Försvarsdepartementet
Rättssekretariatet

fo.remissvar@regeringskansliet.se
Kopia till: visnja.raguz@regeringskansliet.se

Delbetänkande Nya regler om cybersäkerhet (SOU 2024:18)

Sammanfattning

Transportstyrelsen tillstyrker i huvudsak förslaget SOU 2024:18 Nya regler för cybersäkerhet men har följande synpunkter.

Framförallt ser Transportstyrelsen en farhåga i utredningens förslag om att *hela* verksamheten ska omfattas av regleringen. Därtill är det högst olyckligt att MSB (Myndigheten för samhällsskydd och beredskap) inte längre ska ta fram föreskrifter som förtydligar den närmare sektorsbeskrivningen och att tillsynsmyndigheterna, istället för MSB, föreslås få föreskriftsrätt vad gäller systematiskt och riskbaserat informationssäkerhetsarbete, riskhanteringsåtgärder och utbildning. Utredningens förslag om ett utökat anslag på endast två miljoner till Transportstyrelsen i egenskap av tillsynsmyndighet, och inget anslag i egenskap av verksamhetsutövare, kan komma att påverka genomförandet.

Sammanfattningsvis har myndigheten följande huvudsakliga synpunkter:

- Regleringen bör omfatta samhällsviktiga tjänster och inte verksamhetsutövarens verksamhet i sin helhet.
- MSB bör ges i uppdrag att ta fram föreskrifter som förtydligar den närmare sektorsbeskrivningen.
- Krav på riskhanteringsåtgärder i cybersäkerhetslagen bör även vara tillämpliga på säkerhetskänslig verksamhet.
- MSB bör ges i uppdrag att utveckla ett system för registrering, där samtliga verksamhetsutövare kan lämna uppgifter.
- Ledningens ansvar bör framhållas genom att låta artikel 21.2 a) och f) i NIS2-direktivet uttryckligen framgå av lagtexten.
- Tidpunkten för incidentrapportering bör anges som *senast inom* för att främja tidig rapportering.

Transportstyrelsen
Generaldirektör
601 73 Norrköping
Besöksadress
Olai Kyrkogata 35, Norrköping

Telefon 0771-503 503
Telefax 011-185 256

transportstyrelsen.se
kontakt@transportstyrelsen.se

Daniel Jönsson
daniel.jonsson2@transportstyrelsen.se
0104-953 296

- Information till kunder om betydande incidenter bör endast ske *när så är lämpligt* och MSB bör ges föreskriftsrätt att förtydliga hur information ska lämnas.
- Om krav ställs på att verksamhetsutövarna ska ha dygnet runt bemanning bör det tydliggöras i förarbetena.
- MSB bör få föreskriftsrätt vad gäller systematiskt och riskbaserat informationssäkerhetsarbete, riskhanteringsåtgärder och utbildning.
- Tillsynsmyndigheterna bör ges möjlighet att förena beslut om riktad säkerhetsrevision med vite.
- Det bör förtydligas om kollektivtrafik ingår i Transportstyrelsen ansvarsområde innan CER-direktivet omhändertas.
- Tillsynsmyndigheterna bör ges mandat att ingripa vid brister i det systematiska informationssäkerhetsarbetet.
- Det bör endast framgå av lagen vilka omständigheter som ska beaktas i fråga om sanktionsavgift ska tas ut och till vilket belopp.
- De omständigheter som gäller för sanktioner enligt 31 § NIS-lagen bör även gälla för den nya lagen om cybersäkerhet.
- *Falsk eller grovt felaktig information* bör användas istället för oriktiga uppgifter gällande omständigheter som kan göra en överträdelse allvarlig.
- Det bör av lagen framgå att en överträdelse som anses som allvarlig kan leda till högre vite eller sanktionsavgift.
- Utredningen borde ha övervägt om certifiering bör införas i Sverige för verksamhetsutövare som uppfyller lagens krav.
- Ett ökat anslag på två miljoner kronor för Transportstyrelsen i egenskap av tillsynsmyndighet är inte tillräckligt.

Transportstyrelsens synpunkter

5 kap. Cybersäkerhetslagens tillämpningsområde

5.2.2. Verksamhetsutövare

Begrepp

Enligt utredningens förslag ska begreppet *verksamhetsutövare* användas i den föreslagna lagen istället för *entitet*, som används i NIS2-direktivet[1]. Transportstyrelsen instämmer med utredningen att begreppet entitet bör ersättas och anser att verksamhetsutövare är ett lämpligt ordval då det är ett vanligt förekommande begrepp för våra tillsynsobjekt.

[1] Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cyber- säkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

Verksamhetens omfattning

Utredningens bedömning är att verksamhetsutövarens verksamhet *i dess helhet* ska omfattas av den föreslagna lagen. Transportstyrelsen ser stora svårigheter med utredningens förslag i denna del. En verksamhetsutövare kan ha 100-tals, till och med 1000-tals, system – allt från system för att skriva ut besökskort till centrala övervaknings- och kontrollsystem. En central del i nuvarande reglering är att verksamhetsutövaren genomlyser sin verksamhet för att identifiera de system som är nödvändiga för att upprätthålla den samhällsviktiga tjänsten. Att verksamhetsutövare väljer ut och prioriterar de mest skyddsvärda systemen är en viktig övning som även följer av annan lagstiftning, såsom säkerhetsskyddslagstiftningen och luftfartsskydd[2].

Verksamheter som pekas ut i bilaga 1 och 2 till NIS2-direktiet omfattas eftersom de fyller en samhällsviktig funktion och syftet med att identifiera de nödvändiga systemen är att säkerställa att dessa är tillräckligt robusta och prioriteras vid en storskalig incident så att den samhällsviktiga verksamheten kan fortgå eller, i värsta fall, återupptas så snabbt som möjligt.

Om samtliga system hos en verksamhetsutövare ska uppfylla lagens och framtida föreskrifters detaljerade krav på säkerhetsåtgärder, och hänsyn ska tas till alla incidenter som kan påverka dessa system, ser Transportstyrelsens en stor risk att arbetet blir alltför betungande och kostsamt vilket kan påverka förmågan att skydda de system som det utifrån ett samhällsperspektiv verkligen finns ett behov av att skydda. Särskilt med beaktande av att de riskhanteringsåtgärder som ska vidtas enligt 3 kap. 1 § förslag till lag om cybersäkerhet ska utgå från ett allriskperspektiv. Ur ett tillsynsperspektiv blir det också ohållbart att tillsynen ska omfatta alla nätverk och informationssystem hos en verksamhetsutövare.

Transportstyrelsen anser sammanfattningsvis att kopplingen till den samhällsviktiga tjänsten är centralt och därför borde införas även i den nya regleringen.

5.2.12 Enskilda verksamhetsutövare

Enligt 1 kap. 4 § 1 stycket förslag till lag om cybersäkerhet ska enskilda verksamhetsutövare som bedriver verksamhet inom EES, innefattas i bilaga 1 eller 2 till direktivet samt, som utgångspunkt, uppfyller storlekskravet

[2] Enligt punkterna 1.7.1 och 1.7.2 i kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd ska flygplatsoperatörer, lufttrafikföretag och verksamhetsutövare identifiera de kritiska informations- och kommunikationstekniksystem och data som används för civil luftfart i syfte att skydda dessa mot cyberattacker som skulle kunna påverka skyddet av den civila luftfarten.

omfattas av lagen. Utredningen föreslår därtill att regeringen ger tillsynsmyndigheterna i uppdrag att med stöd av MSB skyndsamt utforma en vägledning om de oklarheter som kan föreligga i sektorsbeskrivningarna.

I dag har MSB utfärdat föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2024:4). Föreskrifter innehåller dels tröskelvärden (som vid implementering av NIS2-direktivet ersätts av antal anställda och omsättning) men dels också förtydliganden om vilka aktörer som träffas av regleringen, vilket utredningen nu alltså föreslår ska framgå av tillsynsmyndigheternas vägledning istället.

Transportstyrelsen delar inte utredningens bedömning om det i de flesta fall inte innebär några svårigheter att utröna vilka som omfattas av regleringen. NIS2-direktivets konstruktion att hänvisa till definitioner i andra EU-rättsakter gör istället tillämpningsområdet mycket svårtolkat. Exempelvis är en typ av verksamhetsutövare som omfattas enligt bilaga 1 till NIS2-direktivet (samma lydelse finns i bilagan till det ursprungliga NIS-direktivet) inom delsektorn sjöfart *Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG, inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar*, vilket i MSBFS 2024:4 har förtydligats på så sätt att vad som avses är tjänster som tillhandahålls av en hamninnehavare och tjänster som tillhandahålls av en hamnanläggningsinnehavare.[3] Gällande nämnda sektorsbeskrivningen i direktivet är det också oklart om hamnarna respektive hamnanläggningarna måste omfattas av tillämpningsområdet för rådets direktiv 2005/65/EG[4] respektive förordning (EG) nr 725/2004[5], eller om det endast är definitionerna i nämnda författningar som är relevanta.

Men hänsyn till de stora oklarheter som råder anser Transportstyrelsen att den närmare sektorsbeskrivning, precis som idag, behöver framgå av föreskrifter (men utan tröskelvärden) då en vägledning inte alls har samma rättsliga status vid meningsskiljaktigheter.

Enligt Transportstyrelsens mening är det därför högst angeläget att MSB, med stöd av tillsynsmyndigheterna, även fortsättningsvis får mandat att meddela föreskrifter om den närmare innebörden av vilka verksamheter som omfattas enligt bilaga 1 och 2 till NIS2-direktivet.

---

[3] Se 4 kap. 3 §.
[4] Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd.
[5] Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar.

5.5.4 Undantag för offentliga verksamhetsutövare och 5.5.5 Undantag för enskilda verksamhetsutövare

Enligt utredningens förslag ska den del av verksamheten som är säkerhetskänslig undantas från cybersäkerhetslagens krav förutom vad gäller anmälningsskyldigheten. Kraven i lagen på riskhanteringsåtgärder och incidentrapportering (liksom tillsyn och sanktioner i dessa avseenden) ska således inte gälla.[6]

Transportstyrelsen instämmer med vad Säkerhetspolisen har anfört till utredningen om att NIS2-direktivet skulle kunna utgöra en lämplig ”bottenplatta”, som kan kompletteras av säkerhetslagens bestämmelser.[7] Medan kraven i säkerhetsskyddslagen och val av säkerhetsåtgärder utgår från de antagonistiska hot verksamheten har identifierat utgår NIS2-direktivet istället från ett allriskperspektiv. Det är angeläget att krav på ett systematiskt och riskbaserat informationssäkerhetsarbete och riskhanteringsåtgärder för de mest skyddsvärda verksamheterna i Sverige utgår från ett allriskperspektiv. Däremot anser Transportstyrelsen att bestämmelserna om tillsyn och incidentrapportering i cybersäkerhetslagen inte ska gälla säkerhetskänslig verksamhet, för att undvika oklara gränsdragningar och då hantering av säkerhetsskyddsklassificerade uppgifter och uppgifter om säkerhetskänslig verksamhet ställer mycket höga krav på hantering.

6 kap. Klassificering och registrering

6.2 Register över väsentliga och viktiga verksamhetsutövare

Utredningen föreslår att en verksamhetsutövare som har identifierat att verksamheten omfattas av NIS-regleringen ska anmäla detta till sin tillsynsmyndighet och att varje tillsynsmyndighet ska upprätta ett register över väsentliga och viktiga verksamhetsutövare inom sitt tillsynsområde. Ett första register ska vara upprättat och ingivet till den gemensamma kontaktpunkten (dvs. MSB) senast den 1 mars 2025 och därefter vartannat år.[8] MSB ska i sin tur dela dessa uppgifter med EU-kommissionen.

Transportstyrelsen har idag inget specifikt system avseende uppgifter om anmälda verksamhetsutövare utan tar emot anmälningar på blankett som skickas in via post varvid verksamhetsutövaren förs in i en förteckning i tabellformat på ett fristående lagringsmedium. När NIS2-direktivet har införts kommer Transportstyrelsen att få mångdubblat fler verksamhetsutövare och detsamma gäller övriga tillsynsmyndigheter. Att fortsätta jobba med ett fristående lagringsmedium blir inte hållbart och

---

[6] Delbetänkandet 1 kap. 12-13 §§ lag om cybersäkerhet.
[7] Se s. 137 samt s. 164 i delbetänkandet. Jfr även MSB:s remissvar för delbetänkande SOU 2024:14, daterat 2024-04-10.
[8] Delbetänkandet 14 § förordning om cybersäkerhet.

heller inte önskvärt då det ur ett användarperspektiv är angeläget att verksamhetsutövarna kan anmäla sig direkt i systemet.[9] Transportstyrelsen anser dock inte att det är kostnadsmässigt försvarbart att varje tillsynsmyndighet ska utveckla sina egna system för registrering, särskilt inte med beaktande av de säkerhetskrav som kommer att ställas på ett sådant system. Istället borde det ligga på MSB, som i alla fall ska förses med uppgifterna, att föra ett sådant register.

Eftersom MSB är den myndighet som ska meddela föreskrifter om vilka uppgifter som ska lämnas in av verksamhetsutövarna, hur och när samt att det är till MSB som incidenter ska rapporteras förefaller en sådan ordning logisk. MSB, som för närvarvarande utvecklar en systemplattform som skulle kunna omfatta verksamhetsutövare inom NIS2-direktivet, anser också själva att de bör föra ett sådant register.[10] Naturligtvis behöver dock tillsynsmyndigheterna ha vetskap om sina tillsynsobjekt, en förutsättning är därför att tillsynsmyndigheterna får behörighet som användare i systemet och kan se de tillsynsobjekt som ligger under respektive myndighets ansvarsområde. Annars kommer tillsynsmyndigheterna i alla fall att behöva ta fram parallella system.

7 kap. Riskhantering och incidentrapportering

7.1.2 Riskhanteringsåtgärder

NIS2-direktivet innehåller i artikel 21.2 ett antal riskhanteringsåtgärder som är obligatoriska. När det gäller punkt a) strategier för riskanalys och informationssystemens säkerhet och punkt f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet anser utredningen att detta inte behöver anges särskilt eftersom det följer av förslaget till övergripande reglering. Enligt 3 kap. 1 § förslag till lag om cybersäkerhet ska verksamhetsutövaren vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken.

Transportstyrelsen anser att det är tveksamt om punkterna a) och f) verkligen ryms inom den generella regleringen utan anser, då det är fråga centrala riskhanteringsåtgärder som betonar ledningens ansvar, att dessa uttryckligen borde framgå av lagtexten.

7.3 Incidentrapportering

Tidpunkt för incidentrapportering

[9] Jfr artikel 3.4 NIS2-direktivet om att medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för verksamhetsutövarna att registrera sig själva.
[10] Se MSB:s remissvar för delbetänkande SOU 2024:14, daterat 2024-04-10.

Utredningen föreslår att verksamhetsutövaren som en första varning ska underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten och inom 72 timmar från tidpunkten för kännedom göra en incidentanmälan till CSIRT-enheten.[11] I direktivet följer i detta avseende att verksamhetsutövare som omfattas *utan dröjsmål och under alla omständigheter* inom 24 timmar efter att ha fått kännedom om en betydande incident ska lämna en första varning till CSIRT-enheten och *utan dröjsmål och under alla omständigheter inom* 72 timmar göra en incidentanmälan.[12]

I MSB:s nuvarande föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster (MSBFS 2018:9) följer av 1 kap. 3 § att leverantören ska rapportera in uppgifter om en inträffad incident *senast inom* sex timmar respektive *senast inom* 24 timmar från det att en leverantör har identifierat att en incident är rapporteringspliktig. Transportstyrelsen kan konstatera att det är stor skillnad på den första anmälan, som idag alltså ska göras inom sex timmar, mot en första varning som ska göras inom 24 timmar och att mycket hinner hända inom den tidsrymden. Samtidigt kan verksamhetsutövaren de första timmarna efter att en incident har inträffat ha fullt upp med att hantera incidenten och ska då inte belastas med betungande administration. Det finns alltså skäl till att välja en direktivnära implementering i detta avseende. Dock anser Transportstyrelsen att *senast inom*, som det står idag, bör framgå av cybersäkerhetslagen då det kan ge ett incitament för verksamhetsutövarna att anmäla incidenter i ett tidigt skede.

Information till kunder om betydande incidenter

Enligt utredningens förslag ska verksamhetsutövaren inom 72 timmar från tidpunkten för kännedom även informera kunder som kan antas ha påverkats av en betydande incident. Av NIS2-direktivet framgår i detta avseende i artikel 23.1 att *när så är lämpligt* ska verksamhetsutövaren utan dröjsmål även underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänsterna. Transportsstyrelsen anser att *när så är lämpligt* även borde följa av den svenska lagen, då det inte alltid är ändamålsenligt att gå ut med information om framförallt pågående incidenter eftersom vetskap om sådan kan användas i antagonistiska syften (jfr att uppgifter i incidentrapporter kan sekretessbeläggas med stöd av 18:8 offentlighets- och sekretesslagen (2009:400)).

För att skapa en tydlighet och enhetlighet för verksamhetsutövarna behöver det enligt Transportstyrelsens mening även uttryckligen regleras hur verksamhetsutövarna ska gå ut med information (är det tillräckligt att lägga

[11] Delbetänkandet 3 kap. 5-6 §§ lag om cybersäkerhet.
[12] Artikel 23.4 a) och b).

ut information på verksamhetens webbsida eller ska det vara riktad information till kunderna), hur detaljerad informationen ska vara, i vilka fall det är lämpligt eller direkt olämpligt att gå ut med information (dvs. om Transportstyrelsens förslag vad gäller detta hörsammas) osv. Enligt 4 kap. 2 § förslag till lag om cybersäkerhet ska tillsynsmyndigheten utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs, vilket torde innefatta att verksamhetsutövarna har informerat sina kunder om betydande incidenter. Föreskrifter som närmare preciserar detta krav är således också nödvändig för att tillsynen i detta avseende ska bli verkningsfull. Förslagsvis bör MSB få sådan föreskriftsrätt.

Krav på dygnet-runt bemanning?

Av MSBFS 2018:9 följer att incidenter ska rapporteras senast inom sex timmar från det att leverantören *har identifierat att en incident är anmälningspliktig*. Enligt MSB:s vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen ska inte föreskriftskravet tolkas som krav på ökad bemanning utan tidsfristen för rapportering ska räknas från den tidpunkt då leverantören med stöd av sina interna regler och arbetssätt identifierat en incident som rapporteringspliktig. Som framgår ovan ska tiden framöver istället räknas från det att verksamhetsutövaren *fått kännedom om incidenten*. Transportstyrelsen anser att det behöver förtydligas i förarbetena om detta innebär att det ställs högre krav på 24/7-bemanning än idag.

8 kap. Tillsyn

8.4.2 Tillsynsmyndigheter i Sverige

Transportstyrelsen är för närvarande tillsynsmyndighet över sektorn transport och föreslås enligt utredningen även få tillsynsansvar för sektorn tillverkning, dels vad gäller delsektorn tillverkning av motorfordon, släpfordon och påhängsvagnar samt dels vad gäller delsektorn tillverkning av andra transportmedel.[13] Transportstyrelsen har idag tillsyn över nämnda delsektorer avseende tillverkning i andra hänseenden och ser positivt på förslaget att även dessa inkluderas i vår NIS-tillsyn.

8.4.5 Föreskrifter

Utredningen föreslår att tillsynsmyndigheterna ska ta fram föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning.[14] Vidare föreslås att regeringen ska ge MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för myndigheternas föreskriftsarbete.

[13] Delbetänkandet 8 § förordning om cybersäkerhet.
[14] Delbetänkandet 35 § förordning om cybersäkerhet.

Transportstyrelsen delar inte utredningens bedömning utan anser att MSB ska få föreskriftsrätt i samtliga delar, och att det är tillräckligt att tillsynsmyndigheterna får möjlighet att komplettera sådana central föreskrifter. En liknande ordning råder inom säkerhetsskyddslagstiftningen, som bl.a. innehåller mycket specifika krav vad gäller informationssäkerhet, och skapar förutsättningar för en rättssäker och likvärdig tillsynsutövning. Att MSB tar fram centrala föreskrifter är också en förutsättning för förslaget om att hela verksamheten ska omfattas (se även nedan avsnitt 8.4.7).

Enligt Transportstyrelsens mening ska inte behovet av att sektoranpassa föreskrifterna överdrivas. Våra nuvarande föreskrifter om säkerhetsåtgärder (TSFS 2022:14) grundar sig på de allmänna standarderna ISO 27000 och NIST CFC samt ENISA:s[15] riktlinjer inom cybersäkerhet ”Minimum Security Measures” och riktar sig till aktörer inom samtliga trafikslag. Av utredningen framgår att det är främst inom PTS (Post och telestyrelsen) område som man ser ett behov av att tillsynsmyndigheten får föreskriftsrätt och det är endast PTS som har anfört till utredningen att myndigheten även fortsättningsvis vill ha ensam föreskriftsrätt. Det framgår däremot inte att man har övervägt att ge MSB föreskriftsrätt att ta fram centrala föreskrifter på samtliga områden utom de områden som PTS ansvarar för. Enligt Transportstyrelsens mening skulle detta kunna vara en framkomlig väg. Att MSB först ska ta fram en vägledning, som syftar till att myndigheternas föreskrifter ska bli likvärdiga, istället för att ta fram centrala föreskrifter för samtliga sektorer (utom PTS) förfaller vara en omständlig och tidskrävande ordning. Transportstyrelsen vill även poängtera att vi, till skillnad från utredningen, inte anser att behovet av centrala myndighetsföreskrifter minskar bara för att NIS2-direktivet är något mer detaljerat avseende riskhanteringsåtgärder, då åtgärderna i direktivet fortfarande är beskrivna på en mycket övergripande nivå.

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Säkerhetsrevisioner

Enligt 4 kap. 8 § förslag till lag om cybersäkerhet får tillsynsmyndigheterna om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och redovisa slutresultatet för tillsynsmyndigheten. Med ålägga torde avses samma sak som att förelägga, vilket är ett tydligare ordval som borde användas istället för ålägga. Därtill anser Transportstyrelsen att det borde införas en möjlighet för tillsynsmyndigheterna att förena ett sådant åläggande/föreläggande med vite. Annars riskerar tillsynsmyndigheterna att

[15] Europeiska unionens cybersäkerhetsbyrå.

stå utan påtryckningsmedel om åläggandet/föreläggandet om att utföra en riktad säkerhetsrevision inte följs.

8.4.7 Samordning och informationsutbyte

Verksamhetsutövare som står under tillsyn av flera myndigheter

Utrednings förslag om att hela verksamheten ska omfattas av den nya regleringen innebär inte bara att samtliga system innefattas utan också att en verksamhetens samtliga delar ska omfattas. Detta medför att samma verksamhetsutövare, framförallt kommuner som länsstyrelsen föreslås få tillsynsansvar över i bred bemärkelse, kan få flera tillsynsmyndigheter.

Transportstyrelsen delar idag tillsynsobjekt med Energimyndigheten vad gäller vissa hamnar som omfattas av regleringen dels som hamn- eller hamnanläggningsinnehavare samt dels utifrån samhällsviktiga tjänster kopplat till drivmedel. Transportstyrelsen kan konstatera att detta ställer höga krav såväl på verksamhetsutövaren, som har olika föreskrifter att förhålla sig till och får tillsyn från olika myndigheter, som tillsynsmyndigheterna som behöver samordna sin tillsyn. Utredningens förslag skapar en farhåga för att det idag etablerade tillsynsamordningsforumet under MSB:s försorg endast kommer att ha tid att hjälpa länsstyrelserna och andra tillsynsmyndigheter att samordna sina tillsynsinsatser och sprida information om vilka tillsynsmyndigheter som har agerat gentemot vilka verksamhetsutövare i syfte att exempelvis undvika dubbelbestraffning. Därmed riskerar viktigt erfarenhetsutbyte, harmonisering av tillsynen och andra åtgärder för en effektiv och likvärdig tillsyn, vilket blir än mer aktuellt med ett nytt regelverk och fler tillsynsmyndigheter, att åsidosättas. För att i största mån undvika detta anser Transportstyrelsen att regleringen, såsom idag, bör knyta an till leveransen av den samhällsviktiga tjänsten (jfr ovan avsnitt 5.2.2 Verksamhetsutövare).

Tillsyn över kollektivtrafik?

Transportstyrelsen föreslås som tidigare nämnts bli tillsynsmyndighet för området transport (samt viss del av tillverkningssektorn). Sektor transport inkluderar enligt bilaga 1 till NIS2-direktivet delsektorerna lufttransport, järnvägstransport, sjöfart och vägtransport. Frågan som uppstår är huruvida Transportstyrelsen har något tillsynsansvar över kollektivtrafik, exempelvis spårväg och tunnelbana, som alltså inte utgör en delsektor i bilaga 1 men som Transportstyrelsen idag utövar tillsyn över i andra sammanhang.

Viss kollektivtrafik bedrivs även i regional regi. Som framgått föreslås de olika länsstyrelserna bli tillsynsmyndighet över offentlig förvaltning, vilket bl.a. inkluderar regioner.[16] Eftersom hela verksamheten omfattas enligt

[16] Delbetänkande 8 § förordning om cybersäkerhet.

utrednings förslag skulle detta kunna innebära att länsstyrelsen blir tillsynsmyndighet över spårväg och tunnelbana, som bedrivs i regional regi.

Med anledning av ovan är det viktigt att det förtydligas om kollektivtrafik innefattas i Transportstyrelsens ansvarsområde eller inte. Det ska härvid särskilt beaktas att till skillnad från NIS2-direktivet ingår kollektivtrafik som en delsektor i sektor transport enligt bilagan till CER-direktivet[17]. På grund av den nära kopplingen mellan de båda direktiven bör Transporstyrelsen även bli tillsynsmyndighet för kollektivtrafik enligt cybersäkerhetslagen, och det är högst olyckligt om länsstyrelserna blir tillsynsmyndighet fram tills CER-direktivet omhändertas.[18]

9 kap. Ingripanden och sanktioner

9.3 Vilka överträdelser kan läggas till grund för sanktioner?

Enligt utredningens förslag ska ett antal överträdelser ligga till grund för tillsynsmyndighetens ingripande.[19] Transportstyrelsen välkomnar utredningens förslag om att det även ska vara möjligt att utfärda ett föreläggande vad gäller verksamhetsutövare som har underlåtit att anmäla sig, istället för som idag endast kunna besluta om sanktionsavgift.

Transportstyrelsen kan däremot konstatera att skyldigheten för verksamhetsutövaren att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, som föreslås i 3 kap. 2 § förslag till lag om cybersäkerhet, inte är en skyldighet vars åsidosättande ska kunna föranleda ett ingripande. Detsamma gäller idag enligt 28-29 §§ NIS-lagen[20]. Transportstyrelsen anser att ett långsiktigt, kontinuerligt och metodiskt informationssäkerhetsarbete där verksamhetens ledning styr och är involverade i arbetet är av största vikt, inte minst för att säkerställa direktivets krav på riskhanteringsåtgärder och incidentrapportering. Det är således en brist i dagens reglering att tillsynsmyndigheterna inte har mandat att ingripa vid brister i det systematiska informationssäkerhetsarbetet. Transportstyrelsen anser därför att även åsidosättande av kravet på ett systematiskt och riskbaserat informationssäkerhetsarbete enligt lagen eller föreskrifter meddelade av lagen ska kunna leda till ett ingripande av tillsynsmyndigheterna, såväl vad gäller föreläggande, sanktionsavgift som förbud att utöva ledningsansvar.

---

[17] Europaparlamentet och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.
[18] Jfr s.7 Kommittédirektiv 2023:30 Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft – om att tillsynsmyndigheterna enligt CER-direktivet som utgångspunkt bör vara desamma som tillsynsmyndigheterna enligt NIS2-direktivet.
[19] Delbetänkandet 5 kap. 1 § lag om cybersäkerhet.
[20] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

9.4.2 Vad ska beaktas särskilt vid val av sanktion och utformningen av dem?

Utredningen föreslår i 5 kap 3-4 §§ förslag till lag om cybersäkerhet att tillsynsmyndigheterna vid val av ingripandeåtgärd enligt 2 §, dvs. föreläggande, förbud mot att utöva ledningsfunktion eller sanktionsavgift, tar hänsyn till ett antal faktorer. Av 5 kap. 6 § följer dock att tillsynsmyndigheten får meddela de föreläggande som behövs för att verksamhetsutövaren ska uppfylla skyldigheterna som framgår av lagen och av 5 kap. 8 § följer att det endast är om ett föreläggande inte följts, och överträdelsen bedöms som allvarlig enligt 5 kap. 5 §, som tillsynsmyndigheten får ingripa mot en person som ingår i verksamhetsutövarens ledning.

Transportstyrelsen anser därmed att det som behöver framgå av lagen är endast under vilka förutsättningar som tillsynsmyndigheten ska ta ut en sanktionsavgift och vilken storlek sanktionsavgiften ska bestämmas till (jfr exempelvis 7 kap. 3 och 5 §§ säkerhetsskyddslagen (2018:585)). Genom att använda *eller* i 5 kap. 2 § framstår det också som att tillsynsmyndigheterna inte kan ta ut sanktionsavgift vid val av andra ingripandeåtgärder, vilket som framgår av utredningen inte är avsikten.

Omständigheter som ska beaktas

Tillsynsmyndigheterna ska enligt 31 § NIS-lagen idag ta hänsyn till tre faktorer vid bedömning av sanktionsavgiftens storlek; den skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse och de kostnader som leverantören har undvikit till följd av överträdelsen. Därtill anges i förarbetena ett antal omständigheter som kan påverka beloppets storlek men som inte bedömdes behöva tas in i lagen.[21] Enligt utredningens förslag följer inte mindre än nio omständigheter som *ska* beaktas vid bedömningen. Därtill tillkommer ett antal omständigheter som tillsynsmyndigheterna ska beakta för att bedöma huruvida överträdelsen är att anse som allvarlig eller inte.[22]

Transportstyrelsen anser inte att det är rimligt för tillsynsmyndigheterna att bygga en sanktionsmodell som alltid tar hänsyn till – och tillsynsmyndigheten därmed behöver utreda – alla de omständigheter som anges i den föreslagna lagen, exempelvis hur länge en överträdelse har pågått. En ordning som den nuvarande där vissa omständigheter framgår av lagen och andra av förarbetena skapar däremot en nödvändig flexibilitet vid bedömningen. Transportstyrelsen anser därför att de nuvarande omständigheterna som framgår av 31 § NIS-lagen och som

[21] Se s. 71f. proposition 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster.
[22] Delbetänkandet 5 kap. 3-4 §§ lag om cybersäkerhet.

tillsynsmyndigheterna redan har byggt en sanktionsavgiftsmodell kring även ska vara de omständigheter som ska följa av den nya lagen om cybersäkerhet.

Omständigheter som ska göra att en överträdelse allvarlig, Oriktiga uppgifter

Som framgått ska tillsynsmyndigheterna även ta ställning till om en överträdelse är att beakta som allvarlig eller inte. En omständighet som ska leda till att en överträdelse betraktas som allvarlig är om verksamhetsutövaren har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter.[23] Enligt utredningen avses med ”oriktig uppgift” felaktiga eller missvisande uppgifter, men även utelämnande uppgifter som borde ha lämnats. Av direktivet följer i detta avseende att det ska vara fråga om ”tillhandahållande av *falsk* eller *grovt felaktig* information” (artikel 32.7 a) v)). Oriktiga uppgifter förefaller således mer vittgående och det framgår inte av utredningen varför man inte har valt att följa direktivtexten. Eftersom konsekvensen av överträdelsen är stora då det kan föranleda ett förbud mot att utöva ledningsfunktion, bör lagtexten istället återspegla direktivet i detta avseende.

Omständigheter som ska göra en överträdelse allvarlig, Effekten av att en överträdelse är att betrakta som allvarlig

Av förslaget till den nya lagen framgår att överträdelser som betraktas som allvarliga kan ligga till grund för en ansökan om förbud för en person att vara befattningshavare hos en viss verksamhet.[24] Någon annan konsekvens anges inte utan ska enligt utredningen beaktas som en del av tillsynsmyndigheternas helhetsprövning. Av utredningen följer dock att om en överträdelse är att anse som allvarlig kan det leda till att tillsynsmyndigheten bestämmer ett vite eller en sanktionsavgift till ett högre belopp. Transportstyrelsens anser att detta bör framgå av lagen, inte minst för att skapa en förutsebarhet för verksamhetsutövarna.

9.5.5 Tillfälligt upphävande av auktorisation eller certifiering

Transportstyrelsen instämmer helt i utredningens bedömning att det inte ska införas någon möjlighet till tillfälligt upphävande av en väsentlig verksamhetsutövares auktorisation eller certifiering, eftersom Sverige inte har infört något krav på att verksamhetsutövaren ska beviljas tillstånd eller certifikat för att bedriva den typ av verksamhet som gör att de träffas av cybersäkerhetslagen.

Transportstyrelsen kan dock konstatera att andra länder (såsom Belgien) har valt en annan väg, nämligen att införa ett certifikat för verksamhet som

[23] Delbetänkandet 5 kap. 5 lag om cybersäkerhet.
[24] Delbetänkandet 5 kap. 8 § 3 stycket lag om cybersäkerhet.

uppfyller kraven enligt NIS2-direktivet. Med en sådan ordning är det också rimligt att under vissa omständigheter tillfälligt kunna upphäva certifikatet. Utredningen syntes dock inte ha utrett om certifiering skulle kunna vara en möjlig lösning. Enligt Transportstyrelsens mening finns det fördelar med att införa certifiering och anser därför att det är något som utredningen åtminstone borde ha övervägt att införa i Sverige.

9.6.1 För vilka överträdelser ska sanktionsavgifter införas och när får sanktionsavgift tas ut?

Till skillnad från idag föreslår utredningen att tillsynsmyndigheterna *får* besluta om att ta ut sanktionsavgift vid vissa överträdelser.[25] Transportstyrelsen välkomnar detta förslag. Dagens ordning enligt vilken tillsynsmyndigheterna *ska* ta ut en sanktionsavgift förefaller i vissa situationer omotiverad och allt för betungande, exempelvis om en verksamhetsutövare i många avseenden uppfyller lagens och Transportstyrelsens krav på riskhanteringsåtgärder men brister i något hänseende.

12 kap. Konsekvensanalys

12.6.7 Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för samhällsskydd och beredskap

Utredningen föreslår att befintliga tillsynsmyndigheter, inklusive Transportstyrelsen, ska få ett förstärkt anslag för löpande kostnader med två miljoner kronor vardera för år 2025. Utredningen föreslår vidare att regeringen ska ge Statskontoret i uppdrag att klarlägga de löpande kostnaderna för tillsynsmyndigheterna och MSB för tiden från och med den 1 januari 2026.

Transportstyrelsen har till utredningen uppskattat sin kostnad till 18 miljoner kronor per år (exklusive kostnad för teknisk utveckling och systemstöd) dvs. sammanlagt för treårsperioden skulle kostnaden bli 54 miljoner kronor, vilket inte inkluderar kostnader för teknisk utveckling och systemstöd.[26] Antal tillsynsobjekt förväntas öka från 130 stycken till ca 750 stycken, dessutom blir Transportstyrelsen tillsynsmyndighet för två delsektorer inom den nya sektorn tillverkning.

Transportstyrelsen anser att ett utökat anslag på två miljoner kronor är långt ifrån tillräckligt för att kunna omhänderta NIS2-direktivet. Vid sidan av utredningens förslag om att tillsynsmyndigheterna ska ta fram föreskrifter och vägledning kommer myndigheten att initialt behöva lägga mycket resurser på informationsinsatser (inklusive etablera kontaktvägar till nya

[25] Delbetänkandet 5 kap. 12 § lag om cybersäkerhet.
[26] Delbetänkandet s. 348f.

målgrupper) och samordna tillsynsarbetet med övriga tillsynsmyndigheter – vilket Transportstyrelsen ser ett ökat behov av med en ny reglering, fler tillsynsmyndigheter och överlappande tillsynsområden.

Vidare visar erfarenhet från implementeringen av det ursprungliga NIS-direktivet att arbetet med att identifiera verksamhetsutövare inom myndighetens ansvarsområde och att utföra anmälningstillsyn avseende de verksamhetsutövare som inte anmäler sig frivilligt tar lång tid och mycket resurser i anspråk. Dessutom behöver myndigheten ta fram nya sanktionsmodeller, rutiner, mallar och checklistor för tillsyn enligt nya regler. Sammantaget ser Transportstyrelsen att förslaget om förstärkt anslag på endast två miljoner, tvärtemot utrednings avsikt, skulle fördröja myndighetens möjlighet att utöva tillsyn över verksamheters riskhanteringsåtgärder och systematiska informationssäkerhetsarbete, såväl händelsestyrd som planerad.

Övriga synpunkter

Begreppet *hanterade säkerhetstjänster* som definieras i 1 kap. 2 § 16 och 17 förslag till lag om cybersäkerhet borde rimligtvis istället vara hanterande säkerhetstjänster. Det är inte tjänsterna som hanteras, utan tjänsterna som hanterar cybersäkerhetsrisker.

I definitionen av *verksamhetsutövare* i 1 kap. 2 § 33 förslag till lag om cybersäkerhet nämns leverantör två gånger.

Hänvisningen i 5 kap. 2 § 1 stycket 2 förslag till lag om cybersäkerhet till 7 § avseende förbud mot att utöva ledningsfunktion är felaktig, då detta istället följer av 8 §.

Transportstyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer inom transportsektorn förkortas TSFS 2022:14, inte TFFS 2022:14 som nämns i delbetänkandet på s. 84 och s. 211.

Införandet av EU-direktivet i svensk lag 1 januari 2025 kräver omprioriteringar av berörda verksamheter inom Transportstyrelsen. Ett senareläggande av införandet borde utredas.

Beslut i detta ärende har fattats av generaldirektör Jonas Bjelfvenstam. I den slutliga handläggningen av ärendet deltog överdirektör Ann-Cathrine Wikström, säkerhets- och säkerhetsskyddschef Peter Gustavsson, sektionschef Tomas Åström, inspektör Karin Wahrby och informationssäkerhetsansvarig Daniel Jönsson, den senare föredragande.