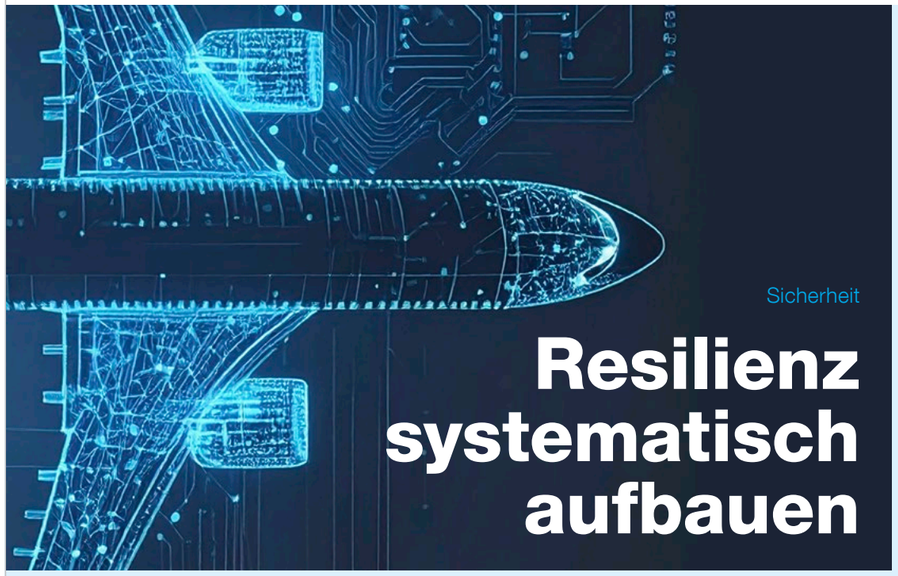

Sicherheit

Resilienz systematisch aufbauen

Erleben wir seit einigen Jahren tatsächlich eine zunehmende reale Gefährdungslage, oder sind wir einer übersteigerten Wahrnehmung ausgesetzt? Cyberangriffe, Sabotage an kritischer Infrastruktur, GPS-Störungen und gezielte Destabilisierung sind heutzutage Teil eines kontinuierlichen hybriden Bedrohungsumfeldes. Die gesamtgesellschaftliche Verantwortung in Sachen Verteidigungsfähigkeit und Resilienz sind längst keine Themen allein für Bundeswehr oder Blaulichtorganisationen. Staat, Wirtschaft, Kommunen und jede einzelne Person müssen sich fragen, welchen Beitrag sie zur Widerstandsfähigkeit leisten können.

Der Staat muss strategische Lagebilder erstellen und Zuständigkeiten klären, rechtliche Rahmenbedingungen schaffen und den Schutz kritischer Infrastrukturen herbeiführen. Die Wirtschaft muss für diese Themen sensibilisiert werden und Maßnahmen ergreifen, die den Staat in seinem Handeln unterstützen. Die Kommunen sind lokal für den Zivilschutz zuständig und sorgen für eine funktionierende Grundversorgung. Resilienz entsteht nicht durch Alarmismus, sondern über das Verständnis für vorhandene Risiken jedes Einzelnen, um handlungsfähig zu bleiben. Die Herausforderung besteht darin, Bedrohungen nüchtern zu analysieren, Wahrnehmungen einzuordnen und Resilienz systematisch aufzubauen.

Es spricht vieles dafür, dass sich das sicherheitspolitische Umfeld real verändert hat. Cyberangriffe auf Verwaltung, Industrie und Gesundheitswesen, Sabotage an Energie-, Kommunikations- und Verkehrsinfrastruktur, GPS-Jamming oder Desinformationskampagnen sind keine hypothetischen Szenarien mehr, sondern mutmaßlich immer wieder vorhanden. Durch die zunehmende Digitalisierung haben wir selbst die Angriffsflächen vergrößert.

Der Kern der Debatte liegt also nicht nur in der Frage der realen Gefährdung, sondern auch darin, wie verwundbar wir insgesamt geworden sind. Verteidigungsfähigkeit und Resilienz sind nicht mehr ausschließlich militärische oder polizeiliche Kategorien, sondern haben mittlerweile eine gesamtgesellschaftliche Dimension erreicht.

Welche Auswirkungen diese allgemeine Lage für den zivilen Bereich hat, zeigt sich in der Notwendigkeit einer neuen Verordnung. Durch die Verabschiedung der Durchführungsverordnung (DVO) (EU) 2019/1583, die seit dem 31. Dezember 2021 in Kraft ist, müssen u. a. Luftfahrtunternehmen zukünftig ein bestimmtes Informationssicherheitsniveau erreichen und garantieren.

Das Ziel der Verordnung sind der Schutz und die Absicherung des zivilen Luftverkehrs vor Cyberangriffen, insbesondere in Bezug auf Sabotageakte und terroristische Anschläge. Hierzu zählen Präventivmaßnahmen im Bereich der Cybersicherheit sowie der Schutz vor entsprechenden Gefahren, aber auch die Detektion von und die Reaktion auf Cyberangriffe. Vor allem der Schutz von kritischen informations- und kommunikationstechnischen Systemen und Daten spielt hierbei eine wichtige Rolle. Außerdem ist der angemessene, praktikable und rechtzeitige Austausch von Informationen über Schwachstellen, Schadsoftware oder Ähnlichem essenziell.

Seit Oktober 2021 ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) damit betraut, die Koordinierung und Steuerung der Maßnahmen zur Informationssicherheit gemäß des § 8 LuftSiG zu übernehmen. Dazu hat das BSI nun eine Broschüre „Cybersicherheit für kleine und mittlere Luftfahrtunternehmen“ herausgebracht.

Diese Broschüre bietet praxisnahe Informationen und Handlungsempfehlungen, wie Luftfahrtunternehmen ihre IT-Infrastruktur, Daten und Geschäftsprozesse vor den wachsenden Cyberbedrohungen schützen können. Dabei gibt die Broschüre wertvolle Impulse, um die Cybersicherheit in kleinen und mittleren Luftfahrtunternehmen zu verbessern. Aufgrund des Checklisten-Charakters eignet sich die Broschüre besonders gut zur Identifizierung von Stärken und Schwächen und liefert zudem konkrete Ansätze, um Maßnahmen gezielt abzuleiten.

75 Prozent aller gewerblichen Luftfahrtunternehmen in Deutschland sind kleine und mittlere Unternehmen – häufig ohne IT-Abteilungen, aber mit hoher sicherheitsrelevanter Verantwortung. Der weit verbreitete Irrglaube in solchen Firmen, sie seien kein attraktives Ziel für Angreifer, wurde deutlich relativiert: Cyberattacken betreffen mittlerweile auch die Luftfahrtbranche in wachsendem Maße.

Ziel muss sein, Cybersicherheit als festen Bestandteil des Alltags in Luftfahrtunternehmen zu verankern – einfach anwendbar, praktisch umsetzbar und branchenweit nutzbar. Aber für die Luftfahrtunternehmen bestehen einige Herausforderungen. Sie stehen vor der Aufgabe, parallel mehrere Regulierungen umzusetzen. Die Abstimmungen zwischen den Abteilungen wie IT, operativem Bereich – also dem Flugbetrieb –, dem Sicherheitsbeauftragten und dem Management muss ineinandergreifen.

Safety, Security und Versorgungssicherheit sind inzwischen sehr eng miteinander verzahnt und verlangen ein gemeinsames Verständnis von Sicherheit über Organisationsgrenzen hinweg. Angriffe betreffen nicht nur IT-Systeme, sondern zunehmend Betriebsprozesse, Lieferketten und die Einsatzfähigkeit. Sicherheit muss deshalb gemeinsam gedacht werden – technisch, organisatorisch und prozessual. Denn sie stärkt die Resilienz von Unternehmen und verlangt klare Verantwortlichkeiten, Risikomanagement und Meldeprozesse.

Das Luftfahrt-Bundesamt (LBA) und das BSI arbeiten bei diesen Themen sehr eng zusammen, und die Luftfahrtunternehmen erhalten in ihrer Umsetzung Klarheit, Effizienz und bessere Steuerbarkeit. Frühzeitige Priorisierung und integrierte Sicherheitsstrukturen gelten mittlerweile als entscheidende Erfolgsfaktoren.

Andreas Mundsinger, Geschäftsführer

Termine

22. – 25. April 2026	**AERO,** Friedrichshafen
27. – 29. Mai 2026	**EBACE,** Genf

Kontakt

German Business Aviation Association e. V.
Georg-Wulf-Straße 2, 12529 Schönefeld

Telefon: +49 152 59522812, Mail: ceo@gbaa.de,
www.gbaa.de

Illustration: AdobeFirefly / Harald Hornig, Foto: GBA