Datum
2025-01-13

Er referens
Fö2024/01550
Vår referens
FS

TechSverige

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

kopia till
alfred.pucek@regeringskansliet.se

Remissvar avseende betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

TechSverige har beretts tillfälle att lämna ett remissvar avseende rubricerat betänkande (dnr Fö2024/01550).

TechSverige är en bransch- och arbetsgivarorganisation för företag inom techsektorn med cirka 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i Svenskt Näringsliv.

Techsektorn är avgörande för Sverige säkerhet och motståndskraft

Bland TechSveriges medlemmar finns telekomoperatörer, it-tjänsteleverantörer, datacenteroperatörer, informations- och cybersäkerhetsföretag, mjukvaruutvecklare, leverantörer av viktiga tjänster som identifiering och många andra slags företag som spelar en stor roll för samhällets funktion i alla lägen från fredstid, dagens hybridhot, kriser, vid höjd beredskap och i krig. TechSveriges medlemmar har kunder i både i privat och offentlig sektor, liksom i en rad andra beredskapssektorer än elektronisk kommunikation och post. Både

Nato och Försvarsmakten har pekat ut verksamheter som TechSveriges medlemmar bedriver som avgörande för det militära försvaret och civilt försvar. Techbranschen är avgörande både för svensk konkurrenskraft och svenskt totalförsvar.

Nedan lämnar Sverige synpunkter på valda delar av betänkandet.

Lagens omfattning

I betänkandet beskrivs av de problem som föreligger avseende otydliga definitioner av begreppen samhällsviktig tjänst och samhällsviktig verksamhet. TechSverige delar utredningens bedömning att det finns ett stort värde i att se över direktivens koppling till det svenska beredskapssystemet, samt möjligheten till att ensa såväl begrepp och sektorer som träffas av olika regelverk.

Det finns i dag flera olika definitioner av olika samhällsviktiga och samhällskritiska verksamheter och därmed ett tydligt behov av att förenkla och samordna begrepp, avgränsningar och prioriteringar av verksamheter. Konsekvensen av dessa otydligheter och bristfälliga analys är att verksamheter som t.ex. skulle kunna nedprioriteras finns kvar och att i stället nya läggs till som en försiktighetsåtgärd.

Ansvarsfördelning mellan statliga myndigheter

TechSverige anser att det är positivt att områden kring digitalisering och telekommunikation samlas under Post- och telestyrelsen. Det vore dock önskvärt om

regeringen vidhöll och att betänkandet också belyste behovet av den ansvarsfördelning som gjordes i det första delbetänkandet.

Regeringen (främst genom Försvarsdepartement) har bedrivit ett parallellt arbete som berör ansvarsfördelning i NIS2- och CER-frågor och närliggande områden. Det gäller bl.a. vilket uppdrag FRA och MSB ska ha och frågor kopplade till NCSC:s verksamhet. TechSverige utvecklade sin syn på detta i remissvaret på delbetänkandet Nya regler om cybersäkerhet samt i remissvaret om NCSC:

https://techsverige.se/app/uploads/2024/05/2024-05-28-Remissvar-Nya-regler-om-cybersakerhet-slut.pdf

https://www.regeringen.se/contentassets/00774d9efdb34c1ca391a95bd07b2a60/techsverige.pdf

Undantag och annan lagstiftning

TechSverige anser att det finns en risk att den sammantagna lagstiftningen blir svårtillämplig. Förtydligande bör tas fram i det fortsatta arbetet.

Många företag inom techsektorn- undantas från vissa delar av CER-direktivet och lagen om motståndskraft skulle inte tillämpas på dem, även om företagen har identifierats som väsentliga verksamhetsutövare. Lagen gäller inte om motsvarande krav regleras i annan lagstiftning, inklusive cybersäkerhetslagen. Dessutom undantas säkerhetskänslig verksamhet, vilket är positivt. Dock kan den sammantagna bilden och konsekvenserna av undantagen i både cybersäkerhetslagen och motståndskraftslagen bli komplexa och svårtillämpliga. Detta då säkerhetsskyddslagen är otydlig och svårtolkad när det kommer till de säkerhetsåtgärder och riskhanteringskrav som ställs på verksamhetsutövare.

Vidare finns det betydande överlappningar mellan denna och andra regleringar som NIS2 och DORA. CER täcker "kritiska verksamhetsutövare/entiteter" och NIS2 täcker "väsentliga eller viktiga enheter". Det finns sannolikt betydande överlappning mellan de två kategorierna samt mellan vad som omfattas av förordningarna (behöriga myndigheter, incidentrapportering, riskhantering etc.). Mot denna bakgrund vore det önskvärt med antingen (1) undantag om företaget omfattas av NIS2 gäller inte CER eller uppfylls genom företagets NIS2-efterlevnad eller (2) harmonisering av skyldigheterna så att de inte är duplicerade. Detsamma gäller DORA, som täcker finansiella institut och it-leverantörer (som t.ex. molnleverantörer).

Det finns också vissa sektorspecifika problem med risk för överlappande regleringar eller krav. Exempel på möjliga överlappningar är CER och NIS2 där finanssektorn sannolikt täckts på samma sätt via CER och den digitala infrastrukturen sannolikt täckts på liknande sätt via NIS2. Det kan också finnas risk för dubbelarbete eller oförutsägbarhet inom sektorerna om de ska följa mycket liknande riktlinjer under två olika regelverk.

Enligt 4 kap §1 i den föreslagna lagstiftningen ska enheter göra en riskbedömning, men det är inte klart om bedömningen ska fokusera på konsekvenser för själva enheten eller för samhället. TechSverige föreslår att detta förtydligas.

TechSverige är i övrigt positivt inställda till att sektorn digital infrastruktur undantas från bestämmelserna i motståndskraftslagen om anmälan, riskhantering och incidentrapportering eftersom dessa skyldigheter finns i cybersäkerhetslagen vilket annars skulle innebära dubbelarbete och en onödig administrativ börda.

TechSverige anser att det kan behöva tydliggöras i föreskrifter vilka specifika delar som är reglerade i cybersäkerhetslagen, och därmed undantaget i lagen om motståndskraft i samhällsviktiga tjänster. Detta kan särskilt vara viktigt för mindre aktörer som inte har stora resurser för dessa legala bedömningar.

Utredningen föreslår under kapitel 5.3.3 att regeringen ger tillsynsmyndigheterna i uppdrag att utreda vilka kategorier av verksamhetsutövare inom respektive tillsynsområde som omfattas av annan lag eller andra bindande unionsrättsakter som innehåller bestämmelser med motsvarande verkan. I detta uppdrag skulle även kunna rymmas klargöranden om vilka specifika skyldigheter som har företräde i cybersäkerhetslagen.

Sanktioner

TechSverige avstyrker förslaget om höjda sanktionsavgifter.

Näringslivsorganisationer och enskilda företag har tidigare kritiserat införandet av sanktioner och deras nivå i säkerhetsskyddslagen. Kritiken har bland annat riktats mot att införa sanktioner inom ett nytt område med otydliga regler. Det är svårt för en enskild verksamhetsutövare att bedöma vad som utgör fara för Sveriges säkerhet. Att nu höja sanktionerna är omotiverat med tanke på den utveckling av säkerhetsskyddslagen som sker i praxis.

Vid införandet av sanktioner 2019 hade utredningen föreslagit 10 mnkr som högsta nivå, något som regeringen justerade till 50 mnkr. Det saknas skäl att höja nivån ytterligare. Det finns inga indikationer på att nuvarande nivåer inte har tillräckligt avskräckande effekt för verksamhetsutövarna. Tvärtom kan mycket höga sanktioner motverka syftet med säkerhetsskyddslagen, något som bl.a. Försvarsmakten förde fram vid remitteringen av förslaget.

Att bedöma vad som utgör fara för rikets säkerhet är inte lätt för verksamhetsutövare. Kraven som ställs på säkerhetsskyddsåtgärder är komplexa. På senare tid har brister i säkerhetsskyddet bl.a. påtalats hos Stockholms tingsrätt och hos Säkerhets- och integritetsskyddsnämnden (SIN), vilket visar att även organisationer och myndigheter med hög juridisk kompetens har haft svårt att tolka och tillämpa regelverket.

I stället för fokus på höga sanktionsavgifter bör regeringen satsa på bättre vägledning och rådgivning till verksamhetsutövarna. Det har framkommit att de myndigheter som utövar tillsyn på området för säkerhetsskydd ser en motsättning mellan deras tillsynsroll och rådgivande roll, vilket gör att de drar sig för vägledande dialoger med verksamhetsutövare som ligger under deras tillsyn. Detta gynnar inte Sveriges säkerhet och regeringen bör göra det tydligt för tillsynsmyndigheterna att den rådgivande verksamheten inte får stå tillbaka p.g.a. att myndigheten även har ett tillsynsansvar.

Med ett så komplext och svårtolkat regelverk och brist på konkret vägledning till verksamhetsutövare, är höjda sanktioner olämpliga och inte rätt väg att gå för att stärka Sveriges säkerhet. TechSverige avstyrker därför förslaget i denna del.

Bakgrundskontroller

I betänkandet ställs krav på att verksamhetsutövaren ska föra en förteckning över befattningar med krav på bakgrundskontroll (befattningsanalys). Befattningsanalysen ska utgå från den kritiska verksamhetsutövarens riskbedömning och skall åtminstone innehålla uppgift om vilka befattningar där deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Befattningsanalysen ska uppdateras årsvis.

TechSverige ser behovet av kontrollerna men vill lyfta fram att en bakgrundskontroll som endast inkluderar styrkande av identitet samt utdrag ur belastningsregister kan vara av begränsat värde. Behov av en mer utförlig kontroll bör utredas för särskilda verksamheter. Samtidigt bör det beaktas att mer omfattande kontroller kommer leda till fler administrativa uppgifter och ökade kostnader varvid ekonomisk kompensation till enskilda företag bör övervägas.

Till skillnad från vad som anges i motståndskraftslagen framgår det inte i cybersäkerhetslagen vad som gäller i fråga om bakgrundskontroller. Av det skälet bör det

införas en rätt för verksamhetsutövare inom sektorn digital infrastruktur att genomföra bakgrundskontroller på motsvarande sätt som i motståndskraftslagen.

Personalsäkerhet är en central och mycket viktig del i de åtgärder som ska vidtas för att stärka motståndskraften och höja cybersäkerhetsnivån. Det ställer krav på tydlighet i lagstiftningen. Det bör också eftersträvas att bakgrundskontroller och dess olika moment bör vara så lika som möjligt oavsett vilken sektor en verksamhetsutövare är verksam inom, exempelvis avseende hur man ska bedöma risk för skada på den samhällsviktiga tjänsten (jfr. s. 201).

I övrigt saknas det i Sverige en samordnad reglering för åtgärder inom personalsäkerhet. Det är snarare så att det genomförs olika regleringsinsatser i varierad grad och per sektor. Tydligast reglering finns inom säkerhetsskyddet där ytterligare förtydliganden väntas (se SOU 2024:88). På ett övergripande plan råder således en stor osäkerhet vad verksamhetsutövare förväntas vidta för åtgärder om personalsäkerhet, vad åtgärderna syftar till, vilka uppgifter som normalt ska omfattas och vilka hot/risker och potentiell skada som ska bedömas. Idag är samhällsviktiga aktörer till viss del utlämnande till de privata aktörer som tillhandahåller bakgrundskontroller som en tjänst. Dessa är i sin tur beroende av att IMY beslutar om att de får behandla uppgifter om brott (se 6 § förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning).

Transparens m.m.

Som alltid är tydlighet och transparens avgörande för att lagstiftning ska få det genomslag och den effekt som avses. TechSverige anser att lagstiftningen måste vara tydlig vad gäller frågan om vilka verksamheter som omfattas och vilka krav som då ställs.

Erfarenheterna från säkerhetsskyddslagen är avskräckande, då det fortfarande, fem år efter att lagen trädde i kraft, råder stor osäkerhet bland privata verksamhetsutövare om och i vilken utsträckning deras verksamhet kan vara av betydelse för Sveriges säkerhet. För mobiloperatörer finns det till exempel stora kvarvarande frågetecken kring hur 5G-licenskraven förhåller sig till säkerhetsskyddslagen.

De som omfattas av kraven behöver ges rimlig tid för att göra de anpassningar som krävs för att efterleva nya eller förstärkta krav. Tio månader är i regel en mycket kort tid för att införa eller ändra om rutiner, 18 månader är ett minimum för att göra större administrativa eller tekniska omställningar. Verksamhetsutövare behöver alltså ges rimlig tid till att genomföra de anpassningar som lagen förutsätter.

Ekonomiska konsekvenser för enskilda kritiska verksamhetsutövare

Konsekvensbedömningen vad avser det privata näringslivet är otillräcklig. Avsnittet borde ha utvecklats av utredaren. Farhågan är att utredaren underskattar kostnaderna och andra konsekvenser, särskilt om företagen behöver genomföra ändringar snabbt för att kunna följa reglerna.

Utredaren bedömer att förslagen inte kommer att innebära några ekonomiska konsekvenser för enskilda kritiska verksamhetsutövare. Även om flera verksamheter som kommer att omfattas av den nya lagen redan i dag omfattas av liknande kravställningar från annan lagstiftning kommer de nya reglerna självklart att innebära kostnader för näringslivet.

Utredaren anger att det först efter att kritiska verksamhetsutövare har identifierats och riskbedömningar har genomförts kan finnas anledning att överväga om det finns behov av att exempelvis införa statligt stöd. Det kan konstateras att utredaren de facto skjuter konsekvensanalysen på framtiden. Detta trots att utredaren själv lyfter fram att PTS exempelvis har anfört att kravet på incidentrapportering inte endast medför kostnader när en incident inträffar. Verksamhetsutövaren måste ta fram en process och kanske

systemstöd för att övervaka och kunna upptäcka incidenter. Vidare krävs att det finns utbildad personal som kan hantera incidenter när de uppstår.

Utredaren borde kunnat se att flera av de åtgärder som krävs av identifierade verksamhetsutövare kommer att föranleda såväl förhöjda investeringar som löpande kostnader. Konsekvensanalysen är således bristfällig.

I många fall kommer reglerna att påverka företag som verkar under hårt konkurrenstryck, både i Sverige och internationellt. Regeringen bör vara tydlig med hur detta ska hanteras framöver, då genomförandet kommer att se olika ut i medlemsstaterna.

Privat-offentlig samverkan

TechSverige instämmer i att privat-offentlig samverkan är en central beståndsdel i att stärka motståndskraften men anser att det krävs tydligare strukturer och incitament för att säkerställa långsiktig och effektiv samverkan.

En viktig del av förslagen i utredningen handlar om behovet av samverkan mellan offentliga och privata aktörer. Det behöver tydligt redogöras för ansvarsfördelning, förväntade bidrag samt hur informationsdelning ska hanteras, för att skapa transparenta och effektiva samverkansformer. TechSverige är även positiv till ett samarbetsforum för att säkerställa att tillsynen är effektiv och väl samordnad. Särskilt när det gäller tillsynsmyndigheter och fokusområden.

TechSverige ser positivt på omnämnandet av ökade offentlig-privata relationer och delning av information. En fråga är hur detta kan genomföras. En observation från Danmark är att det har funnits svårigheter p.g.a. säkerhetskrav för vissa myndigheter inom försvarsområdet. För företagen måste det vara lätt att förstå hur data ska tillhandahållas eller delas och med vem det sker.

De föreslagna ändringarna av OSL för sekretess för incidentrapporter är angelägna. Det bör också beaktas att det också kan finnas företagsrelaterad sekretess som t.ex. molnleverantörer som levererar till myndigheter kan ha för att hålla alla kunder säkra. Även förslaget att tillsynsmyndigheterna ska ges möjlighet att inhämta de uppgifter som behövs från kritiska verksamhetsutövare för att en nationell riskbedömning ska kunna upprättas är det av stor vikt att ett verktyg med tillhörande processer och rutiner införs för att kunna säkerställa att känslig information i inhämtade uppgifter hanteras på ett likadant sätt som sekretessen för rapportering avseende incidenter.

Samverkansplattformar

TechSverige stöder förslaget om samverkansplattformar. För att maximera effekten av de föreslagna plattformarna föreslår TechSverige att de utformas med fokus på enkelhet och tillgänglighet samt att regelbundna övningar hålls för att stärka samarbetet i praktiken.

Näringslivet utgör en vital del av samhällets krisberedskap och bör involveras mer aktivt i planering och genomförande av åtgärder för motståndskraft. Detta kan uppnås genom formaliserade partnerskap och plattformar för dialog. Därför stödjer TechSverige förslaget att inrätta plattformar för informations- och resursdelning mellan offentliga och privata aktörer.

Tillsyn

TechSverige välkomnar förslaget om att inrätta ett samarbetsforum för att säkerställa en enhetlig och effektiv tillsyn. Tillsynsarbetet kommer dock att ställa stora krav på samordning för att undvika inkonsekvenser och betydande skillnader i tillsynen.

TechSverige är positivt till att tillsynsmyndigheten ansvarar för identifieringen av kritiska verksamhetsutövare. Det är också rimligt att denna myndighet beslutar om och

kommunicerar vilka verksamhetsutövare som identifieras som kritiska baserat på riskbedömningen som ska användas av de behöriga myndigheterna vid identifiering av kritiska verksamhetsutövare, samt för att bistå de kritiska verksamhetsutövarna med att vidta åtgärder för motståndskraft.

TechSverige anser att en effektiv samordning mellan tillsynsmyndigheterna är av stor vikt, särskilt med hänsyn till att tillsynsansvaret är delat. Om en verksamhetsutövare tillhandahåller flera samhällsviktiga tjänster och där verksamhetsutövaren kan identifieras som kritisk av flera tillsynsmyndigheter är det därmed viktigt att tillsynen kan ske i så bred samstämmighet som möjligt och i dialog med de olika tillsynsmyndigheterna.

Näringslivets behov av stöd

Näringslivet bör ges stöd i arbetet med att ta fram kontinuitetsplaner genom riktade utbildningar och ekonomiska incitament. TechSverige ser också ett behov av vägledning för att hjälpa företagen att säkerställa regelefterlevnad.

Detta gäller särskilt små och medelstora företag, som ofta saknar resurser att utveckla avancerade beredskapsplaner. Detta kan uppnås genom riktade utbildningar och ekonomiska incitament.

Behovet av statligt stöd för enskilda kritiska verksamhetsutövare bör införas. För många företag, framför allt de mindre, kan statligt stöd i form av medel vara avgörande för att utveckla kontinuitetsplaner och säkerställa regelefterlevnad utan att belasta företagen ekonomiskt. Stora verksamhetsutövare äger sådan infrastruktur som definieras som kritisk och som ska skyddas särskilt. Ekonomiskt stöd till identifierade verksamhetsutövare med särskilt stort ägande av kritisk infrastruktur eller av stor betydelse för andra aktörer och verksamhet bör prioriteras.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Fredrik Sand
näringspolitisk expert