Air2030 – Systeme zum Schutz vor Cyber-Angriffen

Cybersicherheit und die F-35

Cybersicherheit ist für die Hersteller wie die Betreiber moderner Kampfflugzeuge überlebenswichtig. Obwohl das Thema alle vier Kandidaten der Air2030-Kampagne betrifft, wird es in erster Linie bei der Lockheed Martin F-35A Lightning II kontrovers diskutiert.

Viele Jahre lang war der Sprechfunk die einzige Verbindung des Piloten zur Aussenwelt. Über Funk erhielten die Piloten Informationen von ihren Kameraden oder von der Kommandozentrale. Lange Zeit reichte das, um den Auftrag zu erfüllen. Kritisch wurde es schon damals, wenn der Gegner mithören konnte. Mit der Zeit kamen Datenverbindungen hinzu. Damit die übermittelten Daten nicht in falsche Hände gerieten, wurden ausgeklügelte Sicherheitsmassnahmen getroffen und die Daten verschlüsselt übermittelt. Die heutigen Kampfflugzeuge zeichnen sich dadurch aus, dass sie von unterschiedlichen Quellen in der Luft und am Boden Daten entgegennehmen und verarbeiten können.

Zentrale Bedeutung von Cyber-Security

Ein allgegenwärtiges Thema ist heute die Cybersicherheit, die uns in allen Lebensbereichen beschäftigt. Alle elektronischen Geräte, die sich in einem öffentlichen oder privaten Netzwerk befinden, sind dem Risiko von Cyberangriffen ausgesetzt und müssen entsprechend geschützt werden. Moderne Kampfflugzeuge bilden hier keine Ausnahme. Ihr «Gehirn» sind leistungsfähige Computer, die Informationen aus internen und externen Quellen erhalten. Die «Augen» und die «Ohren» sind Sensoren im und am Flugzeug. Erst die Vernetzung aller internen und externen Daten bringt den entscheidenden Nutzen. Der Diebstahl oder die Zerstörung dieser Daten oder der Unterbruch des Datenflusses durch Cyberangriffe sind moderne Bedrohungsszenarien. Eine Luftwaffe wird auch handlungsunfähig, wenn die IT-Infrastruktur am Boden gestört oder zerstört wird. Das betrifft zum Beispiel auch den Unterbruch von Lieferketten für den Unterhalt einer Flotte.

Alle sind betroffen

Cybersicherheit ist für alle vier Kandidaten der Air2030-Kampagne ein entscheidendes Thema. Neben dem Schutz der operationellen Netzwerke müssen auch die Supportnetzwerke geschützt sein. Die Flugzeuge sind in der Luft untereinander vernetzt und können

laufend oder sogar in Echtzeit Daten austauschen. Gleichzeitig sind sie mit boden- oder luftgestützten Systemen verbunden, mit welchen sie ebenfalls Daten austauschen. Dies ist nur möglich, wenn alle luft- oder bodengestützten Systeme vor Cyberangriffen sicher sind. Obwohl es alle vier möglichen Nachfolger für die F/A-18C/D Hornet betrifft, werden die Cyberrisiken in erster Linie in Bezug auf die Lockheed Martin F-35 Lightning II diskutiert.

Grosses Bild linke Seite: Die F-35A kann weder über ALIS oder ODIN noch über ein anderes System ferngesteuert werden. Die Lightning II ist nicht für einen Remote-Betrieb ausgelegt.

Kleines Bild oben: Mit ALIS und später mit ODIN erhält die Bodenmannschaft wertvolle Informationen zum Betriebszustand der Systeme im Flugzeug.

Fotos: Lockheed Martin

Grosse Datenmengen

Die Entwicklung der F-35 begann acht bis zehn Jahre später als jene ihrer Konkurrenten der Air2030-Kampagne. Die Bedeutung von Cybersicherheit nahm in dieser Zeit stetig zu. Die Lightning II ist stark vernetzt und gemäss Hersteller in Bezug auf die Datenmengen und die Geschwindigkeit des Datenaustausches führend. Das macht die F-35 etwas anfälliger als die Konkurrenten, weshalb Cybersicherheit von Anfang an ein Schlüsselthema bei der Entwicklung war. Die F-35 kann Daten über «Link 16», den militärischen Standard-Datenlink der NATO, mit allen möglichen Partnern austauschen. Zusätzlich verfügt die Maschine über einen von Northrop Grumman speziell für Stealth-Flugzeuge entwickelten Datenlink MADL (Multifunction Advanced Data Link). Darüber können noch grössere Datenmengen in diesem spezialisierten Netzwerk noch schneller ausgetauscht werden.

Logistik-System ALIS

Bei älteren Kampfflugzeugen müssen auch funktionierende elektronische Flugzeugkomponenten nach einer vorbestimmten Zeit ausgetauscht werden. In modernen Flugzeugen werden sie ständig geprüft und nur noch bei Störungen ausgetauscht. Dies senkt die Unterhaltskosten und steigert die Flottenverfügbarkeit. Zu deren Optimierung verfügt die F-35 über das Autonomic Logistics Information System (ALIS). Der Betreiber der Lightning II hat jederzeit einen guten Überblick über den Zustand seiner Flotte. ALIS besteht aus über 65 Applikationen und unterstützt den Betreiber beim Training, der Planung, dem Unterhalt und dem Support, um eine hohe Flottenverfügbarkeit zu gewährleisten. Der Betreiber einer kleinen Flotte, wie die Schweiz es wäre, profitiert stark von den Erfahrungen der Länder mit grösseren Flotten oder jenen Luftwaffen, die schon länger mit F-35 fliegen. Die Daten werden in einer Standard Operating Unit (SOU) verwaltet und über einen nationalen Central Point of Entry (CPE) mit Lockheed Martin geteilt. Jeder Nutzer entscheidet selbst, welche Daten er mit Lockheed Martin und damit den F-35-Partnern teilen will. Es ist möglich, ALIS in einem geschlossenen nationalen Netzwerk zu nutzen, ohne Daten mit jemanden zu teilen. Der optimale Nutzen entsteht jedoch erst durch die Vernetzung. Lockheed Martin kann sich damit einen Überblick über den Zustand der weltweit eingesetzten F-35 verschaffen und damit den sicheren Betrieb ständig weiter optimieren. Dies spart Zeit und Geld.

Gemäss Lockheed Martin werden bis 2025 rund 1000 F-35 im Einsatz stehen. Die Abhängigkeit zum Hersteller eines Kampfflugzeugs besteht sowieso und ist nicht typenabhängig. Eine vollständige Unabhängigkeit ist unmöglich. Es müssten riesige Mengen an Ersatzteilen gekauft werden, um für die gesamte Lebensdauer von 30 Jahren unabhängig zu sein. Modernisierungen und Anpassungen an veränderte Rahmenbedingungen sind ebenfalls nur in Zusammenarbeit mit dem Hersteller möglich.

ODIN löst ALIS ab

Mit der Ablösung von ALIS durch das neue System ODIN (Operational Data Integrated Network) erfolgt der nächste Entwicklungsschritt von Lockheed Martin. ALIS wurde zwar seit der Einführung weiterentwickelt, weist aber dennoch einige Defizite auf. Diese sollen durch das Cloud-basierte, in Echtzeit funktionierende ODIN behoben werden. Wie ALIS kann auch ODIN als geschlossenes Netzwerk vom jeweiligen Kunden autonom betrieben werden. Zurzeit sind nur wenige Details zu ODIN bekannt, doch dürfte das System gemäss Lockheed Martin ab 2027 bereit sein. Die Offerte an die Schweiz beinhaltet somit ODIN und nicht ALIS.

Transparenz

Lockheed Martin offeriert der Schweiz bei einem allfälligen Kauf der F-35 den Aufbau eines nationalen Cyber Center of Excellence (CCoE). Damit würde die Schweiz Einblick in alle Daten erhalten und könnte sich ein eigenes, auf Schweizer Bedürfnisse zugeschnittenes Netzwerk aufbauen. Diese Offerte bietet der Schweiz einen vollständigen Einblick in das System F-35 und damit volle Transparenz. Die Schweiz könnte Hard- und Software selber testen. Das durch das CCoE gewonnene Know-how ist für militärische und zivile Anwendungen nutzbar. Gemäss Lockheed Martin ist die Selbstbestimmung über die Verwendung der Daten auch ohne ein CCoE garantiert. Der Betrieb einer F-35-Flotte ist ohne ein CCoE möglich und nicht alle heutigen Lightning II-Nutzer betreiben ein nationales Cyber Center of Excellence. Die Schweiz und auch alle weiteren Betreiber der F-35 bestimmen selbst, ob und mit wem sie ihre Daten teilen wollen. **cp**

Walter Hodel