specialis IT
Für anspruchsvolle Dienstleister

# Schützen Sie Ihre IT:

**Jetzt beraten lassen!**

# Praktische Tipps für eine sichere IT-Infrastruktur

Überblick für Ihre IT-Sicherheit

IT OUTSOURCING
für anspruchsvolle Dienstleister

# Warum KMUs ein attraktives Ziel für Cyberangriffe sind....

Cyberkriminelle sehen KMUs oft als leichte Ziele, da diese Unternehmen häufig nicht über dieselben Ressourcen wie Großkonzerne verfügen. Schwachstellen wie veraltete Software, ungesicherte Netzwerke und mangelndes IT-Wissen machen KMUs zu einer bevorzugten Zielgruppe.

# Warum specialis IT Ihr Partner für IT-Sicherheit ist....

Bei specialis IT haben wir uns darauf spezialisiert, maßgeschneiderte Lösungen für kleine und mittelständische Unternehmen (KMUs) zu entwickeln, um deren IT-Sicherheit nachhaltig zu stärken. Cyberangriffe sind eine ständige Bedrohung – wir lassen ihnen keine Chance.

Unsere Mission ist es, Ihre IT nicht nur zuverlässig, sondern auch einfach und effizient zu gestalten. Mit unserem Know-how und unseren innovativen Ansätzen sorgen wir dafür, dass Ihre IT-Systeme sicher und optimal geschützt sind.

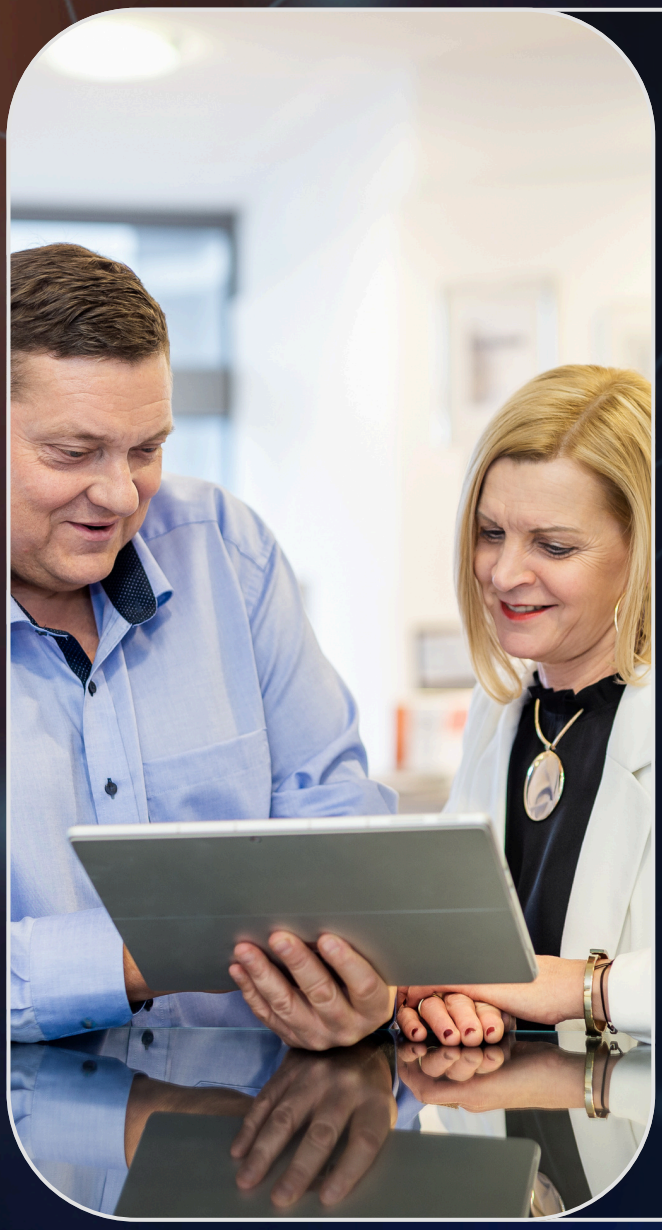
**Ing. Christian Dvorak, Geschäftsführung**

specialis IT
Für anspruchsvolle Dienstleister

# Cyberangriffe erkennen und abwehren...

Cyberangriffe frühzeitig zu erkennen, ist entscheidend. Achten Sie auf verdächtige Aktivitäten wie ungewöhnliche Login-Versuche, unerwartete Datenübertragungen oder plötzliche Systemverlangsamungen. Entwickeln Sie einen Notfallplan, um im Ernstfall schnell zu reagiere

## Was sind die ersten Anzeichen eines Gyberangriffes?



**Verdächtigte Login-Aktivitäten**

Unbekannte Login-Versuche oder Anmeldungen zu ungewöhnlichen Zeiten. Logins von geografischen Standorten, die nicht zu deinem Unternehmen passen.

**Unerwartete Systemverlangsamung**

Plötzliche Verlangsamung der Systeme, ohne offensichtliche Ursache.
Lange Ladezeiten bei Anwendungen oder Diensten.

**Unbekannte Pop-ups oder Warnmeldungen**

Plötzlich auftretende Pop-ups, die nach sensiblen Daten fragen.
Systemwarnungen oder Fehlermeldungen, die ungewöhnlich erscheinen.

**Unerklärliche Benutzerkonten**

Neue Benutzerkonten, die ohne Genehmigung erstellt wurden.
Änderungen an Berechtigungen.

specialis IT
Für anspruchsvolle Dienstleister

# Was sollen Sie tun wenn Anzeichen entdeckt werden?

- System sofort isolieren
- Daten sichern
- Analyse starten

## Systeme isolieren

- Trennen Sie betroffene Geräte und Server sofort physisch oder logisch vom Netzwerk, um eine Ausbreitung des Angriffs zu verhindern.
- Deaktivieren Sie externe Verbindungen, wie etwa zu Cloud-Diensten oder Remote-Desktops.

## Verdächtige Aktivitäten stoppen

- Sperren Sie auffällige Benutzerkonten, IP-Adressen oder Prozesse, die ungewöhnliches Verhalten zeigen.
- Schalten Sie betroffene Anwendungen oder Dienste vorübergehend ab.

## Sicherstellen von Beweismaterialien

- Erfassen und dokumentieren Sie alle relevanten Informationen, wie Log-Dateien, verdächtige Dateien und E-Mails.
- Stellen Sie sicher, dass die Beweise DSGVO-konform gesichert und verwendet werden.

## Daten sichern

- Erstellen Sie sofortige Backups aller wichtigen Systeme und Daten.
- Überprüfen Sie die Backups, um sicherzustellen, dass diese nicht infiziert sind.

specialis IT
Für anspruchsvolle Dienstleister

# Grundlagen der IT-Sicherheit...

Ein effektiver Schutz Ihrer IT-Infrastruktur beginnt mit der Umsetzung bewährter Sicherheitsmaßnahmen. Diese Grundlagen dienen als erste Verteidigungslinie gegen die meisten Cyberbedrohungen und sollten in jedem Unternehmen etabliert werden:

## Firewall - Die digitale Schutzmauer

Eine Firewall überwacht und kontrolliert den Datenverkehr zwischen Ihrem internen Netzwerk und externen Quellen, wie dem Internet. Sie blockiert unbefugte Zugriffe und kann so Angriffe frühzeitig abwehren

## Verschlüsselung - Schutz sensibler Daten

Verschlüsselung ist ein essenzieller Bestandteil jeder IT-Sicherheitsstrategie. Sie stellt sicher, dass Daten nur von autorisierten Personen gelesen werden können.

Warum wichtig?

- Verhindert den Missbrauch von gestohlenen Daten.
- Erfüllt gesetzliche Vorgaben, wie die DSGVO, zum Schutz personenbezogener Daten.

## Multi-Faktor-Authentifizierung (MFA) - Mehr Sicherheit bei Zugriffen

MFA erhöht die Sicherheit durch die Kombination mehrerer Authentifizierungsfaktoren. Selbst wenn ein Passwort kompromittiert wird, bleibt der Zugang geschützt.

Typische MFA-Faktoren:

- Wissen: Ein Passwort oder eine PIN.
- Besitz: Ein Smartphone oder ein Hardware-Token.
- Biometrie: Fingerabdruck oder Gesichtserkennung.

**Kontaktieren Sie uns gerne:**

# Produktlösungen für eine sicher IT-Infrastruktur

Die Umsetzung von Sicherheitsmaßnahmen wie Firewalls, Verschlüsselung und Multi-Faktor-Authentifizierung erfordert nicht nur strategisches Denken, sondern auch die richtigen Werkzeuge. Mit modernen IT-Sicherheitslösungen können Sie Ihre Infrastruktur effektiv schützen und Schwachstellen gezielt schließen.

## specialis Produkt Tipps:

**Mailtresor E-Mail Sicherheit**

Der Mail-Tresor archiviert E-Mails automatisch, schützt vor Datenverlust und erfüllt Aufbewahrungspflichten. Schnell, sicher und effizient.

**Virenschutz Manager**

Der Virenschutz-Manager bietet wartungsfreien Schutz vor Viren und Malware auf allen Endgeräten mit automatischen Updates. Zuverlässig, sicher und plattformübergreifend.

**Account Security: MFA**

Account Security bietet Zwei-Faktor-Schutz für sichere und einfache Zugriffe. Schnell, sicher, komfortabel. Unbefugter Zugriff wird effektiv verhindert, während sensible Daten zuverlässig geschützt bleiben.

**Passwortverwaltung**

Die Passwortverwaltung ermöglicht sichere, zentrale Steuerung und automatische Logins mit nur einem Master-Passwort. Effizient und sicher.

specialis IT
Für anspruchsvolle Dienstleister

Eine starke IT-Sicherheit ist heute unverzichtbar, um Unternehmen vor Cyberangriffen zu schützen.

Ergänzt durch professionelle IT-Dienstleistungen und eine kontinuierliche Überwachung, bleiben Sie den Bedrohungen einen Schritt voraus und schaffen eine solide Grundlage für die digitale Zukunft Ihres Unternehmens

# Wie sicher ist Ihre IT?
# Finden Sie es jetzt heraus:

## Kostenlose Analyse:

Unser IT-Performance Quick View hilft Ihnen potenzielle Schwachstellen zu identifizieren und das Cyberrisiko einzuschätzen.
Mehr Informationen finden Sie hier:
https://www.specialis.at/quickperformanceview

SCAN ME

## Kontaktieren Sie uns gerne:

Sie möchten weitere Informationen oder ein unverbindliches Beratungsgespräch?


+43 59 8052 000
vertrieb@specialis.at
www.specialis.at