STORMSHIELD

MEINUNGEN

GIBT ES EINE FIREWALL IM FLUGZEUG?

Stéphane Prevost
Product Marketing Manager, Stormshield

In Anlehnung an die Entwicklung von Flugzeugen in der Zivilluftfahrt führen Militärflugzeuge immer mehr digitale Technologien mit sich und vervielfachen die Vernetzung mit der Infrastruktur am Boden. Diese Hyperkonnektivität entspricht zwar wichtigen betrieblichen Notwendigkeiten, bringt aber auch neue Schwachstellen mit sich. Welche sind das? Und wie kann man sich davor schützen? Höhenflug in diesem Cyber-Papier.

August 2018, der Sekretär der US-Luftwaffe, Will Roper, erklärt gegenüber der nationalen Presse unmissverständlich:„*Man könnte eines unserer Flugzeuge mit einem einfachen Computer abschießen.*“ Dieses aufsehenerregende Geständnis folgt auf ein vom Pentagon durchgeführtes Experiment, bei dem Gruppen von White Hats versuchen sollten, sich in die Bordsysteme der F-15 der US-Luftwaffe zu hacken. Und diese haben ihr Ziel erreicht: die (theoretische) Möglichkeit, ein Kriegsflugzeug mitten im Flug zum Absturz zu bringen.„*Dieser Hack ist auch das Ergebnis einer jahrelangen Vernachlässigung der Cybersicherheit durch die US-Luftwaffe*“, räumt Will Roper dann ein.

HYPERKONNEKTIVITÄT REIMT SICH AUF EFFIZIENZ UND ... ANFÄLLIGKEIT

Die technischen Elemente dieses Hacks werden natürlich nicht mitgeteilt und bleiben streng vertraulich. Allerdings konnten diese White Hats ein so kritisch wichtiges Kampfflugzeug nur deshalb hacken, weil die F-15 wie viele andere Fluggeräte mittlerweile hochgradig digital und vernetzt ist. *„Die Software moderner Kampfflugzeuge basiert auf Millionen von Codezeilen.Wenn dieser Programmiercode ausgedruckt werden müsste, würde ein Papierstapel von über 10 Metern Höhe entstehen*", erklärt Matthias Bertram, stellvertretender Unterprojektleiter Engineering im Rahmen des Projekts *„Neues Kampfflugzeug*" in der Schweiz, in einem Interview.

Die Herausforderungen des Cyberschutzes von Kampfflugzeugen sind somit ein echtes Anliegen des Augenblicks in der Schweiz, die sich demnächst mit neuen amerikanischen F-35 ausrüsten will. Diese werden zwar als ultramodern angepriesen, aber auch wegen ihrer sehr hohen digitalen Angriffsfläche verunglimpft. Diese Geräte sind daher ein Lehrstück, um zu verstehen, welchen Cyberbedrohungen ein Gerät dieser strategischen Größe heutzutage ausgesetzt sein kann. In einem Bericht des französischen Instituts für internationale Beziehungen (Ifri) über die Bemühungen der französischen Armee, Cyberrisiken zu begegnen, werden drei wichtige Subsysteme der F-35 als problematisch dargestellt: die Software zur Unterstützung der Zielerkennung, eine Software zur vorausschauenden Wartung des Flugzeugs und die Flugsimulatoren, die für dieses Flugzeug bestimmt sind.Das erste Subsystem, *Joint Reprogramming Enterprise*, stellt eine große Anzahl bekannter Signaturen von auf dem Markt befindlichen Kampfflugzeugen zusammen und ermöglicht die automatische Erkennung und Identifizierung von Bedrohungen in der Nähe (Panzer, Drohnen ...).Dadurch erhält der Pilot entscheidende Informationen, die ihm helfen, taktische Entscheidungen in Echtzeit zu treffen.Problem: *„Ein Eingriff in seine Updates könnte es Hackern ermöglichen, falsche Daten in das System einzuschleusen, um bestimmte Ziele unentdeckt zu lassen oder das Feuerleitsystem zu täuschen.*" Das zweite problematische Subsystem, das *Autonomic Logistics Information System*, ist eine weitere On-Board-Software. Es soll die vorausschauenden Wartungsmöglichkeiten des Flugzeugs verbessern, indem es den Verschleißzustand einiger seiner Komponenten selbst einschätzt. Durch die Weiterleitung dieses Informationsflusses an die Zentrale von Lockheed Martin (dem Hersteller des Flugzeugs) können Ersatzteile im Vorgriff auf mögliche Ausfälle beschafft und so die Verfügbarkeit des Flugzeugs optimiert werden. Ein gewichtiger Vorteil in Konfliktsituationen. Sollte dieser Informationsfluss jedoch abgefangen werden, befürchten die Experten, dass er *„mögliche Feinde über die Struktur des Flugzeugs und den Inhalt seiner Missionen informieren könnte.*" Schließlich werden die Piloten der F-35 vor jedem Start in Flugsimulatoren geschult, ein drittes problematisches Subsystem. Diese sind so programmiert, dass sie eine ultrarealistische Pilotenerfahrung bieten. Die Aussicht, dass diese Simulatoren gehackt werden, könnte es Cyber-Kämpfern ermöglichen, *„Schlüsselinformationen über die Funktionsweise von Kampfflugzeugen abzuleiten.*"

Diese verschiedenen Schwachstellen legen den Schwerpunkt auf **die Cyber-Gefahren, die mit dem Datenaustausch zwischen Flugzeugen und Bodeninfrastrukturen verbunden sind. Alain Mingam**, Sicherheitsarchitekt bei Airbus, erklärt: *„Im militärischen Bereich versuchen wir, diese Verbindungen zu minimieren, da sie eine Bedrohung für das Flugzeug darstellen. Die heutigen operativen Realitäten machen es jedoch erforderlich, dass die Kommunikation mit dem Boden durch geeignete Sicherheitsmaßnahmen gewährleistet wird."* In den letzten 15 Jahren ist sich **die militärische Luftfahrtindustrie dieser Anfälligkeit bewusst geworden**. *„Seit mehreren Jahrzehnten ist die Betriebssicherheit fest in den Entwicklungsprozess von Flugzeugen integriert"*, sagt **Christopher Cachelou**, Pre-Sales Engineer bei Stormshield, der auf den Verteidigungssektor spezialisiert ist. *Sie stützt sich auf eine funktionale Risikoanalyse, um sicherzustellen, dass das Gerät sowohl hardware- als auch softwaretechnisch einwandfrei funktioniert. Die Cybersicherheit von Produkten ist ihrerseits viel neuer und weniger in die Entwicklungsprozesse integriert. Sie stützt sich ebenfalls auf eine Risikoanalyse, diesmal jedoch aus dem Cyberspace – wie zum Beispiel bei der EBIOS-Methode."* Alain Mingam bestätigt diese Tatsache, sowohl in der militärischen als auch in der zivilen Luftfahrt. *„Zwischen ACARS (für Flugbetrieb, Flugsicherung, Wartung), FOMAX (für vorausschauende Wartung) und Unterhaltungssystemen (in-flight entertainment, IFE) gibt es in der zivilen Luftfahrt sehr viele digitale und mit dem Boden vernetzte Tools, die schon viel länger im Einsatz sind."* Im Gegensatz zu dem, was man annehmen könnte, ist **es also oft die zivile Industrie, die der militärischen Industrie den Weg in die Cybersicherheit ebnet**. So hätte zum Beispiel der von Airbus entwickelte und der Europäischen Organisation für Rüstungskooperation (OCCAr) vorgeschlagene A400M (militärisches Transportflugzeug) stark von den Cyberschutzstudien für den A380 profitiert.

AUF DEM WEG ZU EINEM CYBER-KRIEG IN DER LUFT?

Die geheime und kaum dokumentierte Natur von Cyberkriegshandlungen reduziert de facto die Anzahl der Studien über die Cyberbedrohung im militärischen Bereich. Interessant ist jedoch der Bereich der Cyberangriffe auf Flugzeuge und Infrastrukturen der Zivilluftfahrt. Nach Angaben der Europäischen Agentur für Flugsicherheit (EASA) übersteigt diese Zahl seit 2016 im Durchschnitt 1.000 Angriffe pro Monat.

Die Informationen rund um die F-15 stammen zwar aus Pentests, **es wurden jedoch bereits Fälle von (mehr oder weniger erfolgreichen) Hackerangriffen auf die militärische Luftwaffenausrüstung mehrerer Länder gemeldet**. Im Jahr 2009 wurden die Computer des Luftwaffenstützpunkts 107 in Villacoublay mit dem Conficker-Virus infiziert, der sich über nicht aktualisierte Windows-Desktops verbreitet haben soll. In einem vertraulichen Schreiben an die Website Intelligence Online heißt es, dass mehrere Rafales zwei Tage lang am Boden geblieben seien. Einige von Edward Snowden enthüllte, als geheim eingestufte Dokumente belegen zudem, dass es den Geheimdiensten der USA und Großbritanniens gelungen war, die Videostreams von israelischen Drohnen und F-16-Kampfflugzeugen abzufangen und zu entschlüsseln, wodurch sie wichtige taktische Informationen am Rande der geopolitischen Spannungen im Iran erhalten konnten. In dem Bericht des Ifri wird auch die Aussage des ehemaligen Leiters der

französischen Cyberverteidigung, Konteradmiral Arnaud Coustillière, wiedergegeben, der erklärt, dass eine französische Drohne des Typs Harfang in Afghanistan einem Entführungsversuch ausgesetzt war. Der Angriff schlug schließlich fehl, hätte aber dennoch die Mission des Fluggeräts gestört.

Schließlich wecken auch sensible Daten, die innerhalb der Bodeninfrastruktur gespeichert sind, Begehrlichkeiten. Im Jahr 2017 wurden fast 30 GB an kommerziellen (aber nicht als geheim eingestuften) Daten im Zusammenhang mit australischen Verteidigungsprogrammen bei einem Cyberangriff auf einen Regierungsdienstleister ausgelesen. Ein weiteres Beispiel aus dem Jahr 2020, als Leonardo, einer der größten europäischen Luft- und Raumfahrtindustriekonzerne (italienischen Ursprungs) einen abnormalen Datenabfluss aus seinen Systemen feststellt und die italienischen Behörden alarmiert. Die Ermittlungen ergeben, dass einer der gehackten Computer geheime Informationen über das Experimentalprojekt „nEUROn" enthielt. Das seit 2012 von Frankreich beaufsichtigte Projekt hat zum Ziel, ein neues Militärflugzeug für die europäische Verteidigung zu entwickeln. In jüngerer Zeit hat eine Gruppe von Cyberkriminellen die technischen Details des schwedisch-kanadischen Globaleye (ein Flugzeug, das für militärische Überwachungs- und Aufklärungsmissionen eingesetzt wird) im Dark Web gepostet. Diese Informationen sollen in den Systemen des kanadischen Industrieunternehmens Bombardier, das an der Herstellung des Flugzeugs beteiligt ist, gesammelt worden sein.

Obwohl selten, wird die Bedrohung durch die Übernahme von Militärapparaten mit digitalen Mitteln von allen Nationen, die sie einsetzen, sehr ernst genommen. In Frankreich hat die Armee bereits ein Kontingent von 1100 Cyber-Kämpfern aufgebaut, das bis 2025 um weitere 5000 Mitarbeiter aufgestockt werden soll, die sich auf die Armeen, die Generaldirektion für Rüstung (DGA) und den französischen Auslandsgeheimdienst (DGSE) verteilen. Befinden wir uns lediglich in Erwartung eines Cyberkriegs? Nein, laut den von Ifri wiedergegebenen Worten des Luftwaffenbrigadegenerals Didier Tisseyre, dem stellvertretenden Direktor des Kommandozentrums Comcyber: „*Wir haben bereits Cyberangriffe in Operationsgebieten eingesetzt, in denen die französische Armee engagiert ist, wie in der Levante oder in der Sahelzone. Dies kann darin bestehen, vor einer Intervention Informationen abzufangen, Luftabwehrradargeräte zu täuschen oder feindliche Verteidigungsanlagen lahmzulegen.*"

WELCHE AUSWEICHMANÖVER?

Der Cyberschutz von Kampfflugzeugen ist daher ein hochsensibles Thema. Im Prinzip ist der Schutz eines Kampfflugzeugs vor Cyberrisiken ähnlich wie der Schutz jedes Terminals, das mit einem zivilen Netzwerk verbunden ist, wie Matthias Bertram erläutert. Um im militärischen Bereich noch weiter zu gehen, wird eine funktionale Aufteilung auf Flugzeugebene in Verbindung mit einer *Safety-Impact-Analyse* insbesondere durch ein Dokument mit dem Namen *Functional Hazard Assessments* (FHA) durchgeführt. „*Dadurch lassen sich die verschiedenen Funktionen des Geräts und die möglichen Folgen einer Fehlfunktion genau ab bilden*", erklärt Alain Mingam. *Wir können dann die*

digitalen Angriffsvektoren, die sie stören könnten, durchgehen, ein damit verbundenes Risiko identifizieren und daraus die Sicherheitsbausteine ableiten, die auf dem Weg des potenziellen Angreifers errichtet werden müssen, um das Risiko akzeptabel zu machen."

Doch welche Verpflichtungen bestehen in diesem Zusammenhang? Auf französischer Ebene müssen sowohl zivile als auch private Betreiber von vitaler Bedeutung die Anforderungen an die Cybersicherheit erfüllen, die in Artikel 22 des Gesetzes zur Militärprogrammierung beschrieben werden. Diese Anforderungen umfassen sowohl organisatorische Prozesse als auch technische Lösungen, die zur Sicherung der physischen und digitalen Infrastruktur eingesetzt werden müssen. Auf europäischer Ebene nimmt die NIS-Richtlinie (Network and Information Security) eine Reihe von Betreibern des Luftverkehrssektors in die Liste der Betreiber wesentlicher Dienste auf.

Aus organisatorischer Sicht beruht die allgemeine Sicherung des Kampfflugzeugs auf der Verschränkung von drei sich ergänzenden Baustellen:

1. **Sicherheit der Bodeninfrastruktur:** Der Standortleiter ist für die Sicherung von Stützpunkten, Flughäfen, Kommandozentralen und anderen militärischen (und zivilen) Strukturen zuständig, die für den Betrieb von militärischem Material unerlässlich sind

2. **Sicherheit von Informationssystemen und Netzwerkinfrastrukturen (ISS):** Sie wird vom OSSI gewährleistet und ist traditionell Gegenstand einer IT-Sicherheitscharta, die die Betriebsabläufe, die Zugriffsrechte und die Einsichtnahme von militärischen und zivilen Mitarbeitern und Personal in digitale Ressourcen usw. regelt

3**. Produktsicherheit:** In den Zuständigkeitsbereich des Product Security Officer (PSO) fallen alle Hard- und Softwarelösungen, mit denen das betreffende Produkt (hier: das Kampfflugzeug) direkt ausgestattet wird, um es an die erforderlichen Sicherheitsstandards anzupassen.

In Bezug auf die Produkte nennt Matthias Bertram als Beispiel den Einsatz von Firewalls, die „*Signaturen, Verschlüsselung, rollenbasierten Zugriff, Virenscanner oder Echtzeit-Scans von laufenden Systemen*" gewährleisten. Diese Lösungen müssen auch so konzipiert sein, dass sie extremen physikalischen Bedingungen (Temperaturen, Druck, Erschütterungen usw.) standhalten und das Gerät in verschiedenen Umgebungen verfolgen können.

UND IN ZUKUNFT?

Das Militärflugzeug muss nun *cybersecured-by-design* (cybersicher gemäß Auslegung) gedacht werden. Wenn dies in Zukunft der Fall sein sollte, stellt sich eine weitere Frage: Wie kann ein angemessener Schutz über den gesamten Lebenszyklus des Geräts aufrechterhalten werden? Eine durchschnittliche Nutzungsdauer, die sich bei einem Kampfflugzeug auf 30 Jahre beläuft. Bei der rasanten Geschwindigkeit, mit der sich die digitale Welt verändert, **werden sich die Cyberbedrohungen von morgen drastisch von denen von heute unterscheiden**. Um diesem Problem zu begegnen, fügen die Hersteller ihrer Dienstleistung In-Service-Support eine weitere hinzu, nämlich In-Security-Support hinzu. „*In-Service-Support gewährleistet die Aufrechterhaltung des Betriebszustands*

des Flugzeugs während seines gesamten Lebenszyklus", erklärt Christopher Cachelou. *Parallel dazu sorgt der In-Security-Support dafür, dass das Flugzeug während seines gesamten Lebenszyklus in einem sicheren Zustand bleibt. Dies sorgt dafür, dass das Gerät angesichts der sich ständig ändernden Cyberrisiken und -bedrohungen ständig auf die richtigen Sicherheitsstufen gebracht wird.*" Die US-amerikanische F-15 wurde zum Beispiel verwundbar durch das Hinzufügen neuer digitaler Funktionen in Verbindung mit einem Mangel an Aktualisierungen der Cybersicherheit.

Alain Mingam blickt noch etwas weiter in die Zukunft. Wo Cybersicherheit heute als ein Stapel von Barrieren gedacht wird, die jeden Versuch eines Cyberangriffs verbieten oder bremsen sollen, planen Hersteller und Software-Entwickler den Gegenschlag. „*Wir stellen Schutzmaßnahmen auf; aber kein Schutz ist undurchdringlich, also müssen wir uns etwas anderes ausdenken*". Was wäre also, wenn diese Schutzmechanismen in der Lage wären, zu reagieren, sich weiterzuentwickeln, um besser auf eine Offensive zu reagieren oder sogar dem Verteidiger einen Gegenangriff zu ermöglichen? „*Wir erfinden Architekturen, die aus Überwachungsgeräten und Reaktionsmöglichkeiten bestehen.Die Entwicklung tendiert zu Echtzeitverfahren für den IT-Abwehrkampf.*" Wie im Krieg würde Cybersicherheit dann nicht mehr darin bestehen, Schläge einzustecken, sondern auch auszuteilen.