företagarna

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
Visnja Raguz

Stockholm	Vår referens	Dnr
2024-05-28	Tobias Adielsson	Fö2024/00496

Remissyttrande av betänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Företagarna har beretts möjlighet att lämna synpunkter på det rubricerade betänkandet och önskar framhålla följande.

Sammanfattning
Den 14 december 2022 antog EU NIS2-direktivet och CER-direktivet. Denna remiss behandlar införlivandet av NIS2-direktivet, som ersätter det tidigare NIS-direktivet från 2016. Det föreslås att en ny cybersäkerhetslag införs, vilket innebär utökade krav på säkerhet i nätverks- och informationssystem och omfattar fler sektorer, från sju till 18, inklusive energi, transporter, bankverksamhet, och digital infrastruktur.

Alla företag och offentliga verksamheter inom dessa sektorer, med undantag för små företag (mindre än 50 anställda eller 10 miljoner euro i årsomsättning), måste följa de nya säkerhetskraven. Företagen måste anmäla sig till en tillsynsmyndighet och vidta åtgärder för att skydda sina system. Tillsynen sköts av sektorspecifika myndigheter, med MSB som samordnare. Brott mot lagen kan leda till sanktionsavgifter och andra åtgärder.

Förslaget medför ekonomiska konsekvenser för både tillsynsmyndigheter och verksamhetsutövare. Tillsynsmyndigheterna får ökade anslag, medan offentliga verksamheter föreslås finansiera sina kostnader inom befintliga ramar. Den nya lagen ska träda i kraft den 1 januari 2025.

Ställningstaganden

Företagarna ser positivt på att cybersäkerhetsfrågan prioriteras för att skapa ökad säkerhet och större motståndskraft mot cyberhot. Riktlinjerna behöver vara tydliga för att den administrativa bördan av anmälningsskyldighet och riskhanteringsåtgärder inte oskäligt ökar kostnaderna för företag, utan i stället ger större fördelar genom att företaget effektivare kan hantera cyberhot som skulle medföra stora kostnader och skador. Därför hade vi sett vikten av en mer gedigen konsekvensanalys för att förstå vad kostnaderna för företagen förväntas bli.

Utredningen anför att sanktionsavgift ska kunna användas, men att det dock medför ett krav på att det ska vara enkelt för verksamhetsutövaren att förstå hur den ska agera för att undvika att drabbas av sanktionen. En generell kritik mot myndighetsutövning är att företag som vill göra rätt ändå drabbats av sanktioner. Företagarna ser därför att det är av stor vikt att ambitionen om enkelhet som beskrivs också följs.

Företagarna är tveksamma till förslaget att hela verksamheten ska omfattas av cybersäkerhetslagen, då det kan leda till ineffektiv tillsyn. Vi föreslår att lagen endast ska gälla de delar som påverkar säkerheten i relevanta tjänster.

Den återstående tidsramen för att implementera NIS2- och CER-direktiven är mycket kort. Därför är det en utmaning för företagen att införa de nödvändiga processer, strukturer och arbetssätt som krävs för att säkerställa regelefterlevnad. Myndigheterna behöver vara tydliga med vilka åtgärder som krävs för att detta ska kunna genomföras inom tidsramen.

Vi ser det som positivt att ökad administrativ börda inte läggs på småföretag. Det är likaså viktigt att de också får hjälp i sitt säkerhetsarbete, genom tydlig och lättillgängliga riktlinjer för hur små företag bör agera för att undvika att de blir sårbara för cyberattacker. I Företagarnas rapport *Är det it-säkert?* 2022 framgick att 59 procent helt eller till stor del höll med om att informations- och kunskapsutbytet mellan företag och myndigheter när det gäller it-säkerhet bör förbättras. Var tredje företagare svarade *Vet ej* på frågan om huruvida de upplever att det finns god tillgång till stöd, verktyg och/eller information från myndigheter när det gäller it-säkerhetsfrågor.

Tobias Adielsson
Näringspolitisk expert
Företagarna

Pernilla Norlin
Samhällspolitisk chef
Företagarna