M365 Tenant Härtung

CAIRO

secure • digital • IT-infrastructures

Schwachstellen-Management für Microsoft 365 & lokales AD / Exchange

Microsoft 365 (Cloud) Lösungen basieren zentral auf dem M365 Tenant und der M365 Entra ID als zentrale Benutzerverwaltung. Häufig wurden während der Corona-Krise diese Cloud-Nutzung und Lösungen wie Exchange Online, MS Teams, OneDrive und SharePoint ad hoc in Unternehmen eingeführt, ohne detailliertes Verständnis der Microsoft Cloud und ohne Fokus auf Sicherheit. Daher sind viele Tenant-Konfigurationen noch nicht wirklich sicher und gehärtet - zumal auch Microsoft seine Strukturen häufig ändert.

Nachfolgend ein kurzer Überblick über die wichtigsten Sicherheitszonen und Konfigurationsbereiche - auch für ein lokales Active Directory.

Entra ID

MFA, Conditional Access, Privilegien/Delegationen, Aktivitäts-Logging der Aktivitäten, Applikation-bezogene Security Einstellungen

Active Directory (OnPrem)

Lokale Anbindung an Windows, lokale Anbindung an die Domän-Controler, Allgemeine Domänen-Einstellungen, Trusts, Domänen-fremde Accounts, Privilegien und Gruppen, Delegationen

Exchange/Mail (Online und OnPrem)

Protokolle wie SMTP/POP, Verschlüsselung, DKIM/DMARC Settings, Domänen-Settings, Malware Handling/Link Check, ATP, Auto-Forward Disable

Teams und Sharepoint

Berechtigungen, Externe Benutzer, File Handling und Sharing, Site Handling und Sharing, Zugang/Link Ablauf, Session Recording, Dokumenten Security mit Data Loss Policies (DLP) und Security Labels

OneDrive

Anyone Links verbieten, Berechtigungen, Zugang/Link Ablauf, nur Firmengeräte

Intune

Nur Firmengeräte, nicht häufig verbunden Geräte auslaufen lassen, PAW, MFA für Intune selbst, App Zugriff regeln, Auto-Löschen von Apps, Update und Patch Management, VPN-Tunnel , Compliance Policies und Richtlinien

Allgemeine Einstellungen

Telemetrie-Daten, Zugriff auf IP-Adressen, Datenstandort, Datenformate nach EU-Standard, BreakGlass Account

Unsere Leistungen

Wir identifizieren Ihre Schwachstellen und härten Ihren M365-Tenant kostengünstig mit Hilfe unserer Microsoft-Experten. Darüber hinaus betreuen wir diese Systeme auf Wunsch im laufenden Betrieb.

Zusätzlich zu den Härtungsmaßnahmen empfehlen wir die Durchführung des CAIRO CyberRisikoCheck (CRC) oder des CAIRO CyberSecurityCheck (CSC). Beide Checks werden gemäß den Vorgaben des BSI durchgeführt und können mit unserer automatischen Schwachstellenanalyse, dem CAIRO HackGuard Scan, gekoppelt werden.

Die M365 Härtungsmaßnahmen sind Teil unseres Security & Compliance Portfolios von normgerechten Security-Prüfungen, über das Schwachstellen-Management bis zum sicheren IT-Betrieb mit modernen Lösungen mit CAIRO Security Managed Service und Security Awareness Trainings.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

Tel.: +49 (0)621 86 75 10
Mail: info@cairo.ag
Web: www.cairo.ag

CAIRO
secure • digital • IT-infrastructures

Kontakt