AIR ZEN

HOMEOFFICE-LÖSUNG

Einfach und Sicher von Zuhause arbeiten.

SMARTER ALLTAG, SMARTES WLAN

Die Netzwerktechnik eines Unternehmens bildet das Fundament für die IT-Sicherheit und aller internen digitalen Vorgänge. Heutzutage stellt nicht nur die zunehmende Nutzung des Homeoffice neue Herausforderungen an diese Technologie und deren Aufbau. Dieses Dokument soll Entscheidungsträger:innen ein genaueres Verständnis geben, um den ganzheitlichen „Network-as-a-Service“-Ansatz der IT-Infrastruktur von AirZen nachzuvollziehen zu können.

Ziel ist es, die Widerstandsfähigkeit der jeweiligen IT-Umgebung zu stärken, dank unserer Expertise eine smarte Netzwerkanwendung sicher zur Verfügung zu stellen und durch eine Verringerung des Administrationsaufwandes mittels AirZen Managed Service für eine Entlastung der IT-Abteilungen zu sorgen.

CYBER-RISIKEN UND HERAUSFORDERUNGEN IM HOMEOFFICE

Fakt ist: Die Digitalisierung hat unsere Arbeitswelt verändert. Prozesse, die früher mit viel Aufwand verbunden waren, laufen nun automatisch. Die standortübergreifende Zusammenarbeit vom Homeoffice aus wird nicht länger als Problem, sondern in Zeiten des Klimawandels als Chance zur Ressourcenschonung und als „Heimvorteil" wahrgenommen. Diese Transformation unserer Arbeitswelt hat auch die Anforderungen und Bedürfnisse der Arbeitnehmer:innen verändert und damit die Bedeutung der Gestaltung sowie die Relevanz der Netzwerktechnik im Unternehmen erhöht. Diese neue Form von „New Work" erfordert eine zunehmend leistungsfähigere und sichere digitale Infrastruktur, die auch das Homeoffice der Mitarbeiter:innen betrifft, was aus digitaler Sicht weitreichende Folgen nach sich zieht.

Haftungsrisiko

Die Geschäftsführung ist für die IT-Sicherheit des Unternehmens verantwortlich – unabhängig davon, ob sich die eigene Expertise auf diesen Bereich erstreckt oder nicht. Eine gewerbliche Haftung gegenüber geschädigten Dritten ist bei einem hohen wirtschaftlichen Schaden bspw. gegenüber Kunden und Lieferanten durch Datenverlust, Erpressungen etc. nicht nur auf die Firma begrenzt.

Auch Versicherungen sind in dieser Beziehung stark eingeschränkt und haben immer mehr Anforderungen an die entsprechenden IT-Systeme. Die Versicherer erleiden erstmals Verluste durch die rasante Zunahme von Schadsoftware – was die Brisanz der Vernetzung von Mitarbeiter:innen im Homeoffice aus IT-Sicht nur umso stärker aufzeigt.

Das AirZen-System kombiniert zahlreichen Maßnahmen, um eine fundierte und sichere IT-Grundlage zu schaffen und der Sorgfaltspflicht in diesem Bereich nachzukommen.

Exponentielles Risiko: Homeoffice

Fehlende IT-Sicherheit

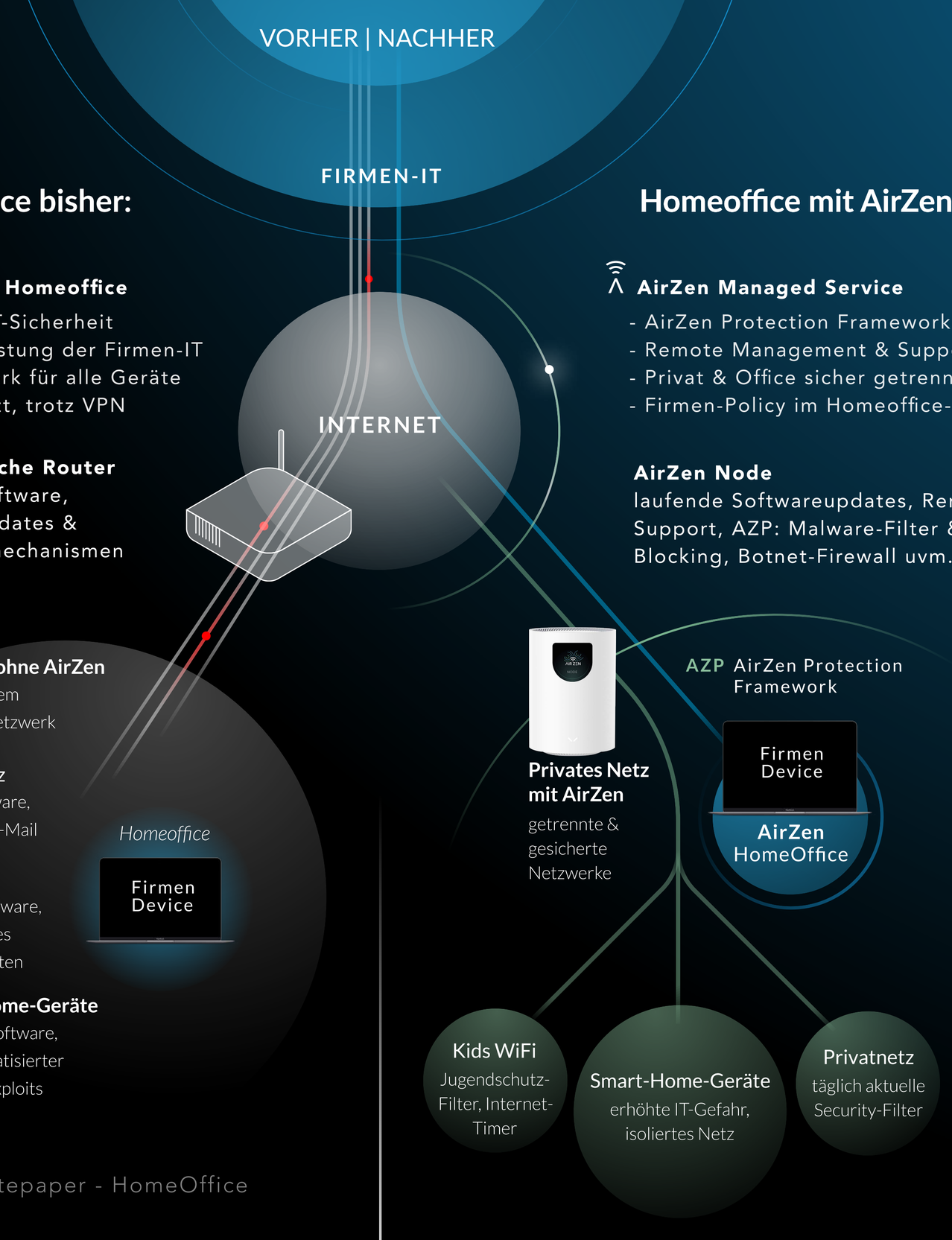
- private Router der Mitarbeiter:innen sind als „Blackbox" von der IT weder wartbar noch einsehbar
- private internetfähige Geräte sind besonders häufig Ziel von automatisierten Hacking-Angriffen
- IT-Risiko & Aufwand für das Unternehmen erhöht sich exponentiell mit jedem Homeoffice

Problematik: Gemeinsames Netzwerk

- Erweiterung des Firmennetzwerks mit jedem Homeoffice
- beim Einsatz von VPN kann Schadsoftware direkt in das Firmennetzwerk gelangen

Unkontrolliertes Nutzerverhalten

- Familienmitglieder nutzen den Internetzugang sorgloser
- Einbindung der privaten Hardware inkl. deren Schwachstellen
- Risikosituationen häufen sich (Social Media, Malware etc.)



Homeoffice bisher:

Unmanaged Homeoffice
- fehlende IT-Sicherheit
- Zusatzbelastung der Firmen-IT
- ein Netzwerk für alle Geräte
- ungeschützt, trotz VPN

Handelsübliche Router
veraltete Software, fehlende Updates & Sicherheitsmechanismen

Homeoffice mit AirZen:

AirZen Managed Service
- AirZen Protection Framework (AZP)
- Remote Management & Support
- Privat & Office sicher getrennt
- Firmen-Policy im Homeoffice-Netz

AirZen Node
laufende Softwareupdates, Remote-Support, AZP: Malware-Filter & Blocking, Botnet-Firewall uvm.

HOMEOFFICE WIFI & SECURITY SYSTEM, MADE IN EUROPE.

Unser Service standardisiert Ihr internes Netzwerk, externe Standorte und verbundenen Homeoffices:

Hohe Netzwerk-Resilienz
- AirZen Protection Framework: Botnet-Blocker, Malware-Filter, Datenschutz für Mitarbeiter:innen
- getrennte & gesicherte Netzwerke
- individuelle Netzwerk-Zugänge je Nutzer:innen mit 2FA
- optionales VPN ab Node

Managed Service & Support
- laufende Softwareupdates
- Plug-&-Play-Installation
- AirZen Managed Service vom Experten via APP, Chat oder Video-Meeting
- optionales Self-Service-Portal

Spürbar besseres WiFi
- Seamless Roaming via Mesh-Technologie
- Datenlimit und Pausenzeiten für Subnetze
- dynamische Netzoptimierung

AIRZEN-HOMEOFFICE-LÖSUNG

Die AirZen-HomeOffice-Lösung besteht aus einem Set von mindestens drei AirZen Nodes (WLAN-Access-Points und Router). Dank Mesh-Technologie bilden die Nodes automatisch ein flächendeckendes Netzwerk im gesamten Homeoffice.

Die AirZen Nodes bauen automatisch eine sichere Verbindung zur AirZen Cloud auf und erhalten von dort die jeweils zugewiesenen Konfigurationen. Alle Konfigurationen werden ausschließlich über die AirZen Cloud verwaltet.

Das AirZen-System unterstützt aktiv nur hauseigene Endgeräte. Sie können vom System überwacht, konfiguriert und administriert werden. An das Netzwerk angeschlossene bzw. betriebene Komponenten anderer Hersteller (sonstige Router, Switches usw.) werden vom AirZen-System nicht beeinflusst oder in der Funktion beeinträchtigt.

IT-Administratoren und autorisierte Personen erhalten Zugriff zur Konfiguration und Administration Ihrer AirZen Nodes. AirZen bietet zudem einen Managed Service an, bei dem AirZen die Administration, Konfiguration und Pflege entsprechend der kundenspezifischen Anforderungen für Sie übernimmt.

Die Firmware der Nodes ist speziell auf die Verbindung zur AirZen Cloud ausgelegt und funktional auf diese abgestimmt. Alle AirZen Nodes können per Netzwerkkabel und/oder WLAN-Verbindung betrieben werden.

Die AirZen Cloud übernimmt unter anderem auch die Zuordnung der Endgeräte zu den physikalischen und logischen Standorten sowie deren Zugehörigkeit, Konfigurationen uvm.:

Die AirZen-Cloud ist zugleich:

- Konfigurationstool
- Administrationstool
- Reporting-Tool
- Monitoring-Tool
- VPN-Koordinator (optional)

Bei der Realisierung einer sicheren Homeoffice-Lösung wird unterschieden in Netzwerke mit und ohne VPN-Anbindung der Nodes. Im Falle einer VPN-Anbindung ist ein AirZen VPN-Endpunkt in der Firmenzentrale notwendig; anderenfalls ist keinerlei Zusatztechnologie notwendig.

Optional: VPN direkt ab Node

Dazu wird zwischen den AirZen Nodes (Homeoffice) und dem AirZen Location Server (Office) eine sichere Direktverbindung in Form eines „Layer 2 VPN-Tunnels“ hergestellt – direkt ab Node. Die Konfiguration und koordinative Zuordnung all dieser spezifischen VPN-Verbindungen erfolgt über die AirZen Cloud. Die eigentliche Datenkommunikation erfolgt stets direkt vom AirZen Node zum AirZen Location Server und umgekehrt. Es können dabei auch bereits bestehende VPN-Technologien verwendet werden.

Neben dem Firmen-PC und -Laptop im Homeoffice können auch Firmen-Drucker, IP-Telefon u. a. wie am Büroarbeitsplatz eingebunden werden. Die anderen, im Homeoffice vorhandenen privaten Geräte nutzen weiter das bestehende Heimnetz, sicher getrennt vom Firmennetz. Eine Ausweitung des Netzwerks kann problemlos durch weitere AirZen Nodes realisiert werden. Die AirZen-OS-Technologie ermöglicht auch mehrere VPN-Verbindungen je Node zu verschiedenen Endpunkten, ganz nach Ihren Bedürfnissen.

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

Ihre Vorteile

Die AirZen-Plattform ermöglicht es, Ihr Firmennetzwerk virtuell in das Homeoffice auszudehnen (und umgekehrt), Ihre IT-Abteilung zu entlasten und die Sicherheit des gesamten Netzwerks zu gewährleisten. Dabei bietet die Plattform umfangreiche Vorteile:

Hohe Netzwerk-Resilienz
Durch innovative & smarte Automatismen, die das Potenzial ihres Netzwerks umfänglich nutzen.

- Automatisierte Softwareupdates und kurze Update-Intervalle verbessern Ihre IT-Sicherheit nachhaltig.
- AirZen Protection Framework für höhere Unternehmenssicherheit und reduzierte Angriffsfläche.
- Teamverwaltung über das Self-Service Portal: Einzigartige Passwörter für Mitarbeiter:innen inklusive Content-Filter.
- Getrennte & gesicherte Netzwerke zur Isolierung des Homeoffice-Netzwerks vom privaten Netz der Mitarbeiter:innen.
- Optionales VPN direkt ab AirZen Node, die Datenkommunikation erfolgt stets direkt vom Node zum Location Server (und umgekehrt).

Kosten- & Zeitersparnis
Voller Service für Ihre Nutzer:innen, umfassender Experten-Support.

- Remote Management & Support, dauerhafte Überwachung der Funktionsfähigkeit, kontinuierliche WLAN-Qualitätsmessung.
- Plug-&-Play WLAN-Set: spielend leichte Installation auch ohne IT-Kenntnisse.
- AirZen Managed Service über die AirZen-App Ticket-System mit integrierter Chat-Lösung: Mitarbeiter:innen können direkt mit dem AirZen Managed Service kommunizieren oder das IT-Team des Kunden wird vorgeschaltet.
- Volle Kontrolle über Ihr Netzwerk durch smarte Verwaltung per App, CLI oder Self-Service-Portal (optional).
- Umfangreiche technische Expertise dank Netzwerk-Know-How von AirZen.

Dynamische WiFi-Optimierung
Neuester WiFi-6-Standard und clevere Automatismen für ein spürbar besseres Netzwerk.

- Die AirZen WiFi-Quality-Technologie dient der Qualitätskontrolle und hilft dabei, WLAN-Probleme zu lösen, bevor sie spürbar werden.
- Bessere WLAN-Verbindungen durch Seamless Roaming: Ihr Endgerät wird immer mit der optimalen Node verbunden.
- Automatische Auswahl des besten WLAN-Funkkanals durch smarte Analysetools.
- Per Beamforming-Technologie wählt die AirZen Node stets die optimale Kombination der WLAN-Antennen für beste WLAN-Qualität.
- Mesh-Technologie: leistungsstarke & lückenlose WLAN-Verbindungen aller Nodes untereinander dank intelligenter Mesh-Technologie.

IMPLEMENTIERUNG DER AIRZEN-HOMEOFFICE-LÖSUNG

Die AirZen-HomeOffice-Lösung bietet eine spürbare Entlastung der IT-Abteilung, eine Erhöhung der Arbeitsqualität sowie eine höhere IT-Resilienz in den Homeoffices unserer Kunden.

AirZen stellt eine Netzwerk-Management-Lösung bereit, die, in direkter Abstimmung mit Ihrem Unternehmen, Netzwerk-Design- und Security-Ansprüche sowie deren Realisierung prüft und umsetzt.

Die Mitarbeiter:innen erhalten ein Plug-&-Play System, welches sie selbstständig installieren und bei Bedarf Hilfe per AirZen Direkt-Support erhalten. Nach Abschluss der Installation steht ein flächendeckendes Netzwerk im Homeoffice der Mitarbeiter:innen zur Verfügung.

Woche 1 *in Kooperation*
Video-Meeting & Projekt-besprechung, Start der Netzwerkplanung

Woche 2 *via AirZen*
Abschluss Netzwerkplanung, Test-Gerät mit geplanter Netz-Konfiguration

Woche 3-5 *via AirZen*
Start des Rollouts, Versand der Geräte, Installation vor Ort via Plug-&-Play. Das Netzwerk steht unmittelbar bereit.

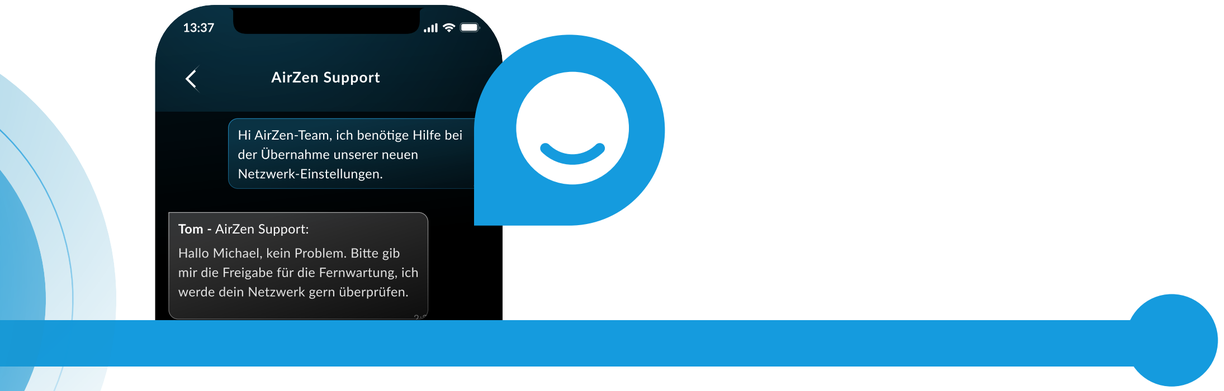
Vorbereitung

In der AirZen Cloud werden die spezifischen Netzwerk- und Standort-Einstellungen festgelegt. Jedes AirZen Set wird darin einer sogenannten „Location" (anhand der Node-Seriennummer) zugeordnet, die den vom Kunden zuvor definierten Netzwerk-Einstellungen folgt. An unterschiedlichen Standorten können dieselben oder verschiedene Konfigurationen gelten. Diese Konfigurationen werden vorwiegend bereits vor der Auslieferung vorgenommen.

Lieferung und Inbetriebnahme per Plug-&-Play

Das AirZen Node Set wird direkt in das Homeoffice oder an den Arbeitsplatz per Paketdienst geliefert. Bei Installationsproblemen der Mitarbeiter:innen hilft der Live-Support von AirZen.

Die AirZen Nodes werden per LAN-Kabel mit dem DSL-Modem am privaten Internetanschluss oder dem vorhandenen Provider-Router verbunden. Darüber erhält die Node per DHCP eine IP-Adresse.



Woche 6-8
Abschluss & Finetuning. Letzte Details werden eingerichtet und abgestimmt. Der operative Betrieb läuft bereits.

Betrieb der AirZen-HomeOffice-Lösung

Sobald die AirZen Node erkennt, dass der Internetzugang besteht, baut sie automatisch eine gesicherte Verbindung zur AirZen Cloud auf und meldet sich in dieser an. Durch diesen Schritt erhält sie ihre gewünschte individuelle Konfiguration. In ihrer Eigenschaft als AirZen Node generiert sie ein WLAN-Netzwerk mit einer konfigurierbaren (Firmen-)SSID zur Einwahl, im Folgenden „HomeOffice“ genannt.

Das jeweilige Endgerät ist dabei sicher vom privaten Heim-Netzwerk getrennt. Es befindet sich sozusagen „ausschließlich“ im Firmennetzwerk. Ein Zugriff aus dem privaten Netzwerk auf das Firmennetzwerk ist nicht möglich.

Getrennte & gesicherte Netzwerke

Die gesamte Datenübertragung im Netzwerk „HomeOffice“ ist geschützt und vom privaten Heim-Netzwerk sicher abgetrennt. Dies gilt natürlich für beide Richtungen.

Bereits die Einwahl in die WLAN-SSID „HomeOffice“ kann durch individuelle Passwörter je Nutzer:innen und Gerät per Self-Service-Portal geschützt werden. Jeder Ethernet-Kabelanschluss der AirZen Node lässt sich einem gewünschten Netzwerk zuordnen. So können Drucker und weitere firmeninterne Geräte sicher im Homeoffice installiert werden.

Erforderliche Anschlüsse & Bandbreiten

Ein Homeoffice-Internetanschluss sollte mindestens über eine Bandbreite von 10 Mbit/s verfügen. Andernfalls kann ein Modell der AirZen Node per 4G/5G-Anbindung ggf. eine höhere Bandbreite ermöglichen. Dieses Modell lässt sich zudem auch als Fail-Over-Gerät einsetzen. Im Falle eines Internetausfalls schaltet die Node dann automatisch vom Kabel auf 4G bzw. 5G um. Für eine solche 4G/5G-Anbindung sind zusätzliche SIM-Karten des jeweiligen Landes-Providers notwendig. Darüber hinaus kann ein VPN-Tunnel aufgebaut werden und das Unternehmen so über verschiedene Uplinks (SD-WAN) verbunden werden.

STATE-OF-THE-ART-TECHNOLOGIE

Mit der AirZen-HomeOffice-Lösung steht am Heimarbeitsplatz ein professionelles WLAN-System zur Verfügung. Anwender:innen erhalten eine sichere Netzwerklösung für ihre privaten und geschäftlichen Anwendungen.

Jede AirZen Node verfügt über mehrere Netzwerke: HomeOffice, Privat, Kids-WiFi & Things. Diese Netze sind sicher voneinander getrennt und verwaltet. Die Firmen IT-Abteilung kann lediglich das HomeOffice-Netz managen, alle weiteren Netzwerke bleiben privat.

Neben der Erweiterungsmöglichkeit (Stichwort „Mesh“) zur optimalen Abdeckung aller Räume sorgt die AirZen Smart-Roaming-Funktion dafür, dass das Endgerät stets automatisch mit dem in der jeweiligen Position leistungsfähigsten AirZen Node verbunden wird. Dies ist z. B. relevant für unterbrechungsfreie Voice-over-IP-Telefongespräche, wenn man sich während des Gesprächs im Haus bewegen will. Dieses neue Verfahren beruht darauf, dass nicht das Endgerät, sondern das WLAN-System regelmäßig prüft, welche Verbindung zwischen dem Endgerät und den erreichbaren AirZen Nodes die beste Übertragungsqualität bietet.

Dem IT-Administrator wie auch den HomeOffice Nutzer:innen stehen mit den AirZen-Tools zahlreiche Statusanalyse-Werkzeuge zur Verfügung, damit im Fall von Verbindungsproblemen schnell die Ursache einer Störung ermittelt werden kann. Das AirZen-System ist so ausgelegt, dass es eigenständig regelmäßig Statusanalysen durchführt und im Fall einer Problemermittlung diese automatisch übermittelt.

Ein autorisierter Administrator kann sich dann über eine VPN-Verbindung direkt in das Homeoffice-Netzwerk einwählen, um die Nutzer:innen aus der Ferne zu unterstützen. Dabei hat der Administrator jedoch kein Zugriff oder Einblick in das private Netzwerk der Nutzer:innen.

Alternativ können die üblichen Tools über das Firmennetzwerk genutzt werden. Je nach Administrator-Berechtigung kann von diesem „per Remote“ eine Konfigurationsänderung am Homeoffice-Netzwerk vorgenommen oder ein WLAN-Passwort zurückgesetzt werden. All diese Vorgänge werden in einem Protokoll festgehalten. Die Nutzer:innen selbst besitzen diese Berechtigungen i. d. R. nicht, da sie zur Nutzung selbst nicht benötigt werden.

Mesh-Technologie

AirZen Nodes sind Mesh fähig. Es können mehrere AirZen Nodes und auch weitere AirZen-Node-Modelle in einem Homeoffice eingesetzt werden. Dadurch lässt sich das Netzwerk auf das gesamte Haus und Outdoor (im Garten und Nebengebäuden) ausdehnen.

Da die Mesh-Funktion ebenfalls mittels Plug-&-Play installiert wird, kann das Netzwerk jederzeit mit mehreren AirZen Nodes nachgerüstet werden. Das „AirZen MeshNode“-Verfahren verbindet alle AirZen Nodes im Homeoffice völlig automatisch ohne weiteren manuellen Konfigurationsaufwand. Die Mesh-Technologie sorgt für flächendeckenden Empfang bei gleichbleibender Übertragungsgeschwindigkeit, da das Mesh von sich aus entscheidet, welche AirZen Node gerade für ein Endgerät die beste Performance liefert – gerade für mobile Endgeräte im Mesh-Bereich.

Cybersicherheit

AirZen überprüft dauerhaft die Ziel-IP-Adressen, welche durch die AirZen Node aufgerufen werden, und filtern dabei aktuelle Viren-Botnetze und andere schädliche Ziel-IPs. Derartige Verbindungen werden geblockt, um bei einem Virus-Befall die Kommunikation zum Viren-Command-Server zu unterbinden.

Das optionale 5G-Modell AirZen Node H5 bietet eine weitere Besonderheit für remote-gemanagte Homeoffice-Netzwerke dar. Das AirZen-Mesh-Set bietet innerhalb des Homeoffice ein perfektes und sicheres WLAN, während das Gateway Node H5 per 5G und privatem DSL-Anschluss das Internet-Management übernimmt. Es ist zudem möglich, das Homeoffice-Netzwerk nur per 5G anzubinden und dazu einen VPN-Tunnel (AirZen VPN oder 3rd Party Anbieter) zu nutzen, wodurch der private DSL-Anschluss ungenutzt bleibt.

Kommen beide Uplinks zum Einsatz, dient jeweils der inaktive als Fallback. Auf diesem Weg können auch Ethernet-Anschlüsse im Homeoffice direkt mit dem Unternehmen verbunden werden. Somit wird buchstäblich der Unternehmens-Ethernet-Anschluss bis in das Homeoffice verlängert. Dadurch bietet Ihnen die AirZen-Plattform eine echte dynamische Unternehmensvernetzung an.

Die AirZen-HomeOffice-Lösung verfügt über unterschiedlich starke Sicherheitsmechanismen und Authentifizierungsverfahren, die bedarfsgerecht und passend zur Netzwerkausprägung und Kundenanforderungen eingerichtet und aktiviert werden. So kann in der höchsten Sicherheitsstufe bspw. konfiguriert werden, dass nur zuvor ausgewählte Anwender und identifizierte Geräte über eine ganz bestimmte Node und an einem festgelegten Standort Zugang erhalten. Sollte also ein Paket beim Versand in die falschen Hände geraten, ist dies unbedenklich, denn es sind stets zusätzliche Sicherheitsmerkmale wie z. B. ein zweiter Passcode notwendig, um die Installation abzuschließen.

Kommt VPN zum Einsatz, so sind in jedem Fall die Einstellungen und Sicherheitsmechanismen des Firmen-Netzwerkes auch im Homeoffice aktiv. Zur Klarstellung sei an dieser Stelle angemerkt, dass mit der AirZen Cloud nicht das Firmen-Netzwerk administriert werden soll und auch nicht administriert werden kann. Die Ausdehnung eines Firmen-Netzwerkes kann immer nur so sicher sein wie das Firmen-Netzwerk selbst.

Der Zugriff auf die AirZen Cloud ist nur über ein Sicherheitszertifikat möglich und ist zusätzlich an einen „Zwei Faktor"-Mechanismus gekoppelt. Die Kommunikation der AirZen Nodes mit der AirZen Cloud geschieht ebenfalls verschlüsselt und Zertifikats-basiert. Diese Kommunikation wird über eine speziell zu diesem Zweck von AirZen entwickelte Software gesteuert.

AirZen-App

Die AirZen-App-Verwaltung ist für die Nutzer:innen besonders einfach und benutzerfreundlich. Die Home-IT-Security-Features sind durch die hohe Anwenderfreundlichkeit der AirZen-App leicht verständlich und werden von den Nutzer:innen erfahrungsgemäß häufig genutzt, um präventiv weitere Sicherheitsmaßnahmen im HomeOffice zu ergreifen. Die Nutzung der Funktionen für das private Netzwerk ist optional. AirZen stellt eine Trennung von Privat- und Arbeitsleben durch innovative und moderne Technologien sicher. Ziel ist es, die Nutzer:innen vor Gefahren aus dem Internet zu schützen.

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.

Erweiterbare Services

Neben der AirZen-HomeOffice-Lösung bietet AirZen noch weitere Lösungspakete, die AirZen Core Solutions.

Alle AirZen-Lösungen sind kompatibel und kombinierbar und basieren auf einer standardisierten Node-Technologie sowie einer gemeinsamen Cloud-Architektur.

AirZen

Public WiFi

Gastzugang mit Portal- und zusätzlichen Marketing-Funktionen zur Verfügung. Dank der vielfältigen Parametrierbarkeit können Erscheinungsbild, Funktionen und Auswertungen der Gastnetzwerke individuell und komfortabel konfiguriert werden.

AirZen

Business

Bietet eine einfache und sichere Netzwerk-Management-Lösung, die Firmennetzwerke jeder Art und Größe schnell bereitstellen und bedarfsgerecht skalieren kann. Hierfür bietet AirZen per Fernwartung eine Vielzahl an Administrationsmöglichkeiten, wodurch die IT-Abteilung spürbar entlastet wird.

AirZen

Education

Bietet Bildungseinrichtungen die Möglichkeit, separate Verwaltungs-, Lehrer- und Schüler-Netzwerke gleichzeitig sicher zu betreiben und eine besonders geschützte Internetnutzung zu gewährleisten. Die Administrationsfunktionen sind auf den besonderen Bedarf dieser Branche zugeschnitten und intuitiv bedienbar.

AirZen

Industrial

Ist speziell für industrielle und behördliche Ansprüche mit seinen besonderen Anforderungen an die IT-Sicherheit und Zuverlässigkeit konzipiert – auch unter schwierigen Einsatzbedingungen wie extremes Wetter oder dynamische Umgebungen.

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.

AirZen Networks Lda.

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

business@airzen.io

www. AirZen.io