



Foto: shock/stock.adobe.com

STANDORTE

Hannover

AirITSystems GmbH
Benkendorffstraße 6
30855 Langenhagen

(Hannover Airport)
Postfach 42 01 62
30661 Hannover

Telefon: +49 511 977 4000
E-Mail: info@airitsystems.de

Frankfurt

Speicherstraße 49 - 51
60327 Frankfurt am Main

AWARO®
Telefon: +49 69 430536 22

Netzwerktechnologien
Telefon: +49 69 3807845 01

Berlin

Rosenthaler Straße 34 - 35
10178 Berlin
Telefon: +49 30 2332905 10

München

Elsenheimer Straße 65
80687 München

AWARO®
Telefon: +49 89 2000526 60

Netzwerktechnologien
Telefon: +49 89 2190959 66

Hamburg

Holstenhofweg 47b
22043 Hamburg
Telefon: +49 40 822128 75

Düsseldorf

Kaiserswerther Straße 85b
40878 Ratingen
Telefon: +49 151 116705 05

Aachen

Topsonic Systemhaus GmbH
Adenauerstraße 20
Europark A2
52146 Würselen
Telefon: +49 2405 4080 60

IMPRESSUM

AirITSystems GmbH

Benkendorffstraße 6
30855 Langenhagen

E-Mail: info@airitsystems.de
Telefon: +49 511 977 4000

Weitere Informationen unter:
www.airitsystems.de

AirIT | ONE

Sicherheitskonzept

WHITEPAPER

AirIT | ONE

Sicherheitskonzept

Unsere Serverinfrastruktur betreiben wir in einem der modernsten Rechenzentrumscluster Europas in Frankfurt am Main. Er ist nach ISO 27001 zertifiziert, bietet höchste Sicherheitsstandards und verfügt über redundante High-Speed Internetanbindungen an alle großen Carrier. Der ebenfalls 27001 zertifizierte Betrieb erfolgt vollständig inhouse durch ein eigenes Administratorenteam. Wir erreichen Verfügbarkeiten von deutlich über 99%.

Ein mehrstufiges Sicherheitskonzept sowie der Einsatz von Virenschutz- und Angriffserkennungsoftware schützen zuverlässig gegen unerlaubten Zugriff. Die konsequente Verschlüsselung sowohl der Dateien, der Passwörter als auch der Kommunikation zwischen Server und Browser stellt sicher, dass niemals Informationen unberechtigt sichtbar sind.

Als Tochterunternehmen der Fraport AG unterziehen wir alle Mitarbeiter einer strengen Zuverlässigkeitsprüfung und verpflichten diese umfassende Datenschutzrichtlinien einzuhalten. Ein eigener Datenschutzbeauftragter prüft die Einhaltung der Maßnahmen.

INHALT

01 Professioneller Betrieb in zertifizierten Rechenzentren	11
02 Schutz gegen unerlaubten Zugriff, Schadsoftware, sowie unerlaubten Zugriff Dritter (Hacking)	12
03 Schutz vor Systemausfall und Datenverlust	14
04 Sichere Datenübertragung	15
05 Minimierung menschlicher Schwachstellen	16
06 Datenübergabe nach Vertragsende	17
07 Einhaltung der Datenschutzkonformität	18
08 Aufrechterhaltung der oben genannten Maßnahmen	19



Höchste Standards unserer Rechenzentren

- ✓ Mehrstufiges Zugangskontrollsystem mit vollständiger Videoüberwachung
- ✓ Die AirIT-ONE-Systeme befinden sich in gesicherten Hardwareschränken
- ✓ Umfassende Brandschutzlösung mit Hochdruckwassernebel und Inertgas
- ✓ Mehrfach redundante Kühlung und Energieversorgung
- ✓ Redundante High-Speed Internetanbindung an alle großen Carrier

Foto: .shock/stock.adobe.com

01 | Professioneller Betrieb in zertifizierten Rechenzentren

Die AirIT-ONE-Cloud wird von der AirITSystems in drei hochsicheren, nach ISO 27001 zertifizierten Rechenzentren betrieben. Die Rechenzentren der Equinix (Germany) GmbH in Frankfurt zählen zu den modernsten und leistungsfähigsten in Europa. Sie genügen höchsten Sicherheitsanforderungen und ermöglichen durch die Anbindung an alle großen weltweit agierenden Carrier und den ebenfalls im Rechenzentrum befindlichen deutschen Internet-austauschknoten DE-CIX eine bestmögliche Internetanbindung. Das Offsite-Backup für Notfallszenarien erfolgt in einem dritten räumlich getrennten Rechenzentrum von Equinix in Frankfurt.

Die Administration aller Komponenten d.h. Netzwerk, Server und Speichersysteme erfolgt vollständig inhouse durch ein Administratorenteam, das ein 24x7 Operating der Lösung durch einen Mehrschicht Betrieb der IT Betriebsführung sicherstellt. Der Betrieb ist ebenfalls ISO 27001 zertifiziert. Wir arbeiten ausschließlich mit namhaften Hersteller zusammen. Mit dieser auf Zuverlässigkeit optimierten und vollständig redundanten Technik und einem automatisierten 24x7-Monitoring der wichtigsten Serverfunktionen erreichen wir aktuell Verfügbarkeiten von deutlich über 99%.



02 | Schutz gegen unerlaubten Zugriff, Schadsoftware, sowie unerlaubten Zugriff Dritter (Hacking)

Die Systeme der AirIT-ONE-Cloud sind durch Firewalls geschützt und werden ständig auf aktuellem Patch Level gehalten. Sicherheitsupdates werden in der Regel am Tag des Erscheinens eingespielt. Durch die Trennung von Frontend und Backend sowie die konsequente Trennung von Applikations- und Datenservern (Storage) haben wir ein mehrstufiges Sicherheitskonzept mit voneinander abgeschotteten Segmenten realisiert.

Zugangserteilung und Passwortsicherheit

Ein leistungsfähiges Rollen- und Privilegienkonzept erlaubt es dem Kunden, selbstständig neue Nutzer in seine AirIT-ONE-Datenräume einzuladen und differenziert zu berechtigen. Die Anmeldung dieser neuen Benutzer erfolgt über einen Aktivierungscode, der nach der Registrierung verfällt. Somit werden keine Zugangsdaten verschickt. Auf Wunsch kann die Aktivierung auch per Brief oder persönlich abgewickelt werden, um Versand von Aktivierungs-codes per E-Mail zu vermeiden.

Um potentiell unsichere Passwörter zu vermeiden, werden bei der Passwortvergabe sowohl die Länge als auch die Komplexität geprüft. Zugänge werden nach mehreren Fehlversuchen temporär gesperrt.

Der administrative Zugang auf die Systeme durch unser Technikteam ist konsequent durch eine 2-Faktoren-Authentifizierung abgesichert. Zusätzlich ist ein automatisches Angriffserkennungssystem (Intrusion Detection System) in die Firewalls integriert. Proaktive Überwachung der IT-Systeme und laufende Analysen zur aktuellen Bedrohungslage durch ein eigenes SOC sorgen für weiteren Schutz.

Jeder Nutzer hat zudem die Möglichkeit, seinen Account über eine 2-Faktor-Authentifizierung (2FA) doppelt abzusichern.

Die Speicherung der Passwörter erfolgt einweg-verschlüsselt nach einem vom National Institute of Standards and Technology (NIST) empfohlenen Verfahren, so dass selbst unsere Systemadministratoren keinen Zugriff auf das vom Nutzer gewählte Passwort haben.

Für sicherheitskritische Anwendungen können auch individuelle Security Policies definiert werden.

Individuelle Security Policies

- ✓ Verpflichtung zu 2-Faktor-Authentisierung (2FA)
- ✓ Erzwingene regelmäßige Änderung von Passwörtern (inklusive Passworhistorie)
- ✓ Automatische Deaktivierung nicht mehr benutzter Zugänge nach einer festgelegten Zeitspanne
- ✓ Beschränkung des Zugriffsortes (IP-Restriction)
- ✓ Anbindung Ihres Identity und Accessmanagementsystems für ein Single Sign-On (SSO) auf Basis von SAML.

Verschlüsselte Speicherung

Alle Dateien werden nach dem Hochladen automatisch verschlüsselt. Somit sind die Daten selbst auf Backups oder bei unbefugtem Zugriff auf die Speichersysteme gesichert. Die Dateien werden erst bei Auslieferung von der AirIT-ONE-Software entschlüsselt und direkt über eine sichere Verbindung an den Nutzer übertragen.

Prüfung auf Schadsoftware

Jede Datei wird vor der Speicherung in der AirIT-ONE-Cloud auf Virenbefall überprüft und befalle-ne Dateien abgelehnt. Virendefinitionen werden spätestens vier Stunden nach Erscheinen aktualisiert.





Foto: Gerdenthorff/stock.adobe.com

03 | Schutz vor Systemausfall und Datenverlust

Redundanz

Alle Systemkomponenten der Betriebsinfrastruktur sind vollständig redundant ausgelegt und auf zwei Rechenzentrumsstandorte verteilt. Zwischen diesen beiden Standorten findet eine Replikation der Daten in Echtzeit statt. Die Leitungswege zwischen den Hochverfügbarkeits-Clustern werden dabei stets disjunktiv geführt. In unserem leistungsfähigen Speichernetzwerk (SAN) setzen wir grundsätzlich per RAID gespiegelte Festplatten ein, so dass selbst ein gleichzeitiger Ausfall von zwei Festplatten keine Unterbrechung oder Datenverlust verursacht. Bestimmte Ausnahmen gelten für den Datenbank-Cluster und den Viewer Server.

Backup

Backup Server und angeschlossene Systeme für die Datenhaltung werden räumlich getrennt vom redundanten SAN Verbund in einem dritten Rechenzentrum betrieben. Für die Daten auf unserem SAN erfolgt täglich ein Backup. Von den Datenbanken wird viertelstündlich und täglich ein Backup durchgeführt und in ein räumlich getrenntes Rechenzentrum gespiegelt. Die jeweiligen Tagessicherungen werden eine Woche lang aufbewahrt.

04 | Sichere Datenübertragung



Die gesamte Kommunikation zwischen der AirIT-ONE-Cloud und Ihrem Rechner wird über TLS (Transport Layer Security, früher SSL genannt) mit mindestens 128-Bit Schlüssellänge verschlüsselt. Schon die Anmeldung erfolgt verschlüsselt, so dass kein Passwort im Klartext übertragen wird. Es werden Algorithmen mit Perfect Forward Secrecy (PFS) bevorzugt.

Die Nutzung von HSTS (HTTP Strict Transport Security) sowie OCSP Stapling verhindert den Einsatz gefälschter oder abgelaufener Zertifikate. Durch den Eintrag in die HSTS preload list wird die Verschlüsselung von allen modernen Browsern ab dem ersten Aufruf erzwungen. Unsere TLS Konfiguration wird regelmäßig auf bekannte Sicherheitslücken geprüft.



05 | Minimierung menschlicher Schwachstellen



Foto: Gorodenkoff/stock.adobe.com

Als ein IT-Tochterunternehmen der Fraport AG und der Flughafen Hannover-Langenhagen GmbH mit seinen sicherheitssensiblen Bereichen stellen wir besondere Anforderungen an unser Personal. Daher sind alle unsere Mitarbeiter nach dem Luftfahrtsicherheitsgesetz §7 einer positiven Zuverlässigkeitsprüfung unterzogen worden.

Revisionsichere Änderungsverfolgung

Jeder Zugriff auf unsere Systeme wird registriert. Unsere Logbücher werden stichprobenartig manuell sowie durch automatische Analysewerkzeuge regelmäßig analysiert. Innerhalb von AirIT-ONE werden alle relevanten Nutzeraktionen wie z.B. Lese- und Änderungszugriffe auf Dokumente, Nachrichten oder Aufgaben revisionsicher protokolliert. Alle vorhandenen Versionen und Arbeitsstände eines Dokuments können lückenlos nachvollzogen werden. Ein leistungsfähiges Rechtekonzept stellt sicher, dass jeder nur die Information sieht, die für ihn bestimmt ist.

In Fachmodulen mit besonderen Anforderungen wird durch die Anwendungslogik der Zugriff erst ab einem bestimmten Zeitpunkt (z.B. Ausschreibungsende) oder nach expliziter Freischaltung nach dem Mehraugenprinzip erlaubt.

Ebenso können dynamische Wasserzeichen in PDF-Dokumenten erzwungen, sowie z.B. der Druck untersagt werden.

06 | Datenübergabe nach Vertragsende



Mit unserem AirIT-ONE-Archiv bieten wir eine ausgereifte Lösung zur Übergabe der Daten auf einem Datenträger bei Projektabschluss oder bei Ausscheiden eines Projektbeteiligten. Um die Vertraulichkeit auch während des Transports sicherzustellen, sind die Daten auf dem Datenträger verschlüsselt. Sie können erst mit dem auf getrenntem Wege verschickten Passwort entschlüsselt und damit gelesen werden. Ein digital signierter Fingerabdruck macht eine unbemerkte Manipulation der Daten unmöglich. Wenn nicht explizit anders vereinbart, werden 8 Wochen nach Kündigung Ihres Projekt- oder Datenraums die Daten bei uns zuverlässig und vollständig gelöscht.



07 | Einhaltung der Datenschutzkonformität



Serverstandort Deutschland

Wir führen eine Auftragsdatenverarbeitung gemäß der europäischen Datenschutzgrundverordnung (DSGVO) durch. Die Speicherung und Verarbeitung der Daten findet ausschließlich auf Systemen in den oben genannten Rechenzentren in Deutschland statt.

Foto: senticus/stock.adobe.com

Personal

Das gesamte mit dem technischen Betrieb und der Benutzerbetreuung befasste Personal ist zur Geheimhaltung aller Plattforminformationen verpflichtet worden und hat eine entsprechende Erklärung zum Datenschutz und zur Geheimhaltung nach §5 BDSG unterzeichnet. Es finden verpflichtend jährliche Unterweisungen zu den Themen Informationssicherheit und Datenschutz statt. Neben der obligatorischen Bestätigung der allgemeinen Nutzungsbedingungen (ANB) im Zuge der erstmaligen Registrierung bei AirIT-ONE für neue User kann auf Wunsch auch die Zustimmung zu kundenindividuellen Vereinbarungen zur Vertraulichkeit eingefordert werden.

Alternativ zur Nutzung der AirIT-ONE-Cloud bieten wir auch einen Betrieb von AirIT-ONE inklusive der Datenspeicherung in der IT-Umgebung des Kunden an (On-Premises).



08 | Aufrechterhaltung der oben genannten Maßnahmen

Die aufgeführten Maßnahmen und Prozesse sind im Rahmen unserer QM- und ISMS-Managementsysteme geregelt und nach ISO 9001 und ISO 27001 zertifiziert. Zusätzlich hat die AirITSystems einen Datenschutzbeauftragten bestellt, der die Geschäftsführung bei der Einhaltung der Datenschutzrichtlinien unterstützt.

Die Wirksamkeit unserer Maßnahmen zum Schutz unerlaubter Zugriffe wird regelmäßig durch unabhängige Penetrationstests von unabhängigen Sicherheitsfirmen geprüft und die Ergebnisse werden zur Optimierung unserer Sicherheitsmaßnahmen genutzt.

In besonderen Fällen räumen wir Kunden auch ein Audit-Recht ein, um die Konformität mit den geforderten, eigenen Compliance Richtlinien selbst prüfen zu können.



ISO 27001 Zertifizierung für Betrieb und Rechenzentren

Wenn Sie Fragen zu diesem Whitepaper haben, sprechen Sie uns an...

Kontakt
AirITSystems GmbH
T +49 511 977 4000

vertriebsinnendienst@airitsystems.de
www.airitsystems.de

