Brev till Mikael Frisell, generaldirektören för Myndigheten för civilt försvar gällande införandet av NIS 2-direktivet

Vi välkomnar Myndigheten för civilt försvarsarbete med att stärka den digitala motståndskraften genom sin roll som central aktör i Sveriges införande av NIS 2-direktivet och den nya cybersäkerhetslagen. Samtidigt vill vi framföra vår starka oro kring utformningen av de föreskrifter som ni föreslår. Vi ser en stor risk att Sverige överimplementerar ett EU-direktiv på ett sätt som leder till höga kostnader för företag och minskad konkurrenskraft – utan att den faktiska operativa cybersäkerheten stärks.

De föreslagna föreskrifterna fokuserar i stor utsträckning på detaljreglering av metoder och tekniska lösningar, snarare än att ange tydliga säkerhetsmål. Detta begränsar verksamhetsutövarnas möjlighet att själva välja de mest effektiva åtgärderna utifrån sin riskprofil och förvandlar säkerhetsarbetet till en checklista, snarare än ett systematiskt riskarbete.

Cybersäkerhetslagen anger att åtgärder ska vara proportionella och lämpliga i förhållande till risk, men de föreslagna föreskrifterna gör det svårt att leva upp till denna princip då flertalet av säkerhetsåtgärderna ska tillämpas oavsett systemens riskprofil och potentiella inverkan på sektors primära leveransförmåga. Detta kan exemplifieras med kravet på årlig uppföljning av alla informationsklassningar, även för perifera system, vilket innebär att företag med många informationsmängder och IT-system tvingas lägga stora resurser på administration istället för att fokusera på att skydda de mest kritiska systemen.

Föreskriften kräver noggrann och omfattande dokumentation som i flera fall saknar praktiskt värde för verksamhetsutövaren. Vidare krävs mycket långa lagringstider för alla cybersäkerhetsrelaterade dokument, inklusive arbetsinstruktioner. I dagens värld är allt väldigt dynamiskt och systemens livscykler förkortas på grund av detta. Kravet att spara varje version av allting i fem år är överväldigande och förbättrar inte säkerheten, det ökar endast byråkratin ytterligare.

Flera krav framstår även som godtyckliga och kostnadsdrivande, såsom ovannämnd dokumenthantering och bevarande av interna regler i fem år, omvärldsbevakning av sju myndigheter, och krav på dataursprung för samtliga system. Detta är exempel på krav som riskerar att skapa betydande kostnader och administrativ börda utan att reducera risken för incidenter. Myndighetens egen konsekvensanalys visar att kostnaderna blir

omfattande och gäller enbart för att uppfylla föreskrifterna, inte för ytterligare riskreducerande insatser.

Om Myndighet för civilt försvar väljer att detaljreglera på detta sätt, medan våra nordiska och baltiska grannar väljer en mer övergripande och riskbaserad ansats, riskerar vi att hamna på efterkälken. Det vore olyckligt - både för det svenska näringslivet och Sveriges förmåga att bygga robusta säkerhetslösningar i samarbete med grannländerna.

Tidsramen för att omhänderta de synpunkter som nu inkommit och genomföra de stora förändringar i föreskriften vi anser nödvändiga är mycket kort. Det måste vara tydligt att förutsättningar finns så att det slutliga resultatet i praktiken stärker hela Sveriges säkerhet och resiliens. Vidare saknas helt konsekvensbedömningen av implementeringskostnaderna för näringslivet, viket ger en falsk bild av vad de förslagna förskrifterna leder till, och dess konkurrenshämmade effekt.

Vi ser gärna att Myndigheten för civilt försvar:

- Utformar föreskrifterna på en övergripande nivå med tydliga säkerhetsmål.
- Ger verksamhetsutövare flexibilitet och anpassa säkerhetsåtgärder utifrån riskprofil (organisatorisk som tekniska förutsättningar).
- Säkerställer proportionalitet och lämplighet i linje med lagens intentioner genom att säkerhetsåtgärder väljs, anpassas och tillämpas utifrån riskprofil.
- Säkerställer myndighetsrekommendationer i allmänna råd och vägledning.
- Harmoniserar implementeringen med våra nordiska och baltiska grannländer.

Vi, representanter från energisektorn, tar gärna en dialog om hur vi kan höja den digitala motståndskraften och stärka Sverige framåt. Om vi gör rätt, bygger vi en robust och konkurrenskraftig digital infrastruktur. Om vi gör fel, riskerar vi att försvaga både säkerheten och det svenska näringslivets konkurrenskraft.

Med vänliga hälsningar,

Jessica Alenius, VD Drivkraft Sverige

Åsa Pettersson, VD Energiföretagen Sverige