Luftfartstilsynet

Notat

Dato
30.09.2021

Referanse
20/21928-5

Saksbehandler
Sissel W. Strandås, tlf. +47 99778755

Kopi til

Høring - Opinion 03/2021 - Management of Information Security Risks

1. Bakgrunn

EASA publiserte 11. juni 2021 Opinion 03/2021 med tittel *Management of information security risks*. Heretter omtalt som Opinion 03/2021.

En finner Opinion 03/2021 og dets vedlegg ved å følgen lenken her:

https://www.easa.europa.eu/document-library/opinions/opinion-032021

EU har på luftfartsområdet igangsatt et arbeid innen digital sikkerhet/informasjonssikkerhet (cyber security) og forslag til mandat for prosjektet Cyber security risks ble publisert januar 2019.

Formålet er å skape et regulatorisk system som på en effektiv måte vil bidra til å beskytte luftfarten mot angrep mot informasjonssikkerheten og mulige konsekvenser av slike angrep. Bakgrunnen er en erkjennelse av at dagens regelverk, ikke i tilstrekkelig grad ivaretar behovet innenfor luftfarten for beskyttelse mot at eksisterende digitale svakheter utnyttes av personer med onde hensikter. Risikoen for slike hendelser har økt i tråd med digitaliseringen og sammenkoblingen av systemene i luftfarten. Stadig flere systemer er koblet mellom hverandre og til flyene.

De stilles krav til både myndigheter og organisasjoner i luftfarten. Kravene handler om å håndtere risiko, herunder identifisere sårbarheter, beskytte seg mot angrep, avdekke og håndtere angrep, samt gjenopprette drift etter angrep som kan påvirke sikkerheten i luftfarten. Dette skal oppnås gjennom et regelverk som skal gjelde for nær sagt alle områder innen luftfarten, eksempelvis produktkontroll, luftdyktighet, luftfartsoperasjoner, bemanning og lufttrafikktjenesten.

Opinion 03/21 har forslag om to nye forordninger som innfører krav til styringssystem for informasjonssikkerhet (ISMS) for tilsynsmyndigheter og aktører i alle deler av luftfarten. I tillegg foreslås endringer i en rekke eksisterende forordninger.

Foreløpig er det identifisert at disse forordningene blir berørt:

- Forordning (EU) nr. 748/2012 (initiell luftdyktighet)
- Forordning (EU) nr. 1321/2014 (kontinuerlig luftdyktighet)
- Forordning (EU) nr. 2017/373 (lufttrafikktjeneste)
- Forordning (EU) nr. 2015/340 (flygeledere)
- Forordning (EU) nr. 139/2014 (landingsplasser)
- Forordning (EU) nr. 1178/2011 (sertifikat til flygende personell)

- Forordning (EU) nr. 965/2012 (luftfartsoperasjoner)
- Forordning (EU) nr. 2021/664 (U-space)

EU har som målsetting at regelverket skal dekke kravene i NIS-direktivet. Hensikten er at når reglene trer i kraft, vil aktører, som også omfattes av NIS-direktivet, oppfylle kravene der ved å følge de nye reglene for luftfarten. For Norges del innebærer dette at NIS-direktivet de facto blir innført for de fleste aktører innen luftfart.

2. Innholdet i Opinion 03/2021

Anslag mot informasjonssikkerheten har potensial til å generere hendelser som kan ha direkte betydning for flysikkerheten. Brudd på informasjonssikkerheten er basert på forskjellige motiver, for eksempel intensjonen og ønsket om å få tilgang til informasjon, skade systemer, forstyrre operasjoner eller trusselen mot tap av menneskeliv.

Det er personer og enheter som er bevisst på jakt etter svakheter i forskjellige systemer, inkludert luftfartssystemer med formål om å skade luftfarten. Potensielle svakheter i systemene er ikke alltid kjent for luftfartsoperatører og andre luftfartsaktører i sivil luftfart. Utnyttelsen av svakheter i informasjonssystemer, selv om de kan virke ufarlige når de vurderes individuelt, kan være kombinert for å forårsake skade som igjen kan ha katastrofale følger. I andre tilfeller kan svakheter i informasjonssystemer av skadelig programvare fordi god informasjonssikkerhet blir neglisjert, og dermed har en negativ effekt på sikkerheten i sivil luftfart.

Svakheter kan være veldig forskjellig; noen forholder seg til maskinvare, noen til programvare, noen til prosesser og noen til den fysiske sikkerheten til et gitt system. Når svakheter kan utnyttes, kalles de sårbarheter. Tidlig reaksjon på kjente sårbarheter er avgjørende for å forhindre potensielle angrep.

Forslag til krav i 03/2021 skal sikre at safety-relaterte systemer i luftfarten er tilstrekkelig beskyttet mot informasjonssikkerhetsrisiko parallelt med det til enhver tid pågående luftfartssikkerhetsarbeidet. Formålet med forslaget er som kjent å ha effektiv beskyttelse av luftfartens informasjonssystemer, beskytte systemer fra hendelser som truer informasjonssikkerheten og gjenoppretter konsekvenser etter evt. angrep. Formålet med regelverket oppnås ved å sette luftfartsorganisasjoner og luftfartsmyndigheter i stand til

- å identifisere og håndtere informasjonssikkerhetsrisiko som kan påvirke informasjon- og kommunikasjonssystemer og data som brukes i sivil luftfart,
- å oppdage hendelser som påvirker eller truer informasjonssikkerheten,
- svare på angrep, og gjenopprette systemer etter hendelser som har påvirket informasjonssikkerheten,
- å gjøre risikovurderinger av egne informasjons- og kommunikasjonssystemer og sikre at relevant data som ikke skal spres, ikke blir spredt,
- å sikre at det etableres styringssystem for informasjonssikkerhet

Opinion 03/2021 inneholder følgende forslag gjengitt som vedlegg I, II, III og IV:

- Vedlegg I: Implementeringsforordning som endrer eksisterende krav til luftfartsmyndigheter som fører tilsyn på alle luftfartsdomener, og organisasjoner på alle luftfartsdomener. Vedlegg I omfatter ikke design- og produksjonsorganisasjoner, flyplassoperatører og tjenesteytere for styring av apron; for disse vil eksisterende regler endres av delegert forordning inntatt som vedlegg III i Opinion 03/2021 (se nedenfor).

Endringene i vedlegg I innfører krav til myndigheter og organisasjoner for å være i stand til å overholde nye Part-IS.AR og Part-IS.OR som finnes i vedlegg II. Samt å legge til nødvendige elementer i regelverket slik at relevant myndighet kan utføre tilsyns- og godkjenningsprosesser.

- Vedlegg II: Implementeringsforordning som introduserer nye krav til informasjonssikkerhet gjennom Part-IS.AR og Part-IS.OR for luftfartsmyndigheter som fører tilsyn på alle luftfartsdomener, og organisasjoner på alle luftfartsdomener. Med unntak av design- og produksjonsorganisasjoner, flyplassoperatører og tjenesteytere for styring av apron – da deres eksisterende regler suppleres av delegert forordning inntatt som vedlegg IV i Opinion 03/2021.

- Vedlegg III: Delegert forordning som endrer eksisterende regler for design- og produksjonsorganisasjoner, flyplassoperatører og tjenesteytere for styring av apron.

  Endringene i vedlegg III er gitt for å sette nevnte organisasjoner i stand til å oppfylle krav etter Part-IS.OR.

- Vedlegg IV: Delegert forordning som introduserer nye krav til informasjonssikkerhet for design- og produksjonsorganisasjoner, flyplassoperatører og tjenesteytere for styring av apron.

Det er viktig å merke seg at selv om det her er to forordninger (implementeringsforordning og delegert forordning) som begge inneholder Part-IS.OR, der hver forordning gjelder ulike sett med organisasjoner, er begge Part-IS-kravene nærmest identiske. Skillet mellom forordningene er gjort for å overholde krav til regelverksprosess etter basisforordningen. Skille mellom disse to regelverksettene har ingen kvalitativ betydning for innholdet.

Vedtakelse av regelverket er ventet i tredje kvartal i 2022. Det er ikke satt endelig implementeringsdato for regelverket, men implementeringsperioden skal vare i ett år etter vedtakelse.

3. Vurdering av regelverket

Ved vurderingen av om forslaget i Opinion 03/2021 på et senere tidspunkt skal tas inn i norsk rett, har Luftfartstilsynet tatt utgangspunkt i de føringer som ligger i regjeringens utredningsinstruks. Et minimumskrav er å besvare følgende seks spørsmål:

- Hva er problemet, og hva vil vi oppnå?
- Hvilke tiltak er relevante?
- Hvilke prinsipielle spørsmål reiser tiltakene?
- Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?
- Hvilket tiltak anbefales, og hvorfor?
- Hva er forutsetningene for en vellykket gjennomføring?

a) Hva er problemet, og hva vil vi oppnå?

Problemene som ønskes løst med forslaget slik det er i Opinion 03/2021 er at man i for liten grad har regulert informasjonssikkerheten i luftfartens systemer når det har vist seg at risikoen for angrep mot informasjonssikkerheten og utnyttelsen av sårbarheten i systemene har økt.

Forslaget fokuserer på konsekvensene som trusler og hendelser mot informasjonssikkerheten i luftfartens systemer kan ha for sikkerheten i sivil luftfart. Luftfarten er et system av systemer som kan omfattes av flere krav (NIS-direktiv og forordning (EU) 2015/1998). Innholdet i Opinion 03/2021 skal

skape et sømløst og konsistent regelverk der grensesnittene mellom safety og security blir dekket. Foreslåtte krav søker også å demme opp for hull og duplikasjoner i ulike regelverksett som har samme formål.

Luftfartsmyndigheter og luftfartsorganisasjoner skal gjennom etablering av ISMS (*information security management system*) kunne ha kontroll på informasjonssikkerheten i virksomheten. De som omfattes av regelverket må gjøre en risikoanalyse og angi hva er akseptabel risiko og hva er gjeldende prinsipper for håndtering av risiko knyttet til informasjonssikkerheten. Organisasjoner og myndigheter må ha på plass tiltak for å håndtere uakseptabel risiko knyttet til informasjonssikkerheten, samt være i stand til å detektere uønskede hendelser, respondere og gjenopprette normaltilstand etter angrep.

b) Hvilke tiltak er relevante?

Norge har gjennomført de fleste forordninger som forslaget i Opinion 03/2021 tar sikte på å endre og supplere med nye krav. Riktignok er ikke forordning (EU) 2021/664 (U-space), som er hjemlet i ny EASA-basisforordning (EU) 2018/1139 åer dags dato hverken tatt inn i EØS-avtalen eller gjennomført i norsk rett.

Forslaget slik det fremstår per nå legger opp til at Norge må etablere en egen forskrift som fastsetter krav som gjelder for relevante myndigheter.

Siden forslaget slik det er per nå, både gjør endringer i eksisterende forordninger samt pålegger norske luftfartsaktører og myndigheter nye krav, anses det eneste aktuelle tiltaket å gjennomføre forordningene gjennom EØS-avtalen og nasjonale forskrifter.

c) Hvilke prinsipielle spørsmål reiser tiltakene?

Regelverket reiser etter Luftfartstilsynets vurdering ingen spørsmål av prinsipiell karakter slik dette er beskrevet i utredningsinstruksen.

d) Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?

Den viktigste positive siden av det foreslåtte regelverket er at det sørger for en mer effektiv måte å beskytte luftfarten mot angrep mot informasjonssikkerheten og mulige konsekvenser av slike angrep. Styrking av informasjonssikkerheten har fordeler for de som er involvert i sivil luftfart på en eller annen måte. Å sikre sårbarheter og avdekke potensielle svakheter i systemene som opprinnelig ikke var godt kjent for virksomheten er utelukkende positivt for sikkerheten i luftfarten. Trygg informasjonssikkerhet er viktig i alle ledd for å unngå at informasjon på avveie brukes til å påvirke sikkerheten i luftfarten. Det handler om at alt fra opplysninger gitt fra passasjerer i forbindelse med billettbestilling til informasjon om selskapenes sikkerhetsstyring ikke kommer på avveie eller benyttes på en slik måte at det påvirker sikkerheten i luftfarten på en negativ måte.

De negative sidene ved regelverksforslaget knytter seg til kostnader. Det kan bli kostbart å imøtekomme alle nye krav til informasjonsstyringssystemer, som særlig retter seg mot luftfartsorganisasjoner. Spesielt økonomisk krevende venter vi at det vil være for mindre luftfartsaktører. Vi antar at større luftfartsaktører i Norge allerede har på plass systemer som ivaretar informasjonssikkerheten i mer eller mindre grad i dag. For eksempel vil aktører som Avinor Flysikring AS ikke nødvendigvis merke kostnadsmessige ulemper med de nye kravene da systemene sannsynligvis allerede er etablert.

Annen potensiell negativ side er at både organisasjoner og myndigheter må etablere løsning for rapportering av uønskede hendelser. Slik rapportering skal foregå på siden av systemet som er

etablert gjennom forordning (EU) 376/2014 (rapporteringsforordningen). Det er usikkert om det vil oppleves som en ulempe å ha to måter å rapportere på innenfor luftfarten da rapporteringsforordningen er godt innarbeidet i luftfartsmiljøet. Det er verdt å merke seg at rapportering av uønskede hendelser som skissert i Opinion 03/2021 kan sies å ha samme formål som rapportering av hendelser etter rapporteringsforordningen, men behandling og oppbevaring av informasjonen er ulik. Det kan tenkes at ulempen er størst for myndigheten som skal håndtere informasjonen ved siden av rapporteringsforordningen.

e) Hvilket tiltak anbefales, og hvorfor?

Luftfartstilsynets deltar i Forum for digital sikkerhet i luftfarten hvor flesteparten av norske luftfartsforetak er representert. Innholdet i Opinion 03/2021 har vært gjennomgått og presentert for deltakerne i forumet. Luftfartstilsynet forstår det slik at deltakerne i forumet er positive til det nye regelverket. Det er foreløpig ikke identifisert at det er utfordringer knyttet til implementeringsperioden frem til en senere fastsatt dato i 2023.

Forslaget i Opinion 03/2021 vil bety endringer i gjeldende forskrifter i tillegg til etablering av ny forskrift for å sikre blant annet gjennomføring av myndighetskrav og der det ellers er påkrevd. Luftfartstilsynet påpeker at regelverket er i tidlig fase. Hittil har behandlingen i EASA-komiteen vært begrenset til presentasjon av regelverket. Det er ventet at regelverket i større grad vil være gjenstand for diskusjon i komitemøter i 2022. Formålet med høring av Opinion 03/2021 i denne sammenhengen er informasjonsdeling. Luftfartstilsynet har hittil ikke identifisert behov for nasjonale tilpasninger slik forslaget fremstår per nå. Vi ber høringsmottakerne gi tilbakemelding dersom de ser sådanne behov.

Luftfartstilsynet vil gjennomføre høring av forskriftsendringer i de ulike regelverksettene som påvirkes av forslaget i Opinion 03/2021, og ny forskrift som pålegger nye krav til organisasjoner og myndigheter.

f) Hva er forutsetningene for en vellykket gjennomføring?

Forutsetningene for en vellykket gjennomføring er at luftfartsmyndigheter og luftfartsaktører som berøres klarer å implementere og følge kravene, innen en senere fastsatt frist.

Det er viktig å merke seg at kravene som foreslås i Opinion 03/2021 er gitt med hjemmel i ny basisforordning (EU) 2018/1139. Ny basisforordning er ennå ikke tatt inn i EØS-avtalen og er dermed ikke gjort gjeldende i norsk rett. Vi forventer at dette vil skje i løpet av 2022.

4. Høring

Luftfartstilsynet understreker at dette regelverksforslaget er gjenstand for ytterligere behandling i EASA-komiteen og at denne høringen har til formål å dele informasjon i tidlig fase. Det er mulig å påvirke innholdet i Opinion 03/2021 i komitemøter i 2022. Høring av nasjonale forskriftsendringer og ny nasjonal forskrift kommer senere og etter hvert som behandling i EASA-komiteen skrider frem. Planlagt vedtakelse er tredje kvartal 2022 med virkning ett år etter vedtakelse.

Vi ber høringsinstansene om å gi sine innspill på bakgrunn av det ovennevnte.

Frist for tilbakemeldinger i denne høringsrunden settes til 1. februar 2022.

Innspill til høringen kan sendes til Luftfartstilsynet på epost postmottak@caa.no, og merkes saksnummer 21/21928.

Spørsmål av faglig karakter kan rettes til seniorrådgiver cyber security Sjur Hartveit (sjh@caa.no), mens spørsmål knyttet til den rettslige prosessen kan rettes til juridisk seniorrådgiver Sissel Walla Strandås (sst@caa.no).