AIR ZEN

Das AirZen System:

REMOTE MANAGEMENT & NETZWERKRESILIENZ

Für Entscheidungsträger:innen in der IT-Abteilung

Executive Summary

Ihre Netzwerktechnik ermöglicht alle digitalen Vorgänge und schützt Ihr Unternehmen und die Daten Ihrer Kunden. Zwischen Homeoffice, Zero-Day-Attacken, Hacker-Kultur und den volatilen Anforderungen smarter Infrastruktur steigen die Anforderungen an Ihr System beständig. Dieses Dokument gibt einen Einblick in Funktionsweise, Aufbau und Prozesse des AirZen-Systems sowie dessen Anspruch an Sicherheit und Benutzerfreundlichkeit. Network-as-a-Service bedingt für uns fortlaufende Entwicklung, maximale Souveränität für User und zukunftstaugliche Sicherheitskonzepte.

INHALTSVERZEICHNIS

ÜBER AIRZEN

NETWORK-AS-A-SERVICE

Unsere Plattform besteht aus eigener Hardware und intern geschriebener Software. Diese holistische Herangehensweise macht uns unabhängig und ermöglicht einen umfassenderen Ansatz für Sicherheit und Bedienkomfort.

Durch homogene Prozesse und fortschreitende Automatisierung kann unsere Inhouse-Software enthusiastischen Home-Usern den gleichen Service bieten wie komplizierten industriellen Anwendungen oder komplexen Unternehmen mit zahlreichen Homeoffices. Unser System verbindet verschiedene Standorte sicher und souverän, mit minimaler Setup-Zeit und dynamischer Erweiterung. Ohne Downtime.

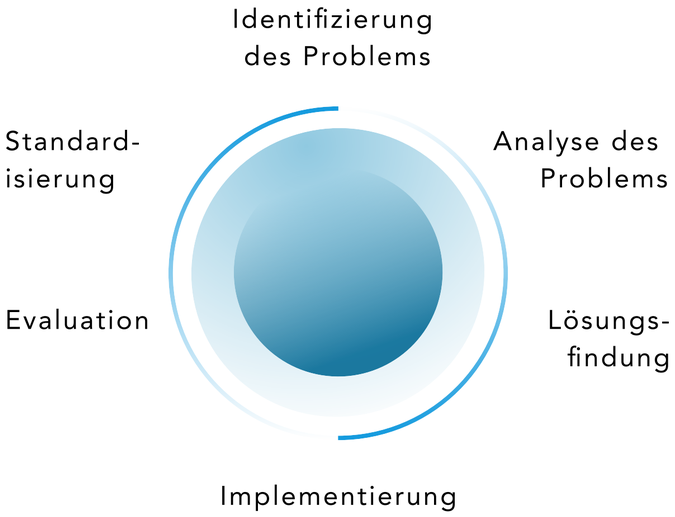
Unsere Hardware umfasst ein Portfolio von Heimanwendungen bis zu industriellen Anforderungen, basierend auf Dual-WiFi 6 oder 5G (optional). Wir testen das Setup vor jedem Versand und optimieren es nach Ihren Wünschen.

Stand 2022 nutzen mehrere namhafte Finanzinstitute unsere Technologie. Damit haben wir Wettbewerber aus den USA und China abgelöst. Industrie, Wirtschaft sowie staatliche Organe verspüren immer stärkeren Druck, unabhängige Lösungen zu wählen. Wir sind motiviert, diese Nachfrage zu erfüllen und schauen erwartungsvoll in die Zukunft eines sich ständig entwickelnden Netzes.

Parallel zu diesem Whitepaper existieren weitere Whitepaper für die angebotenen Lösungen für die Bereiche Business, Homeoffice & Kunden-WLAN.

IT-SECURITY:
UNTERNEHMENSRISIKO UND LÖSUNG

Internationale Konflikte haben spätestens im Jahr 2022 das Risiko von Cyberattacken auf Unternehmen drastisch erhöht. Die Ernsthaftigkeit dieses Themas wird spätestens durch die staatlichen Interventionen in Form neuer Gesetzesfassungen sowie Regulierungen auf nationaler Ebenen sichtbar bis hin zur Haftung durch die Geschäftsführung. Wir entwickeln unseren Service kontinuierlich weiter und erfüllen einen Großteil der Anforderungen bereits vor ihrer legislativen Verbindlichkeit.



Identifizierung und Analyse des Problems

Nicht zuletzt durch internationale Konflikte wird IT-Technologie mehr denn je als Spionage-Werkzeug benutzt.

Bekannte Hersteller stehen immer mehr im Fokus von Hacker-Angriffen, da Infrastrukturtechnologien eine große Bandbreite an Firmeninformationen beinhalten und Eintrittspforten für Mitarbeiter:innen darstellen.

Der Einsatz im Homeoffice hat die potenzielle Angriffsfläche drastisch erhöht, da Unternehmen nicht nur ihr Netzwerk am Firmensitz selbst, sondern auch das ihrer Mitarbeiter:innen zu Hause absichern muss.

Lösungsfindung

Wie bereits von den jeweiligen Staaten festgestellt, ist der Lösungsansatz unter anderem in der Herkunft der Technologie zu finden.

Ein weiterer maßgeblicher Ansatz ist die Verwaltung aller Netzwerkstandorte samt der Vielzahl der individuellen Nutzer:innen.

Aufgrund der stetig wachsenden Zahl von Angriffen auf die Netzwerkinfrastruktur ist nachhaltige Sicherheit nur in einem System denkbar, das stets mit Updates und zusätzlichen Security-Features wie denen des AirZen Protection Framework versehen wird.

Langfristig planen wir, unsere Technologie unter Open-Source-Lizenz zu veröffentlichen, um die Netzwerksicherheit auf ein neues Niveau zu heben.

Implementierung der Lösung

Die Installation der AirZen-Router erfolgt remote per Managed Service und folgt einem standardisierten Rollout- und Sicherheitskonzept.

Die Verwaltung aller Netzwerkstandorte inkl. deren Nutzer:innen wird von AirZen remote per Managed Service angeboten. Kunden können hierbei ein für sie passendes Lizenzmodell wählen.

Grundlage des AirZen-Systems ist das Lizenzmodell, da nur regelmäßige Software-Updates und die Möglichkeit der direkten Abwehr aktiver Bedrohungen Sicherheit bieten.

Die Netzwerktechnologie von AirZen kann somit als ein am Markt einzigartiges europäisches „Netzwerk-Betriebssystem“ verstanden werden.

Die Implementierung und Überprüfung der AirZen-Technologie erfolgte in den Bereichen Privat- und Unternehmensnetzwerke ebenso wie in komplexen industriellen Netzwerkprojekten mit sehr hohen Sicherheits- und Konformitätsansprüchen.

Evaluierung der Anforderungen

Für die Entwicklung der AirZen- Technologie wurden die Sicherheitsanforderungen des Finanzsektors evaluiert – aus IT-Sicht das wohl schwierigste Branchensegment, da der Datenschutz und die DSGVO-Konformität neben der Vielzahl von Anforderungen an die Netzwerksicherheit hier nur eine untergeordnete Rolle spielen.

Der Anspruch an die Sicherheitsanforderungen, an modulare Netzwerke und der direkten Verwaltung, deren Mitarbeiter:innen und Filialkund:innen sowie an Homeoffices sind bei Finanzinstituten besonders hoch und eignet sich daher perfekt zur Evaluierung unserer Produkte.

Standardisierung

Fehlende Updates, veraltete Geräte oder unkontrollierte Kommunikation mit ihrem Firmengerät wird unweigerlich zum Sicherheitsrisiko ihres Netzwerks. Die potenzielle Angriffsfläche steigt enorm, wenn ihr Netzwerk durch eine Vielzahl unterschiedlicher Router auf Arbeitnehmerseite durch die Arbeit im Homeoffice unterwandert wird.

AirZen liefert ein standardisiertes Produkt, welches alle zuvor genannten IT-Sicherheitsaspekte erfüllt und durch neuartige Remote-Lösungen für Inbetriebnahme, Support und Nutzerverwaltung zudem Zeit- und Kostenersparnisse bietet.

DAS AIRZEN SYSTEM
FUNKTIONSWEISE UND AUFBAU

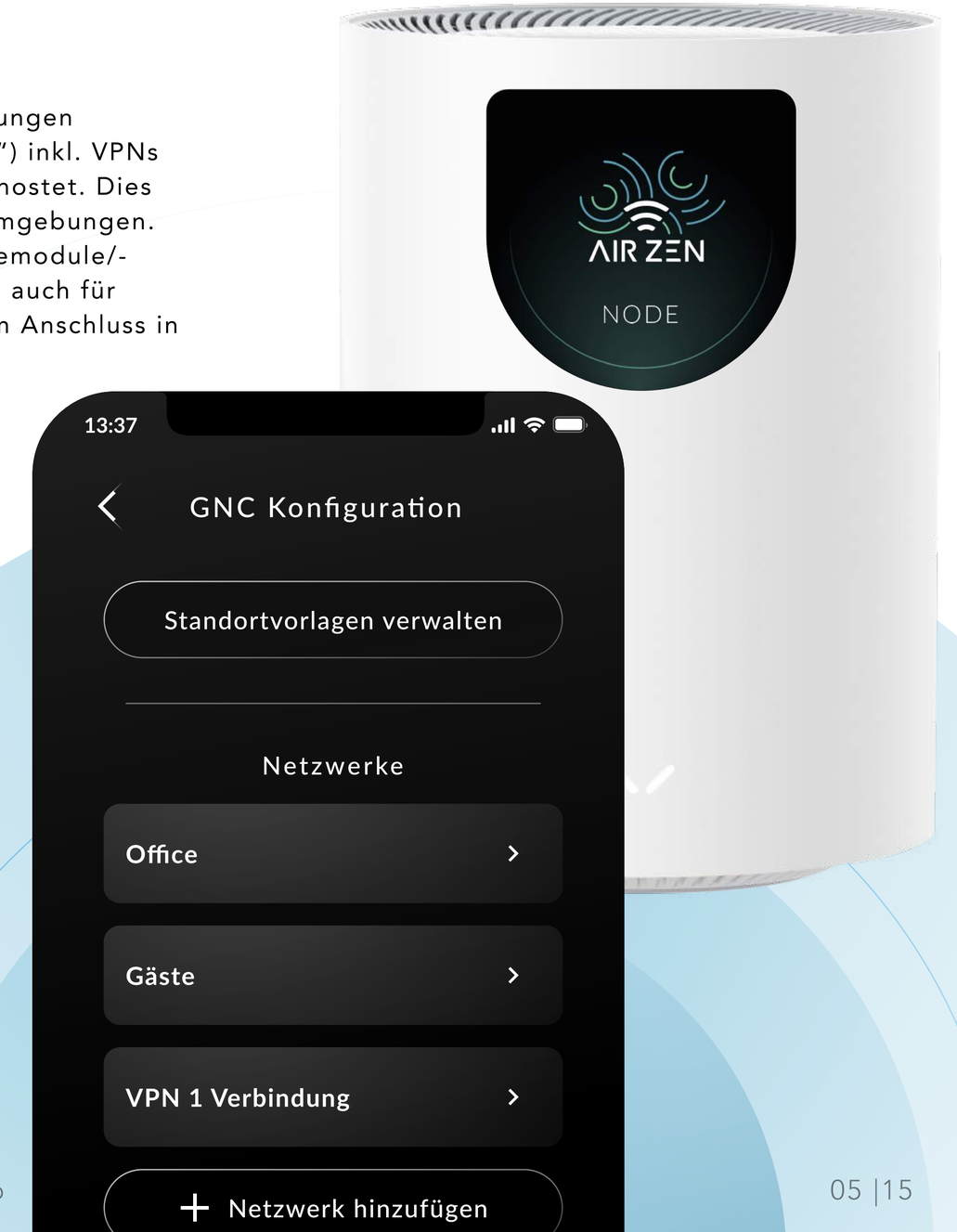
Unsere Plattform

Das AirZen-System basiert auf propritärer Hardware und Software mit eingebundenen „Open Source“-Elementen und OEM-Modulen. Die AirZen-Software-Gesamtlösung ist aufgeteilt in Server-, Client- und Komponentenfunktionen. Die AirZen-Hardware kann mit optionalen Software-Modulen erweitert werden.

Das AirZen-System unterstützt aktiv nur eigene Access Points, Router etc. (genannt „AirZen Nodes“). Diese Komponenten werden vom System überwacht, konfiguriert und administriert. Alle sonstigen an das Netzwerk angeschlossenen Komponenten (Router, Switches etc.) können an das AirZen-WLAN angeschlossen und im WLAN betrieben werden.

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

Alle von AirZen betriebenen Anwendungen (innerhalb der beschriebenen „Cloud“) inkl. VPNs werden bei einem Cloud-Anbieter gehostet. Dies gilt auch für Entwicklungs- und Testumgebungen. Neue bzw. weiterentwickelte Softwaremodule/-komponenten werden gegebenenfalls auch für lokale Umgebungen entwickelt und im Anschluss in die jeweiligen Systeme geladen.



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.

Unterstützte Interfaces verschiedener AirZen Node Produkte:

Kabel
Fiber &
Ethernet

Bluetooth
bis zu 50 m

WiFi 6
bis zu 500 m,
bis zu 10 km
mit Zubehör

AirZen IoT
Sensordaten
bis zu 10 km

4G & 5G
mobiler
Datenempfang
in Highspeed
bis zu 15 km

Starlink
Internet-Uplink
bis zu 550 km
Entfernung

GNSS/GPS
Standort-
verfolgung bis
zu 20.000 km

Iridium
Satelliten Verbindung,
geringe Bandbreiten
für Sensordaten

Modulare System – Archtitektur

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

- funktionsweise Aufteilung aller Dienste und Prozesse
- Minimierung von Abhängigkeiten
- klare Regelung von Zugriffsfragen

Die primären Vorteile eines modularen Systems:

- Einzelne Anwendungen bzw. Komponenten lassen sich im Störungsfall leichter zurücksetzen, neu aufsetzen oder austauschen.
- Der Programmcode ist überschaubarer, weniger fehleranfällig und leichter zu pflegen.
- Einfachere Überarbeitung oder (teilweise) Neuentwicklung einzelner Komponenten, da an anderen Komponenten keine oder nur wenige Anpassungen erforderlich werden.
- Eine ausgefallene Komponente (z. B. ein einzelner Dienst) beeinflusst abhängige Prozesse nur unmittelbar in ihrer Funktion.

Komplizierte Software-Stacks werden bei der Entwicklung weitestgehend vermieden. Die Tokens, mit denen Schnittstellenbenutzer:innen autorisiert werden, sind präzise und verständlich definiert, sodass immer klar ist, auf welche spezifischen Systemressourcen die Benutzer:innen Zugriff erhalten. Die Netzwerkkonfiguration darf von den Routern nur gelesen werden; Schreibzugriff hat nur die Konfigurations-API.

Ein Administrator hat stets nur Zugriff auf spezifische Systeme (Server und Datenbanken), niemals auf das gesamte System. Die Entwickler haben Zugriff auf die Software-Komponenten, die sie jeweils bearbeiten. Im Einzelfall, z. B. bei Neuentwicklungen oder umfangreichen Testmaßnahmen, nutzt ein Entwicklerteam gegebenenfalls einen anderen Hoster oder separate, eigens dafür eingerichtete Server.

Die Daten verschiedener Kategorien werden immer getrennt gespeichert (siehe „Datenkategorien“). Auf diese Weise beeinflusst bspw. eine höhere Last der Datenbank für WLAN-Sitzungen nicht die systemkritische Datenbank für die Netzwerkkonfiguration.

Trennung vom Heimnetzwerk

Zahlreiche Hacking-Angriffe auf Unternehmen erfolgen über Homeoffices. Mitarbeiter:innen, die per LinkedIn einem Unternehmen zuzuordnen sind, lassen sich leichter per Malware angreifen, wenn sie sich in ihrem Heimnetz befinden. Auch eine VPN-Verbindung auf nur einem Endgerät schützt hierbei nicht ausreichend. Im Gegenteil ist der VPN-Tunnel oftmals ein direktes Einfallstor in das Unternehmen.

Hier bietet die AirZen-Lösung jedoch einen wesentlichen Schutz im Homeoffice der Mitarbeiter:innen. Dabei werden die Privat- und Unternehmensnetzwerke getrennt und zusätzlich aktive Schutzmaßnahmen wie z. B. die Blockierung von IP-Adressen von Command-&-Control-Servern ausgeführt.

Ist eine Schadsoftware (Virus) eingedrungen, benötigt er Befehle von diesen Servern. Die Blockierung der IP-Adresse verhindert bzw. erschwert die Kommunikation und macht die Schadsoftware nutzlos. Die „Sperr-Listen“ derartiger Command-Server werden von AirZen täglich aktualisiert und Malware-Seiten per DNS-Filter blockiert.

Umgang mit Störungsfällen

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. Sollte dies nicht zum Erfolg führen, muss der Server vollständig ersetzt werden. In diesem Fall wird der neue Server erst dann aktiviert, wenn die DNS-Rekords zu den IPs des alten Servers abgelaufen sind. Die Systemarchitektur ermöglicht ebenfalls, Teile des Backends in einem eigenen Rechenzentrum zu betreiben oder bei einem anderen Anbieter zu hosten. Im Falle eines DDoS-Angriffs können so die angegriffenen Dienste bspw. auf eigene Server ausgelagert werden, um benachbarte Dienste zu schützen.

Service-Kategorien

Die AirZen-Services 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.

SD-Wan

Diese Funktionalität ermöglicht die Nutzung mehrerer Internet-Quellen. Fällt eine Leitung aus, schaltet das System automatisch auf eine andere Quelle um. Es stehen Glasfaser, 5G und Gigabit-Ethernet zur Verfügung. Dadurch können DSL, Glasfaser- und 5G-Verbindungen mit nur zwei Geräten abgedeckt werden. Dieses System verfügt über industrielles 5G & 4G basierend auf Basis einer MiMo-Technik, die mehr Bandbreite als übliche LTE/5G-Router bereitstellt.

Das Gerät kann im Falle eines Internet-Ausfalls des Kabel-Netzwerks (DSL o. Ä.) automatisch die 5G-Fallback-Verbindung aktivieren. Somit können alle Mitarbeiter:innen eines Standorts unterbrechungsfrei weiterarbeiten. Auch im Supportfall (z. B. Problem mit dem Internet-Uplink) kann AirZen auf einen Standort zugreifen, auch wenn die Hauptinternet-Leitung gestört ist.

SD-WAN Beispiel
Ein mit AirZen mögliches Szenario ersetzt de facto eine MPLS/Standleitung, egal ob am Unternehmensstandort oder im Homeoffice.

Uplink 1
AirZen Node mit zwei Glasfaser-Anschlüssen. Ein Anschluss für den Glasfaser-Uplink vom Provider, der zweite für die Anbindung am Switch.

Uplink 2
An der Node wird zusätzlich oder als eigenständiges Gerät eine reguläre DSL-Verbindung (keine Glasfaser) genutzt. Das externe Provider-Modem wird an die Node angeschlossen und stellt somit einen zweiten Uplink zur Verfügung.

Uplink 3
Die AirZen Node baut mittels 4x4 MiMo eine der schnellsten 5G-Verbindungen auf.

AirZen Generic Network Controller (GNC)

Der Cloud-basierte AirZen Generic Network Controller stellt die Basis der AirZen-Konfiguration dar. Die einzelnen AirZen Nodes nutzen eine zentral gespeicherte und per Location definierte Konfiguration als Betriebsgrundlage. Gleichzeitig werden Monitoring-Ereignisse wie z. B. Logins von der AirZen Node an die Cloud übertragen und dort erfasst. Eine Datenerhebung auf der AirZen Node selbst erfolgt – wenn überhaupt – nur temporär. Dadurch sind die AirZen Nodes innerhalb eines Netzwerks leicht zu installieren und auszutauschen. Beim ersten Start bezieht die AirZen Node Ihre Zuordnung samt initialer Konfiguration über die AirZen Cloud.

AirZen GNC ist selbst in mehrere Schichten unterteilt, die miteinander logisch verknüpft sind:

- Radio Config (Hardware-Settings für WiFi, 5G, 4G, LoRa etc.)
- Networks (VPN-Tunnel, UFPE, Private-Uplink, Public-Uplink)
- SSID
- Portal (Kunden-WiFi)

Über diese AirZen-Tools kann zwischen den einzelnen Schichten eine logische Verknüpfung hergestellt werden. Die Aufteilung in Schichten ermöglicht eine große Anzahl an Kombinations-möglichkeiten. Die Einrichtung erfolgt hier vorwiegend über die Kommandozeile.

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

Logging
Die AirZen Nodes erfassen und übertragen regelmäßig Statusinformationen und speichern diese für einen begrenzten Zeitraum.

Zu diesen Statusinformationen gehören u.a. :

- IP- und MAC-Adressen lokaler Gateways
- MAC-Adressen, Signalstärken und Übertragungsraten von WLAN-Clients

Künftig ist vorgesehen, folgende Informationen zusätzlich zu speichern:

- Liste der jeweils aktuellen DHCP-„Leases“
- 4G/5G-Verbindungsinformationen

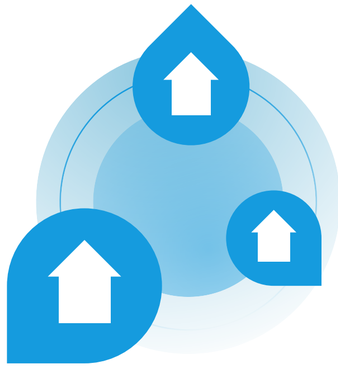
Die AirZen Nodes speichern nur Informationen, die für die eigentliche Routing-Funktion und die Funktionsweise des Gerätes erforderlich sind.

Portal-Funktionen
Das Portal benötigt für den Betrieb die Konfiguration, die Sitzungen und Nutzungsdaten lediglich den 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 Anwendern/Clients den Zugriff auf das Netzwerk vermitteln, da die Portal-Konfigurationen lokal und persistent zwischengespeichert werden. Nutzereingaben 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.

BETRIEB DES AIRZEN-SYSTEMS
BEISPIELHAFTER ROLLOUT

Beispielunternehmen Finanzinstitut:
30 Standorte inklusive Mitarbeiter:innen, Geräte und Kunden. Zusätzlich 50 Mitarbeiter:innen im HomeOffice.



Rollout abgeschlossen

Woche 1 *in Kooperation*
Video-Meeting &
Projektbesprechung,
Start Netzwerkplanung

Nach Abschluss unseres Standard-Vertrages für Unternehmenskunden (dieser wurde von Finanzinstituten, deren Rechtsabteilungen und Datenschutzexpert:innen bereits geprüft), beginnt das Projekt mit der Lieferung der Hardware ab Lager in die D-A-CH-Regionen.

Woche 2 *via AirZen*
Abschluss Netzwerkplanung,
Testgerät mit geplanter
Netzkonfiguration

Der **AirZen Managed Service** als Kern-Element unserer Lösung wird direkt von AirZen oder einem zertifizierten Partner ausgeführt. Dieser Service führt durch das Projekt und ersetzt einen In-House-Experten auf Ihrer Seite. Der Fokus liegt auf **Netzwerk-Planung** und **IT-Security**. Der Managed Service entwirft mit Ihnen das Netzkonzept, stellt die richtigen Fragen und setzt Ihre Netzwerk-Anforderungen in die Realität um.

Woche 3-5 *via AirZen*
Start des Rollouts, Installation vor Ort via Plug-&-Play - das Netzwerk steht unmittelbar zur Verfügung

Die Installation der Nodes erfolgt an den jeweiligen Standorten via Plug-&-Play. Unser Remote Managed Service unterstützt die IT-Abteilung bei der Installation. Gemeinsam werden alle Standorte aktiviert.

Nutzer:innen und Geräte via Tastendruck hinzufügen oder sperren, Benutzer-gruppen spezifizieren.

AirZen Managed Service über die AirZen-App (Ticket-System mit integrierter Chat-Lösung). Auf Wunsch können Mitarbeiter:innen direkt mit dem AirZen-WiFi-Support kommunizieren oder das kundeneigene IT-Team wird vorgeschaltet.

Woche 6-8
Abschluss & Feintuning. Letzte Details werden eingerichtet und abgestimmt.

Der Produktiv-Betrieb läuft bereits und erste Mitarbeiter:innen werden über das Self-Service-Portal hinzugefügt.

Zusammenfassung

Nach Abschluss der Installation per Plug-&-Play steht via Mesh Technologie ein flächendeckendes Netzwerk zur Verfügung. Dies erhöht neben der Arbeitsqualität auch die IT-Sicherheit und ermöglicht ein reibungsloses flexibleres Arbeiten. Optional kann mittels AirZen-Router auch eine direkte VPN-Verbindung zur Zentrale aufgebaut werden. Der Rollout der AirZen-Business-Lösung stellt somit insgesamt eine deutliche Entlastung der jeweiligen IT-Abteilung dar. Optionale VPN-Lösungen auf Endgeräten wie Laptops etc. werden davon nicht beeinträchtigt.

- Installation mit eigenem IT-Personal vor Ort
- Nodes beziehen via Plug-&-Play zuvor erstellte, abgestimmte und getestete Netzwerk-Konfiguration
- Konfiguration in direkter Kunden-Abstimmung mittels AirZen Managed Service
- Nodes synchronisieren sich automatisch (kein Update einzelner Geräte notwendig)
- AirZen Nodes werden dauerhaft auf ihre Funktionsfähigkeit hin überwacht
- Das System misst kontinuierlich die WLAN-Qualität und übermittelt Störungen automatisch an den AirZen-Support

ZENPSK - AUTOMATISIERTE IT-SICHERHEIT IM ONBOARDING PROZESS

Schwachstelle: WLAN-Passwort

Standard-WLAN-Verschlüsselung ermöglicht nur ein WLAN-Passwort je WLAN. Dieses WLAN-Passwort ist für alle WLAN-Nutzer:innen gleich. Eine beabsichtigte oder unbeabsichtigte Weitergabe des Passworts kann i. d. R. nicht verhindert werden und stellt ein großes Sicherheitsproblem dar. Teils verfügen sogar ehemalige Mitarbeiter:innen noch über das aktuelle Unternehmens-Passwort, was einem Angreifer Tür und Tor öffnet.

Hierfür bieten WLAN-Standards mit dem sogenannten WPA-EAP–Verfahren eine Alternative. Es ist sicher, aber umständlich und findet im Unternehmensalltag vorwiegend aus organisatorischen Gründen daher wenig Verwendung.

Um dieses Verfahren anwenden zu können, ist der Einsatz eines speziellen „Radius-Servers" sowie die Verwendung zusätzlicher Zertifikate notwendig. Hierbei müssen diese Zertifikate zuvor auf jedes(!) Endgerät übertragen werden, was die Anwendbarkeit des EAP-Verfahrens einschränkt. So ist dieses Verfahren nicht für Anwendungsfälle geeignet, bei denen kein direkter Zugriff (z. B. mittels Mobile Device Management MDM) auf die Client-Geräte besteht. Zudem ist die administrative Verwaltung dieser Technologie sehr zeitintensiv und erfordert zusätzliche Infrastruktur.

Multi-Faktor-Authentisierung

IT-Sicherheit hat im Finanzsektor einen sehr hohen Stellenwert. Hier konnte sich AirZen mit seinen Security-Features klar gegenüber internationalen vergleichbaren Anbietern als europäischer Netzwerkanbieter abgrenzen.

Über ein Self-Service-Portal erhalten alle Mitarbeiter:innen ein individuelles WLAN-Passwort. Dies verkleinert die Angriffsfläche gegen das Unternehmen drastisch.

Die von AirZen entwickelte ZenPSK-Technologie ermöglicht die Verwendung mehrerer verschiedener WLAN-Passwörter (WPA2/3-PSK). Nach einmaliger Eingabe eines Passworts durch die Nutzer:innen im Endgerät ist eine verschlüsselte Verbindung dauerhaft aktiv. Die Verbindung zum AirZen-WLAN wird dabei an allen zugeordneten AirZen-Standorten automatisch aufgebaut, wenn Mitarbeiter:innen oder Kund:innen des Unternehmens die jeweiligen Geschäftsräume betreten.

Der Grundgedanke ist „Ein Passwort pro Gerät". Dabei wird per AirZen Secure-Access-Verfahren jeder Client-MAC-Adresse ein persönliches Passwort zugeordnet, um zu verhindern, dass Nutzer:innen – beabsichtigt oder unbeabsichtigt – ein Passwort weitergeben.

Das Verfahren basiert darauf, dass zuvor generierte Passwörter im System hinterlegt sind. Bei der erstmaligen Eingabe ordnet das AirZen-System das eingegebene PSK-Passwort fest der spezifischen Mac-Adresse zu. Dieses wichtige Sicherheitsfeature entlastet die Firmen-IT und generiert ein sehr hohes Maß an IT-Sicherheit durch den Identitäts-nachweis von Nutzer:innen sowie jedem genutzten Endgerät, zur Abwehr von Angriffen von außen.

Praktische Anwendungsmöglichkeiten von ZenPSK

Für Mitarbeiter:innen
Innerhalb eines Unternehmens steht ein Self-Service-Portal über die AirZen-App oder einer gesonderten Web-URL zur Verfügung. Über wählbare Zugangsoptionen zu diesem Self-Service-Portal können Mitarbeiter:innen selbstständig ein Passwort für ihr Endgerät generieren.

Um die Sicherheit zu erhöhen, kann der Zugang bspw. auf Mitarbeiter:innen beschränkt werden, die eine Firmen-E-Mail-Adresse besitzen. Der Zugang zum Self-Service-Portal setzt dann z. B. die Eingabe der Firmen-E-Mail-Adresse voraus. Per E-Mail wird dann ein einmalig nutzbarer Web-Link zur Geräteaktivierung übermittelt. Dieser Vorgang ist sehr einfach und dauert nur wenige Sekunden oder Minuten. Je nach Unternehmenskonfiguration des AirZen-Netzwerks können Mitarbeiter:innen auch mehrere Geräte zu ihrem Account hinzufügen. So ist das Netzwerk leicht verwaltbar und ausscheidende Mitarbeiter:innen können vom Administrator direkt deaktiviert werden. Außerdem lassen sich alle nicht mehr verwendeten Geräte automatisch deaktivieren. Die „Idle-Time“ ist hierfür konfigurierbar und beträgt i. d. R. 6 Monate. Das Resultat ist ein „sauberes“ Netzwerk, in dem alle aktiven Nutzer:innen ein persönliches Passwort nutzen.

Dies erhöht die IT-Sicherheit und ermöglicht einen besseren Support. Per Self-Service-Portal können neben der Passwortgenerierung auch direkte Supportfälle gemeldet werden.

Für Kunden bspw. in einem Hotel
Kunden-WLAN wird oftmals über ein „Portal-System“ angeboten. Sicherheitstechnisch ist dagegen nichts auszusetzen, wenn sich der Zugang auf wenige Stunden beschränkt. Für anspruchsvolle Hotelgäste ist diese Form der WLAN-/Internet-Nutzung jedoch aufgrund ständiger Verbindungsabbrüche nicht praktikabel.

Nach Zugang zum Hotel-Zimmer scannt der Gast den AirZen QR-Code. Daraufhin öffnet sich eine Website, auf der der Gast die Internet-, Nutzungs- und Datenschutzbedingungen zuvor akzeptieren muss, um sich dann sein persönliches Passwort zu erstellen. Vor allem Endgeräte aus dem Hause Apple reagieren zuweilen renitent auf WLAN-Netze mit vorgeschalteten Portalen. Im AirZen-Netzwerk fühlt sich der Hotelgast dagegen „wie zu Hause“ und bietet so ein unterbrechungsfreies digitales Kundenerlebnis. Zusätzlich steht dem Gast ein WLAN-Portal zur Verfügung, um auch ohne Passworteingabe Zugang zu erlangen. Wenn gewünscht, kann dieser Zugang zeitlich limitiert werden.

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

In der digitalen Welt von heute ist den meisten Nutzer:innen die Notwendigkeit von Updates ihres Laptops, Handys etc. zum Schutz ihrer Daten bewusst; der WLAN-Router selbst wird jedoch meist stiefmütterlich behandelt.

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

Ein WLAN-Router, der keine regelmäßigen und automatisierten Software-Updates erhält, stellt ein zentrales Sicherheitsrisiko dar. Zahlreiche WLAN-Router sind bereits ab Werk mit einer Firmware ausgerüstet, die zum Zeitpunkt des Kaufs veraltet ist und der aktuellen Cyber-Bedrohungslage nicht mehr gerecht wird. Dennoch werden diese WLAN-Router oftmals nur mangelhaft aktualisiert. Ein zusätzlich beschafftes Sicherheitssystem nützt dann kaum, wenn das wichtigste Gerät direkt am Internet das Hauptproblem darstellt.

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.

Regelmäßige Updates
Die regelmäßige Aktualisierung von Software bietet zweifachen Nutzen. Erstens ermöglicht sie das Schließen von Sicherheitslücken, noch bevor diese öffentlich bekannt werden. 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