

Firmennetzwerk prüfen: Internet, WLAN und Sicherheit

Eine verständliche Arbeitsunterlage für Geschäftsführung und interne Ansprechpartner. Markieren Sie, was geklärt ist. Für offene Punkte reicht zunächst eine Bestandsaufnahme, bevor Geräte oder Leitungen ersetzt werden.

Wichtig: Langsames WLAN oder kurze Ausfälle bedeuten nicht automatisch, dass alles neu gebaut werden muss. Häufig helfen zuerst Messung, Dokumentation und eine saubere Eingrenzung der Ursache.

1. Geschäftliche Anforderungen und Störungen

Zuerst wird geklärt, welche Arbeitsabläufe vom Netzwerk abhängen und wo Probleme tatsächlich auftreten.

- ☐ Kritische Abläufe wie Telefonie, Warenwirtschaft, Cloud-Zugriff oder Produktion sind bekannt.
- ☐ Es ist dokumentiert, wann, wo und bei welchen Geräten Verbindungsprobleme auftreten.
- ☐ Langsame Anwendungen werden von einem langsamen Internetzugang oder WLAN unterschieden.
- ☐ Standorte, Räume, Homeoffice- und Außenzugänge sind in der Betrachtung enthalten.
- ☐ Für wichtige Ausfälle ist bekannt, wer intern entscheidet und wer technisch kontaktiert wird.

2. Internetzugang und Ausfallsicherheit

Vertrag, Anschluss und Ersatzweg sollen zum tatsächlichen Geschäftsrisiko passen.

- ☐ Anbieter, Tarif, Bandbreite, Vertragsinhaber und Störungsnummer sind dokumentiert.
- ☐ Die tatsächlich verfügbare Leistung wurde zu typischen Arbeitszeiten geprüft.
- ☐ Bei einem Ausfall ist klar, welche Dienste noch funktionieren und welche sofort betroffen sind.
- ☐ Für besonders wichtige Abläufe ist ein sinnvoller Ersatzweg geprüft, etwa Mobilfunk oder Zweitleitung.
- ☐ Öffentliche IP-Adressen, Fernzugänge und notwendige Portfreigaben sind nachvollziehbar festgehalten.

3. WLAN, Gäste und mobile Geräte

Gute Abdeckung, Kapazität und klare Trennung sind wichtiger als möglichst viele Zugangspunkte.

- ☐ Arbeitsbereiche wurden auf Abdeckung, Störungen und typische Auslastung geprüft.
- ☐ Zugangspunkte sind sinnvoll platziert und werden zentral oder nachvollziehbar verwaltet.
- ☐ Gäste, private Geräte und interne Arbeitsgeräte verwenden getrennte Zugänge.
- ☐ WLAN-Namen, Kennwörter und Freigaben werden nicht unkontrolliert weitergegeben.
- ☐ Drucker, Scanner, Telefone und Spezialgeräte sind dem richtigen Netz zugeordnet.

Das bestehende Netzwerk verlässlich betreiben

Ein Firmennetzwerk muss nicht möglichst kompliziert sein. Entscheidend sind klare Zuständigkeiten, geschützte Zugänge, bekannte Geräte und Änderungen, die auch später noch nachvollziehbar bleiben.

4. Firewall, Trennung und Fernzugriff

Zentrale Schutzregeln sollen verständlich begründet und auf das notwendige Maß begrenzt sein.

- ☐ Firewall, Standort und verantwortlicher Betreiber sind eindeutig bekannt.
- ☐ Administratorzugänge gehören dem Unternehmen und sind mit mehrstufiger Anmeldung geschützt.
- ☐ Server, Arbeitsgeräte, Gäste, Kameras und technische Geräte sind soweit sinnvoll getrennt.
- ☐ Fernwartung und Homeoffice-Zugänge sind auf berechnigte Personen und benötigte Systeme begrenzt.
- ☐ Alte Portfreigaben, ungenutzte VPN-Zugänge und ehemalige Dienstleisterzugänge werden geprüft.

5. Komponenten, Verkabelung und Aktualisierung

Geräte müssen nicht gleichzeitig ersetzt werden, sollten aber identifizierbar und betreibbar bleiben.

- ☐ Router, Firewall, Switches und WLAN-Zugangspunkte sind mit Modell, Standort und Aufgabe erfasst.
- ☐ Wichtige Leitungen, Verteiler, Anschlüsse und Beschriftungen sind nachvollziehbar.
- ☐ Konfigurationen und Sicherungen zentraler Netzwerkgeräte sind geschützt verfügbar.
- ☐ Updates und bekannte Sicherheitslücken werden regelmäßig und geplant berücksichtigt.
- ☐ Nicht mehr unterstützte Komponenten sind bekannt und nach Risiko statt nur nach Alter priorisiert.

6. Überwachung, Änderungen und Betreuung

Kleine Abweichungen sollen sichtbar werden, bevor daraus ein längerer Betriebsausfall entsteht.

- ☐ Ausfälle, ungewöhnliche Last und knapper Speicher zentraler Komponenten werden bemerkt.
- ☐ Änderungen an Firewall, WLAN, Verkabelung und Zugängen werden kurz dokumentiert.
- ☐ Zuständigkeiten, Eskalationsweg und erreichbare technische Ansprechpartner sind festgelegt.
- ☐ Ein aktueller Übersichtsplan zeigt Internet, Firewall, zentrale Geräte und wichtige Verbindungen.
- ☐ Offene Punkte sind nach Geschäftsrisiko, Nutzen und Aufwand geordnet statt pauschal erneuert.

Die drei wichtigsten offenen Punkte

Netzwerk verständlich prüfen und verbessern

Quansatech prüft den bestehenden Stand, erklärt Engpässe und plant Verbesserungen ohne unnötigen Komplettumbau. OÖ als Kerngebiet, österreichweit nach technischer Möglichkeit.

+43 720 895056 | office@quansatech.at
www.quansatech.at/netzwerktechnik/