

# CyberSafe! Ihr Wissensboost zu VPN & Fernzugriffe

Fernzugriffe auf Unternehmensdaten sind heute unverzichtbar, ob für Homeoffice, externe Dienstleister oder Partner. Doch mit der Flexibilität des Arbeitsortes steigen auch die Risiken für Ihr Business: Cyber-Angriffe, Datenverlust und Industriespionage können gravierende Folgen haben. Sorgen Sie dafür, dass Fernzugriffe auf Unternehmensdaten sicher und zuverlässig funktionieren – so minimieren Sie Risiken und stärken Ihre IT-Sicherheit im digitalen Alltag!

## Trainingsvideo: VPN & Fernzugriffe

Gemeinsam mit unserem IT-Krisendienstleister geben wir praxisnahe Einblicke, wie Fernzugriffe und VPN aufgesetzt sein müssen. Erhalten Sie im Expertenvideo konkrete Tipps, wie Sie mit gezielten Maßnahmen Risiken minimieren und Vertrauen bei Kunden und Partnern schaffen.

## Expertentipps zum Nachlesen

Lesen Sie hier die wichtigsten Take-Aways aus dem Expertenvideo:

- **Inventarisierung aller Systeme und Software:**  
Erfassen Sie sämtliche eingesetzte Software und Geräte – nur wer weiß, was im Einsatz ist, kann gezielt schützen.
- **Datenzugriff gezielt schützen:** Gewähren Sie ausschließlich so viele Zugriffsrechte, wie es für die jeweilige Tätigkeit erforderlich ist. Dadurch senken Sie das Risiko für unbefugte Zugriffe und minimieren die Angriffsfläche Ihres Unternehmens.
- **Passwort-Schutz optimieren:** Verlassen Sie sich nicht nur auf Passwörter, da diese häufig durch Phishing oder automatisierte Angriffe kompromittiert werden können. Nutzen Sie starke, einzigartige Passwörter und ergänzen Sie diese stets durch eine Mehrfaktor-Authentifizierung (MFA), um Ihr System besser zu schützen.
- **Mehrfaktor-Authentifizierung (MFA) verpflichtend nutzen:** Setzen Sie neben dem Passwort immer mindestens einen weiteren Authentifizierungsfaktor ein, z.B. eine Authenticator-App, ein Token oder ein Gerätezertifikat. Dadurch verhindern Sie, dass Angreifer mit gestohlenen Zugangsdaten ungehindert Zugriff auf Ihr System erhalten.
- **Zugriffsrechte klar regeln und Zugriffe segmentieren:**
  - Vergeben Sie Berechtigungen rollenbasiert: Bündeln Sie Zugriffsrechte nach Abteilungen oder Aufgabenbereichen und weisen Sie diese gezielt zu. So behalten Sie den Überblick und reduzieren Fehlerquellen.
  - Stellen Sie sicher, dass Zugriffe auf das Notwendige beschränkt sind und segmentieren Sie Nutzergruppen, um die Verwaltung zu erleichtern.
  - Koppeln Sie den Zugang technisch an autorisierte Geräte (z.B. durch Gerätezertifikate im VPN), damit nur berechtigte Endgeräte auf das Firmennetzwerk zugreifen können.



[Zum Expertenvideo](#)

## Wissensboost: VPN & Fernzugriffe

Fernzugriffe zählen zu den häufigsten Einfallstoren für Cyber-Kriminelle. Ein professionell eingerichtetes VPN und sichere Fernzugriffe sind daher essentiell für den Schutz Ihrer Unternehmensdaten und zentraler Baustein moderner IT Sicherheit.

### Was versteht man unter Fernzugriff und was ist ein VPN?

Unter Fernzugriff versteht man den Zugriff auf IT-Systeme, Netzwerke oder Daten eines Unternehmens von außerhalb des internen Firmennetzwerks – also über das Internet oder andere externe Netze. Ein VPN (Virtual Private Network) stellt eine verschlüsselte Verbindung zwischen externen Geräten und dem internen Firmennetz her.

### Warum stellen unsichere Fernzugriffe ein Risiko dar?

Unsichere Passwörter, fehlende Mehrfaktor Authentifizierung oder falsch konfigurierte Zugänge ermöglichen Angreifern oft den direkten Weg ins Unternehmensnetz. Ein kompromittierter VPN Zugang kann den Zugriff auf das gesamte Netzwerk ermöglichen. Häufige Folge: Ransomware Angriffe, Datendiebstahl, Betriebsunterbrechungen

## Checkliste: Das sollten Sie prüfen

|    |                                                                                                                                     |
|----|-------------------------------------------------------------------------------------------------------------------------------------|
| Ja | Sind Fernzugriffe klar geregelt und technisch abgesichert?                                                                          |
| Ja | Verwenden Sie für alle internetbasierten Zugänge mindestens zwei Faktoren und unterschiedliche Passwörter für verschiedene Dienste? |
| Ja | Nutzen Sie einen Passwort-Manager, um komplexe und individuelle Passwörter sicher zu verwalten?                                     |
| Ja | Prüfen Sie regelmäßig Ihre Fernzugriffslösungen: Sind MFA und Gerätezertifikate aktiv? Sind die Zugriffsrechte klar definiert?      |
| Ja | Vermeiden Sie direkte Portfreigaben ins Firmennetzwerk?                                                                             |
| Ja | Nutzen Sie bereits VPN-Lösungen mit sicherer Authentifizierung, um Ihr Unternehmen bestmöglich zu schützen?                         |

## Cyber-Versicherung: Allround-Schutz bei digitalen Risiken

Die genannten Tipps helfen dabei, die Cyber-Sicherheit zu stärken. Leider lässt sich aber auch mit umfassenden Schutzmaßnahmen ein Cyber-Angriff nicht vollständig ausschließen. Um im Ernstfall handlungsfähig zu bleiben, sollten Sie das Restrisiko zusätzlich absichern. Zum Beispiel mit einer Cyber-Versicherung von Hiscox. Als Experte für Cyber-Gefahren und Pionier am deutschen Versicherungsmarkt hält Hiscox Selbstständigen und Unternehmen den Rücken frei – vorbeugend, mitten in der Krise, bei der Schadenregulierung und bei der nachgelagerten Sicherheitsanalyse.

### Hiscox

Bernhard-Wicki-Straße 3, 80636 München

#### Für Makler

**T** +49 89 54 58 01 100

**E** [hiscox.info@hiscox.de](mailto:hiscox.info@hiscox.de)

**W** [makler.hiscox.de/cyber](https://makler.hiscox.de/cyber)

#### Für Endkunden

**T** +49 89 54 58 01 700

**E** [myhiscox@hiscox.de](mailto:myhiscox@hiscox.de)

**W** [hiscox.de/cyber](https://hiscox.de/cyber)

#### Hiscox in Social Media

