BDLI Fachausschuss Cybersicherheit

EXEMPLARISCHE CYBERBEDROHUNGEN IN DER LUFT- UND RAUMFAHRT

Online lesen/
read online:

BDLI

Bundesverband der Deutschen Luft- und Raumfahrtindustrie e. V. (BDLI)

BDLI Fachausschuss Cybersicherheit

EXEMPLARISCHE CYBERBEDROHUNGEN IN DER LUFT- UND RAUMFAHRT

Online lesen/
read online:

EINLEITUNG

Cyber-Bedrohungen sind heute allgegenwärtig und machen auch nicht vor der Luft- und Raumfahrtindustrie halt. Fast schon täglich gibt es Meldungen in den Medien zu erfolgten Cyber-Attacken und viele Unternehmen sind selbst schon Opfer von dementsprechenden Angriffen geworden. Bei den Verantwortlichen von Unternehmen und anderen Organisationen macht sich Verunsicherung breit. „Sind wir auch im Fadenkreuz von Cyber-Angreifern?“, „Welche Bedrohungen und Risiken betreffen uns wirklich?“ und „Was müssen wir tun um uns effektiv zu schützen?“ – Das sind typische Fragen, die sich Unternehmenslenker heutzutage stellen, oft genug ohne entsprechende Antworten zu bekommen. Bei vielen ist die Konsequenz, dass sie diese potentiellen Bedrohungen eher ignorieren anstatt sich ihnen zu stellen und grundlegende Maßnahmen zur Absicherung in die Wege zu leiten.

Wie auch andere Branchen ist die Luft- und Raumfahrtindustrie betroffen. Neben herkömmlichen Auswirkungen durch Beeinträchtigung des IT-Betriebs sowie Wirtschaftsspionage gibt es auch eine Reihe von Luft- und Raumfahrt-spezifischen Bedrohungen und Schwachstellen für die geeignete Schutzmaßnahmen getroffen werden sollten. Das vorliegende Papier soll zu möglichen Schwachstellen und Bedrohungen in der Luft- und Raumfahrtindustrie sensibilisieren. Hierzu werden im Folgenden einige Beispiele vorgestellt. Neben einer kurzen Beschreibung von Schwachstelle bzw. Bedrohung werden jeweils mögliche Auswirkungen skizziert und Sicherheitsmaßnahmen umrissen.

INHALT

TYPISCHE BEISPIELE FÜR SCHWACHSTELLEN

TYPISCHE BEISPIELE FÜR SCHWACHSTELLEN UND BEDROHUNGEN

BEISPIEL 1: KOMPROMITTIERUNG VON HARDWARE

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Sowohl marktverfügbare Hardwarekomponenten, als auch extern auftragsgefertigte eigene Hardwareentwürfe können Funktionalitäten enthalten, welche die Integrität der zu verarbeitenden Informationen und der Einsatzumgebung gefährden können. Dabei können gezielte Manipulationen in der Produktion oder auf dem Transportweg durch Angreifer vorgenommen werden. Die Entdeckung dieser Hardware-Manipulationen ist äußerst schwierig.

Online mehr erfahren

BSI-Pressemitteilung vom 05.10.2018: Spionage-Chips in Serverplatinen

Fraunhofer Institut - HARDWARE-TROJANER: Überblick und Bedrohungslage (08/17)

TYPISCHE AUSWIRKUNGEN

Beispielsweise wurden im Jahr 2008 PIN-Terminals für Kreditkartenzahlungen in der Supply-Chain so manipuliert, dass die Terminals Authentifizierungs-Informationen der genutzten Karten an die Angreifer gesendet haben. In ähnlicher Weise könnte kompromittierte Hardware genutzt werden um Leistungsdaten, Flugeigenschaften, Verbrauchsdaten und Systemausfälle eines Luftfahrzeuges abzugreifen und diese Daten konkurrierenden Unternehmen/Herstellern zugänglich zu machen.

MASSNAHMEN

Um das Risiko der Hardware-Kompromittierung zu verringern, müssen wirksame Maßnahmen im Bereich der Supply-Chain-Security ergriffen werden. Dazu zählen die Auswahl vertrauenswürdiger Lieferanten bzw. Fertigungsbetrieb, Auswahl zertifizierter Hardware (z.B. nach Common Criteria) oder der Rückverlagerung von Outsourcing für kritische Fertigungsprozesse.

Online mehr erfahren

BSI-Grundschutz-Katalog M 2.563
Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme

BSI-Grundschutz-Katalog M 2.66
Beachtung des Beitrags der Zertifizierung für die Beschaffung

BEISPIEL 2: SOFTWARE-MANIPULATIONEN

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Die Entwicklung von Software ist und wird zunehmend komplexer. Zum einen gibt es Software-Projekte, an denen eine Vielzahl von Personen mitarbeitet. Und zum anderen werden vermehrt Quelltexte oder Bibliotheken von Dritten, zum Beispiel aus OpenSource Projekten, eingebunden. Hierbei besteht die Gefahr, dass Schad- oder Spionagefunktionalitäten unbemerkt Bestandteil von selbst entwickelten Software-Projekten werden können. Des Weiteren können Angreifer u.U. durch vorhandene Sicherheitslücken in der eigenen Software zum Ausführungszeitpunkt Schadcode einschleusen.

Online mehr erfahren

When Good Software Goes Bad: Malware In Open Source

Distributing Malware By Becoming an Admin on an Open-Source Project

TYPISCHE AUSWIRKUNGEN

Die Folgen von Software-Manipulationen können vielseitig sein. Angreifer können sich Zugriff auf Informationen verschaffen, welche zur Bloßstellung von Geschäftsgeheimnissen führen kann – daraus kann sich ein signifikanter Wettbewerbsnachteil entwickeln.

Es ist auch möglich, dass die manipulierten Software-Bestandteile erst in der Nutzung, wie im Luftfahrzeug aktiv werden und dort zu Systemstörungen führen können. Im besten Fall beschränken sich die Auswirkungen daraus auf einen Reputationsverlust für das eigene Unternehmen, im schlimmsten Fall hingegen kann die Flugfähigkeit des Luftfahrzeugs beeinträchtigt werden.

MASSNAHMEN

Um das Risiko der Software-Kompromittierung zu verringern, sollten u.a.

- externe Quelltexte oder Bibliotheken nur aus zuverlässigen, nachvollziehbaren Quellen verwenden,
- regelmäßige Code-Checks durch externe Spezialisten durchgeführt werden.
- Um nachträgliche Manipulationen zu erkennen, bietet sich der Einsatz von kryptografischen Verfahren an, wie bspw. signierte Software-Komponenten.
- Bei häufigen Aktualisierungsintervallen der Software sollten darüber hinaus automatisierte Test-Verfahren zur Code-Analyse und -Verifikation implementiert werden.

Online mehr erfahren

BSI–IT-Grundschutz-Katalog M 2.573: Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung

BSI–IT-Grundschutz-Katalog M 4.93: Regelmäßige Integritätsprüfung

BEISPIEL 3: WIRELESS ON-BOARD NETWORKS

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Im zivilen Luftfahrtbetrieb verspricht eine zunehmend vernetzte Kabine optimierte Abläufe für das Kabinenpersonal bei ihrer täglichen Arbeit. Die Entwicklung geht auch zu kabellosen Geräten, um das Kabinenpersonal zu unterstützen. Bereits heute sind WiFi-Geräte erhältlich, um in Flugzeugen verbaut zu werden. Durch die Eigenschaften, dass das Übertragungsmedium Luft frei zugänglich ist und dass WiFi Geräte auf dem freien Markt verfügbar sind, ist eine technische Zugänglichkeit zu diesen Geräten leicht herzustellen. Aus diesem Grund stellt eine solche offene Kommunikationsschnittstelle einen möglichen Angriffsvektor dar. WiFi Sicherheit wird über das WPA (WiFi Protected Access) Protokoll hergestellt. Aktuell in der zweiten Generation, weißt WPA 1 und WPA 2 Sicherheitsmängel auf, welche in Flugzeugkabine ausgenutzt werden können. Dazu benötigt ein Angreifer wenig Spezial Hardware, ein WiFi mit vielen Teilnehmern und ausreichend Zeit.

Online mehr erfahren

Aircrack-ng, Tool zum brechen älterer WiFi Verschlüsselungen wie WPA1

Key Reinstalation Attacks (KRACK-Attacks) on WPA2

Dragonblood – Sicherheitslücke in WPA3 -Personal

TYPISCHE AUSWIRKUNGEN

Durch die strenge Trennung der Kabinensysteme von den flugkritischen Systemen ist zwar nicht von einer Gefährdung der funktionalen Sicherheit auszugehen, allerdings wäre es denkbar, dass es zu Einschränkungen in der Operabilität der Kabine kommen kann. Dadurch wären Verzögerungen am Flughafenterminal denkbar oder auch Änderungen der operationellen Abläufe des Kabinenpersonals während des Flugs.

MASSNAHMEN

Typische Maßnahmen zur Minderung dieser Bedrohung umfassen zum Beispiel die Verschlüsselung der Datenübertragung zwischen kabellosen Geräten und den WiFi Access Points, Detektionsmechanismen zum Erkennen von WiFi Angriffen und die Authentifizierung der kabellosen Geräte.

BSI – IT-Grundschutz-Kataloge M 2.381 bis M 2.390
Organisatorische Maßnahmen aus BSI-GS-Maßnahmenkatalog zum WLAN-Einsatz

Online mehr erfahren

BEISPIEL 4: WARTUNGS-/DIAGNOSE-SCHNITT-STELLEN

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Wartungs- und Diagnose-Schnittstellen des Lfz stellen Schwachstellen dar.
An den Wartungs- und Diagnose-Schnittstellen des Lfz können entsprechende Prüfgeräte/Tester (sog. Bodenprüfgeräte/AGE - Aircraft Ground Equipment) an das Lfz angekoppelt werden und mit dem Lfz Daten zu Prüf- und Kontrollzwecken austauschen (Sensorenprüfung, Kalibrierung, Fehlerdatenauslesung, etc.). Dies betrifft insbesondere computergestützte Prüfgeräte mit entsprechender Datenverarbeitung. Ebenso können über dedizierte Schnittstellen neue Software-Versionen bzw. Patches für Lfz-Systeme eingespielt werden.

Bedrohungen sind
- Kompromittierte Wartungsgeräte
- Unbekannter uni- bzw. bidirektionaler Datenfluss zwischen AGE und Lfz
- Laden manipulierter oder mit Schadsoftware belasteter Software für Lfz-Systeme

TYPISCHE AUSWIRKUNGEN

Über diese Schnittstellen könnten einerseits vertrauenswürdige, sensitive Daten aus dem Lfz abgegriffen werden wie auch schadhafte Daten und/oder Software in das Lfz eingespielt werden, die zu Störungen und dem Ausfall von Systemen bis hin zum Kontrollverlust über das Lfz führen können.

Auswirkungen für Zulieferbetriebe von Prüfgeräten oder Software
- Verstoß gegen IT-Sicherheitsanforderungen (keine Akkreditierung und Freigabe zur Nutzung, keine Abnahme)
- Verstoß gegen luftfahrtrechtliche Vorschriften (Safety / DEMAR-Regelungen)
- Verstoß gegen datenschutzrechtliche Bestimmungen
- Regressforderungen bei Störungen und im Fehlerfall sowie bei der Kompromittierung von Daten bzw. Manipulation von Software

MASSNAHMEN

Technische Maßnahmen:

- IT-Sicherheitsmaßnahmen für computergestützte Prüfgeräte vorsehen (Virenscanner, Rollen /Rechte, Autorisierung)
- IT-Sicherheitsmaßnahmen für Anschlüsse/Ports der Prüfgeräte vorsehen[2]:
  - Deaktivierung von Ports im BIOS (passwort-geschützt); Aktivierung nur zum Zeitpunkt der aktiven Nutzung
  - Physikalische Sperrung von Ports durch verriegelbare Schutzkappen etc. oder Trennung der Kabelverbindung
  - Ggf. keine Standard-Anschlüsse, sondern spezielle Ports mit nicht spezifischen Buchsen und Steckern
- Offenlegung des Datenflusses zwischen Prüfgerät und Lfz (Schnittstellendokument)
  - Datenfluss vom Prüfgerät in das Lfz
  - Datenfluss vom Lfz zum Prüfgerät
- Einsatz von zertifizierten Verfahren sowie Formaten und Protokollen für den Datenaustausch
- Einsatz von Code-Signaturen zur Sicherstellung der Integrität und Herkunft der Daten bzw. Software

Organisatorische Maßnahmen:

- Zutrittsbeschränkung/-regelung für Lfz
- Keine offen zugänglichen Ports
- Sichere, manipulationsgeschützte Verwahrung der Prüfgeräte
- Einrichtung und Verwendung einer geeigneten Signatur[3] (Certfication Authority, Ausgabe und Verwendung von Zertifikaten, Überprüfbarkeit von Signaturen)

BEISPIEL 5: UNGESICHERTE ÜBERTRAGUNG SENSITIVER DATEN

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Sensitive Daten wie z.B. Personaldaten oder sensitive Daten werden ohne bzw. nicht ausreichenden Schutz leitungsgebunden, per Datenträger oder per Funk übertragen.
Die Daten könnten von nicht berechtigten Personen / Stellen abgehört und mitgelesen werden zum Schaden der Dateneigentümer.

Beispiele/Referenzen zu Vorfällen oder Schwachstellen

- Offenlegung von Personaldaten der Besatzung
- Offenlegung von Gesprächen im Cockpit (Cockpit Voice Recorder)
- Offenlegung technischer Daten/Maintenancedaten, die der Airline bzw. dem Hersteller vorbehalten sind (technische Probleme, Ausfall, Störungen am Lfz)

TYPISCHE AUSWIRKUNGEN

Die Offenlegung von personenbezogenen Daten kann zu einem Verstoß der datenschutzrechtlichen Regelungen (Bundesdatenschutzgesetz) führen und somit geahndet werden. Betroffene Personen, deren Daten offengelegt wurden, können beeinträchtigt werden. Bei der Offenlegung sensitiver Daten können geheimschutzrechtliche Regelungen verletzt werden.

Die Offenlegung technischer Daten kann zu Vertrauensverlust (Reputation) führen und Nachteile für die Airline bzw. den Hersteller bewirken.

MASSNAHMEN

Technische Maßnahmen:

- Separierung von schützenswerten, sensitiven Daten
- Einsatz von zertifizierten und zugelassenen Kryptoverfahren und Kryptogeräten für die Übertragung
- Kryptierte Datenspeicher (Laufwerke, Datenträger) zur Datenspeicherung

BEISPIEL 6: SPOOFING VON ZEITEMPFÄNGERN

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Unterschiedlichste Industrien wie Mobilfunk- und Satelliten-Kommunikations-Systeme, Monitoring- und Steuerungs-Systeme für Energieverteilungsnetze, Finanz-Transaktions-Systeme und Transportsysteme etablieren Zeitsynchronizität an z.T. weit auseinanderliegenden Orten häufig durch den Einsatz von Satellitennavigations-Empfängern.

Satnav-Empfänger berechnen zur exakten Bestimmung ihres Ortes auch die Zeit des Satellitenavigations-Systems, dessen Signale sie verarbeiten. Zu diesen Systemen gehören GPS, Galileo, GLONASS und Beidou. Satnav-Empfänger dienen daher auch als langzeitstabile Zeitnormale oder "Zeit-Empfänger" und werden für o.g. Systeme eingesetzt.

Für zivile Anwendungen werden dabei die öffentlich verfügbaren, unverschlüsselten Signale der Satnav-Systeme genutzt, was das Stören (Jamming) und das unbeabsichtigte bzw. absichtliche Fälschen (Spoofing) der empfangenen Signale durch Dritte ermöglicht.

TYPISCHE AUSWIRKUNGEN

Das Spoofen von Zeitempfängern kann zum Ausfall von z.B. Mobilfunksystemen führen, da die empfangenen Signale der Mobilteile an der gespooften Basisstation zu anderen Zeiten erwartet werden als sie tatsächlich eintreffen. Moderne Energieverteilungs-Netze werden durch dezentrale Monitoreinheiten überwacht, die oft mit GPS-Empfängern ausgestattet sind. Das Spoofen dieser Monitoreinheiten um wenige Mikrosekunden könnte zum Zusammenbrechen der Netze führen [1].

Angreifer auf Finanztransaktions-Systeme könnten sich durch Beeinflussen der Zeitstempel eines Handelsplatzes Vorteile durch entsprechend geplante Transaktionen verschaffen.

MASSNAHMEN

Die Art der Maßnahme hängt von den Genauigkeitsanforderungen an das Zeitnormal ab. Eine Analyse muss erfolgen ob ein System kritisch auf Abweichungen im Nano- und Mikrosekundenbereich reagiert oder ob Abweichungen höheren Grades tolerierbar sind.

Um im ersteren Fall gegen direkte Auswirkungen von Jamming und Spoofing gewappnet zu sein müssen Zeitempfänger bzw. NTP-Server mit genauen Uhren ausgestattet sein, um einen GPS-Signalausfall überbrücken und eine Fälschung des GPS-Signals erkennen zu können. Dazu gibt es auf dem Markt Zeitempfänger mit Temperatur-stabilisierten Quarzoszillatoren die für typischerweise einige Stunden eine kontinuierliche Zeitreferenz liefern.

Im Gegensatz zu herkömmlichen Satnav-Empfängern mit nur einer Antenne arbeiten Spoofing-gehärtete Satnav-Empfänger beispielsweise mit Array-Antennen um die Quelle der ausgesandten Signale feststellen zu können. Z.B. lässt sich dadurch die Elevation von echten Satellitensignalen von der typischerweise niedrigen Elevation von terrestrischen Spoofern unterscheiden.

Kryptographisch gesicherte Signale sind außer bei Galileo nur für militärische Nutzer vorgesehen. Galileo bietet mit dem Public Regulated Service (PRS) ein nicht oder nur schwer fälschbares Signal auch für zivile Nutzer wie Blaulichtkräfte und kritische Infrastrukturen. Bei diesem Anwenderkreis sollten daher auf dem PRS-basierende Zeit-Empfänger in Betracht gezogen werden.

Für Anwendungen mit geringeren Anforderungen an die Genauigkeit können Zeitempfänger auf redundante Zeitquellen wie Mobilfunksysteme und DCF77 zur Zeitstabilisierung zurückgreifen.

---

[2] Auch für Anschlüsse/Ports, die in Verbindung mit dem Lfz nicht genutzt werden, aber am Prüfgerät vorhanden sind.
[3] Prüfung, welche Stufe der Signatur (einfach, fortgeschritten, qualifiziert) zum Schutz der Daten/SW erforderlich ist
[1] "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks", Daniel P. Shepard et al. ION GNSS 2012.

BEISPIEL 7: AUFHEBUNG DER VERTRAULICHKEIT MITTELS QUANTENCOMPUTING

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Die etablierten Verfahren zur asymmetrischen Verschlüsselung, zur Erstellung von Signaturen und dem Aushandeln von symmetrischen Schlüsseln basieren auf herkömmlichen Computern nur schwer lösbaren mathematischen Problemen, beispielsweise der Primfaktorzerlegung großer Zahlen und dem diskreten Logarithmus. Quantencomputer werden in der Lage sein diese Probleme effizient und damit in kurzer Zeit zu lösen, sodass die Vertraulichkeit von übertragenen oder gespeicherten Informationen ab dem Zeitpunkt der Verfügbarkeit dieser Quantencomputer nicht mehr gewährleistet werden kann. Z.Z. sind in Laboren Quantencomputer mit 72 Qubits Stand der Technik. Man schätzt, dass zum Lösen o.g. mathematischen Probleme Quantencomputer mit 1000 Qubits nötig sein werden. Weiterhin erwartet man, dass derartige Geräte in ca. 10-20 Jahren verfügbar sein werden. Symmetrische Verschlüsselungsverfahren sind bei ausreichender Schlüssellänge nicht betroffen. Dies betrifft alle Industrien, die verschlüsselte Netzwerkkommunikation für z.B. E-Mail, Dateiaustausch und VPNs nutzen.

TYPISCHE AUSWIRKUNGEN

Viele Anwendungen nutzen das Internet als öffentlich zugängliches Netz um mittels Verschlüsselung Daten vertraulich zu übertragen. Um die vertrauliche Sitzung zu starten kommt dabei häufig das Diffie-Hellman-Verfahren zum Einsatz, um einen gemeinsamen Schlüssel zwischen zwei Parteien auszuhandeln. Wird der Datenverkehr während der Sitzungs-Initiierung von einem Angreifer aufgezeichnet, der im Besitz eines entsprechend ausgerüsteten Quantencomputers ist, kann der ausgehandelte Schlüssel mit gewisser Wahrscheinlichkeit berechnet werden. Alle darauffolgende Kommunikation der beiden Kommunikationspartner ließe sich dann durch den Angreifer dechiffrieren. Dieser Angriff betrifft den Austausch aller Art von Daten über das Internet oder virtuelle private Netzwerke vom Datentransfer mit Servern über die Kommunikation mit Cloud-Computern bis zur Kommunikation der E-Mail-Korrespondenz.

Auch wenn die Zeitspanne bis zum Verfügbarwerden von Quantencomputer und den darauf zu implementierenden Algorithmen lang erscheint, sollten Maßnamen zum Quantencomputer-Schutz bereits heute in Systemdesigns einfließen, z.B. durch die Wahl ausreichend langer Schlüssel.

Bodenbasierte Systeme können rechtzeitig ausgetauscht werden, wenn bestimmte kryptographische Verfahren durch Quantencomputer gebrochen wurden. Bei weltraumbasierten Systemen ist dies nicht möglich: Satelliten haben Lebensdauern von ca. drei bis 20 Jahren. Während dieser Laufzeit können i.A. keine Hardware-Updates im Orbit durchgeführt werden. Für zukünftige Systeme können Updatefähigkeiten der Software zum Verbessern der kryptographischen Funktionen an Board von Satelliten vorgesehen werden.“

MASSNAHMEN

Für Signaturverfahren kann schon heute das quantencomputer-sichere und als RFC 8391 standardisierte eXtended Merkle Signature Scheme (XMSS) verwendet werden.
Für Anwendungen und Missionen mit Bedarf nach langfristigem Schutz der Vertraulichkeit sollten Postquantum-Kryptographieverfahren und symmetrische Verfahren mit entsprechend gewählten Schlüssellängen eingesetzt werden, z.B. AES-256.

Online mehr erfahren

XMSS: eXtended Merkle Signature Scheme

BEISPIEL 8: DESTRUKTIVES VERHALTEN VON (EHEMALIGEN) MITARBEITERN

BESCHREIBUNG DER SCHWACHSTELLE/BEDROHUNG

Mitarbeiter und externe IT-Dienstleister verfügen über Insider-Wissen zur Unternehmens-IT und über Zutritt, Zugang und Zugriff zum Lesen und Bearbeiten von Daten und ggf. Systemkonfigurationen. Daneben sind in KMU häufig keine oder nur unzureichende technische und organisatorische Maßnahmen gegen Sabotage oder Spionage durch Innentäter etabliert. Mit den daraus resultierenden weitreichenden Handlungsmöglichkeiten können Mitarbeiter zum einen sehr flexibel die IT-Systeme nutzen und externe Dienstleister mit weniger Aufwand ihre Dienste durchführen. Zum anderen aber, sind ebenso leicht böswillige Manipulation oder Datenabflüsse durch frustrierte oder rachesuchende (z.T. ehemalige) Mitarbeiter und beauftragte Unternehmen möglich. Dieses Risiko besteht grundsätzlich auch bei externen Dienstleistern, was in den bekannten Fällen aber nur selten im Vergleich zu Mitarbeitern auftritt.

bitkom-Studie 2018:
Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

Online mehr erfahren

TYPISCHE AUSWIRKUNGEN

In einer Wirtschaftsstudie durch Bitkom Research wurde festgestellt, dass ca. 60% der befragten Unternehmen bereits durch ehemalige Mitarbeiter geschädigt wurden. Dabei werden sehr häufig Daten gestohlen und gelöscht, wie beispielsweise E-Mails, Kontakt- und Finanzdaten oder sensible Geschäftsgeheimnisse. In Fällen, in denen die Mitarbeiter über weitergehende Rechte verfügen, werden auch IT-Systeme sabotiert. Das Löschen von Geschäftsdaten kann zu erheblichen Störungen in den Arbeitsabläufen und zu Image-Verlusten bei Kunden führen. Durch das Löschen von Konfigurationsdaten durch Administratoren, kommt es zu Ausfall der IT-Systeme mit einer langen Wiederanlaufphase.

ZUSAMMENFASSUNG

Die eben vorgestellten Beispiele sollten einen möglichst breiten Überblick zu möglichen Bedrohungen und Schwachstellen geben, die spezifisch für Unternehmen in der Luft- und Raumfahrtindustrie sind. Es wird nicht der Anspruch erhoben, dass die Bedrohungslage dieser Industrie vollständig erfasst wird. Vielmehr dienen die Beispiele der Sensibilisierung von Entscheidungsträgern. Bei den Beispielen wurden jeweils weitergehende Informationsmöglichkeiten referenziert, insbesondere auch bei den empfohlenen Maßnahmen. Das Papier ersetzt damit aber nicht eine professionelle Beratung zu spezifischen, für ein Unternehmen jeweils relevanten Bedrohungen und den damit zusammenhängenden Risiken. Entscheidungsträgern wird daher empfohlen, sich bei einschlägigen Cyber-Security Dienstleistern Rat zu holen und eine maßgeschneiderte Empfehlung zur Behandlung relevanter Risiken erstellen zu lassen. Der BDLI kann bei der Vermittlung geeigneter Dienstleister Unterstützung anbieten.

IHR ANSPRECHPARTNER IM BDLI

Robert Friebe
Referent Digitalisierung, Cybersicherheit und UAV

Herausgeber:
Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. (BDLI)
Tel.: +49 (0)30 206140-0
kontakt@bdli.de
www.bdli.de

Fotocredits: Adobe Stock

November 2019

BDLI Fachausschuss Cybersicherheit