
BLUE CONSULT.

Netzwerksicherheit

# Netzwerksicherheit & Netzwerkdesign: Das Fundament eines jeden Unternehmens

## Sicherheit. Stabilität. Verfügbarkeit. – Schaffen Sie die unsichtbare Grundlage für Ihre tägliche Arbeit

Als Unternehmen ist man täglich Tausenden von Cyberangriffen ausgesetzt, wobei Ausfälle in Sekunden hohe Verluste verursachen können. Viele unterschätzen, wie stark ihre Wettbewerbsfähigkeit, Produktivität und selbst ihr Ruf von der Zuverlässigkeit ihrer IT-Infrastruktur abhängen - eine stabile und sichere Netzwerkinfrastruktur ist kein Luxus – sie ist überlebenswichtig.

Auch wenn Cyber-Prävention immer besser wird, die Cyber-Angriffe nehmen massiv zu, Schäden erreichen Rekordhöhen, und nur ein Bruchteil der Unternehmen ist wirklich vorbereitet.

### Fakten-Check: Cybersecurity-Lage in Deutschland 2024 – Übersicht

- **78 % mehr Cyberangriffe** auf deutsche Unternehmen im 3. Quartal 2024 im Vergleich zum Vorjahreszeitraum.
- **266,6 Milliarden Euro Schaden** durch digitale Angriffe für die deutsche Wirtschaft im Jahr 2024.
- Nur **2 % der deutschen Unternehmen** sind laut Cisco-Index auf aktuelle Cyberbedrohungen vorbereitet.
- **1.220 Cyberattacken pro Woche** trafen deutsche Organisationen im Durchschnitt.

*Quellen: Studien und Berichte 2024 von IT-Sicherheit.de, Bitkom, Cisco und Security Insider.*

IT-Abteilungen stehen vor der Herausforderung, hybride Netzwerke abzusichern – bestehend aus On-Premises-Systemen und Cloud-Diensten. Oft fehlt die Transparenz über Datenflüsse, verdächtige Aktivitäten bleiben unentdeckt, und Sicherheitslücken werden zu spät geschlossen. Die Folge: große Angriffsflächen für Cyberkriminelle. Ein wichtiger Sicherheitsbaustein ist die Segmentierung – also die logische Trennung des Netzwerks, z. B. per VLANs. So lassen sich Systeme mit unterschiedlichem Schutzbedarf, wie Industrieanlagen oder externe Zugänge, klar voneinander abgrenzen. Ebenso wichtig ist eine strikte Zugriffskontrolle: Nur autorisierte Nutzer und Geräte dürfen auf bestimmte Segmente zugreifen – sonst reicht ein infiziertes Besuchergerät für einen Angriff. Weitere Risiken entstehen durch fehlendes oder manuelles Schwachstellenmanagement. Ohne Automatisierung bleiben Lücken bei neuen Bedrohungen oft bestehen. Erschwerend kommen Schatten-IT, fehlende Protokollierung und uneinheitliche Sicherheitsrichtlinien zwischen lokalen Systemen und der Cloud hinzu.

### Wie ist die Lage bei Ihnen?

- Wird Ihr Netzwerk regelmäßig auf Schwachstellen geprüft und optimiert?
- Sind alle Zugänge und Schnittstellen Ihres Netzwerks gesichert und gemonitort?
- Kennt Ihre IT den lückenlosen Datenverkehr und die Kommunikationsflüsse innerhalb Ihres Netzwerks?
- Erneuern Sie regelmäßig Hardware, welche den Lebenszyklus überschritten hat?
- Gibt es ein aktuelles, dokumentiertes Netzwerkdesign – inklusive Sicherheitsarchitektur?
- Wissen Sie, wie schnell Ihr Unternehmen nach einem Ausfall oder Angriff wieder arbeitsfähig wäre?

# Workshop-Angebot - Analyse Ihrer Netzwerkinfrastruktur:

In diesem 2- tägigen Workshop analysieren wir Ihre bestehende Netzwerkinfrastruktur und bewerten sie hinsichtlich Sicherheit, Stabilität und Skalierbarkeit. Sie erhalten eine strukturierte Übersicht über bestehende Schwachstellen und Risiken – als Entscheidungsgrundlage für mögliche nächste Schritte.

**Workshop-Inhalte**

- Aufnahme und strukturierte Dokumentation Ihrer aktuellen Netzwerkarchitektur
- Bewertung von Sicherheitsaspekten wie:
  - Netzsegmentierung (z. B. VLANs)
  - Zugriffskontrollen
  - Monitoring und Alarmierungsmechanismen
- Identifikation von Schwachstellen, Engpässen und Risiken – inklusive möglicher Auswirkungen
- Berücksichtigung hybrider Infrastrukturen (On-Premises & Cloud)
- Abschlussbesprechung mit Präsentation der Ergebnisse und Handlungsempfehlungen

Ein zuverlässiges und zukunftssicheres Netzwerk schafft die Basis für Innovation, digitale Transformation und eine nachhaltig stärkere Wettbewerbsfähigkeit.

## Benefits

- Sicherheit:
  Schutz vor Angriffen, Ausfällen und Datenverlust
- Zukunftssicherheit:
  Skalierbares Design, ausgerichtet auch auf zu erwartendes Wachstum des Unternehmens
- Transparenz & Kontrolle:
  Detaillierte Übersicht über ihre Datenflüsse, Geräte und Sicherheitszustände
- Erfüllung gesetzlicher und branchenspezifischer Compliance-Anforderungen
  DSGVO, ISO 27001, etc. werden durch moderne Sicherheitsarchitekturen leichter erfüllt.
- Entlastung Ihrer IT:
  durch klar strukturiertes Design, Automatisierung und optionales Management durch externe Experten

## Ergänzende Dienstleistungen: Netzwerk-Renewal & -Redesign

Strukturiertes Netzwerk-Renewal:

- Austausch veralteter Hardware (Switches, Firewalls, Access Points)
- Software- & Firmware-Updates zur Schließung von Sicherheitslücken
- Optimierung der Topologie für bessere Performance und Ausfallsicherheit
- Integration moderner Sicherheitslösungen wie SD-WAN und Zero Trust
- Sanfte Migration mit minimalen Ausfallzeiten
- Einsatz energieeffizienter Komponenten (Green IT)

Netzwerkdesign-Überarbeitung:

- Neugestaltung der Sicherheitsarchitektur mit Segmentierung, Network Access Control, ZTNA
- Performance-Steigerung durch optimierte Datenflüsse und neue Hardware
- Zukunftssicheres Design für Cloud, IoT, Remote Work
- Hohe Skalierbarkeit und einfache Erweiterbarkeit
- Vollständige technische Dokumentation und Management-Transparenz

## Kontakt

Stephan Trastl, Adolf-Dembach-Str. 2, 47829 Krefeld
stephan.trastl@blue-consult.de, Telefon: +49 2151 6500 10

BLUE CONSULT.