Branschorganisationen
för dagligvaruhandeln

Ärendenummer: MSB 2025-13269
Inskickat: 2025-12-09
Ansvarig tjänsteman: Ulrika Dahlin

Från:
Svensk Dagligvaruhandel

Till:
MSB
registrator@msb.se

Remiss avseende myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning (MSB 2025-13269)

Svensk Dagligvaruhandel är branschorganisationen för dagligvaruhandeln i Sverige. Våra medlemsföretag är Axfood, Coop Sverige, ICA Sverige, Lidl Sverige och Livsmedelshandlarna. Tillsammans står vi för drygt 95 procent av dagligvaruhandeln i Sverige, med fler än 3 000 butiker över hela landet.

Varje vecka möter vi i stort sett alla människor i Sverige i våra butiker. Dagligvaruhandeln sysselsätter runt 110 000 personer, varav en tredjedel är unga (15-24 år) och en fjärdedel har utländsk bakgrund. Branschen skapar jobb, ger möjlighet att äta hållbart och hälsosamt och är en viktig samhällsfunktion i alla delar av Sverige.

Svensk Dagligvaruhandels remissvar

Svensk Dagligvaruhandel har tagit del av *förslaget till myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning* och tackar för möjligheten att inkomma med synpunkter.

Synpunkter på enskilda paragrafer och stycken bifogas i MSB 2025-13269 svarsmall men vi menar att denna remiss även kräver en övergripande kommentar från Svensk Dagligvaruhandel.

Företagen inom dagligvaruhandeln arbetar i dagsläget redan systematiskt och riskbaserat framgångsrikt med en fungerande dagligvaruhandel trots en utmanade

cybersäkerhetsmiljö där våra medlemmar är under daglig attack. Det är i denna kontext som den föreslagna föreskriften mottages och responderas på.

Vi står i första försvarsled i ett brinnande (cyber)krig där angreppen haglar och våra myndigheter vill genom de nu föreslagna föreskrifterna att vi ska fokusera på att så detaljerat som möjligt dokumentera hur vi byggt våra skyttegravar och försvarslinjer istället för att analysera, förutspå och agera för att skydda oss och Sverige mot de kontinuerligt pågående angreppen.

I grunduppdraget till införandet av NIS2-direktivet i Sverige låg kravet från regeringen att direktivet inte skulle överimplementeras i Sverige. Utredningen som sedan skedde hade dessvärre element av detta men efter remissrundan så är nuvarande lagförslag betydligt mer i linje med det direktivet. Med föreslagen föreskrift och allmänna råd för säkerhetsåtgärder och utbildning ser vi återigen en kraftig överimplementering av tillämpningen av den kommande Cybersäkerhetslagen vilket innebär att vi ser en stor risk för en ökad administration i företagen utan en ökad säkerhetsnivå.

Redan idag ligger den administrativa bördan för företagens cybersäkerhetsavdelningar på ca 40% och vi genom deltagande i IVAs projekt om Resilient Digital Infrastruktur därför redan föreslagit en rad regelförenklingar för att minska denna börda och i stället öka förmågan till faktisk resiliens.

Svensk Dagligvaruhandel menar att NIS2-direktivet och den föreslagna Cybersäkerhetslagen inte syftar till en generell implementering av informationssäkerhet utan riktar sig särskilt mot tillgänglighet och kontinuitet i leveransen av digitala samhällsviktiga tjänster. Vi menar därmed att de föreslagna föreskrifter och allmänna råden går för långt och som de nu är formulerade omfamnar ett större uppdrag än lagen de ska vara föreskrifter för.

Svensk Dagligvaruhandel upplever föreskrifterna som framtagna för en offentlig verksamhets totala behov av informationssäkerhetsarbete och inte bara med utgångpunkt i NIS2-direktivet. Vår rekommendation är därför att lyfta bort detaljerade krav för offentlig verksamhet, dessa skulle i stället kunna ligga i vägledningar för dessa verksamheter inom till exempel SKR.

Svensk Dagligvaruhandel menar vidare att föreskrifterna inte är genomförbara i sin nuvarande form för en stor privat verksamhet, de är alldeles för detaljerade och statiska. Vi menar i stället att föreskrifterna måste vara effektmål som bygger på ett riskbaserat arbetssätt. Därtill är det anmärkningsvärt att föreskriften inledningsvis rekommenderar användandet av standarder men sedan inte utgår från dessa. Svensk Dagligvaruhandel önskar att föreskrifterna hade hänvisat till standarderna och sedan beskrivit vilka effektmål företagen ska arbeta mot för att

uppnå kraven i Cybersäkerhetslagen och lämna hur:et till företagen själva. Jämför exempelvis med kommissionens genomförandeförordning (EU) 2024/2690 som gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet som gäller för bland annat leverantörer av molntjänster, datacentraltjänster, leverantörer för utlokaliserade driftstjänster och tillhandahållare av betrodda tjänster. I dessa föreskrivs att

> *berörda entiteterna ska för nätverks- och informationssystem säkerställa en säkerhetsnivå som är lämplig för de risker som finns när de genomför och tillämpar de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning. De ska därför ta vederbörlig hänsyn till sin riskexponeringsgrad, sin storlek, sannolikheten för att incidenter ska inträffa och incidenternas allvarlighetsgrad, inklusive de samhälleliga och ekonomiska konsekvenserna, när de uppfyller de tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet som fastställs i bilagan till denna förordning.*
> *Om bilagan till denna förordning föreskriver att en teknisk eller metodologisk specifikation för en riskhanteringsåtgärd för cybersäkerhet ska tillämpas ”när så är lämpligt”, ”om tillämpligt” eller ”i den mån det är genomförbart”, och om en berörd entitet inte anser att det är lämpligt, tillämpligt eller genomförbart för den berörda entiteten att tillämpa vissa tekniska och metodologiska specifikationer, ska den berörda entiteten på ett begripligt sätt dokumentera sina skäl.*

Vi menar också att den svenska implementeringen måste harmoniseras med övriga europeiska länder, dels då flera företag har verksamhet i flera EU-länder men kanske framför allt för att upprätthålla den svenska konkurrenskraften på en europeisk marknad. Vi ställer oss därför också bakom remissvaret från Lantmännen som närmare exemplifierar denna utmaning.

Övergripande synpunkter på föreskrifterna

- <u>Föreskriftens detaljeringsgrad går långt utöver etablerad internationell praxis</u>
    - Den föreslagna föreskriften och konsekvensutredningen innehåller ett stort antal tvingande, detaljerade och teknikspecifika krav som avviker från internationella standarder som NIST CSF och ISO 27001 vilka medvetet är teknikneutrala och riskbaserade.
- <u>Detaljstyrning riskerar att hämma säkerhetsinnovation och effektivitet</u>
    - Hög detaljnivå i regleringen riskerar att:
        - binda verksamheter till specifika arbetssätt, arkitekturer och säkerhetsmodeller
        - minska förutsättningarna att använda moderna teknologier (t.ex. Zero Trust, molnbaserade arkitekturer, automatiserad säkerhet)
        - skapa onödiga kostnadsdrivande åtaganden
- <u>Betydande risk för överreglering och administrativa bördor</u>
    - Krav på dokumentation, löpande övningar, utbildningsinsatser, tekniska förteckningar och segmenteringsnivåer innebär en administrativ börda som inte står i proportion till riskerna i alla sektorer.

- Otydlig gränsdragning mellan föreskriftskrav och allmänna råd
    - De allmänna råden innehåller formuleringar som riskerar att tolkas som bindande, vilket skapar osäkerhet i tillämpning.
- Föreskrifterna tillämpar en omfattande kravbild utan att möjliggöra lämplighet och proportionalitet.
    - NIST CSF och ISO 27001 bygger på nivåanpassning efter risk och verksamhetsförutsättningar. Flera krav i föreskrifterna saknar möjligheter till riskbaserade undantag.

Utöver dessa övergripande synpunkter lämnar Svensk Dagligvaruhandel nedan några mer detaljerade synpunkter per område (dessa återfinns även angiven excell-mall). Notera att vi här har valt ut några av de för oss viktigaste inspelen och inte är att betrakta som ett komplett och uttömmande svar på alla delar av föreslagen föreskrift.

Detaljerade synpunkter:

1. Interna regler och arbetsprocesser (2 kap. 3–5 §§)

Problem:

Föreskrifterna kräver att interna regler ska dokumentera *vad, när, hur, av vem,* och att alla sådana dokument ska bevaras i minst fem år.

Konsekvens:

- Kraftigt ökade administrativa krav
- Risk för fokus på att producera dokumentation i stället för faktisk säkerhet
- Avvikelse från internationell standard, som inte specificerar processformat eller omfattning

Rekommendation:

Inför möjlighet till *lämplighet och proportionalitet* och skriv att dokumentation och processer ska vara ”ändamålsenlig utifrån risk och verksamhetens förutsättningar”.

2. Ledningens utbildningskrav (2 kap. 9 § samt konsekvensutredningens tidsåtgångsidéer)

Problem:

Kravet på specificerat innehåll och obligatoriska utbildningsmoment för ledningsgruppen är mer detaljerat än både NIS2 och internationella standarder kräver.

Konsekvens:

- Höga kostnader och tidsåtgång
- Risk att utbildningens form går före faktisk effekt
- Inget utrymme för att anpassa utbildningen till organisationens egna bedömda behov

Rekommendation:

Formulera kravet som: ”Ledningen ska säkerställa och genomföra adekvat utbildning om cybersäkerhet anpassad efter verksamhetens behov.”

3. Omvärldsbevakning och krav på obligatoriska källor (2 kap. 12 §)
Problem:
Föreskrifterna kräver att verksamhetsutövaren ska bevaka ett antal specifika myndigheter och system, samt obligatoriskt ansluta sig till ANTS.
Konsekvens:

- Avvikelse från internationella standarders riskbaserade arbetssätt
- Ökad börda utan tydlig koppling till risk
- Risk att information överlastas eller inte är relevant för vissa sektorer

Rekommendation:
Ersätt ”ska minst bevaka” med ”ska bedöma behovet av att bevaka”.

4. Informationsklassning och riskhantering – överdetaljerade krav (2 kap. 13–16 §§)
Problem:
Krav på årlig uppföljning av klassning och riskanalyser, samt krav på hantering av aggregerade risker och ackumulerad information.
Konsekvens:

- Går långt utöver internationella standarder som inte specificerar metod, nivåer eller frekvenser
- Mycket resurskrävande för verksamheter med stora mängder information*
- Informationsklassificering är inte en meningsfull utgångspunkt för riskbedömning av OT

Rekommendation:
Tillåt att uppdatering sker ”vid behov baserat på förändringar i riskbild, verksamhet eller teknik”.

5. Kontinuitetskrav (2 kap. 18–20§§)
Problem:
Kravet på att verksamheten ska kunna bedrivas trots otillgänglig systemmiljö är inte alltid genomförbart i tex helautomatiserade logistikcenter.
Konsekvens:

- Medför risk för att verksamheter med helautomation per automatik kommer att bryta mot föreskrifterna.
- Samma utmaningar gäller för produktionssystem, finansiella tjänster, elektroniska kommunikationer

Rekommendation:
Gå på regeringens rekommendation att ”verksamheterna ska planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar.”

6. Tekniska och nätverksmässiga krav – arkitekturstyrning (3 kap. 11–14 och 15–21 §§)
Problem:
Krav på omfattande segmentering, separata kataloger, placeringskrav för system, och filtreringskrav mellan segment.

Konsekvens:

- Regleringen specificerar arkitektur snarare än mål
- Kan försvåra modern teknik såsom mikrotjänster, moln och Zero Trust

Rekommendation:
Fokusera på *resultatkrav* (t.ex. ”begränsa lateral rörelse”) i stället för *designkrav*.

7. Krav på robust och spårbar tid kopplad till en specifik nationell källa (3 kap. 28 §)
Problem:
Kravet på tid synkroniserad till SP-tid är unikt internationellt.
Konsekvens:

- Kan vara svårt att implementera i molntjänster
- Avviker från internationell praxis där NTP-synkronisering räcker

Rekommendation:
Tillåt ”robust och spårbar tid mot betrodd källa”, utan nationell bindning.

8. Fysiska skydd – krav på byggnader, IT-utrymmen och redundans (4 kap. 1–7 §§)
Problem:
Föreskrifterna innehåller bindande krav på skalskydd, zonindelning, särskilda IT-utrymmen, klimatkrav och redundans.
Konsekvens:

- Betydande investeringskrav, särskilt för små och medelstora aktörer
- Går långt utöver internationella standarders principiella krav på fysiska skydd
- Fysisk separation i olika zoner är inte alltid genomförbart i produktionsanläggningar

Rekommendation:
Verksamheten ska utifrån det bedömda behovet vidta lämpliga och proportionella säkerhetsåtgärder.

**Ett exempel på detta:*
I en verksamhet med 800 system och ett genomsnitt på 1,25 unika risker per system innebär detta 1000 risker (givet ett allriskperspektiv). Varje risk renderar i ca 100 kontroller (i enlighet med ISO 27000). Dessa kontroller ska sedermera utvärderas var tredje månad, varje sådan utvärdering uppskattas ta ca 20 minuter. Det innebär att 800 system med 1000 risker med 100 kontroller för varje risk som utvärderas 20 min fyra gånger om året renderar i 135 000 timmar om året per verksamhet.

Konsekvensbedömningen av föreskriften i sin nuvarande form

NIS2-direktivet pekar på att incitamenten att bedriva ett cybersäkerhetsarbete behöver stärkas generellt och att det ska göras genom dels införandet av finansiella sanktioner som påföljd, dels genom en höjning av kunskapsnivån vilket inkluderar nationell utbildning, kompetenshöjningskrav och forskningssatsningar, ex den i Sverige utpekade cybersäkerhetsstrategin. Svensk Dagligvaruhandel

menar därför också att det föreslagna motivet i konsekvensanalysen från MSB kan ifrågasättas.

Konsekvensbeskrivningen överensstämmer inte heller med Svensk Dagligvaruhandels uppfattning av kostnadsbilden. Kvarstår föreslagna föreskrifter i sin nuvarande form kommer detta signifikant påverka slutpriserna till konsument, något vi inte kan ställa oss bakom.
År 2023 publicerade Svensk Dagligvaruhandel en rapport kallad Butikshundringen och som syftade till att granska hur en hundralapp som konsumenten spenderar i en livsmedelsbutik fördelas över butikens kostnader. Den rapporten visar på att av 100 kronor går 5,08 kronor till säkerhet och svinn. Med föreslagen föreskrift kommer de administrativa kraven att innebära en signifikant ökning av denna kostnad. Vi hänvisar även här till Lantmännens remissvar som närmare exemplifierar detta.

Avslutande sammanfattning

Svensk Dagligvaruhandel menar således att föreslagen föreskrift och konsekvensbedömning innehåller krav som:

- går längre än NIS2-direktivets ambitionsnivå
- är mer detaljerade än internationell standard (NIST CSF och ISO 27001) och EU-kommissionens genomförandeförordning som gäller andra sektorer
- riskerar att skapa kostnadsdrivande åtagande och bli en administrativ börda
- kan minska flexibiliteten och effektiviteten i cybersäkerhetsarbetet

→ NIS2 pekar på att det är incitamenten som behövs stärkas men de detaljerande föreskrifter riskerar att bli demotiverande och hämmande och minska företagens incitament till att kontinuerligt vidareutveckla sitt cybersäkerhetsarbete.

Vi rekommenderar att MSB justerar föreskrifterna så att de:

1. blir **riskbaserade**
2. blir **teknikneutrala**
3. fokuserar på **resultat** snarare än *hur* åtgärder ska implementeras
4. förtydligar vad som är *obligatoriskt* och vad som är *god praxis*
5. minskar krav som saknar tydligt samband med riskreducering

Vi **avstyrker** således föreslagna föreskrifter och tillhörande konsekvensanalys i sin nuvarande form.