2014/13 Lifestyle

https://shop.jungle.world/artikel/2014/13/hacker-der-luft

Cyberkrieg und verschwundene Flugzeuge

Hacker der Luft

Von **Boris Mayer**

Das Computersystem eines Flugzeugs zu hacken, ist verblüffend einfach. Ob ein Cyberangriff eine Maschine verschwinden lassen kann, ist eine andere Frage.

»Kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberspace, mit Mitteln vorwiegend aus dem Bereich der Informationstechnik.« So definiert Wikipedia den Begriff »Cyberkrieg«, wobei auch im deutschsprachigen Raum das Wort »Cyberwar« viel gebräuchlicher sein dürfte. Es geht dabei um Angriffe auf militärische Infrastruktur, deren Ziel es ist, die digitale Kommunikation auszuschalten oder in Rechnersysteme einzudringen, um Informationen zu erhalten, die Systeme abzuschalten oder die Kontrolle über sie zu übernehmen. Bei den zivilen Systemen könnten das Stromnetz, Ampelschaltungen oder Atomkraftwerke zum Ziel von Cyberangriffen werden.
Unter den vielen Vermutungen im Drama um den Flug MH370 der Malaysian Airlines gab es auch die, ein Hacker-Angriff habe stattgefunden. Theoretisch ist das möglich. Doch wie funktioniert Cyberwar in der Luft?
Moderne Flugzeuge funktionieren computergestützt, was bedeutet, dass die Funktionen und die Kontrolle einer Maschine von Computern abhängig sind. Ohne Computer funktioniert bei modernen Flugzeugen fast nichts – deshalb sind gleich drei Systeme davon an Bord. Dies dient einerseits dazu, dass man noch Reservesysteme hat, falls ein Rechner mal ausfällt, aber auch dazu, dass automatisch bemerkt wird, wenn mit einem davon etwas nicht stimmt, er also andere Ergebnisse liefert als die beiden anderen. Man weiß dadurch auch gleich, bei welchem Computer die Fehler auftreten – in der Theorie zumindest.
Zu erkennen sind die computergestützten Flugzeuge am Cockpit, bei dem anstatt der klassischen Rundinstrumente mit Zeigern Mehrzweckdisplays vorhanden sind – also Bildschirme, auf denen der Computer die gerade benötigten Instrumente einblenden kann. Im Airbus gibt es nicht mal mehr einen klassischen Steuerknüppel vor den Pilotensitzen, sondern nur einen kleinen Joystick an der Seite. Bei Boeing gibt es den Steuerknüppel noch, allerdings generiert auch dieser elektronische Signale und bewegt nicht mehr wie früher die Klappen direkt über ein Hydrauliksystem.
Die Computer und die Programme, die für die Flugzeugsteuerung verwendet werden

dürfen, werden deshalb nach strengen Kriterien getestet und nach »DO-178B Level A« zertifiziert. Damit soll vermieden werden, dass kritische Systeme abstürzen oder falsche Berechnungen enthalten – und aufgrund der Abhängigkeit von den Computern zu einem katastrophalen Unfall führen können. Der Ausfallsicherheit kommt in der Luftfahrt verständlicherweise große Bedeutung zu.

Doch Ausfallsicherheit ist nicht die Art von Sicherheit, die gegen Angriffe auf Computersysteme durch Hacker oder Cyberkrieger schützt. Denn kann man ein Computersystem kompromittieren, dann gelingt dies auch mit mehreren. So erreichte den Flugzeughersteller Boeing im November 2013 eine Nachbesserungsaufforderung, nachdem er im August 2012 die Einführung eines Entertainment-Netzwerks für die Passagiere beantragt hatte. Das Netzwerk für die Unterhaltung, auf die jeder Passagier Zugriff haben sollte, war nicht ausreichend von den kritischen Computersystemen getrennt, die für den reibungslosen Flug sorgen sollen. Ein Hacking-Versuch aus der Passagierkabine wurde von der Zertifizierungsstelle offenbar für durchaus möglich gehalten.
Für diese vom Hersteller zunächst nicht beachtete Angriffsmöglichkeit muss man aber immerhin selbst im Flugzeug sitzen. Dass es auch anders geht, zeigte im Mai 2013 auf der Amsterdamer Security Conference mit dem Titel »Hack in the Box SecConf« der Spanier Hugo Teso, der bei einer IT-Security-Firma arbeitet und Fachkenntnis als Pilot mitbringt. In seinem Vortrag »Aircraft Hacking: Practical Aero Series« deckte Teso Sicherheitslücken auf und zeigte, wie er mit einer Smartphone-App Flugzeuge unter Kontrolle bringen und fernsteuern kann – natürlich nur für Demonstrationszwecke in einer virtuellen Umgebung. Einige Details ließ er dabei bewusst aus, um zu vermeiden, dass Nachahmer seinen Vortrag als Anleitung nehmen könnten, etwas Vergleichbares zu programmieren.
Flugzeugcomputer sind keine abgeschlossenen Systeme. Sie kommunizieren per Funk mit Satelliten und Bodenstationen, zum Beispiel über das durch den Fall des Fluges MH370 bekannt gewordene Aircraft Communications Addressing and Reporting System (Acars), aber auch über Automatic Dependent Surveillance-Broadcast (ADS-B) mit anderen Flugzeugen oder Stationen am Boden. Diese Kommunikationssysteme funktionieren ohne Zutun der Piloten automatisch. ADS-B nutzt keinerlei Verschlüsselung und übermittelt Daten wie Flughöhe, Richtung, Geschwindigkeit und Position. Es kann also mit einem passenden Empfänger abgehört werden und mit einem passenden Sender könnte das System sehr einfach überlastet werden, indem man Daten immer wieder absendet oder auch falsche Daten einspielt. Mit falschen Daten könnte zum Beispiel ein virtuelles Flugzeug vorgetäuscht werden, das auf einem Kollisionskurs fliegt und so ein Flugzeug zu einem Ausweichmanöver zwingt, weil es oft als Radarersatz eingesetzt wird. Dies ist aber noch keine richtige Kontrollübernahme, weil ja nur die Piloten zu einer unnötigen Aktion verleitet werden – ein Flugzeug umleiten kann man damit nicht.

Acars allerdings bietet weit mehr Möglichkeiten. Auch dieses System ist im Normalfall unverschlüsselt, manchmal jedoch wird ein monoalphabetisches Verschlüsselungssystem benutzt. Eine solche Verschlüsselung ist relativ einfach zu knacken, da nur jeder Buchstabe durch einen anderen ersetzt wird – und zwar jedes Mal durch den gleichen. Selbst das Enigma-System aus dem Zweiten Weltkrieg war gleich mehrere Ligen sicherer. Für Acars gibt es zwei Service Provider, die miteinander konkurrieren und die deshalb ihren Kunden möglichst viel Funktionalität anbieten wollen. Daher bietet das System die

Möglichkeit, zusätzliche Software zu installieren – über Funk, man braucht dafür nur zu wissen, welche Geräte mit welcher Softwareversion in einem bestimmtem Flugzeug verbaut sind. Und dies kann man mit großer Sicherheit aus den von dem jeweiligen Flugzeug gesendeten Acars-Nachrichten erschließen. Dadurch ist es möglich, in einem Flugzeug eigene Software nachzuinstallieren. Und da es intern in den Computern keine Sicherheit gibt, kann man so Zugriff auf alle anderen Systemkomponenten erlangen, vom Autopiloten über die Instrumentenbildschirme bis hin zu der Innenbeleuchtung. Ob ein neuer Flugplan eingegeben wird, das Flugzeug Kurs auf den Boden nimmt oder auf einem Bildschirm des Piloten eine Chat-Oberfläche angezeigt wird, wäre dem Hacker überlassen. Dazu müsste ein Angreifer nicht mal direkt in Kommunikation mit dem Flugzeug stehen, denn es wäre ihm möglich, mit Programmen wie dem von Teso geschriebenen vorzugeben, dass zum Beispiel eine Flugplanänderung erst dann aktiviert werden soll, wenn das Flugzeug in die Nähe einer bestimmten Geokoordinate kommt. Sollten die Piloten merken, dass etwas nicht stimmt, dann könnten sie eingreifen, indem sie den Autopiloten abschalten und auf ein Notsystem wechseln. »Aber die Piloten kann der Hacker auch einsetzen, weil er ihre Reaktionen auf bestimmte Vorfälle kennt: Im Flugbetrieb läuft alles nach Checklisten«, so Teso.

Mit echten Flugzeugen hatte Teso sein Programm zum Zeitpunkt der Konferenz noch nicht ausprobiert, lediglich mit der Originalsoftware aus Flugzeugen. Er habe aber mit den Herstellern Kontakt aufgenommen, diese zeigten sich interessiert und wollten mit ihm zusammenarbeiten, berichtete er.

Auf die Nachfrage, ob man wirklich nicht im Flugzeug sitzen müsse, um es zu hacken, erwiderte Teso: »Die wichtigste Regel ist, niemals in dem Flugzeug zu sitzen, das man hackt. Es kann viel schiefgehen. Bumm.«