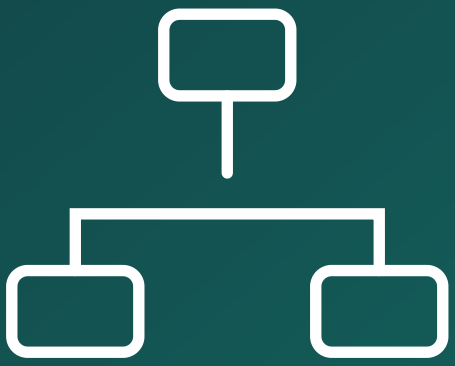

WHITEPAPER · NETZWERK

Netzwerk-Design für kleine Unternehmen

Segmentierung, WLAN, Firewall-Regelwerk und Dokumentation – inklusive Zone für Produktion, Maschinen und Roboter.

DAS ERHALTEN SIE

- Zonenmodell mit Beispiel-VLAN-Plan
- WLAN-Planung: Roaming, Band Steering, 802.1X
- Firewall-Matrix nach dem Zero-Trust-Prinzip
- OT-/Roboter-Zone und Industrie-DMZ

AUF EINEN BLICK

Für	**IT-Verantwortliche, Betriebe mit Büro und Produktion**
Zeitbedarf	**ca. 2 Stunden Planung**
Stand	**16. November 2026**
Version	**2.0**

Unverbindliche Praxishilfe – keine Rechtsberatung, kein Audit

1 Grundprinzipien

> Ein verständliches Netzwerkdesign trennt unterschiedliche Vertrauensbereiche, begrenzt unnötige Verbindungen und macht Fehlerbehebung reproduzierbar.

- **Datenflüsse zuerst**: Wer muss mit wem sprechen? Daraus folgen Zonen und Regeln – nicht aus einer beliebigen VLAN-Vorlage.
- **Minimale Verbindungen**: Zwischen Zonen ist alles verboten, was nicht ausdrücklich erlaubt ist.
- **Zero Trust**: Netzwerkposition allein begründet kein Vertrauen; Identität, Gerätezustand und Verschlüsselung zählen.
- **Verwaltung getrennt**: Switches, Firewalls, Access Points und Hypervisoren werden nur aus dem Management-Netz administriert.
- **Dokumentiert und reproduzierbar**: Pläne, Konfigurationen und Änderungen sind aktuell und versioniert.

Aufbau

Ebene	Aufgabe
Internet-Edge / Firewall	Übergang zum Internet, VPN, Regeln zwischen allen Zonen
Core	Zentrale Switches, Routing zwischen VLANs (über die Firewall, wenn Regeln greifen sollen)
Access	Anschluss von Arbeitsplätzen, Druckern, Access Points; Port-Sicherheit
DMZ	Aus dem Internet erreichbare Dienste, getrennt vom internen Netz

2 Zonen und Beispiel-VLAN-Plan

Die VLAN-Nummern und Adressbereiche sind Beispiele. Wählen Sie Bereiche, die sich nicht mit typischen Heimnetzen (z. B. 192.168.0.0/24 und 192.168.1.0/24) überschneiden – das vermeidet Probleme bei VPN-Verbindungen.

VLAN	Zone	Beispielnetz	Inhalt
10	Management	10.10.10.0/24	Verwaltungsschnittstellen von Netzwerk, Servern, Hypervisoren
20	Server	10.10.20.0/24	Domänencontroller, Datei- und Anwendungsserver
30	Clients	10.10.30.0/23	Arbeitsplätze und Notebooks
40	Drucker & Peripherie	10.10.40.0/24	Drucker, Scanner
50	VoIP	10.10.50.0/24	Telefone, mit QoS
60	IoT / Gebäude	10.10.60.0/24	Kameras, Zutritt, Gebäudetechnik
70	OT / Produktion & Roboter	10.10.70.0/24	Maschinen, Roboterzellen, AMR-Netz (siehe Abschnitt 5)

VLAN	Zone	Beispielnetz	Inhalt
80	Industrie-DMZ	10.10.80.0/24	MQTT-Broker, OPC-UA-Gateways, Flottenmanager, Fernwartungs-Gateway
90	Gäste	10.10.90.0/24	Nur Internet, Client-Isolation
—	DMZ (Internet)	10.10.100.0/24	Öffentlich erreichbare Dienste

3 WLAN-Planung

- **Ausleuchtung messen** statt schätzen: Vor-Ort-Messung oder Planungssoftware mit Grundriss; Wände, Regale und Metall beachten.
- **Wenige SSIDs**: z. B. Mitarbeitende, Gäste, ggf. IoT/Roboter – jede zusätzliche SSID kostet Sendezeit.
- **Mitarbeitende**: WPA3-Enterprise bzw. WPA2/WPA3-Enterprise mit 802.1X und RADIUS, Zuweisung des VLANs nach Identität.
- **Gäste**: Eigenes VLAN, Client-Isolation, nur Internet, Bandbreitenbegrenzung.
- **Roaming**: 802.11k/v/r unterstützen schnelle, reibungslose Übergaben zwischen Access Points – wichtig für Telefonie und mobile Roboter.
- **Band Steering** zu 5 GHz bzw. 6 GHz, passende Kanalbreiten und Sendeleistungen statt maximaler Leistung.
- **Zentrale Verwaltung** der Access Points mit Firmware-Pflege.

Mobile Roboter (AMR) im WLAN

Autonome mobile Roboter benötigen flächendeckende Abdeckung entlang der Fahrwege, schnelles Roaming und geringe Latenz. Planen Sie ein eigenes Roboter-Netz, prüfen Sie die Herstellervorgaben zu Frequenzband und Roaming und messen Sie die Abdeckung in Fahrhöhe der Roboter.

4 Firewall-Regelwerk

Ein Regelwerk ist nur so gut wie seine Begründung. Jede Regel hat Zweck, Eigentümer und Prüfdatum. Die Matrix zeigt ein typisches Ausgangsbild.

Von ↓ / Nach →	Server	Clients	Mgmt	OT	Ind.-DMZ	Internet
Clients	nötige Dienste	—	×	×	nur Dashboards	über Proxy/Filter
Server	nach Bedarf	nach Bedarf	×	×	nach Bedarf	Updates
Mgmt	✓ Verwaltung	✓ Verwaltung	—	✓ Verwaltung	✓	Updates
OT	×	×	×	—	definierte Protokolle	×

Von ↓ / Nach →	Server	Clients	Mgmt	OT	Ind.-DMZ	Internet
Ind.-DMZ	ERP/MES-Schnittstelle	×	×	definierte Protokolle	—	nur freigegeben
Gäste / IoT	×	×	×	×	×	nur Internet

- Standardregel am Ende: alles verweigern und protokollieren.
- Keine Regeln mit „any/any“; Ziele und Dienste konkret benennen.
- Fernzugriff nur über VPN mit MFA; keine Verwaltungsports im Internet.
- Regelwerk mindestens halbjährlich prüfen; ungenutzte Regeln entfernen.

5 Produktion und Roboter: OT-Zone und Industrie-DMZ

Roboter, Maschinen und Steuerungen haben andere Anforderungen als Büro-IT: lange Lebenszyklen, eingeschränkte Patch-Möglichkeiten und Hersteller, die Fernwartung benötigen. Die Normenreihe **IEC 62443** beschreibt dafür das Modell aus **Zonen** (Bereiche mit gleichem Schutzbedarf) und **Conduits** (kontrollierte Verbindungen zwischen Zonen).

Trennen

- Eigene OT-Zone; Roboterzellen ggf. weiter unterteilt
- Kein direkter Verkehr zwischen Büro-Clients und Steuerungen
- Echtzeit-Steuerung bleibt in der Roboterzelle

Vermitteln

- Industrie-DMZ zwischen OT und IT
- MQTT-Broker mit TLS und Zertifikaten für Telemetrie
- OPC UA mit Signatur und Verschlüsselung für MES/ERP

Fernwartung

- Herstellerzugang über Gateway in der Industrie-DMZ
- Zeitlich begrenzt, protokolliert, mit MFA
- Keine dauerhaft offenen Ports

Bestand & Altgeräte

- Inventar aller OT-Geräte mit Firmware-Stand
- Protokoll-Gateway für ältere Maschinen (z. B. Modbus, S7)
- Nicht patchbare Geräte strikt isolieren

Sicherheit von Mensch und Maschine

Netzwerkänderungen in der Produktion nur in Abstimmung mit Betrieb und Hersteller. Sicherheitsfunktionen wie Not-Halt und Schutzeinrichtungen dürfen niemals vom Netzwerk oder von Cloud-Diensten abhängen.

Mehr zur Anbindung von Robotern an das Firmennetz: **kontorit.de/robotics**

6 Grunddienste, Monitoring und Dokumentation

Bereich	Empfehlung
DNS / DHCP	Redundant auslegen; Reservierungen für Infrastruktur; DHCP-Snooping auf Access-Switches
Zeit (NTP)	Einheitliche Zeitquelle für alle Geräte – Voraussetzung für auswertbare Protokolle
Monitoring	Verfügbarkeit und Auslastung per SNMPv3; zentrale Syslog-Sammlung; Alarm mit Vertretung
Port-Sicherheit	Ungenutzte Ports deaktivieren; 802.1X/MAB, wo möglich
Notfallzugriff	Out-of-Band-Zugang (z. B. separater Mobilfunk-Router oder Konsolenserver) zu Firewall und Core
Dokumentation	Netzplan, VLAN- und IP-Plan, Regelwerk mit Begründung, Konfigurations-Backups nach jeder Änderung

	Prüfpunkt	Verantwortlich	Termin / Nachweis
DESIGN			
☐	Datenflüsse und Zonen sind dokumentiert.	_____	_____
☐	Management-Netz ist getrennt und nur für Admins erreichbar.	_____	_____
☐	Gäste und IoT sind isoliert.	_____	_____
☐	OT/Roboter haben eine eigene Zone mit Industrie-DMZ.	_____	_____
BETRIEB			
☐	Firewall-Regeln haben Zweck, Eigentümer und Prüfdatum.	_____	_____
☐	WLAN-Abdeckung ist gemessen (inkl. Roboter-Fahrwege).	_____	_____
☐	Monitoring und Syslog sind aktiv.	_____	_____
☐	Konfigurationen werden versioniert gesichert.	_____	_____
☐	Notfallzugriff ist getestet.	_____	_____

Quellen & weiterführende Referenzen

- BSI IT-Grundschutz-Kompendium, Bausteine NET.1.1 „Netzarchitektur und -design“, NET.2.1 „WLAN-Betrieb“, NET.3.2 „Firewall“, IND.1 „Prozessleit- und Automatisierungstechnik“, bsi.bund.de
- IEC 62443 – Industrielle Kommunikationsnetze: IT-Sicherheit für Netze und Systeme
- BSI: ICS-Security-Kompendium und Top-10-Bedrohungen für Industrial Control Systems, bsi.bund.de
- IEEE 802.1X, 802.11k/v/r; Wi-Fi Alliance: WPA3
- OPC Foundation: OPC UA Security; OASIS: MQTT Version 5.0
- KONTORIT: Robotik-Integration (kontorit.de/robotics)

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0