Stellungnahme zum Entwurf
zur Umsetzung der DVO (EU) 2019/1583 der Kommission vom 25. September 2019 zur Änderung der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr
(§§ 9 und 9a LuftSiG)

Vorbemerkungen:

Der Bundesverband der Luftsicherheitsunternehmen – BDLS - bedankt sich für die Möglichkeit zur Stellungnahme zum Entwurf zur Umsetzung der DVO (EU) 2019/1583 der Kommission vom 25. September 2019 zur Änderung der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr (§§ 9 und 9a LuftSiG). Die Mitgliedsunternehmen des BDLS beschäftigen rund 15.000 private Sicherheitskräfte, die u. a. die Aufgaben der §§ 5, 8, 9 und 9a LuftSiG ausüben sowie als Beteiligte der sicheren Lieferkette agieren. Sie sind somit unmittelbar durch die Regelungen des vorliegenden Entwurfes betroffen.

Gerne machen wir von der eingeräumten Möglichkeit zur Stellungnahme Gebrauch.

Vor dem Hintergrund der historischen Vorfälle rund um Cyberangriffe ist es gut, dass wir endlich eine Umsetzungsvorgabe erhalten um die seit 2021 bindenden Vorgaben der EU-KOM in den Betrieben anwenden können.

Vorab ist erneut die Frage aufzuwerfen (wurde bereits im Verbändegespräch im Mai durch den BDLS aufgeworfen) ob dieses Dokument als Teil des Anhanges zum NLSP richtig positioniert ist. Der Anhang des NLSP ist Verschlusssache und ist den Stellen nicht zugänglich.

Weiterhin lässt der vorliegende Entwurf eine etwas detailliertere Abstufung der beteiligten Stellen vermissen. Im vorliegenden Entwurf werden Luftfahrtunternehmen und Fluglatzbetreiber einem Transporteur (i.d.R. Geschäftsführer und Kraftfahrer in einer Person), oder auch einem bekannten Lieferanten für Bordvorräte der ggf. nur mit dem Transport betraut ist, ohne Differenzierung gleichgestellt. Für diese Betriebe ist bereits die Auswertung dieses Maßnahmenkataloges, wie auch die anschließende Durchführung der vorgeschriebenen Risikoanalyse eine ungleich höhere Belastung wie für andere Stellen.

Darüber hinaus ist derzeit keine Reflektion darüber zu finden, wie zu verfahren ist, wenn die Administration eines relevanten KIKS nicht in Deutschland, sondern im internationalen Ausland erfolgt. Gerade im Bereich der bekannten Versender ist dies aber durchaus nicht unüblich.

Demnach drängt sich bei erster Betrachtung des Entwurfes der Verdacht auf, dass die Stellen die eigene Risikoanalyse entsprechend bewerten, um keine Maßnahmen umsetzen zu müssen und so diese Klippen zu umschiffen. Alternativ dazu werden weitere Unternehmen Ihren Status in der Luftsicherheit abgeben (müssen) und demnach bspw. die Kapazitäten für den Transport von Lieferungen, Bordvorräten oder Luftfracht zusätzliche fehlen. Die letzte Welle der Statusrückgabe wurde ja bspw. bei den Transporteuren durch die nicht nachvollziehbare Abschaffung des externen Sicherheitsbeauftragten ausgelöst.

Folgende grundlegende Anmerkungen und Änderungswünsche haben wir:

- Zusammenfassung der Schulungsinhalte in ein Grundmodul für alle Stellen, damit der Schulungsaufwand bei Kooperation unterschiedlichen Stellen sich nicht doppelt
- Die Stellenspezifischen Schulungen/Einweisungen KIKS der einzelnen Stellen on top
- Erreichung von großzügigen Übergangsfristen zur Umsetzung, da hierzu auch die notwendigen personellen Ressourcen sichergestellt werden müssen.

Im Einzelnen

Punkt	Überschrift	Anmerkungen
2	Begriffsbestimmungen	Definitionen: Stelle – ist bereits in der VO(EG) Nr. 300/2008 mit anderer Bedeutung definiert Aufgrund der allgemeinen Zusammenhänge fallen Dienstleister unter die Begrifflichkeit „Stelle“. Eindeutig ist dies jedoch nicht formuliert. Hierzu wäre eine Klarstellung für alle Beteiligten sinnvoll. Im weiteren Verlauf unserer Stellungnahme gehen wir weiterhin davon aus, dass Dienstleister unter den Begriff „Stelle“ fallen. Es wäre im Sinne aller Marktteilnehmer, wenn die Einhaltung bestehender Zertifizierungen (z. B. ISO 27001) anerkannt werden, damit die Systematik solcher Normen demzufolge explizit genehmigt ist.
3	Zuständige Behörde	- Es fehlt im Text eine klare Abgrenzung zu Unternehmen nach § 9a, welche nicht durch das LBA zugelassen werden. Bekannte Lieferanten von Flughafenlieferungen werden, mit Ausnahme von überlassenen Bereichen, durch die Flughäfen anerkannt und unterliegen der Aufsicht durch die zuständigen Landesluftsicherheitsbehörden nach § 8 LuftSiG. - Es ist nicht klar ersichtlich, unter welcher Aufsicht Unternehmen stehen, die mehrere Anerkennungen bzw. Zulassungen nach § 9a LuftSiG führen. So sind eine Vielzahl von Unternehmen als bekannter Lieferant von Bordvorräten und gleichzeitig als bekannter Lieferant von Flughafenlieferungen anerkannt. Hier ist eine Formulierung zu finden, welche verhindert, dass unterschiedliche Behörden abweichende Umsetzungen im Unternehmen verlangen.
4	Ermittlung von KIKS	- Die Stellen (bspw. Transporteure oder auch bekannte Lieferanten oder Versender) sind i.d.R. nicht in der Lage zu bewerten und entscheiden welche ihrer Systeme, auch in „sekundärer Abhängigkeit“ Einfluss auf die Sicherheit des zivilen Luftverkehrs haben können. Wer/Welche Behörde entscheidet abschließend? - Tabelle mit Bereich/Funktion – KIKS, Daten: Zugangskontrollen: sind hier bspw. Aufschaltungen der EMAs auf NSLs der Sicherheitsdienstleister

		mitzuinvolvieren, wenn ja, wie weit? Muss das NSL-Personal auch geschult und geprüft werden? Warum Gefahrenmeldeanlagen? Was hat bspw. eine BMA mit Luftsicherheit zu tun? Kontrolltechnik: sind hier nur vernetzte Geräte gemeint, oder auch die Softwareupdates durch den Hersteller? Informationssicherheit: sind wirklich Laufwerke gemeint, auf denen die Beteiligten der Lieferkette Kopien der Schulungsnachweise und der Zuverlässigkeitsüberprüfungen speichern, oder die Ausweisbüros der Flugplatzbetreiber? - Wo sind greifbare Beispiele für die sichere Lieferkette, bspw. was ist mit Systemen mit denen Luftfrachtbriefe erstellt werden? Was ist mit Systemen auf denen Dokumente mit vergebenen Sicherheitsstatus (Luftfracht) gespeichert oder übertragen werden?
5	Zur Risikobewertung	- Zur Risikobewertung soll bspw. das Lagebild Luftsicherheit des BKAs herangezogen werden. Die Stellen erhalten dieses nicht. - Risikobewertung und Cyberreaktionsplan müssen im Rahmen der nächsten Revision des Sicherheitsprogrammes durch das LBA vorgelegt werden – d.h. bei den Transporteuren wird das u.U. erst in 5 Jahren der Fall sein da sich bei einem Transporteur i.d.R. keine Änderungen stattfinden. Ein Bekannter Lieferant für Bordvorräte hat keine Zulassung des LBAs! Er wird vom reglementierten Lieferanten für Bordvorräte anerkannt. Wie ist damit zu verfahren? Seite 5: Dieser Satz ist nicht eindeutig erläutert: „Bei der Ermittlung der relevanten KIKS ist insbesondere der informationstechnische Zugang zu folgenden Bereichen zu berücksichtigen.“ Es sollte eindeutig und klar formuliert werden, ob beispielsweise die reine <u>Bedienung</u> einer Türsteuerung oder die <u>Konfiguration</u> der Türsteuerung gemeint sein soll. Hierbei sollte deutlich zwischen der reinen Bedienung der relevanten KIKS und der Konfiguration unterschieden und eindeutiger formuliert werden. Im weiteren Verlauf unserer Stellungnahme gehen wir davon aus, dass nur die Konfiguration, also der Systemzugriff, gemeint sein soll. Andernfalls wären hier alle Sicherheitsmitarbeiter und Kontrollpersonen zu schulen. Diese Vorgehensweise wäre nicht verhältnismäßig und nicht zielführend. Die technischen Maßnahmen sowie die einzusetzenden Sicherheitsprogramme und deren Risikobewertung beziehen sich auf die Schutzziele, Verfügbarkeit, Integrität und Vertraulichkeit, auf die BSI-Normen oder alternativ auf die ISO 2700X Familie. Aus unserer Sicht sollte klar definiert werden, ob die Zertifizierung zwingend erforderlich oder eine Anlehnung an den Standard ausreichend ist.

6	Sicherheitsprogramm	„Bei Reaktionen auf einen Cyberangriff sowie der entsprechenden Bewältigung des Angriffs ist insbesondere sicherzustellen, dass der Cyberangriff sich nicht auf di Sicherheit der Zivilluftfahrt auswirkt“. Bitte neue Formulierung: „Bei Reaktionen auf einen Cyberangriff sowie der entsprechenden Bewältigung des Angriffs ist *nach vernünftigen Maßstäben* sicherzustellen, dass der Cyberangriff sich nicht auf di Sicherheit der Zivilluftfahrt auswirkt.“ Welche Stelle koordiniert die weiterführende Maßnahmen bei Luftfahrtunternehmen oder Flugplatzbetreiber, denn diese sind i.d.R. „last Line of defense“
6.1.	Sicherheitsmaßnahmen	Nach dieser Formulierung sind m.E. die Maßnahmen umzusetzen, ob die Stelle nun KIKS identifiziert hat oder nicht. Bitte präzisieren.
6.3	Erkennen von Cyberangriffen	DER.1: Das Dokument hat bereits 8 DIN A4 Seiten, verweist dann noch auf !!17!! Kreuzreferenztabellen. Wie soll das ein KMU umsetzen?
6.4	Reaktion auf Cybervorfälle	Die verschiedenen DER Standards weisen „Muss-Vorgaben“ aus. → KMU Erfüllung??? Hier sind in den meisten KMU die angeführten Rollen und deren Zuständigkeit wohl nicht vorhanden.
7	Zulassung durch die zuständige Behörde	Wie wird das LBA dazu strukturiert? Werden diese Inhalte auch in den Außenstellen geprüft und zugelassen? Wir haben schon bezüglich der Luftsicherheitsvorgaben dort schon keine durchgängig einheitliche Auffassung und Kenntnisstand zu den notwendigen umzusetzenden Maßnahmen!
8	Melde- und Informationswesen	- Alle Unternehmen haben sich zu registrieren? Was sollen die Sicherheitsbeauftragten der Alleinunternehmer noch im Blick haben?? - „Eine eindeutige Antwort, wann eine Störung erheblich ist, nicht möglich.“ Wie soll dann eine Stelle ermitteln können, ob das System relevant ist oder nicht??
9	Zuverlässigkeitsüberprüfungen	Fernzugriff - Protokollierung aller Zugriffe und Tätigkeiten. Überprüfung der Protokolldateien ist durchzuführen die zu dokumentieren ist. In welchem Rhythmus? Wer soll das bei KMU machen/bezahlen? Wahrscheinlich bekommt ein KMU das bei externer Dienstleistung/Unterstützung gar nicht mit. Wir weisen darauf hin, dass am Markt Programme im Einsatz sind, die diese Vorgaben nicht umsetzen können. Es ist nicht genannt, wie lange diese Aufzeichnungen vorzuhalten sind und wie mit Bestandsprogrammen, die diese Vorgaben nicht erfüllen, umgegangen wird.
10.1	Erforderliche Fähigkeiten und Eignung	Welche Eignungen werden erwartet? Es gibt hier keine Beispiele. Diese werden auch von Dienstleistern und Lieferanten erwartet. Wie soll das gehen. Hier haben die Betriebe keine Durchgriffsmöglichkeit.
10.2	Schulungen	- Wer sind die Ausbilder? - Wie wird die Schulung bescheinigt/nachgewiesen?

		- Wie ist eine Anerkennung der Schulung möglich, wenn eine Person aus einem anderen Betrieb eingestellt wird und eine Schulung bereits durchgeführt wurde, wenn die Inhalte nicht für die Stelle ersichtlich sind (Anhang zum NLSP)? - Werden die Schulungsinhalte in der Schulungstabelle (ehemals Modulsystem und Anlage zur LuftSiSchulV) für alle gleich vorgegeben?
10.2.2	Fortbildung	- Jährliche Sensibilisierung ist durchzuführen. Wieder die Frage: wie sensibilisiert sich der Alleinunternehmer → Analogie zur Sicherheitskultur bei Transporteuren!! Eine weitere zusätzliche Schulung deren Fristen individuell auf das jeweilige Schulungsdatum verwaltet werden muss. Die Sensibilisierung macht jeden Unternehmen mit individuellen Inhalten. Wie kann eine solche bei Einstellung einer geschulten und wiederholt sensibilisierten Person durch den einstellenden Betrieb geprüft/anerkannt werden? - Warum muss hier alle 3 Jahre neu geschult werden und nicht wie in der Luftsicherheit üblich im 5 Jahresrhythmus? Sind diese Personen den Luftsicherheitskontrollpersonen in der Gewichtung gleichgestellt (ReZi alle 3 Jahre)? Hier reicht ein 5 Jahresrhythmus definitiv aus.
11	Überwachung	Richtet sich nach dem NQP. - Heißt das es wird Tests im Sinne von Realtests geben? - Wie sind die jährlichen internen Audits dazu zu gestalten, bzw. wie soll die Stelle bewerten, ob der Dienstleister seine Sicherungsaufgaben für die Systeme ordnungsgemäß durchführt (warum wird denn ein Dienstleister eingesetzt?).

Berlin, im September 2023

Impressum

BDLS Bundesverband
der Luftsicherheitsunternehmen
Friedrichstr. 149
10117 Berlin
Telefon +4930275785700
E-Mail mail@bdls.aero