Försvarsdepartementet

fo.remissvar@regeringskansliet.se

kopia: visnja.raguz@regeringskansliet.se

REMISSYTTRANDE
dnr Fö2024/00496

Göteborg 2024-05-28

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

Föreningen Svensk Sjöfart är en branschorganisation för svensk sjöfartsnäring och representerar ett 60-tal rederier med verksamhet över hela världen. Den svenska sjöfarten är en del av det europeiska sjöfartsklustret som sammantaget kontrollerar drygt 40 procent av världshandelsflottan. Mer än 90 procent av Sveriges utrikeshandel går via sjöfarten och årligen reser över 30 miljoner passagerare med färjor till och från Sverige.

Svensk Sjöfart har tagit del av det remitterade delbetänkandet och önskar lämna följande synpunkter.

Inledning och bakgrund

I juli 2016 antog Europaparlamentet NIS-direktivet (*the Network and Information Systems Directive*) med syfte att minska sårbarheter och höja säkerheten i digitala tjänster och för samhällsviktiga tjänster. År 2020 presenterade EU-kommissionen ett förslag på ett nytt NIS direktiv, kallat NIS2. Syftet med det reviderade direktivet är att harmonisera de olika medlemsländernas cybersäkerhetskrav och tillämpning av cybersäkerhetsåtgärder. NIS2 beslutades av EU i december 2022. Det remitterade delbetänkandet redovisar förslag om införlivning av NIS2, som ersätter nuvarande NIS-direktiv, och föreslår att en ny lag om cybersäkerhet träder i kraft den 1 januari 2025.

Svensk Sjöfart välkomnar syftet med direktivet. Arbetet med informations- och cybersäkerhet är mycket viktig och Svensk Sjöfart är positiva till det arbete som sker internationellt för sjöfartssektorn inom bland annat IMO (FN:s internationella sjöfartsorganisation). På grund av rederiers internationella verksamhet är det av största vikt att tillämpningen för sjöfartssektorn sker enhetligt och harmoniserat mellan länder.

Rederiers säkerhet- och skyddsarbete

Den internationella regleringen av sjöfarten bygger på Internationella sjöfartsorganisationens (IMO) konventioner. Skyldigheter som gäller rederiernas riskhantering finns i den internationella säkerhetsorganisations-koden (ISM-koden) som grundar sig på SOLAS-konventionen. Inom EU har koden genomförts genom Europaparlamentets och rådets förordning (EG) nr 336/2006 om genomförande av Internationella säkerhetsorganisationskoden i gemenskapen. Även systemet för rapportering av händelser ingår i kraven i ISM-koden.

Den internationella sjöfartsorganisationen IMO antog år 2017 en resolution om cyberriskhantering i säkerhetshanteringssystem. Resolutionen anger att cybersäkerhet anses vara en operativ fråga som ska behandlas i fartygs SMS (*Safety Management System*) och ingå vid den första årliga kontrollen av rederiets DoC (*Document of Compliance*) efter 1 januari 2021.

År 2017 antog IMO även rekommendationer där det bland annat hänvisas till de branschriktlinjer som den internationella redareföreningen (ICS) med flera tagit fram. Beslut om uppdaterade rekommendationer togs vid IMO:s Sjösäkerhetskommitté, MSC 108, maj 2024.

Lex specialis

I nuvarande NIS-direktiv står: *”När medlemsstaterna identifierar operatörer i sjöfartssektorn, bör de ta hänsyn till befintliga och framtida internationella koder och riktlinjer som utvecklats särskilt av Internationella sjöfartsorganisationen, i syfte att skapa ett enhetligt tillvägagångssätt för enskilda sjöfartsoperatörer.”* I NIS2 saknar vi nuvarande skrivningar om sjöfartssektorn med hänvisning till så kallad *lex specialis* och internationella koder och riktlinjer.

I svenska utredningen om genomförande av NIS-direktivet står *”I dag finns bestämmelser om informationssäkerhet för nätverk och informationssystem i flera nationella regelverk. Det finns också sektorer som regleras av sektorspecifika EU-rättsakter (lex specialis). Sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur är t.ex. i hög grad harmoniserade på unionsnivå.”*

I NIS2 står att tillämpningen av direktivet begränsas ytterligare av att om det finns sektorsspecifika EU-akter med likvärdiga eller högre krav på cybersäkerhet, gäller inte direktivets bestämmelser, se artikel 4, stycke 1. Vi noterar att det i betänkandet, vad avser tillämpning, står *”Om det i sektorsspecifika unionsrättsakter föreskrivs att verk-samhetsutövare ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och dessa krav har minst samma verkan, ska de relevanta bestämmelserna i NIS2-direktivet inte tillämpas på sådana verksamhetsutövare”.* Vi saknar analys vad avser sjöfartens och internationella regler i detta avseende.

Harmoniserad implementering och enhetlig tillämpning

Svensk Sjöfart får olika signaler på tillämpning av direktivet i medlemsstaterna vad gäller sjöfartssektorn. Med aktuell information i det remitterade delbetänkandet är det inte möjligt att bedöma i vilken utsträckning förslaget gäller för rederier och sjöfart. Svensk Sjöfart understryker att det är av största vikt med harmoniserad implementering och att tillämpningen för sjöfartssektorn sker enhetligt mellan länder. Vi ställer i dessa delar oss bakom Svensk Näringslivs remissyttrande som lyfter att det är största vikt att medlemsstaterna implementerar direktivet så enhetligt som möjligt. Enhetlig implementering är central för konkurrens på lika villkor. Vi reagerar, i linje med Svenskt Näringsliv, på tolkningen att hela verksamheten som huvudregel ska omfattas av lagen. Det är inte utgångspunkten när entiteter ”*samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv*”, se skäl 21 i NIS2.

I utredningen saknar vi bland annat analys och jämförelse med implementering i andra länder. Detta är som sagt särskilt viktigt för en internationell bransch som sjöfarten.

Vad avser tillämpningen av direktivet förutsätter vi att det är skattefinansierad verksamhet.

Samverkan

För upplysning vill vi passa på att framföra att vi ser behov av ökad samverkan mellan myndigheter och näring vad avser informations- och cybersäkerhet. Vi har i olika sammanhang lyft bland annat nedan frågor som vi önskar mer information och samverkan kring:

- Myndighetssamverkan och ansvar (både nationellt och internationellt)
- Kontaktpersoner och informationsvägar
- Delande av erfarenheter mellan olika branscher
- Myndigheternas/statens syn på de hot som riktats mot transportörer/transportinfrastrukturen i Sverige
- Hotbilden framåt
- Vilket stöd finns från staten och vad förväntas av företagen

Slutligen vill vi framföra att vi gärna deltar i processen med regelverk kring införande av NIS2 samt arbete med informations- och cybersäkerhet.

Göteborg som ovan,

Föreningen Svensk Sjöfart

Christina Palmén