VC-POLICY
IT-SECURITY

DEFINITION

Die IT-Security beschreibt Eigenschaften von IT-Systemen, die zum Schutz vor Gefahren und Bedrohungen definiert und angewendet werden. Die Schutzziele sind Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, die gespeichert und verarbeitet werden.

Diese Policy beschreibt die Situation und die besonderen Erfordernisse zur IT-Security in Verkehrsflugzeugen und des gesamten dazu gehörenden Umfelds.

SITUATION

Computersysteme sind seit Jahrzehnten nicht mehr aus Verkehrsflugzeugen wegzudenken. Eine Vielzahl an elektronischen Steuerungs- und Überwachungssystemen an Bord eines Verkehrsflugzeuges trägt maßgeblich zur sicheren Flugdurchführung bei.

Diese Systeme waren bisher zumeist hardwareseitig getrennt ausgeführt. Die Kommunikation der Systeme untereinander erfolgte über klar definierte Schnittstellen. Wie in anderen Bereichen der Informationstechnologie gehen Hersteller dazu über, Systeme zu integrieren und enger zu vernetzen, sowohl um neue Anwendungsmöglichkeiten zu schaffen als auch um diese wirtschaftlicher zu gestalten.

Die rasante Entwicklung der letzten Jahre eröffnet neue Möglichkeiten, die nicht ohne Risiko sind: Es ist heutzutage möglich, durch schnell und kostengünstig aus der Ferne durchgeführte Hacker-Attacken, ganze Flugbetriebe lahmzulegen. Die bisherigen Attacken waren größtenteils gegen die Bodeninfrastruktur der Airlines gerichtet. Aber auch Attacken auf die Flugsicherungsinfrastruktur oder sogar die Flugzeugsteuerungssysteme selbst sind denkbar.

Um die Sicherheit und Integrität der sicherheitsrelevanten Daten zu gewährleisten, muss die gesamte Kommunikationskette über alle verbundenen Anwendungen hinweg betrachtet werden; jedes vernetzte System ist nur so stark, wie sein schwächstes Glied. Eine damit verbundene Sicherheitsstrategie umfasst gestaffelte Sicherheitsebenen (sog. „Defense in Depth Strategie“), die Personen, Daten, Software, Hardware, Netzwerk und Organisation einschließen. Die Daten müssen während ihres gesamten Lebenszyklus, in dem sie sich in Netzwerken bewegen, verarbeitet werden oder abgelegt sind, geschützt werden.

STANDPUNKT / FORDERUNGEN

Die Computersysteme in einem Flugbetrieb und aller daran angeschlossenen Prozesspartner sollen folgenden Voraussetzungen entsprechen:

- Datenverarbeitungssysteme müssen gegen Bedrohungen von innen und außen geschützt sein.
- Systeme müssen einem regelmäßigen und transparenten Updatezyklus unterliegen.
- Anwendungen sollen nur die unbedingt nötigen Funktionen ausführen können.
- Das Gesamtsystem und alle Komponenten sollen robust gegenüber unerwarteten Zuständen sein.
- Datensicherungen müssen regelmäßig an einem geografisch entfernten Ort hinterlegt werden.
- Unabhängige „Penetration Tester“ sollen regelmäßig das Gesamtsystem auf Verwundbarkeit überprüfen.
- Schwachstellen müssen zentral gemeldet und als Lerngrundlage veröffentlicht werden.
- Systeme müssen gegen unbefugten physischen Zugriff gesichert sein.
- Datenspeicher müssen verschlüsselt und sicher gegen unbefugten Zugriff sein.
- Dienstlich genutzte Geräte dürfen nicht privat verwendet werden.
- Alle Schutzmechanismen sollen dem aktuellsten Stand der Technik entsprechen und laufend auf Wirksamkeit geprüft werden.
- Hochsensible Systeme (z.B. Avionik) sollen strikt von extern zugänglichen Systemen (z.B. Internet) getrennt sein.
- Jeglicher Datenverkehr soll in einer Weise erfolgen, sodass die Vertraulichkeit (Dritte können Nachrichteninhalte nicht einsehen), Integrität (Manipulation von Nachrichten wird verhindert oder zumindest erkannt) und Authentizität der Kommunikation gewährleistet ist. Sämtlicher Datenverkehr soll protokolliert werden.

Alle Prozessbeteiligten sind regelmäßig über IT-Security-Bedrohungen, Schutzmaßnahmen und ihre Verantwortung als Benutzer zu schulen.

Personenbezogene Daten unterliegen darüber hinaus den Bestimmungen des Datenschutzes und der Mitbestimmung durch Betriebsrat/Personalvertretung.

Wirksame Bestimmungen, die den Missbrauch und die Manipulation von sensiblen Daten unter Strafe stellen, sind vom Gesetzgeber sicherzustellen.

ERLÄUTERUNG: INTEGRIERTE SICHERHEITSTECHNIKEN

Die Vereinigung Cockpit versteht unter integrierten Sicherheitstechniken gegen interne und externe Bedrohungen Folgendes:

Physische Trennung der Avionik

Die Verwendung gemeinsamer Datenbusse, die mehreren Sensoren, Geräten und Systemen als Übertragungsweg dienen, ist wirtschaftlich verlockend. Wirtschaftliche Interessen dürfen aber nicht zulasten der Flugsicherheit gehen.

Es muss ausgeschlossen sein, dass jemand Anzeigen oder gar die Flugsteuerung manipulieren kann. Daher muss jedes Netz, das Funkanbindungen, Schnittstellen, die mit eingebrachten Geräten kommunizieren, oder offene Anschlüsse außerhalb des Cockpits hat, als Gefahrenpotential betrachtet werden. Solche Netze müssen so von allen Cockpitsystemen getrennt sein, dass außerhalb der vorgeschriebenen Kanäle (z.B. TCAS, CPDLC) keine Signalübertragung in Richtung System stattfinden kann (kein Rückkanal).

Aus dem gleichen Grund verbietet es sich, (beispielsweise Wetter-) Daten aus dem Internet auf Cockpitinstrumenten anzuzeigen.

Es existieren Angriffe, die das Einschleusen von Daten in abgekapselte Systeme ermöglichen.

Datensicherheit

Wir verlassen uns täglich darauf, dass die Basis unserer Entscheidungen und Navigationshilfen (Wetter, Anflugkarten, etc.) korrekt und aktuell ist. Viele Apps zur Anzeige von METARs und TAFs laden ihre Informationen heute unverschlüsselt übers Netz und lassen sich mit simplen Werkzeugen zur Anzeige gefälschter Wettersituationen bewegen.

Konsequente Verschlüsselung von Endpunkt zu Endpunkt (z.B. EFB zu Wetterserver) in Verbindung mit Authentifizierung und Integritätssicherung ist mit heutigen Mitteln problemlos möglich und erschwert Datenmanipulation. Dabei sollten Hash- und Krypto-Verfahren stets auf dem aktuellen Stand gehalten werden.

Sogenannte Man-In-The-Middle-Attacken können reduziert werden, wenn nur die notwendigen Certificate Authorities (CAs) in den entsprechenden Clientsystemen hinterlegt sind. Insbesondere sind Gefahren bei firmeneigenen Zertifizierungsstellen durch interne Sabotage oder mangelhafte Konfiguration zu erwarten.

Nicht vertrauenswürdige Verschlüsselungszertifikate müssen ohne weiteres Eingreifen des Nutzers verworfen und die Verbindung zurückgewiesen werden. Es darf kein Zurückfallen auf unverschlüsselte Verbindungen geben.

Viele Daten, die durch die Hände von Piloten gehen, sind entweder sicherheitskritisch oder unter dem Aspekt des Datenschutzes behutsam zu

behandeln. Es muss sichergestellt sein, dass Außenstehende keinen Zugriff auf Passagier- und Passdaten o.ä. erlangen.

Sabotage und externe Angriffe können auch auf der Serverseite gewaltige Auswirkungen auf die Sicherheit haben. Flugbetriebe müssen sicherstellen, dass die IT-Systeme im Haus stets den aktuellen Empfehlungen für Administratoren entsprechen.

Softwaresparsamkeit

Die Anzahl der Programme, die auf einer Hardware laufen, potenziert das Risiko einer Schwachstelle. Es muss grundsätzlich das Ziel sein, möglichst wenig ausführbaren Code auf sicherheitskritischen Geräten wie EFB zu betreiben. Die Wartungsqualität steigt, wenn sie sich auf wenige Programme konzentriert.

Daher empfiehlt die Vereinigung Cockpit, nur die Software auf EFBs zu installieren, die für die Flugdurchführung unabdingbar ist. Überflüssige Software sollte entfernt werden. Dazu zählen auch Antivirenprogramme, da sie in der Regel die Angriffsfläche vergrößern und oftmals eingebaute Sicherheitsmechanismen des Betriebssystems außer Kraft setzen.

Private Software ist in diesem Kontext vermutlich das gefährlichste Einfallstor für Schadcode. Eigene Apps oder Programme sollten nicht auf dienstlich genutzten Geräten installiert oder verwendet werden. Private Daten sind umgekehrt vor der Neugier des Arbeitgebers schlecht geschützt.

Keine dienstliche Software auf Privatgeräten, keine private Software auf Dienstgeräten!

Datensparsamkeit

Heute wird eine Vielzahl von Sensordaten live aus dem Flugzeug zu ATC, Hersteller oder Operator übertragen. Notwendige Informationen (z.B. Passnummern in der GenDec) sollten verschlüsselt oder in Papierform übermittelt werden. Andere Daten (z.B. Fuel Quantity), die auch zur Leistungskontrolle hergezogen werden können, sollten nicht übertragen werden, solange dies nicht gesetzlich vorgeschrieben ist. Ein kontinuierlicher Stream als Ersatz oder Erweiterung für Flight Data Recorder oder Cockpit Voice Recorder liefert potentiellen Angreifern darüber hinaus Feedback, ob eine Fernmanipulation erfolgreich ist.

Falls das Internet von Geräten im Cockpit aus genutzt wird (z.B. von EFB oder Privatgeräten), muss dem Nutzer klar sein, dass er dies im Kontext des Netzwerks öffentlich tut. Dritte können bei paketvermittelten Netzen aus technischen Gründen einsehen, wann zu welchen Servern eine Verbindung hergestellt wird, und in welchem Umfang Daten ausgetauscht werden. Dies gilt auch für Arbeitgeber, die jederzeit in der Lage sind, mit Hilfe von Logdaten das Nutzungsprofil der Angestellten auszuwerten.

Regelmäßige Sicherheitsupdates

Bereits heute werden kritische Datenverarbeitungssysteme Zertifizierungen unterzogen. Leider finden diese immer nur im Kontext und auf Basis des Forschungsstands zum jeweiligen Zeitpunkt statt. Da sich dieser in der Informationsverarbeitung rasch ändern kann, sollten in regelmäßigen Abständen Re-Validierungen stattfinden. Jedes neue Feature, aber auch bestehende Software muss dabei einem unabhängigen offenen Code-Audit und Penetrationstests unterzogen werden.

Sollten bei diesen Tests oder im Alltag Sicherheitsprobleme gefunden werden, müssen diese an eine zentrale Stelle gemeldet und nach angemessener Frist offengelegt werden. Die öffentliche Stelle sollte darüber wachen, dass die Sicherheitsprobleme in einem akzeptablen Zeitraum gefixt werden. Das Konzept der vermeintlichen Sicherheit durch Geheimhaltung der Funktionsweise (Security by Obscurity) ist strikt abzulehnen.

Besondere Probleme entstehen, falls der Hersteller nicht mehr existiert, das Produkt nicht weiter aktualisiert oder Systemkonzepte inhärente Sicherheitslücken aufweisen. Sobald Re-Validierungen oder Updates für ein Gerät nicht mehr realisierbar sind, sollte dieses Gerät unverzüglich seine Luftfahrtzulassung verlieren und entfernt werden.