AIR ZEN

Das AirZen System:

IT-SICHERHEITSKONZEPT

Für Sachverständige aus dem IT-Security Bereich

Executive Summary

AirZen ist Dienstleister, der seine Kunden dabei unterstützt, WLAN für deren Eigenbedarf und/oder deren Gäste bzw. Kunden zu betreiben. Diese Dokumentation beschreibt die zum o.g. Zweck von AirZen den Kunden zur Verfügung gestellte und betriebene Infrastruktur und insbesondere die zugehörigen Maßnahmen zur Einhaltung und Maximierung der verschiedenen Sicherheitsaspekte.

INHALTSVERZEICHNIS

AIRZEN NETZWERK SYSTEM

Das AirZen System besteht aus eigenentwickelter Hardware und Software mit eingebundenen „open source“ – Elementen und OEM - Modulen.

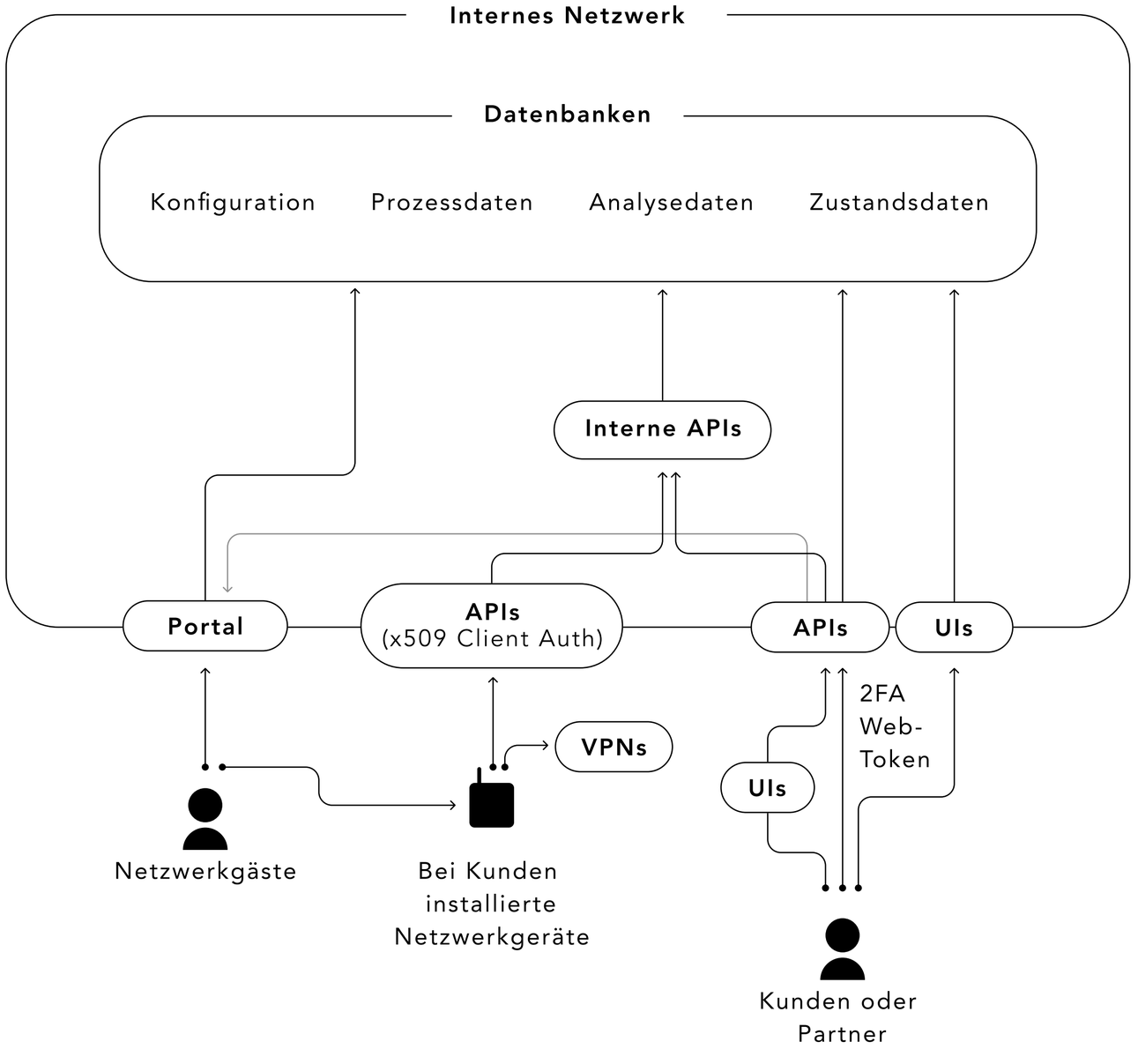
Die AirZen-Software-Gesamtlösung ist aufgeteilt in Server-, Client- und Komponenten-Funktionen. Die AirZen Hardware ist aufgeteilt in einzelne, geschlossene Geräte und abhängig vom Gerätetyp mit optionalen, i.A. integrierten Modulerweiterungen.

Das AirZen System unterstützt aktiv nur eigene, d.h. AirZen Accesspoints, -Router, etc.; d.h. dass solche Komponenten, die vom System überwacht, konfiguriert und administriert werden können. Alle sonstigen an das Netzwerk angeschlossenen Komponenten (Router, Switches, etc.) können an das AirZen-WLAN angeschlossen und im WLAN betrieben werden. Das AirZen System kann allerdings nur den allgemeinen Status dieser Geräte registrieren, z.B. ob sie eingeschaltet sind.

Die AirZen Plattform ist als Cloud-WLAN-System konzipiert, wobei die AirZen Accesspoints je nach Konfiguration über verschiedene Standorte hinweg als eine Einheit gesehen werden können.

SYSTEMÜBERSICHT

Die folgende Grafik veranschaulicht die Zugangs-Beziehungen zwischen den verschiedenen Systemkomponenten der von AirZen betriebenen Infrastruktur und den Anwendern sowie externen Diensten. Arbeitsbereiche, die nicht datentechnisch mit dem Back-End zum Betrieb der Netzwerke verknüpft sind, z.B. Vertrieb, sind in obiger Skizze nicht aufgenommen. Alle von AirZen betriebenen Anwendungen (innerhalb der angedeuteten „Wolke“) inkl. VPNs werden bei einem Cloud-Anbieter gehostet. Dies gilt auch für die Entwicklungs- und Testumgebungen. Neue bzw. weiterentwickelte Softwaremodule/-komponenten werden gegebenenfalls auch in lokalen Umgebungen entwickelt und dann in die jeweiligen Systeme geladen.



MODULARE SYSTEMARCHITEKTUR

Die wichtigsten Architektur-Prinzipien bei der Gestaltung und Ausprägung eigener technischer Lösungen von AirZen sind:

- die funktionsweise Aufteilung aller Dienste und Prozesse
- die Minimierung von Abhängigkeiten
- die klare Regelung von Zugriffsfragen bereits durch die Konfiguration

Die primären Vorteile daraus sind:

- Einzelne Anwendungen bzw. Komponenten lassen sich leichter zurück- oder neu aufsetzen oder austauschen, falls Störungen auftreten.
- Der Programm-Code ist überschaubarer, weniger fehleranfällig und besser pflegbar.
- Eine Überarbeitung oder (teilweise) Neuentwicklung einzelner Komponenten ist beherrschbarer, da entweder gar keine oder nur wenige Anpassungen an anderen Komponenten erforderlich werden.

Eine ausgefallene Komponente (z.B. ein einzelner Dienst) beeinflusst nur unmittelbar funktional abhängige andere Prozesse.

Security by Design
Bei der Entwicklung werden komplizierte Software-Stacks möglichst vermieden. Die Tokens, mit denen Schnittstellenbenutzer autorisiert werden, sollen präzise und verständlich sein, sodass immer klar ist, auf welche Ressourcen spezifischer Systeme ein Benutzer Zugriff erhält.

Die Netzwerkkonfiguration darf durch die Router nur gelesen werden, Schreibzugriff hat nur die Konfigurations-API; etc. Ein Administrator hat stets nur Zugriff auf spezifische Systeme (Server und Datenbanken), niemals auf alle. Die Entwickler haben Zugriff auf diejenigen Software-Komponenten, die sie jeweils bearbeiten. Im Einzelfall, bspw. bei Neuentwicklungen oder umfangreichen Testmaßnahmen, nutzt ein Entwicklerteam gegebenenfalls einen anderen Hoster oder separate, eigens eingerichtete Server. Die Daten verschiedener Kategorien werden immer getrennt gespeichert (siehe “Datenkategorien”). Auf diese Weise beeinflusst beispielsweise eine höhere Last der Datenbank für WLAN-Sitzungen nicht die systemkritische Datenbank für die Netzwerkkonfiguration.

SICHERHEITSANFORDERUNGEN

Da sowohl Hardware als auch Software niemals davor gefeit ist, fehlerhaft zu sein oder gezielt oder unbeabsichtigt verändert zu werden, sind einerseits Maßnahmen zur Betriebssicherheit und Systemstabilität und andererseits zum Schutz vor Eindringen und vor Manipulation erforderlich.
In weiteren Abschnitten dieses Konzepts sind entsprechende Maßnahmen in Bezug auf die wesentlichen System-Komponenten, System-Funktionen und Betriebs- wie auch Stör-Szenarien detailliert beschrieben.

Organisation der Sicherheit
Die federführende Zuständigkeit für die Regelung der Sicherheit und deren Fortschreibung / Anpassung liegt für das AirZen System bei der AirZen Networks Geschäftsführung. Das IT-Sicherheitskonzept wird in jeder AirZen Tochtergesellschaft für die jeweilige Zuständigkeit in Kraft gesetzt. Insbesondere mit Berücksichtigung von Systemerweiterungen und -Anpassungen wird das Sicherheitskonzept regelmäßig geprüft und bei Bedarf den jeweiligen Anforderungen angepasst.

Sicherheit beim AirZen-Personal und Sub-Dienstleistern
Alle Mitarbeiter:innen der AirZen Gruppe sowie externe Dienstleister:innen werden schriftlich hinsichtlich Vertraulichkeit und Datenschutz verpflichtet. Darüber hinaus ist dieser Personenkreis verpflichtet etwaige Vertraulichkeits- oder Datenschutz-Verstöße sofort anzuzeigen.

Die unverzügliche, gegenseitige Informationspflicht zu etwaigen Datenschutzverletzungen ist vertraglich auch zwischen AirZen und seinen Kunden vereinbart. Die Bearbeitung solcher Meldungen geschieht jeweils unter direkter Leitung der zuständigen AirZen-Geschäftsführung.

Als Hosting-Dienstleister werden von AirZen nur solche Einrichtungen hinzugezogen, die sich ihrerseits vertraglich und öffentlich zur Einhaltung der DSGVO verpflichten, nachweislich über eine Datenschutzorganisation und ein Informationssicherheitsmanagement verfügen und zuverlässige Verfahren zur Daten- und Systemsicherung anwenden.

Physische Sicherheit des AirZen-Systems
Alle zentralen Komponenten befinden sich im abgesicherten Rechenzentrumsbetrieb eines Hosting-Dienstleisters. Der Zugang zu den AirZen Servern ist nur den vom Betreiber explizit autorisierten Mitarbeitern gestattet. Die Zugangskontrolle ist gewährleistet.

Die AirZen-Administrations-Konsolen befinden sich in den Büros von AirZen. Hierbei handelt es sich um übliche Arbeitsplatzrechner, die mit den notwendigen Softwarekomponenten ausgestattet sind. Es gelten büroübliche Zugangsregeln bzw. Beschränkungen. Eine spezielle physische Sicherung dieser Terminals ist nicht erforderlich, da der Zugriff auf das AirZen System per Software und über mehrstufige Identifizierungsschritte gesichert ist; d.h. die Administrationshardware ist jederzeit austauschbar bzw. ersetzbar.

Die AirZen-Router / -Accesspoints werden innerhalb der Büro- und Betriebsräume der AirZen-Kunden oder im Freiland innerhalb deren Liegenschaften/Einrichtungen installiert.

Abhängig vom jeweiligen Publikumsverkehr, der spezifischen Branche und den örtlichen Gepflogenheiten haben sowohl Mitarbeiter:innen als auch Gäste Zutritt zu diesen Örtlichkeiten. In der Regel ist der Zugang zu den Accesspoints nicht speziell gesichert.

Dies ist nicht erforderlich, da alle Accesspoints permanent vom System überwacht werden und im Fall einer Manipulation entweder nicht mehr funktionieren oder diese Manipulation automatisch eine Zurücksetzung der Konfiguration auslöst. Zusätzlich sind bei nicht mechanischer Manipulation die Geräte i.d.R. per Fernadministration schnell rekonfigurierbar. Alle Konfigurationsänderungen und somit auch eventuelle Konfigurations-„Manipulationen“ werden in Log-Files festgehalten.

SOFTWARE DEFINED NETWORK TECHNOLOGY
über 40 Microservices
& digitale Infrastruktur

HARDWARE

AirZen Nodes
Router, Access,
Mesh & Security

TOUCHPOINTS

WiFi6
mehrere virtuell
getrennte Netze

Portal
umfassender
Self-Service

APP
volle Transparenz

Command Line
volle Kontrolle

AirZen Team
Managed Service

SERVICES

Administration
smarte Automatismen,
umfassende Analysetools,
autonome Updates

Nutzer-Netzwerke
mehrere Standorte im selben
Netz oder mehrere Subnetze
in einem Standort

Gäste-Netzwerk
sicher abgetrennt und mit
Marketingfunktion

Geräte & Internet of Things
volle Konnektivität mit hohen
Sicherheitsstandards

AirZen Protection Framework
VPN, Malware-Filter, BotNet-
Blocker uvm.

BETRIEB DES AIRZEN-SYSTEMS - KOMPONENTEN UND DIENSTE

Die Services von AirZen lassen sich in folgende Kategorien aufteilen:

- Betrieb und Pflege der AirZen Cloud
- Betrieb und Verwaltung von "VPN"-Gateways
- Betrieb und Administration von Routern, Access Points u.ä.
- Betrieb und Steuerung von Nutzerschnittstellen
- Konfiguration und Überwachung von Internet-Zugängen

AirZen Cloud
Die AirZen Cloud stellt die zentrale Schnittstelle zwischen ausführenden Techniker:innen und den AirZen-Routern dar. Eingaben erfolgen hierbei per Kommandozeile oder die AirZen App. Die Konfiguration basiert auf einem Software-Defined-Network-(SDN)-Prinzip. Dabei wird eine Konfiguration erstellt und in einer Datenbank gespeichert. Standortübergreifend beziehen die AirZen Router automatisch die Konfiguration, sobald eine Änderung erfolgt. Die AirZen Cloud unterstützt ausschließlich AirZen Router, keine fremde Hardware.

Gateway-Server
Auf Gateway-Servern werden keine Verbindungsprotokolle von Netzwerknutzer:innen erfasst. Log-Informationen zu Verbindungsversuchen werden standardisiert von den Routern erfasst und im Zuge der Log-Rotation regelmäßig gelöscht.

AirZen Router
Die AirZen Router speichern nur alle solchen Informationen, die für die eigentliche Routing-Funktion und die Funktionsweise des Gerätes erforderlich sind. Wenn die Router-API nicht erreichbar sein sollte, sind Netzwerkverbindungen weiterhin möglich. Auch das Gästeportal funktioniert, solang das Portal erreichbar ist. Einige Dienste, wie z.B. die Freischaltung neuer WLAN-Zugänge, setzen allerdings eine Verbindung zur AirZen Cloud und deren Funktion voraus.

Die AirZen Router erfassen und übertragen regelmäßig Statusinformationen. Alle diese Statusinformationen werden in einer flüchtigen Datenbank für einen begrenzten Zeitraum gespeichert.

Portal-Funktion
Das Portal benötigt für den Betrieb der Konfiguration, Sitzungen und Nutzungsdaten lediglich Zugang zu den Datenbanken. Zur Aktivierung einer „Sitzung“ kommuniziert ein Client-Gerät immer direkt mit dem Router. Falls die Konfigurationsdatenbank ausfällt, kann das Portal für alle bereits geladenen Konfigurationen weiteren Anwender:innen/Clients den Zugriff auf das Netzwerk vermitteln, da die Portal-Konfigurationen lokal und persistent zwischengespeichert werden. Nutzer:innen-Eingaben werden während eines Verbindungsausfalls zur entsprechenden Datenbank nicht gespeichert.

Besonderheiten im Betrieb
Die für die Verwaltung der Router kritischen Endpunkte und VPN-Gateways werden besonders gemanagt und administriert, da sie funktionsgemäß schlechter skalieren als andere Dienste und einzelne Server nicht gleichermaßen performant von allen Orten aus erreichbar sind. Daher werden im Betrieb beide auf die jeweilige Routeranfragen dynamisch zugewiesen. So lässt sich VPN-Traffic auf beliebig viele Gateways aufteilen. Gleiches gilt auch für die Routing-Endpunkte. Zudem lassen sich einzelne Systeme/Dienste im Problemfall durch dynamisch veränderbare Host-Namen jederzeit austauschen, ohne auf den Ablauf von DNS-Einträgen warten zu müssen.

KONZEPT ZUR GEWÄHRLEISTUNG & SICHEREN BEREITSTELLUNG DER AIRZEN NETZWERKDIENSTLEISTUNGEN

Um die Verfügbarkeit der Komponenten des Netzwerkbetriebes bei AirZen zu optimieren werden verschiedene Leitlinien angewendet:

- Auswahl geeigneter Architekturen
- Nahezu alle Probleme lassen sich in logische Einheiten einteilen. Die Einteilung sollte so gewählt werden, dass sie möglichst verständlich und technologisch sinnvoll ist. Meistens resultiert daraus eine Minimierung von Abhängigkeiten und eine besonders einfache Einarbeitung von Ingenieuren, die mit der Domäne vertraut sind.
- Nachhaltige Technologieentscheidungen
- Informatische Anwendungen stehen vor ständig wandelnden Anforderungen und Bedingungen. Bei der Auswahl von Komponenten und Tools sollte darauf geachtet werden, dass sie auch in absehbarer Zukunft unter Berücksichtigung neuer Möglichkeiten oder geänderter Sicherheitsstandards sinnvoll und nutzbar sind. Zum Beispiel wird zur Beendigung verschlüsselter Verbindungen oft auf Open-Source-Software zurückgegriffen, wodurch einfache Updates oft ausreichen, um Sicherheitslücken zu schließen.
- Monitoring und Fehlerbehebung
- Informationen zu im Betrieb auftretenden Fehlern werden für begrenzte Zeit vorgehalten und gegebenenfalls eine Benachrichtigung veranlasst. Sofern die Vertraulichkeit persönlicher Daten nicht beeinträchtigt wird, ist es wichtig, Endnutzer:innen möglichst transparent über auftretende Fehler zu informieren. Zur Vorbeugung von Ausfällen aufgrund hoher Last werden Speicherauslastung, Netzwerkverbindungen und CPU-Auslastung überwacht.
- Aktive Tests
- In einigen Prozessen ist es erforderlich, Informationen über die kurzfristige Verfügbarkeit von Abhängigkeiten zu haben, um im Fehlerfall eine minimale Funktionsfähigkeit sicherzustellen. Ein Beispiel hierfür ist der Diagnose-Endpunkt, den das Portal bereitstellt und den AirZen Nodes nutzen, um nicht nur den Zustand des Dienstes zu überprüfen, sondern auch Informationen über die Verbindung zwischen dem lokalen Netzwerk und dem Portal zu erhalten. Dadurch wird es möglich, Endnutzern gezielte Fehlermeldungen anzuzeigen, bevor sie selbst versuchen, eine Verbindung herzustellen.

Sowohl Server als auch Nodes können in Reaktion auf bestimmte Fehler automatisch E-Mails mit detaillierten Informationen an AirZen versenden. Wenn ein Eingriff zur Fehlerbehebung erforderlich ist, werden betroffene Kunden in den Prozess einbezogen. Meldungen, die nicht automatisch verarbeitet werden können, werden in das Ticketsystem übertragen, und die Zuweisung zur Bearbeitung erfolgt durch die entsprechenden Mitarbeiter:innen.

Ausfälle aufgrund von Fehlern / Störungen / DDoS-Angriffen
Ausgefallene oder gestörte Anwendungen werden nach Einschätzung und Ermessen des bearbeitenden System-Experten entweder ersetzt, korrigiert, rekonfiguriert oder reinitialisiert. Sollte ein kompletter Server fehlerhaft sein, kann er mit der gleichen IP neu aufgesetzt werden. Wenn dies nicht zum Erfolg führt, muss der Server vollständig ersetzt werden. In diesem Fall wird der neue Server erst dann aktiviert, wenn die DNS-Records zu den IPs des alten Servers abgelaufen sind.

Die Systemarchitektur ermöglicht auch, Teile des Back-Ends bei einem anderen RZ-Anbieter zu hosten oder in einem eigenen Rechenzentrum zu betreiben. Im Falle eines DDoS-Angriffs können die angegriffenen Dienste z.B. auf eigene Server ausgelagert werden, um benachbarte Dienste zu schützen.

ZUGRIFFSKONTROLLE UND DATENMANAGEMENT

Nutzungskategorien
Als Zugriffsberechtigte sind folgende Gruppen vorgesehen:

- Administratoren (Konfiguration und Zugriff auf Statusinformationen)
- Support-Partner (durch AirZen für definierte Aufgaben autorisierte Dritte)
- Netzwerkanwender:innen (Benutzer:innen der Netzwerke)
- Partner-Nutzer:innen (durch AirZen Kunden autorisierte Dritte)

AirZen selber hat u.a. spezifische interne Rollen für:

- Entwicklung
- Pflege und Wartung
- Betrieb und Systembetreuung
- Auslieferung und Logistik
- Kunden- und Anwendungsbetreuung
- Hotline

Netzwerkanwender:innen treten auf dem für das Medium/System üblichen Weg einem Netzwerk bei und werden dabei durch die für den Betrieb notwendigen/üblichen Informationen (MAC-Adresse/DHCP-Hostname) identifiziert und fallbezogen auf eine für das Medium/System vorgesehene Weise autorisiert (z.B. WPA2-PSK).

Alle Anwender:innen von Web-Schnittstellen sind für den Zugriff auf definierte Ressourcen bestimmter Kunden/Kundengruppen autorisiert. Auf ähnliche Weise können auch andere Dienstleister/Subunternehmen (“Partner”) zielgerichtet autorisiert werden.

Funktionen für interne Rollen von AirZen werden über ein eigenes Berechtigungsverfahren geregelt. Eine Ausnahme bilden dabei die sog. “Self-Service”-Dialoge, wie sie z.B. über eine Aktivierungsseite für WLAN-Passwörter zur Benutzung durch Netzwerk-Gäste oder über eine Übersichtsseite für Kunden, bei denen allein die URL den Zugriff ermöglicht, verfügbar sind. Der Zugriff auf das WLAN-Portal benötigt keinen eigenen Sicherungsmechanismus, da das Portal für alle Netzwerknutzer:innen erreichbar sein muss.

Datenkategorien
Daten folgender Kategorien werden vom AirZen System im Zusammenhang des Betriebes und der Nutzung der Netzwerke erhoben und gespeichert:

- notwendige Stammdaten (z.B. Netzwerkkonfiguration, Standortdaten, Kontaktinformationen, u.ä.)
- notwendige persistente Bewegungsdaten (z.B. Bestellungen, Vorgangsprotokolle zum Projekt- und Betriebs-Status, u.ä.)
- flüchtige Bewegungsdaten (z.B. verschiedene Echtzeitinformationen zu Betrieb und Nutzung der Netzwerke)
- sonstige Bewegungsdaten (z.B Eingaben von Nutzer:innen im Portal, Verfolgbarkeitsinformationen für den Betrieb und die Dienstebereitstellung, u.ä.)

Neben diesen Daten werden zusätzlich Verkehrsdaten erhoben. Eine Zusatzbeschreibung hierzu erfolgt an anderer Stelle in diesem Dokument.

Daten der ersten beiden und letzten Kategorie werden in PostgreSQL-Datenbanken gespeichert, von denen der Hosting-Dienstleister / RZ-Betreiber regelmäßige Backups anfertigt.

Flüchtige Bewegungsdaten verfallen automatisch nach einigen Wochen, einerseits aufgrund der maximalen Speicherfrist in REDIS (expire), andererseits wegen der Überschreibungen beim „rotierenden“ Logging-Verfahren.

Nicht flüchtige Bewegungsdaten, die zugleich einer Person zuzuordnen sind, werden anonymisiert gespeichert; die weitere Erörterung erfolgt im nachstehenden Abschnitt “Nutzungsdaten in der Sitzungsverwaltung“.

Datensicherheit / Integrität
Die Datenbankenzugänge sind per Rollenkonzept aufgeteilt. Ein potentieller Angreifer, der bspw. Zugangsdaten aus dem Portal extrahiert, kann mit diesen Daten lediglich lesenden Zugriff auf die Portalkonfiguration und auf die Eingaben, welche im Portal gemacht werden, erhalten.

Firmware-Entwickler haben z.B. keinen Zugriff auf Bestelldatenbanken, etc. Die Verbindung zu den Datenbankservern erfolgt verschlüsselt. Übertragungen nach außen sind mit HTTPs gesichert (mit Ausnahme der WLAN-Portale, die öffentlich sind).

Lese- und Schreibzugriffe von Benutzer:innen der API werden per Token autorisiert. Pro Kunde wird individuell entschieden, welche Nutzer:innen/ Partner Zugriff auf welche Ressourcen erhalten.

Daten bei Dritten
Außerhalb des Netzwerksystems werden Daten ausschließlich zum Zweck des Vertriebs in einem CRM bei close.io & HubSpot.com erhoben und gespeichert.

Authentifizierungsverfahren
Abhängig von der Nutzungskategorie wird für die verschiedenen Authentifizierungen i.A. jeweils eine Kombination folgender Verfahren genutzt:

- JWT-Token zur Autorisierung von API-Benutzern werden RS512-signiert
- 2-Faktor-Authentifizierung von Nutzer:innen
- Server-Zugriff für Entwickler:innen erfolgt per SSH (Ablehnung unzeitgemäßer Schlüssellängen in Umsetzung)
- Zugriff auf Sourcecode über SSH
- HTTPs mit „x509“ Client-Authentifizierung für Maschinenschnittstellen
- HTTPs mit „let’s encrypt“ für Benutzerschnittstellen
- Bevorzugte Crypto-/Hash-Verfahren: Salsa20 und SHA256

Maßnahmen zur lokalen Daten-Verschleierung
In den für den öffentlichen Zugriff vorgesehenen Netzen leiten die Router Verbindungen mittels “IP-Masquerading” an das lokale Gateway oder an ein VPN-Gateway weiter. Dadurch sind die IP- und die MAC-Adressen der Clientgeräte im lokalen Netzwerk von außen nicht einsehbar. DNS-Anfragen werden aus einem Cache auf dem Router beantwortet. Im lokalen Netzwerk ist dann lediglich die erste Anfrage auf eine Ressource zu sehen. Diese sieht aus wie eine der eigenen Anfragen des Routers, und das Ergebnis wird mit anderen Nutzer:innen geteilt.

Es wird darauf hingewiesen, dass der Traffic durch die optionalen VPN-Gateways nicht zusätzlich verschlüsselt wird, da die Pakete ohnehin unverschlüsselt in das Internet weitergeleitet werden. Netzwerk-Nutzer:innen sollten so wie üblicherweise an ihrem eigenen Internetanschluss möglichst „End-to-End“-Verschlüsselung (bspw. HTTPs oder DNSSEC) anwenden.

Änderungswesen und Protokollierung
Viele Daten werden im System sowohl zum Betrieb als auch zur Vorgangsprotokollierung gespeichert. AirZen verzichtet immer dann auf Log-Verfahren, wenn solche Protokolle einfach über Auswertungen aus den in der Datenbank ohnehin gespeicherten Informationen erstellt werden können.

Nutzungsdaten in der Sitzungsverwaltung
Für die jeweilige Sitzungsverwaltung eines Anwenders müssen Geräte eindeutig identifiziert werden. Dazu wird aus der spezifischen MAC-Adresse und der eindeutigen ID des Netzwerks ein Hash gebildet. Das verwendete Hash-Verfahren ist SHA256 und die in dieser Datenbank unbekannte Netzwerk-ID fungiert als „schwacher Salt“. Die MAC-Adresse wird aktuell nur für den Hash übermittelt und nicht gespeichert. Zukünftig soll der Hash bereits auf den Routern berechnet werden, um die Identität der Gäste auch während der Übertragung noch besser zu schützen.

Durch die Verwendung des Hashs lassen sich aus den gespeicherten Sitzungsdaten nur mit unverhältnismäßig hohem technischen Aufwand die MAC-Adressen extrahieren. Um einen Eintrag zu einer Person gezielt finden zu können, muss die MAC-Adresse dieser Person und das benutzte Netzwerk bekannt sein.

Unter Angabe der MAC-Adresse und eines Netzwerknamens, können auf eine konkrete Anfrage von Strafverfolgungsbehörden entsprechende Auskünfte erteilt werden.

Die Sitzungsstartzeiten aller Nutzer:innen werden vom AirZen System gespeichert. Dies geschieht in erster Linie zu dem Zweck, die Nutzungs-Datenmenge einzelner Anwender:innen feststellen und berücksichtigen zu können. Damit beim Löschen der alten Sitzungsdaten die Informationen über die Häufigkeit und das Volumen der vergangenen Nutzung erhalten bleibt, werden die Sitzungen aufsteigend nummeriert.

Andere personenbezogene oder -beziehbare Daten
Für die Aktivierung einer Sitzung (“Internetzugang erhalten“) müssen alle Nutzer:innen die Geschäftsbedingungen von AirZen und abhängig von den vereinbarten Rahmenbedingungen evtl. auch diejenigen des Kunden akzeptieren. Der Kunde von AirZen, in dessen Geschäftsräumen das AirZen WLAN zur Nutzung zur Verfügung gestellt wird, bestimmt, ob und welche Daten im Aktivierungsportal erhoben werden sollen. Der eigentliche Aktivierungsprozess an sich erfordert keine weiteren Daten-Eingaben.

Es liegt im Ermessen und der Entscheidung des Kunden, die Bedingungen bzw. das Prozedere für die Datenerfassung zur Zugangsaktivierung zu bestimmen. Motivation für die Datenerhebung beim Aktivierungsprozess könnte bspw. sein ausgewählten Nutzer:innen besondere Zugriffsrechte zu gewähren oder einzuschränken, eine übermäßige Netzwerknutzung zu verhindern oder z.B. gezielt Erstnutzer anzusprechen.

Im Fall von leeren Eingaben ist es sowohl möglich, die Aktivierung zu blockieren, als auch zuzulassen. Die Dateneingaben und die Sitzungs-Startzeiten aller Nutzer:innen werden vom AirZen System gespeichert. Der Kunde von AirZen erhält Zugriff auf diese Daten, da er deren Erhebung beauftragt hat.

Im Rahmen der künftigen Weiterentwicklung des AirZen Systems ist geplant, die eingegebenen Daten bereits zum Zeitpunkt der Eingabe sofort per „Webhook“ an den Kunden übermitteln zu können, und damit die Erfordernis der (Zwischen-) Datenspeicherung im AirZen System zu vermeiden. Vom AirZen System werden die von Nutzer:innen eingegeben Daten weder ausgewertet noch in anderer Weise als der oben beschriebenen verarbeitet.

Protokolle für Entwicklung/Support
Zu Diagnose-Zwecken können auch tiefer gehende Protokolle angefertigt werden. Dies geschieht üblicherweise im Zusammenhang mit der Entwicklung von Systemkomponenten durch einen AirZen-Experten oder im Rahmen einer Wartungsmaßnahme durch den Kunden selbst oder einen vom Kunden beauftragten Dienstleister (Dritter oder auch AirZen).

Im Support-Fall initiiert die die Wartung durchführende Person die Erfassung eines entsprechenden Protokolls im AirZen System. Das die maßgeblichen Daten erfassende Gerät befindet sich i.d.R. im Eigentum des Kunden. Eine Speicherung in der AirZen Cloud erfolgt nur für die Dauer der Datenübertragung an den Anforderer.

Die Verantwortung und Entscheidung über die Art der Speicherung, Anonymisierung und Löschung (gemäß DSGVO) liegt beim Empfänger der übertragenen Daten. Im Entwicklungs-Fall muss der verantwortliche Entwickler die Entscheidung treffen, welche Daten, wie und für welche Dauer gespeichert werden müssen, um das Entwicklungsziel zu erreichen.

AirZen verpflichtet die Entwickler, dass sie diese Einschätzung proaktiv wahrgenommen wird, eine mögliche Pseudonymisierung der Daten vorgenommen wird und die vorgegebenen Löschfristen eingehalten werden.

Rest-Risiken bei der Datenspeicherung durch Anwender:innen oder Dritte
Grundsätzlich verzichtet AirZen auf sonstige eventuell in Betracht kommende Maßnahmen zur Verhinderung einer Datenspeicherung, wenn diese zu umständlich, mit unverhältnismäßig hohem Aufwand zu implementieren und aufrecht zu erhalten, leicht zu umgehen (bspw. Handykamera) sind, oder ein trügerisches Bild von Sicherheit vermitteln.

AUTOMATISCHES SOFTWARE-UPDATE-SYSTEM FÜR WLAN-ROUTER UND CLOUD-SYSTEME

Bei AirZen wird grundlegend ein hohes Update-Intervall gepflegt. Die Accesspoints prüfen dazu jeweils automatisch einmal täglich (nachts) ob neue Versionen verfügbar sind. Steht ein Update bereit, wird es automatisch ausgeführt und der Betrieb nach wenigen Minuten wieder fortgesetzt. Dies ermöglicht die schnelle Bereitstellung von zeitkritischen Sicherheitsupdates sowie Funktionserweiterungen. Updates können auch manuell initiiert werden, zudem besteht die Möglichkeit, Updates basierend auf einem zuvor definierten Zeitplan durchzuführen.

Kritische Sicherheitsupdates
Auf den Servern erfolgt die automatische Installation von Sicherheitsupdates für Standardkomponenten spätestens vier Stunden nach deren Veröffentlichung. Bei von AirZen entwickelten Anwendungen ist die Struktur so gestaltet, dass sicherheitsrelevante Komponenten, wie zum Beispiel die Verbindungsverschlüsselung, von Standardkomponenten übernommen werden, die auf diese Weise regelmäßig aktualisiert werden. In Ausnahmefällen, in denen dies nicht möglich ist, erfolgen Updates nach einer Einschätzung der beteiligten Entwickler:innen.

Die Freigabe von Updates unterliegt ebenfalls der Zustimmung eines oder mehrerer beteiligter Entwickler:innen. Die Aktualisierung der Firmware auf den Nodes erfolgt, wie es bei kleinen Netzwerkkomponenten üblich ist, ausschließlich im Gesamten. Dies liegt daran, dass aufgrund begrenzter Platzkapazitäten die Aufrechterhaltung der Integrität bei partiellen Updates und die Kombination verschiedener Paketquellen kaum realisierbar sind. Im Falle der Entdeckung einer Sicherheitslücke erfolgt eine Einschätzung ihrer Dringlichkeit.

Grundsätzlich wird der Quellcode der Firmware stets in einem Zustand gehalten, der es ermöglicht, eine neue Firmware mit aktualisierten Komponenten jederzeit zu erstellen. Im Fall einer akuten Sicherheitsbedrohung kann die Firmware innerhalb eines Zeitraums von 24 Stunden neu kompiliert und ausgerollt werden.

Prävention schlägt Reaktion: Regelmäßige, automatisierte Updates sind hierbei von fundamentaler Bedeutung.

Regelmäßige Updates
Die regelmäßige Aktualisierung von Software bietet zweifachen Nutzen. Erstens ermöglicht sie das Schließen von Sicherheitslücken, noch bevor diese öffentlich bekannt werden – insbesondere in Fällen, in denen die Veröffentlichung der Patch-Informationen zurückgehalten wurde. Zweitens reduziert sie das Risiko, dass Schnittstellenänderungen in zwischenzeitlichen Versionen die reibungslose Installation dringend benötigter Aktualisierungen behindern. Da die Mehrheit der Angriffe auf bereits bekannten Sicherheitslücken basiert, erweisen sich regelmäßige Updates als von höchster Dringlichkeit.

Feature-Updates
Die bereitgestellten Updates setzen neue Produktanforderungen um. In Fällen, in denen Updates zur Anpassung und Erweiterung der Funktionalität veröffentlicht werden, beinhalten sie nach Möglichkeit auch Aktualisierungen für das übrige System.

AIRZEN-IDENTITÄT

AirZen ist Hersteller für europäische, innovative, qualitativ hochwertige und einfach zu nutzende Netzwerk-Lösungen. Unser wegweisender Network-as-a-Service-Ansatz stärkt die IT-Sicherheit und optimiert nachhaltig die IT-Verwaltung, um einen maximalen Kundennutzen zu gewährleisten.

Verantwortungsbewusstsein ist die Leitlinie für die Entwicklung und den Einsatz der AirZen-Produkte und -Lösungen. Dabei stehen Sicherheit, Zuverlässigkeit und Leistungsfähigkeit im Mittelpunkt.

Als Hersteller schätzen wir die direkte Zusammenarbeit mit Kunden genauso wie die Partnerschaften mit erfahrenen IT-Partnern. AirZen bietet umfassende Lösungen, bestehend aus eigenen Hardware- und Software-Komponenten.

Weitere Informationen und Ansprechpartner finden Sie auf www.airzen.io.

AIR ZEN

AirZen Networks Lda.

Avenida Arriaga 30 / 1A
9000-064 Funchal
Madeira / Portugal

business@airzen.io

WWW. AirZen.io