Svenska Flygbranschen
Ett förbund inom TRANSPORTFÖRETAGEN

Myndigheten för samhällsskydd och beredskap
Attn: Helena Andersson
651 81 Karlstad
Via email: registrator@msb.se

Stockholm 2018-09-04

Ref Remiss av MSB:s föreskrifter NIS-direktivet

Hej Helena,

Svenska Flygbranschen (SFB) lämnar härmed kommentarer på Remissen av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter angående genomförandet av NIS Direktivet i Sverige.

Genomförandet av NIS Direktivet i Sverige kommer att påverka många av SFB's medlemmar direkt. SFB vill därför tacka MSB för att erbjuda oss tillfälle att delta i arbetet på ett metodiskt och effektivt sätt.

Kommentarer:

a) Användning och tillit till befintliga system för informationssäkerhet och hantering av IT incidenter

SFB vill redan från början uppmärksamma det vi ser som MSBs viktigaste utgångspunkt i remissen. I konsekvensutredningen noterar MSB att de flesta leverantörer antagligen redan idag arbetar med informationssäkerhet och hanterar IT incidenter. Man bedömer därför att den tillkommande kostnaden för leverantören att rapportera incidenter till MSB är begränsad eftersom företagen redan har rutiner för att upptäcka och hantera incidenter.

När det gäller själva rapporteringen till MSB av incidenter noterar MSB vidare att befintliga arbetsprocesser och rutiner sannolikt måste anpassas för att stämma överens med föreskrifterna och för det tekniska gränssnittet för rapportering. Men man bedömer att tillkommande administrativa kostnader för extern rapportering inte är omfattande eftersom intern rapportering ofta finns.

Då de flesta av SFBs medlemmar som omfattas av reglerna redan arbetar systematiskt med informationssäkerhet och hanterar IT incidenter i enlighet med branschstandarder, vill vi bekräfta MSB utgångspunkt men framförallt vädja till inblandade myndigheter att man i så hög grad som möjligt lutar sig mot dessa system i sitt regel- och tillsynsarbete. Varje annat synsätt kommer att medföra väldigt stora kostnader för dessa företag och i så fall faller argumentationen i konsekvensutredningen.

Konkret anser SFB att denna viktiga utgångspunkt måste synas ännu tydligare i reglerna, dvs att reglerna klart ger företagen möjligheten att använda befintliga system för att uppfylla sina åtaganden under NIS-regelverket men även att tillsynsmyndigheten i sitt arbete måste 'acceptera' dessa vid sin

Svenska Flygbranschen Storgatan 19, Box 5384, 102 49 Stockholm
Tel 08 762 71 00 ***E-post*** sfb@transportforetagen.se ***Hemsida*** transportforetagen.se/sfb

tillsyn. Naturligtvis måste vissa anpassningar av befintliga system göras, precis som MSB noterar i remissen, men i stort blir då uppgiften för företaget att fokusera på eventuell skillnad mellan sitt befintliga system och NIS-kraven, samt för tillsynsmyndigheten att titta på helheten inklusive befintliga system och att företaget hanterat *skillnaden* korrekt.

b) Vad konkret den samhällsviktiga tjänsten är?

Mer vägledning efterlyses för att hjälpa företagen analysera vad den samhällsviktiga tjänsten är. I lag 2018:1174 2§4 står att en samhällsviktig tjänst är ”en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet”. Ett flygbolag transporterar passagerare och gods från A till B inom en viss tid. Är den samhällsviktiga tjänsten då att enbart transportera mellan A och B eller även att göra det inom viss tid? Vi söker MSBs vägledning i denna fråga så att företagens analys blir korrekt och harmoniserad.

c) Gränsytor till andra leverantörer av samhällsviktiga tjänster

Det framgår inte i remissen hur gränsytorna till andra leverantörer av samhällsviktiga tjänster ska dras/hanteras och vi önskar mer vägledning här. Många störningar ”ägs” av någon annan leverantör men drabbar våra medlemmar. Till exempel får en IT-störning hos flygtrafikledningen stora konsekvenser för flygbolagens verksamhet. Likaså påverkar en störning vid en flygplats’ informationssystem produktionen av flygningar. Vår utgångspunkt här är att bara de störningar som ”ägs” av en leverantör omfattas av NIS-regleringen, dvs bara störningar som ligger inom leverantörens rimliga kontroll och ansvar, omfattas av t.ex. rapporteringsplikten. Vi noterar och accepterar i sammanhanget att leverantören är ansvarig för sina underleverantörer som utför sådan verksamhet.

d) Rapportera, till vem?

Flyget är internationellt och en störning som sker i Sverige kan få stora följdverkningar i andra länder, t.ex. då trafiken går i en slinga. Om många passagerare i andra länder påverkas – direkt eller indirekt – kan fråga uppstå vem operatören ska rapportera till. Här förutsätter vi att rapporteringen enbart ska gå till det land som utfärdat AOC’et. Då denna aspekt inte diskuteras i remissen vill vi lyfta upp den till MSB för kommentar.

e) Skillnad på trafik och trafik

Förutom att chartertrafik inte omfattas gör de föreslagna reglerna ingen skillnad på vilken typ av trafik som bedrivs. Men vi menar att det finns en skillnad här eftersom det i Sverige finns olika typer av reguljär trafik: upphandlad och icke-upphandlad. Att en upphandlad linje verkligen får sina reglerade (oftast få) avgångar per dag står i stark kontrast till att alla avgångar på en högtrafikerad icke-upphandlad linje äger rum. På t.ex. sträckan Stockholm-Malmö är dessutom flera operatörer aktiva och det är ett stort antal flygningar per dag. De föreslagna reglerna tar inte hänsyn till detta utan hanterar all trafik på samma sätt. Men konkret kan en mindre störning på en upphandlad linje med låg volym ha stora samhälleliga konsekvenser som vida överstiger en störning på en vältrafikerad linje. Vi vill uppmärksamma MSB på detta förhållande och efterlyser er syn på frågan.

f) Sekretess, hantering och rapportering av inrapporterade incidenter

Remissen tar inte upp frågan om sekretess för inrapporterade incidenter, och hur hanteringen och vidarerapporteringen av incidenterna ska gå till. SFB menar att denna fråga måste uppmärksammas i den fortsatta beredningen och garantera företagen ett fullgott skydd för sina inrapporterade uppgifter då rapporterna kommer att innehålla mycket känslig information, både it-säkerhetsrelaterad information och information om verksamheten. Som en jämförelse är sekretessen inom flygsäkerhetsområdet för inrapporterade händelser väl utvecklad och helt central för att rapporteringen ska fungera. Vi menar att ett motsvarande skydd måste finnas när det gäller NIS-rapporter. Vi vill även veta vad som kommer att rapporteras vidare i myndigheternas egen offentliga statistik samt vad som kommer att delas med EU samt med andra myndigheter (i Sverige eller andra länder). Vi vill understryka hur viktig den här frågan är för våra medlemmar.

g) Frivillig rapportering

När det gäller den frivilliga rapporteringen observerar vi att den *inte* gäller leverantörer som redan omfattas av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Eftersom 3§1 i lagen, med sin hänvisning till bilaga 2 av NIS direktivet medför att samtliga flygbolag med operativ licens omfattas av lagen, ser vi ingen större konsekvens av den frivilliga rapporteringen.

Men vi vill gärna förstå anledningen till varför MSB redan nu avser införa frivillig rapportering. Enligt förordningen 15§ är det inget krav för MSB att införa frivillig rapportering och eftersom leverantörer som omfattas av lagen (2018:1174) inte omfattas av den frivilliga rapporteringen är det svårt för oss att se fördelarna med att i nuläget införa denna extra uppgift och administration i systemet.

h) Avgränsningen för sjötransporter

Av förslag till föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, 4 kap. 3§ framgår, såvitt vi kan se, att *sjöfart med passagerartrafik* inte omfattas. Detta trots att Direktivets bilaga 2 definierar tillämpningsområdet att täcka transportföretag som bedriver *persontrafik* och godstrafik på inre vattenvägar, till havs och längs kuster […]. SFB undrar därför med vilket stöd MSBs har avgränsat tillämpningsområdet att *inte* gälla sjöfart med passagerartrafik?

i) Tidsfrist och metod för rapportering

I direktivets art. 16 står att rapportering skall ske utan onödigt dröjsmål. Samma text ”utan onödigt dröjsmål” finns i 18§ i lagen (2018:1174). MSB’s har fått ett bemyndigande i förordningen (2018:1175) att meddela närmare föreskrifter om inom vilken tid incidentrapportering ska göras. MSB har i 2§ i förslaget om föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, definierat tidsfristerna för rapporteringen på följande sätt:

- Redovisa 3§ punkterna 1-8 utifrån en initial bedömning, ”utan onödigt dröjsmål, dock senast sex timmar från det att leverantören har identifierat en incident som rapporteringspliktig”.
- Kompletterande rapport, inkl. planerade åtgärder för att minimera följderna av incidenten, ”inom 24 timmar”.
- Fullständig rapport, inkl. vidtagna och planerade åtgärder för att förhindra upprepning av liknande incidenter, ”inom fyra veckor”.

När en rapporteringspliktig händelse inträffar måste företaget först och främst ta ansvar för sina passagerare, sin personal samt att säkerheten upprätthålls. Samtidigt sätts den interna processen att processa störningen igång vilket kräver stora resurser och ett stort fokus från inblandad personal. Att i detta läge dessutom kräva en relativt omfattande rapportering redan inom 6 timmar anser vi inte kan göras utan men för verksamheten. Samtidigt förstår vi betydelsen av att myndigheten får in rapporter om störningen i ett tidigt stadium så att man bl.a. kan identifiera dess omfattning och om det t.ex. rör sig om en storskalig cyberattack. För att möta detta behov, men för att avlasta företaget i ett svårt läge, förslår SFB istället följande rapporteringssekvens:

- Inom 12 timmar: informera kortfattat om händelsen.
- Inom 12-24 timmar: Redovisa 3§ punkterna 1-8 utifrån en initial bedömning.
- Inom 2 veckor: Kompletterande rapport, inkl. planerade åtgärder för att minimera följderna av incidenten.
- Inom 4 veckor: Fullständig rapport, inkl. vidtagna och planerade åtgärder för att förhindra upprepning av liknande incidenter.

Rapporteringen inom 12 timmar görs bäst i en i förväg definierad form, t.ex. rapporteringsmall, men kan även behöva göras per telefon eller liknande beroende på vilka system som finns tillgängliga under störningen. Stor flexibilitet anmodas här och principen bör vara ”enkelt - snabbt”. Genom att uppge kontaktperson för händelsen i mallen kan ansvarig myndighet lätt få mer information om så behövs.

Angående rapportering vill SFB även veta vilka krav som kommer att ställas på mottagarsidan. Rapportering måste kunna göras även om befintliga system ligger nere, måste vara tillförlitligt och erbjuda tekniskt skydd för informationen (hård kryptering). Dessutom framgår inte av underlagen hur mottagande myndighet ska hantera rapporten och vi föreslår att detta tydliggörs i reglerna (se även ovan gällande sekretesskrav).

j) Spridande av relevant information, rapporter

I ett läge där en eller flera leverantörer upplever störningar och rapporterar dessa till myndigheten är det mycket viktigt att andra leverantörer snabbt får ta del av störningsinformationen för att eventuellt vida skyddsåtgärder. Det framgår inte av underlagen hur denna spridning av information ska gå till och vilka krav som kommer att ställas på myndigheten och informationsspridnings-systemet. SFB menar att informationsflödet måste vara konstruerat att det går ”båda vägarna” för att vi ska uppnå de positiva effekter som våra medlemmar förväntar och som lagstiftningen förutser och anser att regleringen bör omfatta även denna viktiga aspekt.

Med vänlig hälsning,

Fredrik Kämpfe
Branschchef
Svenska Flygbranschen

Svenska Flygbranschen Storgatan 19, Box 5384, 102 49 Stockholm
Tel 08 762 71 00 ***E-post*** sfb@transportforetagen.se ***Hemsida*** transportforetagen.se/sfb