskyddade i offentlighets- och sekretesslagen (2009:400).

Förslag: Utredningen bör specificera att tillsynsmyndigheten i likhet med CSIRT-organisationerna enbart har behörighet att utföra icke-inkräktande skanning av allmänt tillgängliga nätverks- och informationssystem. Organisationer ska kunna undanta resurser (exempelvis publika gästnätverk, OT-nätverk) från att omfattas av

skanningen. Vidare bör lagen förtydliga att rapporter från sårbarhetsskanningar ska klassificeras och skyddas som kvalificerat hemliga eller hemliga i enlighet med Säkerhetsskyddslagen.

Föreskriftsrätten

I utredningens förslag till förordning om cybersäkerhet specificeras bland annat myndigheternas rätt att meddela föreskrifter i 33-36 §§. I 33 § som ger MSB rätt att utfärda föreskrifter över vilka verksamhetsutövare som omfattas av lagen om cybersäkerhet samt 36 § som ger MSB rätt att meddela föreskrifter om vad som utgör en betydande incident noteras att *”Tillsynsmyndigheten ska ges tillfälle att yttra sig”.* Vi anser att detta ger den sektorspecifika tillsynsmyndigheten – som trots att den troligen är väl förtrogen med den sektor den verkar i – en tämligen svag ställning gentemot MSB i fråga om utformningen av dessa föreskrifter. Vi anser därför att utredningen bör stärka tillsynsmyndighetens ställning gentemot MSB så att de inte bara ska ges tillfälle att yttra sig utan att tillsynsmyndigheten ska förväntas yttra sig och att MSB ska vara skyldig att inhämta och beakta tillsynsmyndighetens yttrande.

I 35 § anges vidare att tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning och att MSB för dessa föreskrifter ska ges tillfälle att yttra sig. Vi anser det märkligt att MSB som är expertmyndighet inom cybersäkerhet inte föreslås få en starkare ställning vad avser dessa föreskrifter. Vi ser en stor risk för att föreskrifterna från olika tillsynsmyndigheter kommer skilja sig åt mellan de olika tillsynsmyndigheterna snarare än att härröra från ett standardiserat och etablerat informationssäkerhetsramverk. Det kan leda till att de krav som ställs inte är harmoniserade över olika sektorer och att verksamhetsutövare som står under tillsyn från flera olika tillsynsmyndigheter får olika krav på sitt informations- och cybersäkerhetsarbete. Detta står i direkt konflikt med NIS2-direktivets syfte om att införa en gemensam cybersäkerhetsnivå inom unionen i syfte att förbättra den inre marknadens funktion (Kap 1, artikel 1.1 eller artikel 25 som anger att europeiska och internationella standarder ska uppmuntras för att främja en enhetlig tillämpning av de riskhanteringsåtgärder direktivet syftar till att införa). Även detta lyfts fram av Livsmedelsverket i deras remissvar.

Förslag: Utredningen bör föreslå att utpekad tillsynsmyndighet får utfärda föreskrifter om vilka verksamheter inom utpekade sektorer som omfattas av lagen, men att MSB får föreskriftsrätt för det systematiska informationssäkerhetsarbetet.

NIS2-direktivets bestämmelse om ledningens ansvar bör inkluderas i cybersäkerhetslagen

Utredningen medför i sitt förslag en risk för otydlighet beträffande innebörden av begreppet ledningen, samt ledningens ansvar för det systematiska och riskbaserade

informationssäkerhetsarbetet. Detta med hänvisning till nuvarande reglering i dagsaktuell lagstiftning i Sverige, Aktiebolagslagen (2005:551). NIS2-direktivet understryker i artikel 20 §1 vikten av verksamhetsutövares ledningsorgans aktiva ålagda ansvar: *”…ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem…”*. Detta är nödvändigt att reglera i kommande svenskt införlivande av NIS2, med anledning av, att ovan citerade aktiviteter är av den karaktär som Aktiebolagslagen kap 8 §29 beskriver som *”löpande förvaltning”*, vilket därmed bör hamna på VD:s ansvar.

Givet att utredningen väljer att avstå tydligare reglering av verksamhetsutövares ledningsorgans ansvar, medför detta risk att förbigå NIS2-direktivets syfte samt tillföra risk för oklarheter för enskilda verksamhetsutövares implementering av detta ansvar, med hänsyn till nuvarande lagstadgad fördelning av ansvar enligt Aktiebolagslagen.

Styrelsens ansvar som framförs enligt Aktiebolagslagen behöver inte nödvändigtvis förtydligas med hänsyn till NIS2-direktivet, då styrelsen, genom sitt ordinarie styrelsearbete, bör följa upp VD:s ansvar för efterlevnad av NIS2-direktivet. Därmed avstyrker vi utredningens förslag att styrelsen och VD har ett delat ansvar.

Då utredningen löpande i sitt förslag konstaterar att NIS2-direktivet bedöms vara ett minimidirektiv, där enskilda medlemsstater kan välja att stärka krav på åtgärder, behöver kommande svensk lagstiftning reflektera NIS2-direktivet.

Förslag: Vi, i likhet med livsmedelsverket, föreslår att ledningens ansvar i cybersäkerhetslagen bör implementeras. Vi föreslår även att ansvaret bör förtydligas i enlighet med den ansvarsfördelning som framgår ur aktiebolagslagen.

Rapportering av Incidenter

I utredningen införs en skyldighet att lämna en varning för incidenter inom 24timmar. Vi ser positivt på, och tillstyrker utredningens förslag om 24 timmars tidsfrist i stället för 6 timmar som anges i dagens MSBFS 2018:9.

Enligt utredningens förslag ska verksamhetsutövare bland annat tillhandahålla, information som beskriver huruvida incidenten är gränsöverskridande och/eller uppsåtligt orsakad. Detta kräver att verksamhetsutövaren genomför en (säkerhets)analys av incidenten. Med hänsyn till komplexiteten av dessa analyser i praktiken, vilket kräver information från flera olika källor och en djup orsaksanalys förfaller sig en tidsfrist om *minst* 24 timmar som rimlig. I synnerhet med hänsyn att de flesta verksamheter använder sig av fler underleverantörer som tillhandahåller tjänster som ingår i den reglerade delen av verksamheten. Enligt vår praktiska erfarenhet är ett tidsintervall på 24 timmar redan kort för att avsluta analysen med tillräcklig kvalitet för att förebygga onödig eller även felaktig rapportering.

Förslag: Vi tillstyrker utredningens förslag om minst 24 timmars tidsfrist för den initiala rapporteringen vid rapporteringsskyldiga säkerhetsincidenter.

Definitionen av livsmedelsföretag

I förslaget till cybersäkerhetslag 4 § anges att lagen gäller för sådana verksamheter som omfattas av bilaga 1 eller 2 i NIS2-direktivet.

I NIS2-direktivet bilaga 2 punkt 4 anges avseende sektorn ”Produktion, bearbetning och tillverkning av livsmedel” att livsmedelsföretag enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 178/2002 *som bedriver grossisthandel och industriell produktion och bearbetning* ska omfattas.

Av ordalydelsen ska således endast sådana livsmedelsföretag som bedriver såväl grossisthandel som industriell produktion och bearbetning omfattas. Motsvarande tolkning stärks när vi läser NIS2-direktivets engelsk- och tysk-språkiga versioner.

Genom hänvisningen till denna bilaga i NIS2-direktivet framstår det som något oklart om ordalydelsen sammanfaller med utredningens avsikt, d v s att cybersäkerhetslagen endast ska omfatta sådana livsmedelsföretag som bedriver såväl grossisthandel som industriell produktion och bearbetning eller om dessa olika led ska anses vara alternativa, d v s att de livsmedelsföretag som bedriver grossisthandel *eller* industriell produktion och bearbetning (eller bådadera) omfattas. Det är naturligtvis en grundläggande förutsättning att en verksamhetsutövare vet om en viss lag gäller dem eller inte. Svensk Dagligvaruhandel önskar därför ett förtydligande i lagen rörande vilka livsmedelsföretag som ska omfattas av cybersäkerhetslagen. Att det är otydligt vilka verksamheter inom livsmedelssektorn som omfattas är också något som Livsmedelsverket lyfter i sitt remissvar.

Förslag: Utredningen behöver förtydliga i lagen vilka livsmedelsföretag som ska omfattas av cybersäkerhetslagen eftersom nuvarande skrivningar öppnar för tolkningar.

Den svenska regleringen ur ett internationellt perspektiv

Vi vill slutligen belysa att det finns en stor vinning av att hålla sig till den internationella standarden i den svenska lagstiftningen och inom de krav som senare kommer att ställas av de utpekade tillsynsmyndigheterna. Kraven bör i sin utformning och omfattning i möjligaste mån stämma överens med de krav som ställs i andra EU-länder. Det är för oss viktigt att både incidenter och revisioner hanteras på liknande sätt i Sverige som i övriga länder.

Incidentrapporteringen bör följa europeisk standard. Det bör också vara möjligt att rapportera en global incident som drabbar flera länder som en och samma incident.

Rapporteringen bör göras på samma sätt och med samma informationskrav i alla länder. Fördelen är ökad transparens inom EU samt minskad administration för företagen i varje enskilt land.

Kraven och framtida revisioner bör följa en och samma europeiska standard. Revisionerna bör vara väldefinierade, standardiserade och specificerade på förhand. Detta ger en minskad administration för de företag som är representerade i flera länder. Det möjliggör även att samma IT-säkerhetsramverk kan användas i alla länder där företaget är verksamt, vilket höjer kvaliteten och minskar kostnaden för företagen.

Bedömningen av vad som är en väsentlig eller viktig verksamhet samt vilka konsekvenser detta får bör också följa europeisk standard samt vara tydligt formulerad. Även om hela verksamheten omfattas, bör det ändå framgå vilka delar av verksamheten som är ändamål för revisioner och incidentrapportering. Detta borde också följa europeisk standard för att möjliggöra användningen av globala IT-säkerhetsramverk.

Vi ser positivt på att förslaget till största delen väljer att följa NIS2-direktivet. Vi noterar dock att det finns skillnader och rekommenderar att dessa hålls till ett minimum. Ett exempel återfinns i 3 kap 1§. Första punkten "strategier för riskanalys och informationssystemets säkerhet" saknas i det svenska förslaget. Sådana skillnader skulle kunna innebära olika tolkningar i Sverige jämfört med andra länder. Våra medlemsföretag verkar i och samarbetar med flera andra europeiska länder på olika sätt och våra leverantörer är ofta internationella aktörer. Att i möjligaste mån hålla sig till en enhetlig europeisk standard innebär därför minskade kostnader för administration, ökad transparens samt slutligen en högre kvalitet på säkerhetsarbetet.