

IT Security / Q&A

1. Wie sicher ist unsere IT gegen Cyberangriffe?

*Eine professionelle IT Risikoanalyse schafft Transparenz über den aktuellen Sicherheitsstatus Ihres Unternehmens. Dabei identifizierten wir **kritische Schwachstellen, Fehlkonfigurationen und Single Points of Failure**. Daraus entsteht eine priorisierte Roadmap mit konkreten Massnahmen zur Verbesserung Ihrer Cyber Security.*

2. Wie erkennen wir Schwachstellen in unserer IT-Infrastruktur?

*Ein kontinuierliches **Vulnerability Management** identifiziert Sicherheitslücken in Servern, Clients, Netzwerkkomponenten, Cloud-Services und Applikationen. Automatisierte **Vulnerability Scans, CVE-/CVSS-Bewertungen und Exposure Management** helfen dabei, Risiken frühzeitig zu erkennen und richtig zu priorisieren.*

*In Kombination mit konsequentem **Patch Management** und gezielten **Security Tests** lassen sich kritische Schwachstellen beheben, bevor sie von Angreifern ausgenutzt werden.*

3. Wie kann ich unsere Microsoft-365-Umgebung besser absichern und gleichzeitig einfacher verwalten?

*Eine sichere **Microsoft-365-Umgebung** basiert auf einem zentralen Identity-, Access- und Device-Management. Mit **Microsoft Entra ID, Conditional Access, Multi-Factor Authentication (MFA), Microsoft Intune und Endpoint Protection** können Benutzer, Geräte und Zugriffe zentral verwaltet und abgesichert werden.*

4. Wie setzen wir Zero Trust und Identity Security um?

*Bei einem **Zero-Trust-Ansatz** wird ein Zugriff nicht allein deshalb als vertrauenswürdig eingestuft, weil er aus dem Unternehmensnetzwerk erfolgt. Benutzer, Gerät, Standort, Anwendung und Risiko werden bei der Authentifizierung und Autorisierung berücksichtigt.*

5. Wie können wir neue Mitarbeitende automatisch onboarden und austretende Mitarbeitende sicher offboarden?

*Mit **Entra ID, Microsoft Intune, Windows Autopilot und rollenbasierten Berechtigungskonzepten (RBAC)** können zusätzlich Endgeräte automatisiert provisioniert und Security Policies angewendet werden. Beim Offboarding werden Zugriffsrechte kontrolliert entzogen und nicht mehr benötigte Accounts deaktiviert.*

6. Wie schützen wir unsere Backups gegen Ransomware?

*Ein sicheres Backup-Konzept schützt nicht nur vor Datenverlust, sondern stellt sicher, dass Backups bei einem Cyberangriff nicht mitverschlüsselt oder gelöscht werden können. Regelmässige **Restore-Tests und Disaster-Recovery-Tests** stellen sicher, dass Backups nicht nur vorhanden sind, sondern im Ernstfall tatsächlich funktionieren.*

7. Brauchen wir ein zusätzliches Backup für Microsoft 365?

*Ein unabhängiges **Microsoft 365 Backup / M365 Backup** kann zusätzlichen Schutz für **Exchange Online, SharePoint Online, OneDrive und Teams** sowie weiterer **Komponenten** bieten und die Wiederherstellung geschäftskritischer Daten unterstützen. Microsoft selbst sichert die Daten max. während 90 Tagen.*

8. Wie stellen wir sicher, dass unsere IT nach einem Cyberangriff oder Ransomware-Vorfall schnell wieder funktioniert?

*Ein funktionierendes **Business-Continuity- und Disaster-Recovery-Konzept** definiert bereits vor einem Security Incident, welche Systeme geschäftskritisch sind und in welcher Reihenfolge sie wiederhergestellt werden müssen.*

*Dazu gehören **Incident Response, Disaster Recovery, Backup & Recovery, Notfallzugänge, Eskalationsprozesse, Kommunikationswege** sowie definierte **RPO- und RTO-Ziele**. Regelmässige Recovery- und Notfalltests zeigen, ob die geplanten Prozesse unter realistischen Bedingungen funktionieren.*

9. Wie erkennen wir Cyberangriffe und verdächtige Aktivitäten frühzeitig?

*Firewalls und Endpoint Protection allein reichen für eine moderne **Cyber Security** nicht immer aus. Entscheidend ist, sicherheitsrelevante Ereignisse **aus Endpoints, Identitäten, Microsoft 365, Servern, Netzwerk und Cloud-Services** zentral zu überwachen und miteinander zu korrelieren. Technologien wie **EDR/XDR und SOC MDR** bieten Lösungen dazu.*