Datum
2024-05-28

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

Vår beteckning: SJCM-2024-0002-014
Ert diarienr: Fö2024/00496

Handläggare
Gunnar Alexandersson
Tel. 070-003 69 77
E-post: gunnar.alexandersson@sj.se

Yttrande om delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

SJ AB (SJ) har tagit del av detta delbetänkande från Utredningen om genomförande av NIS2- och CER-direktiven och lämnar synpunkter på några utvalda områden i detta yttrande.

Inledningsvis vill SJ framhålla att vi överlag ser positivt på utredningens förslag och har förståelse för behoven av de nya regelverken.

Knapp tid för genomförande och framtagning av tillhörande föreskrifter

De båda EU-direktiv som föranlett utredningen, NIS2-direktivet och CER-direktivet, kommer att vara tillämpliga i Sverige redan från 18 oktober 2024. Förslaget till ny lag om cybersäkerhet och tillhörande förordning föreslås dock inte börja gälla förrän 1 januari 2025. Denna diskrepans är i sig ett problem, men även om man bara tar hänsyn till den nya lagen blir det en väldigt kort tid för de verksamheter som omfattas att anpassa sig till de nya regelverken. Det gäller särskilt som det i flera delar är oklart vilka specificerade regler, krav, kriterier och grunder som ska tillämpas för efterlevnad och tillsyn av den nya lagen. En tillkommande problematik är att utredningen inte förrän i september ska leverera de kvarvarande förslag som rör införlivandet av CER-direktivet. Det är bara en månad innan båda direktiven ska börja tillämpas och bara drygt tre månader innan den tilltänkta svenska lagen träder i kraft.

Aktuell tillsynsmyndighet på transportområdet är Transportstyrelsen, som sannolikt kommer att behöva uppdatera och/eller ta fram nya föreskrifter. Det föranleder flera frågor:

- Kan vi förvänta oss nya rapporteringsregler till tillsynsmyndigheten som SJ behöver följa?
- Kan vi förvänta oss nya eller ändrade krav eller kriterier som ersätter de sektorspecifika krav som i dag finns i TSFS 2022:14?
- Kan vi förvänta oss nya eller ändrade bedömningsgrunder för efterlevnad och föreläggande?

Den knappa tiden till införandet kommer att göra det mycket svårt för tillsynsmyndigheten att i tid få fram och remisshantera eventuella föreskrifter.

Informationsdelning och kompetens

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. Myndigheten driver ett flertal forum för informationsdelning rörande cybersäkerhet i olika sektorer” (sid 310). SJ menar att MSB:s arbete vad gäller informationsinsatser i transportsektorn inte är så omfattande som det framstår i delbetänkandet. Det finns också exempel på situationer där myndigheten brustit i att informera berörda verksamhetsutövare om förestående cybersäkerhetshot och verksamhetsutövarna i stället fått ta del av sådan information via media eller andra kanaler. För att cybersäkerhetsarbetet i Sverige ska kunna fungera krävs en tillfredsställande informationsdelning både från verksamhetsutövare till myndigheter och omvänt.

SJ menar också att det kommer att finnas ett stort behov av vägledningar från myndigheter som MSB och Transportstyrelsen för att underlätta företagens möjligheter att efterleva den nya lagstiftningen. För detta krävs särskild kompetens vad gäller informationssäkerhetsspecialister, som utgör en generell bristkompetens som inte nödvändigtvis finns tillgänglig inom Transportstyrelsen i dag.

Konsekvensanalys och sanktioner

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, vilket förefaller vara en övertolkning av de faktiska kraven i NIS2-direktivet. Vidare omfattas även fysiska lokaler. SJ menar att konsekvenserna för enskilda verksamhetsutövare är allt för sparsamt beskrivna i delbetänkandet, med en generell hänvisning till liknande krav som för offentliga verksamhetsutövare och att kraven kommer ”att medföra kostnader, men samtidigt även stöd

och övergripande besparingar” (sid 357). Mot bakgrund av antalet större incidenter som registrerades i SJs verksamhet 2023 bedömer SJ att kraven kommer att medföra betydande merkostnader snarare än besparingar.

SJ konstaterar att den nya lagen medför väsentligt högre sanktioner vid överträdelse och att även företagets ledning kan bli föremål för sanktioner som i praktiken innebär yrkesförbud. Även om också offentliga myndigheter kan bli föremål för sanktioner finns en tydlig obalans i dessa till enskilda verksamhetsutövares nackdel.

Kombinationen av kort genomförandetid, stora behov av vägledning och anpassningar hos både verksamhetsutövare och myndigheter, samt skärpta sanktioner, motiverar en övergångsperiod där fokus ligger på att skapa goda förutsättningar och samarbetsstrukturer för att upptäcka och avvärja cyberrelaterade risker och attacker, innan det blir aktuellt att styra branschens aktörer via tillsyn och därtill kopplade sanktioner.

Förhållande till annan lagstiftning

SJ bedömer att det skulle kunna behövas ytterligare överväganden om förhållandet mellan ny föreslagen lagstiftning och säkerhetsskyddslagen, men vi har hittills inte haft möjlighet att undersöka detta närmare. SJ kan komma att återkomma i frågan när utredningen lämnat sitt slutbetänkande i september, också eftersom detta var en av de frågor som regeringen i sitt tilläggsdirektiv i januari gav utredningen förlängd tid att analysera.

Monica Lingegård
VD SJ AB