Tågföretagen

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Tågföretagen är bransch- och arbetsgivarorganisation med cirka 90 medlemmar som har närmare 19 000 medarbetare. Bland medlemmarna finns de flesta av Sveriges aktiva tågoperatörer och ett flertal järnvägsinfrastrukturföretag.

Tågföretagen har tagit del Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven (SOU 2024:18).

Tågföretagens yttrande

Tågföretagen välkomnar NIS2 och anser att nya regler om cybersäkerhet är välkommet. Dock ser vi några områden som vi anser behöver adresseras.

Vad som omfattas av begreppet hela verksamheten behöver förtydligas

Tågföretagen noterar att utredningen tolkat att hela verksamheten ska omfattas av lagen. Tågföretagen är av annan åsikt då följande skrivning i NIS 2 påvisar att inte hela verksamheten omfattas när entiteter ”samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv”, se skäl 21 i NIS2.

Kort tid för genomförande och framtagning av tillhörande föreskrifter

Förslaget om en ny lag och förordning föreslås gälla från 1 januari 2025 medan de båda EU-direktiven, NIS2-direktivet samt CER-direktivet ska vara införda redan 18 oktober 2024. Dessa två införanden måste gå hand i hand. En ny lag innebär att berörda verksamheter behöver anpassa sig till de nya regelverken och tiden för detta är tillfredställande. En försvårande omständighet till detta är att det finns många områden där det råder oklarhet i vilka regler, krav, kriterier och grunder som ska gälla för efterlevnad av lagen samt tillsyn av den. Utredningen har därtill aviserat att den i september kommer att leverera sin slutleverans av förslag för att införliva CER-direktivet vilket är en månad innan direktiven ska börja tillämpas och endast tre månader innan den tilltänkta lagen träder i kraft.

Transportstyrelsen kommer sannolikt att behöva säkerställa att föreskrifterna harmonisera med direktiv och ny lag och den minimala tidsramen gör det svårt att hinna med såväl uppdateringar som ett remisshantera det som behövs.

Tågföretagen menar på att det är viktigt att vi har en sansad implementation som sker stegvis och som taktar med hur andra länder implementerar och tolkar

direktivet för att inte skapa konkurrensfördelar respektive nackdelar mellan olika länder.

Här delar vi Teknikföretagens förslag om en grace period

Tågföretagen uppmanar regeringen att i de uppdrag som kommer att ges till myndigheter att ansvara för tillsyn betonar vikten av att dessa etablerar och/eller fördjupar fora för förtroendefulla samarbeten med verksamheterna inom sina respektive sektorer.

Informationsdelning

Enligt NIS2-direktivet ska medlemsstaterna anta en nationell strategi för cybersäkerhet. Strategin ska bland annat innehålla riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter.

Utredningen föreslår att Myndigheten för samhällsskydd och beredskap (MSB) även fortsatt ska vara s.k. CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige. I delbetänkandet sägs att ”CSIRT-enheten bedriver i dag ett omfattande arbete med samverkan för att sprida information samt vid behov samordna åtgärder. Idag samordnar myndigheten informationsdelning rörande cybersäkerhet i olika sektorer men Tågföretagen menar på att informationsdelning i transportsektorn idag inte är tillfredställande. Cybersäkerhetshotet ökar inom transportsektorn men trots detta informeras det minimalt kring hotbild samt reella aktioner som sker inom transportområdet. Den informationen fås via egna kontakter samt att vi har exempel på när den informationen erhållits via media. MSB behöver stärka sin förmåga att nå ut till verksamhetsutövarna och vice versa.

Tågföretagen vill betona vikten av att ansvariga myndigheter måste skapa proaktiva insatser för att ge företagen möjlighet att utveckla sin förmåga över tid under ständigt nya förutsättningar i syfte att hindra eller stoppa antagonistiska attacker och hot.

Incidentrapportering

Utredningen föreslår att rapporteringsskyldigheterna ska bli mer långtgående än tidigare samt att tillbud och cyberhot som kan orsaka en allvarlig driftsstörning ska rapporteras. av tillbud är oproportionerlig när man ser till administrativ börda vilket behöver utredas hur det påverkar verksamheterna. Det är också långt ifrån klart när ett hot blir betydande. Detta ökar företagens omotiverade rapporteringsbörda och kommer att vara rättsosäkert att tillämpa i praktiken.

För att stärka den inre marknadens funktion och minska företagens administration är det centralt att incidentrapportering hanteras på samma sätt i medlemsstaterna. Här skulle en gemensam EU-mall vara att föredra och rapportering bör alltid kunna ske på engelska för att vara användbar inom hela EU.

Personalsäkerhet

Kommande slutsatser från CER-utredningen vad avser bakgrundskontroller bör också beaktas i verksamheter som omfattas av CSL. Behov kan förekomma att även inom cybersäkerhetsområdet göra bakgrundskontroller. Behovet av bakgrundskontroller av personal kommer med all sannolikhet öka, oavsett om det rör säkerhetskänslig verksamhet, föreslagen CSL eller kommande implementering av CER-direktivet. Det är viktigt att denna möjlighet inte inskränks och därmed försvårar möjlighet till bakgrundskontroller. En bakgrundskontroll bör även följas upp under den tid som deltagandet i den av NIS2 eller CER reglerade verksamheten pågår. Syftet är att behålla och fördjupa personkännedomen.

Konsekvensanalys och sanktioner

Direktiven och den föreslagna nya lagen får ett mycket bredare genomslag än dagens lagstiftning, i och med att kraven kommer att gälla hela verksamheten och inte bara samhällsviktiga och digitala tjänster. Vidare omfattas även fysiska lokaler. Tågföretagen saknar en konsekvensanalys för enskilda verksamhetsutövare. Givet antalet större incidenter som registrerades hos medlemmar förra året bedömer vi att kraven snarare kommer att innebära betydande merkostnader snarare än besparingar.

Tågföretagen konstaterar att sanktioner vid överträdelse är avsevärt högre samt att företagens ledning kan bli föremål för sanktioner av betydande karaktär för den enskilde. Trots att även offentliga myndigheter kan bli föremål för sanktioner finns en tydlig obalans mellan dem och den enskilda näringsutövaren.

Tågföretagen anser att sanktionerna måste stå i relation till branschens förväntade lönsamhet för att få ett rättvist sanktionssystem. Vi noterar att man i särbehandlat offentliga myndigheter i detta hänseende.

För Tågföretagen den 28 maj 2024,

Lina Lagerroth
Näringspolitisk expert