SVENSKT NÄRINGSLIV

Myndigheten för civilt försvar
registrator@mcf.se

Vår referens/dnr:
2026–83

Er referens/dnr:
MCF 2026–04554

2026-05-15

Remissvar

Förslag till Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

Svenskt Näringsliv yttrade sig i december 2025 över förslag till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt cybersäkerhetslagen. Med anledning av att Myndigheten för civilt försvar nu remitterat ett reviderat förslag lämnas härmed uppföljande synpunkter.

Svenskt Näringsliv anser att EU, regeringen och ansvariga myndigheter behöver underlätta regelefterlevnaden och effektivisera den komplexa uppsättningen cybersäkerhetsregler som antagits på senare år. Reglerna som styr cybersäkerhet behöver vara så effektiva som möjligt och proportionerligt begränsa den kostsamma regulatoriska bördan.

Det reviderade förslaget innebär flera förbättringar jämfört med den tidigare remitterade versionen. Det kvarstår dock behov av ytterligare ändringar för att föreskriften fullt ut ska vara förenlig med cybersäkerhetslagens riskbaserade och proportionella utgångspunkter samt vara praktiskt tillämpbar för verksamhetsutövare.

Det är positivt att betydande delar av det som tidigare var detaljstyrning i föreskriften har flyttats till allmänna råd. Det stärker förutsättningarna för ett riskbaserat cybersäkerhetsarbete i överensstämmelse med cybersäkerhetslagen. Samtidigt innehåller det reviderade förslaget alltjämt bestämmelser som är alltför långtgående eller otillräckligt anpassade till verksamhetsutövarnas skilda förutsättningar, inte minst beroende på om verksamheten är viktig eller väsentlig enligt cybersäkerhetslagen.

Ledningens ansvar

När det gäller ledningens ansvar och utbildning innebär det reviderade förslaget en tydlig förbättring. Svenskt Näringsliv välkomnar särskilt att MCF har tagit bort detaljerade och

obligatoriska krav som i praktiken tilldelade ledningen operativa uppgifter på ett sätt som inte är förenligt med en ändamålsenlig ansvarsfördelning.

Första stycket **i 3 kapitlet 4 §** bör dock ändras enligt följande eftersom det är oklart vad som avses med ledningens godkännande och övervakning av genomförandet.

”För att verksamhetsutövaren ska kunna vidta lämpliga och proportionella säkerhetsåtgärder ska ledningen ~~**godkänna och övervaka genomförandet av säkerhetsåtgärder genom att**~~ säkerställa att /…/”

I 3 kap. 4 § punkt 5 anges att ledningen vid behov, men minst en gång per år, ska informeras om genomförandet av säkerhetsåtgärder och verksamhetsutövarens cybersäkerhetsnivå. Ett sådant minimikrav framstår som onödigt styrande. Behovet av rapportering bör bedömas utifrån verksamhetens riskbild, organisation och faktiska förutsättningar. Ett föreskrivet krav på årlig rapportering riskerar att leda till formaliserad dokumentation utan motsvarande säkerhetsnytta. Bestämmelsen bör därför utformas så att ledningen bör informeras regelbundet samt vid behov.

Ersätt ”~~minst en gång per år~~” med ”**vid behov och av ledningen fastställda intervall**”.

Riskhantering

Föreskriften innehåller fortfarande detaljerade krav på arbetssätt, metoder och tekniska lösningar. Det begränsar verksamhetsutövarens handlingsutrymme att välja de åtgärder som, utifrån verksamhetens förutsättningar, behov och risker, är mest effektiva för att uppnå en faktisk säkerhetshöjning. Föreskrifterna bör i högre grad ange vilket resultat som ska uppnås och lämna åt verksamhetsutövaren att avgöra hur detta bäst sker.

En särskilt allvarlig brist gäller omfattningen av den sårbarhetshantering som förutsätts enligt förslaget. Det är inte proportionerligt att ställa krav som i praktiken omfattar varje sårbarhet i varje system, oavsett systemets betydelse eller kritikalitet. Under 2025 publicerades 48 148 sårbarheter. Om verksamhetsutövare förutsätts bedöma, dokumentera och motivera relevansen av varje enskild sårbarhet för varje enskilt system medför det en ohanterlig administrativ belastning som riskerar att tränga undan faktiska säkerhetshöjande åtgärder. Föreskrifterna bör därför utformas så att verksamhetsutövare ges ett tydligt utrymme att prioritera bort sårbarheter som saknar relevans för den egna verksamheten och i stället fokusera på de åtgärder som ger störst säkerhetsnytta.

Svenskt Näringsliv anser exempelvis att 3 kap 12 § bör ändras:

”För att kunna identifiera vilka lämpliga och proportionella säkerhetsåtgärder som ska genomföras i den digitala miljön ska verksamhetsutövaren identifiera, analysera och värdera risker utifrån deras konsekvens och sannolikhet. Verksamhetsutövaren ska utforma nivåer och tillhörande kriterier för bedömning av konsekvenser och sannolikhet så att risker kan jämföras över tid. Risker ska värderas för
1. all informationsbehandling i system,
2. enskilda **sektorskritiska** system ~~**och segment i produktionsmiljön,**~~ samt
3. den digitala miljön i sin helhet.
/…/”

Tekniska och driftrelaterade säkerhetsåtgärder

Svenskt Vardagligvaruhandel har identifierat ytterligare fyra mycket problematiska paragrafer och framför i sitt remissvar detaljerade förslag och motiv för ändringar i 4 kap 1, 10, 19 och 31 §§.

SVENSKT NÄRINGSLIV

Carolina Brånby

Maria Althin