Positionspapier

Cyber-Sicherheit in der Luftfahrt

28.06.2017

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Marc Bachmann
Bereichsleiter Luftfahrt und Verteidigung
T +49 30 27576-102
m.bachmann@bitkom.org

Marc Fliehe, CISSP
Bereichsleiter Information Security
+49 30 27576-242
m.fliehe@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Die Digitalisierung erfasst viele Branchen und macht auch vor der Luftfahrt nicht halt: Die darin liegenden Potenziale wollen genutzt werden, die sich ergebenden Risiken müssen erkannt und abgesichert werden. Die Sicherheit der digitalen Produkte und Services ist elementar wichtig für das Vertrauen der Anwender, Passagiere und Märkte. Insbesondere in der so bedeutenden Branche der Luftfahrt sieht Bitkom hier drängende Herausforderungen, die reale und sehr ernsthafte Folgen nach sich ziehen könnten. Das bestehende Bewusstsein für Sicherheitsüberlegungen im Kontext der Digitalisierung hält Bitkom für nicht ausreichend. Insbesondere sind diese bisher politisch nicht oder nur unzureichend adressiert und lassen sich nur mit einer gemeinsamen Anstrengung von Politik, Wirtschaft und Wissenschaft bewältigen. Bitkom richtet deshalb konkrete Forderungen an die Politik, die in diesem Papier weiter ausgeführt werden:

1. Die Bundesregierung muss ihr Augenmerk stärker auf den Schutz des Luftverkehrs als kritische Infrastruktur vor Cyberangriffen richten, um die Sicherheit auch in Zukunft gewährleisten zu können.

2. Die Bundesregierung muss gemeinsam mit der Industrie gesetzliche Vorschriften und Regelungen so anpassen, dass Innovationen zum Schutz vor Cyberangriffen deutlich schneller Marktreife erlangen und zertifiziert werden, um „atmende Systeme“ und dynamische Prozesse zu ermöglichen. Nur so kann auf neu auftauchende Risiken zeitnah reagiert werden.
3. Die Autoren fordern die Politik dazu auf, gemeinsam mit der Industrie eine ressortübergreifende Dialogplattform zu schaffen, um Mahnahmen zu entwickeln und zu koordinieren sowie eine stärkere Mitgestaltung auf europäischer Ebene zu ermöglichen.
4. Die Bundesregierung sollte die Forschungs- und Entwicklungsarbeit im Bereich der Cybersicherheit in der Luftfahrt analog zu dem sehr erfolgreichen LuFo gezielt mit einem Förderprogramm flankieren.
5. Piloten müssen Hacker-Angriffe auf Flugzeuge erkennen und trainieren: Hierzu bedarf es einer erweiterten Ausbildung und entsprechende Handlungsanweisungen.
6. Ausbildung von Cyber-Sicherheitsexperten mit Branchen-Know-How speziell für die Luftfahrt.
7. Safety von der Security zusammen denken: Beide Konzepte bedingen sich gegenseitig und müssen zusammen gedacht werden.
8. Redundante CNS-Infrastruktur schaffen, die ergänzend zur Safety auch Schutz im Sinne der Security schaffen.
9. Resilienz-by-Design: Heutige Systeme müssen widerstandsfähig gegenüber denen von Übermorgen werden.
10. Unternehmens- und praxisnahe Forschung um Innovationen voranzutreiben und die Ausbildung von Fachkräften stärker zu fördern.
11. Sicherheit in der Praxis statt Checklisten-Mentalität: Unklare Regulierung und sich widersprechende Vorgaben und Richtlinien vermeiden und stattdessen die Technik in der Luftfahrt als komplexe sozio-technische Systeme ganzheitlich betrachten.

1. Fachspezifische Sicherheitsthemen

Die Bedrohung durch Cyberangriffe in der deutschen Industrie und Gesellschaft, sind mittlerweile weitgehend bekannt. In Cyber-Physischen Systemen besteht grundsätzlich das Risiko, dass unautorisierte Nutzer diese Systeme zweckentfremden. Im speziellen Fall der Luftfahrt gibt es einige Merkmale, die in anderen Branchen weniger kritisch sind. So ist zum Beispiel die Abhängigkeit von veralteter Hardware problematisch, oder das Angriffspotential über die Funkschnittstelle wie die Manipulation von GPS-Signalen oder das unerlaubte Sprechen über den Flugfunk. Eine zusätzliche Herausforderung sind zu lange Entwicklungszyklen, die einer sich immer schneller ändernden Bedrohungssituation aus dem Cyber-Raum gegenüberstehen. Somit sind die in der IT-Sicherheit üblichen Security-Patches nicht zeitnah anwendbar.

Ein großes Risiko birgt auch die unvollständige Umsetzung von Richtlinien und Vorgaben, die dazu führen kann, dass sich eine „Checklisten-Mentalität“ verbreitet, die sich mehr auf die Erfüllung der Regularien ausgerichtet, als auf die Mitigation der in der Praxis existierenden Bedrohungen. Es fehlt in Deutschland ein Mechanismus, um die Verantwortung über solche Risiken angemessen zuzuordnen. Ebenso muss die Aufarbeitung von Zwischenfällen besser geregelt werden.

1.1. Internationale, europäische und nationale Gestaltungsstrukturen

Auf internationaler Ebene ist die wichtigste Institution die International Civil Aviation Organisation (ICAO), eine Sonderorganisation der Vereinten Nationen (UN). Sie schlägt Standards und Praktiken vor, die von den nationalen Behörden umgesetzt werden.

Auf die Gewährleistung der Versorgungssicherheit der europäischen Bevölkerung zielen Regularien zum Schutz der kritischen Infrastrukturen ab. Auf europäischer Ebene wurde hierzu im Jahr 2016 eine Direktive des EU-Parlaments zur Sicherheit von Netzwerk- und Informationssystemen (Network and Information System Security – NIS) erlassen. Bereits im selben Jahr wurde diese Direktive in Deutschland durch das IT-Sicherheitsgesetz in nationales Recht umgesetzt. Welche Betreiber durch das IT-Sicherheitsgesetz betroffen sind wurde in Deutschland sukzessive durch Umsetzungsverordnungen festgelegt. Die zum 1. Juni 2017 in Kraft getretene Verordnung zielt dabei unter anderem auf den Bereich Transport und Verkehr ab, der explizit auch Betreiber im Kontext des Lufttransports (Cargo & Passenger) umfasst. Daraus resultiert ein Umsetzungsdruck bei den entsprechend betroffenen Unternehmen in Deutschland.

Neben dieser Regulierungslinie steht die Gewährleistung der Flug- und Luftverkehrssicherheit (im Sinne der funktionalen Sicherheit) im Fokus. Seit dem Jahr 2015 wird Cyber-Sicherheit als ein zu beachtendes Themengebiet in der europäischen Luftfahrtstrategie berücksichtigt. Ein wesentliches Element in diesem Kontext ist die grundlegende Verordnung der EC Regulation 216/2008. In der aktuell in Ausarbeitung befindlichen Neufassung soll auch Cyber-Sicherheit explizit berücksichtigt werden.

Ausgehend von den Schwerpunktsetzungen der europäischen Cyber-Sicherheitsstrategie aus dem Jahr 2013 gibt es drei wesentliche Linien der Regulierung mit Relevanz für die Luftfahrt. Zum einen verabschiedet das EU-Parlament Direktiven, die in Deutschland durch Gesetze (z.B. das IT-Sicherheitsgesetz) in nationales Recht umgesetzt werden. Des Weiteren gibt es europäische Behörden, die sich mit dem Thema beschäftigen, wie z.B. die European Aviation Safety Agency (EASA), deren Regularien nahezu alle Unternehmen im Luftfahrtkontext betreffen (u. a. Hersteller, Lieferanten, Wartung, Flugsicherung, Airlines, Flughafenbetreiber). Als dritter Punkt bleibt noch der Datenschutz, der europaweit über die Grundverordnung von 2016 geregelt wird und in Deutschland mit dem Datenschutzgesetz umgesetzt wurde. Allgemein müssen aus Sicht des Datenschutzes Cyber-Sicherheitsmaßnahmen in informationsverarbeitenden Systemen umgesetzt werden. Dies gilt auch im Luftfahrtbereich überall dort, wo personenbezogene oder personenbeziehbare Daten verarbeitet werden.

Im Kontext der Cyber-Sicherheit gibt es bereits eine Vielzahl von Kooperationsplattformen und Initiativen auf nationaler, europäischer und internationaler Ebene. So ist auf EU-Ebene insbesondere die „Public-Private-Partnership on Cyber-Security“ zu nennen, eine Kooperationsplattform im Bereich Cyber-Sicherheit. Diese steht im engen

Zusammenhang mit der europäischen Digital Market Initiative sowie dem Forschungsrahmenprogramm Horizon 2020 und dem Single European Sky ATM Research Joint Undertaking (SESAR JU).

Im Bereich der Luftfahrt gibt es bereits seit längerem Bestrebungen, in Ergänzung zum US-zentrierten Aviation Information Sharing and Analysis Center (A-ISAC) ein entsprechendes europäisches Pendant einzurichten. Gleichzeitig plant EASA die Einrichtung einer Cyber-Security-Kooperationsplattform gemeinsam mit CERT-EU. Auf nationaler Ebene gibt es zahlreiche Initiativen und Arbeitsgruppen, die sich mit der Thematik der Cyber-Sicherheit auseinander setzen. Nur wenige davon sind auf spezielle Aspekte der Luftfahrt ausgerichtet und agieren häufig isoliert voneinander. Um deutsche Interessen auf europäischer und internationaler Ebene vertreten zu können, muss daher die Kooperation der relevanten Initiativen auf nationaler Ebene gestärkt werden.

1.2. Resilienz

Wie in anderen Sektoren ebenfalls üblich, wurde auch in der Luftfahrt bisher ein stark auf Prävention basierender Ansatz der IT-Sicherheit zur Anwendung gebracht. Dabei wurde (irrtümlicherweise) die Annahme getroffen, dass Systeme und Daten vor fremdem Zugriff und Missbrauch geschützt werden können, falls nur genug Aufwand bei der Absicherung getroffen wird. Die Realität hat allerdings gezeigt, dass ein entschlossener Angreifer, der über ausreichend Ressourcen verfügt, selbst die bestgeschützten Systeme infiltrieren oder in ihrer Funktionsweise beeinträchtigen kann. Daher müssen auch in der Luftfahrt neben klassischen präventiven Schutzmaßnahmen ergänzende, proaktive Maßnahmen ergriffen werden, welche die Resilienz (Widerstandsfähigkeit) der Systeme und Daten der Luftfahrt erhöhen. Hierzu gehören Fähigkeiten zur Detektion von Angreifern und Behandlung von Sicherheitsvorfällen genauso wie Vorkehrungen der Notfallplanung und Business Continuity. Darüber hinaus sollte die Widerstandsfähigkeit von Systemen schon während der Planungs- und Aufbauphasen berücksichtigt werden (Resilience-by-Design). Da es sich bei den Systemen der Luftfahrt um komplexe sozio-technische Systeme handelt, müssen neben technischen Fähigkeiten und Maßnahmen auch organisatorische Aspekte und der Anwender selbst als Risiko für die IT-Sicherheit berücksichtigt werden.

Ein besonderes Beispiel für die Schutzbedürftigkeit einer Kritischen Infrastruktur zeigt sich in der Luftfahrt im Teilbereich der Kommunikation, Navigation und Überwachung (auf Englisch CNS: Communication, Navigation, and Surveillance) der Flugsicherung betrachtet. Die CNS-Infrastruktur besteht aus mehreren Radio- und IT-Systemen, die für die Aufgabenerbringung der CNS genutzt werden. Dazu gehören unter anderem Funkfeuer, Radaranlagen, Sprechfunkstationen und Navigationssatelliten. Gemein an diesen Systemen ist die Vulnerabilität, die dadurch entsteht, dass sie über normierte Funkschnittstellen funktionieren.

Die Standards für die jeweiligen Funksysteme sind öffentlich verfügbar und die Funktionsweisen der verschiedenen Systeme weit bekannt. Aus der Perspektive eines potentiellen Angreifers bedeutet dies, dass sich vorhandene und oft architekturbedingte Schwachstellen leichter ausnutzen lassen, da die Systemzusammenhänge in den öffentlichen

Standards dokumentiert sind. Hinzu kommt, dass viele dieser Systeme schon sehr lange in Betrieb sind und auch noch lange in Betrieb bleiben müssen. Das heißt, dass die Systeme aus Sicht der Cybersicherheit nicht den heutigen Schutzanforderungen genügen, wenn sie nicht durch Updates oder neue Systeme aktualisiert werden.

Unter allen möglichen Angriffsmodalitäten unterscheidet die Fachliteratur üblicherweise zwei Arten: Jamming und Spoofing. Jamming bezieht sich auf ein blindes Belegen des Frequenzspektrums, so dass in einem gewissen Band keine Radioübertragungen mehr möglich sind. Damit werden z.B. GPS-Signale ausgeblendet, um Ortungsdienste funktionslos werden zu lassen. Beim Spoofing werden gezielt manipulierte CNS-Signale vorgetäuscht. Damit lassen sich z.B. GPS-Koordinaten verfälschen, ohne dass Ortungsdienste dies bemerken. Über die CNS-Systeme hinaus unterliegen noch weitere Systeme physikalischen und logischen Attacken z.B. auf die On-Board-Connectivity oder die allgemeine Flugzeug-Datenkommunikation. Daher ist ein adäquater Schutz des Radiospektrums gegen Jamming und Spoofing ebenso wichtig wie angemessene Schutzmaßnahmen aller beteiligten elektrischen Geräte und IT-Systeme.

1.3 Entwicklungszyklen

Ein wichtiger Aspekt bei Konzeption, Umsetzung und Steuerung von Cyber-Sicherheitsmaßnahmen ist die Eingliederung der zugehörigen Aktivitäten in die Entwicklungs- und Betriebsprozesse der entsprechenden Systeme. Bei reinen IT-Systemen funktioniert diese Eingliederung auf Grund der langjährigen Erfahrungen und Entwicklungen von Best Practices heutzutage vergleichsweise gut.

Bei cyber-physikalischen Systemen, in denen Geräte durch Industriesteueranlagen oder eingebettete Systeme gesteuert werden, ist die Situation in der Regel weitaus schwieriger. Aufgrund organisatorischer Gegebenheiten, unterschiedlicher kultureller Hintergründe und sich widersprechender Anforderungsbereiche werden Cyber-Sicherheitsaspekte hier häufig stark getrennt von den operationellen Aspekten der Systeme behandelt. Dies führt zu Inkonsistenzen von Anforderungen und Maßnahmen, die im Nachhinein häufig nur sehr schwer aufgelöst werden können. Dazu kommt, dass typische IT-Sicherheitsmaßnahmen stark auf die kurzen Lebenszyklen im IT-Bereich von ca. 3-5 Jahren ausgerichtet sind. Im Bereich der eingebetteten Systeme hat man es allerdings häufig mit Lebenszyklen in der Größenordnung von 10 bis 20 oder mehr Jahren zu tun. Dies gilt im Besonderen auch im Luftfahrtbereich, wo häufig die Situation entsteht, dass auf Grund verschiedener Anforderungen IT-Systemanteile weit über ihre eigentliche Lebenszeit hinaus im Einsatz sind.

Speziell im Luftfahrtbereich wird die Situation im Zusammenhang mit Safety-kritischen Systemen verschärft, bei denen ganz eigene Anforderungen gelten und aufwendige Prüfverfahren besonders lange Zykluszeiten von Komponenten bedingen. Bei der Konzeption und Umsetzung von Safety-Maßnahmen in der Luftfahrt werden in aller Regel keine absichtlichen Handlungen berücksichtigt. Eine strukturierte und umfassende Analyse hierzu gibt es nicht, da Safety und Security in der Luftfahrt, abgesehen von einigen Ausnahmen, getrennt voneinander behandelt werden (siehe Kapitel 2.2.).

Um die Situation in der Luftfahrt zu verbessern, muss Cyber-Sicherheit in allen Phasen des Lebenszyklus von Systemen (bzw. des System-of-Systems) berücksichtigt werden. Dabei ist eine Trennung bei der Berücksichtigung von Safety und Security kontraproduktiv – beide Aspekte müssen kombiniert oder zumindest aufeinander abgestimmt behandelt werden. Besonders wichtig für die Berücksichtigung der Cyber-Sicherheit sind dabei die frühen Phasen der Anforderungserhebung sowie des System-Designs (im Sinne eines „Security-by-Design"). Genauso wichtig ist aber auch eine kontinuierliche Überprüfung und Verbesserung von Sicherheitsanforderungen und -Maßnahmen. In diesem Zusammenhang bedarf es einer systemweiten Anstrengung bei allen im Kontext des Luftfahrtbetriebs relevanten Organisationen sowie bei den Herstellern und ihren Lieferketten.

2. Querschnittsthemen

2.1. Zertifizierung und Normierung

Zertifizierung und Normierung, u.a. ICAO, EUROCAE und RTCA im Luftfahrtbereich und generell im IT-Bereich, ermöglichen die Abstimmung von Elementen und Prozessen für die Realisierung der Cyber-Sicherheit. Die Komplexität und globale Dimension bewirkt jedoch, dass zumeist entweder ein eher grundlegendes Verständnis beschrieben wird oder ein für Subsysteme und Prozesse relevantes Regelwerk definiert wird. Kürzer werdende Innovationszyklen sind eine weitere Herausforderung, auf die Luftfahrtsysteme flexibel reagieren müssen, da bereits ein Subsystem einen kritischen Einfluss für ein Gesamtsystem haben kann.

2.2. Safety / Security

Die englische Sprache unterscheidet zwei verschiedene Begriffe, die ins Deutsche mit „Sicherheit" übersetzt werden: Safety und Security. Mit dem Begriff „Safety" wird die betriebliche Sicherheit bezeichnet, worunter der Schutz von Personen vor Systemen zu verstehen ist. „Security" hingegen zielt auf den Schutz der Systeme vor dem Menschen und vor anderen Systemen ab, worunter auch unautorisierte menschliche Eingriffen fallen.

In vielen Fällen können sich beide Konzepte ergänzen. In manchen Fällen aber sind sie unterschiedlich oder gar gegensätzlich. So kann ein Navigationssystem wie Galileo betriebssicher sein (praxiserprobt, zuverlässig), ohne aber die Sicherheit gegen absichtliche Eingriffe zu gewährleisten (spoofing-anfällig).

Eines der wichtigsten Prinzipien, in der Entwicklung sicherheitskritischer Systeme, ist Redundanz (im Sinne von Safety). In der Luftfahrt, zumindest an Bord, wird oft mit dreifach redundanten Systemen gearbeitet (Flugregler, Stellglieder, Sensorik), nicht aber in der CNS-Infrastruktur. Hier ist es oft schwierig überhaupt Redundanz zu gewährleisten. Solche nicht redundanten CNS-Systeme haben sich über die letzten Jahrzehnte als betriebssicher (also „Safe") erwiesen, jedoch ist die Sicherheit gegen gezielte Störungen (also „Security") oft mit den Mitteln eines heutigen Angreifers ungenügend, wenn überhaupt vorhanden.

Es liegt also ein starker Forschungsbedarf vor an Systemen, die „Security by design“ bieten, bei denen also die Störsicherheit als Designkriterium berücksichtigt wird. Im Vergleich zu gegenwärtigen Methoden brauchen solche Systeme kürzere Entwicklungsprozesse und somit schnellere Zertifizierung. Gleichzeitig werden Systeme in der Luftfahrt immer komplexer und enger miteinander vernetzt, weshalb angemessenes Konfigurationsmanagement mitentwickelt werden muss.

In dieser Hinsicht stehen sich „Safety“ und „Security“ gegenüber; soll ein System „Safe“ sein, braucht es lange Erprobungszeiten. Die „Security“ hingegen, lässt sich am besten gewährleisten, wenn schnell auf neue (oder neubekannte) Bedrohungen reagiert werden kann. An dieser Stelle kann die Luftfahrt eventuell von der Erfahrung in der Software-Security profitieren.

Eine große Herausforderung stellt, in der Luftfahrt, die hohe Latenz in der Systementwicklung dar: lange Entwicklungszyklen, bei denen Anforderungen veraltet sein können, wenn das System zugelassen wird. Die Anforderungen ändern sich oft schneller, als der Entwicklungsprozess folgen kann, was eine Vorbereitung auf zukünftige Veränderungen innerhalb der Systeme erfordert (z.B. für künftige Verschlüsselungsverfahren). Am Beispiel der Satellitennavigation lässt sich gut erkennen, wie das Navigationssystem, das als „safe“ akzeptiert wird, seit einiger Zeit als nicht „secure“ gilt, weil sich Signale fälschen lassen und Navigationsempfänger getäuscht werden können.

Konkreten Handlungsbedarf gibt es hier in der Entwicklung von effizienteren, zeitgemäßen Zulassungsprozessen, in denen die Modularität der Systeme berücksichtigt wird. So muss z.B. ein bereits zugelassenes Flugzeug nach Überholung eines obsoleten Bauteils komplett neu zugelassen werden. Stattdessen könnte die Zertifizierung auf Schnittstellenebene modularisiert werden, um Betreibern schnelleres Handeln zu ermöglichen. Damit könnten also Safety und Security miteinander in Einklang gebracht werden. Auf längere Sicht muss auch daraufhin gearbeitet werden, dass gesamtheitliche Ansätze entwickelt werden, um Safety und Security zu stützen. Dazu müssen Synergien identifiziert werden, aus denen interdisziplinäre Lösungen für gemeinsame Probleme entstehen. Gleichzeitig müssen jedoch Lücken (sowohl in der Verantwortung als auch in der Systementwicklung) zwischen beiden Konzepten vermieden werden.

2.3. Bildung + Forschungsprogramme + Lehrstühle

Das Thema Aviation Cyber Security stellt besondere Herausforderungen an Bildung & Forschung. Anders als oftmals in anderen Branchen praktiziert, reicht es nicht, die Bereiche Cyber und Aviation getrennt zu betrachten und an irgendeiner Stelle zusammen zu führen. Dies führt zu umständlichen Abstimmungsprozessen, die in einem Gebiet, welches schnelle Handlungsfähigkeit erfordert, in gefährlichen Verzögerungen resultieren. Vielmehr müssen diese Bereiche sowohl in der Bildung als auch in Forschung schon ganz früh zusammengedacht werden. Bildungs- und

Forschungsprogramme müssen maßgeschneidert auf die Bedürfnisse der Unternehmen ausgerichtet werden. Nur so ist es möglich gemeinsam die komplexen Herausforderungen zu meistern.

In aktuellen Aufrufen zu Forschungsprogrammen (LuFo-V3, Horizon 2020 u.a.) werden diese Themen partiell adressiert, allerdings gibt es hier noch Steigerungspotential. Dazu ist auch eine stärkere Koordination zwischen den Projektträgern, den ausschreibenden Organisationen und den maßgeblichen Forschungseinrichtungen notwendig.

Um Forschung nicht zum Selbstzweck durchzuführen, sollte bei jedem Forschungsprojekt auch ein Bildungsanteil enthalten sein. Bildung in der Forschung und Forschung in der Bildung, z.B. mittels Anteilen zum Thema Aviation Cyber Security in Studiengängen. Dies ermöglicht frühzeitige Abstimmungen zwischen Bildung und Forschung, welche nicht später aufwendig nachgeholt werden muss. Ergänzt durch Einbeziehung von Unternehmen, lässt sich so sicherstellen, dass wirklich Aviation Cyber Security Experten ausgebildet werden und zeitnah zur Verfügung stehen.

Dafür müssen entsprechende Lehrstühle eingerichtet werden. Auch die inhaltliche Ausgestaltung aktueller und zukünftiger Studien- und Ausbildungsgänge muss angepasst werden. Es müssen die Themen der Digitalisierung in aktuellen technischen, die Luftfahrt betreffenden, Studiengängen stärker Eingang finden. Aber auch für das Thema Aviation Cyber Security braucht es ganz spezielle Expertise, welche über die Aus-, Fort- und Weiterbildung bereitgestellt werden muss. Eine umfassende Expertise in allen Teilaspekten der Aviation Cyber Security kann nicht durch ein einzelnes Ausbildungsprofil bereitgestellt werden. Vielmehr muss Grundlagenwissen zur Cyber-Sicherheit Eingang in die Ausbildung von Ingenieuren und Betriebspersonal einfließen. Desgleichen muss Grundlagenwissen zu luftfahrtspezifischen Themen in der IT-orientierten Ausbildung zumindest teilweise enthalten sein.

Eine hohe Expertise im Bereich der Cybersicherheit ist jedoch auch für den Betrieb selbst unabdingbar. Die Abwehr von Angriffen auf die IT-gestützten CNS-Systeme bleibt nicht nur die Aufgabe der Entwicklung oder Forschung und der unterstützenden Ressourcen und Prozesse, sondern wird zukünftig auch Teil der Kompetenz eines Piloten sein müssen. Das betrifft in besonderer Weise die Fähigkeit, derartige Angriffe (etwa auf die Integrität von Flugdaten) zu erkennen oder sie zumindest in anomalen Flugsituationen in Betracht zu ziehen. Insofern sieht Bitkom auch in der Pilotenausbildung Handlungsbedarf und regt eine dahingehende Erweiterung der Flugausbildung an.