IT für Unternehmen.
Lösungen für Menschen.

Securing Cloud Services

Integrierte Sicherheitsfunktionen richtig nutzen!

Manfred Pascher
Geschäftsführender Gesellschafter
ua Certified Data & IT Security Expert
www.mp2.at/manfred.pascher

Michael Bendl
MP2-Standortleiter Wien
ua Microsoft Azure Solutions Architect Expert
www.mp2.at/team/michael.bendl

MP2 IT-Solutions

IT-Unternehmen seit 1999 → Wien – Graz – NÖ/Zwettl

IT Services & Security | Software & App | Web & Shop | Digital Healthcare | Consulting & Training

- Kunden aus den untersch. Branchen & Größen
- technische & organisatorische Informationssicherheit
- ISO 27001 & ISO 9001 → Vorgaben & Abläufe
- zertifizierte Expert:innen im Bereich Cyber Security

Inhalt

- Zahlen & Fakten
- 10 empfohlene Security-Einstellungen
- Hybride Cloud-Architektur
- Redundanz, Datensicherung, Datenarchivierung

Aktuelles Thema

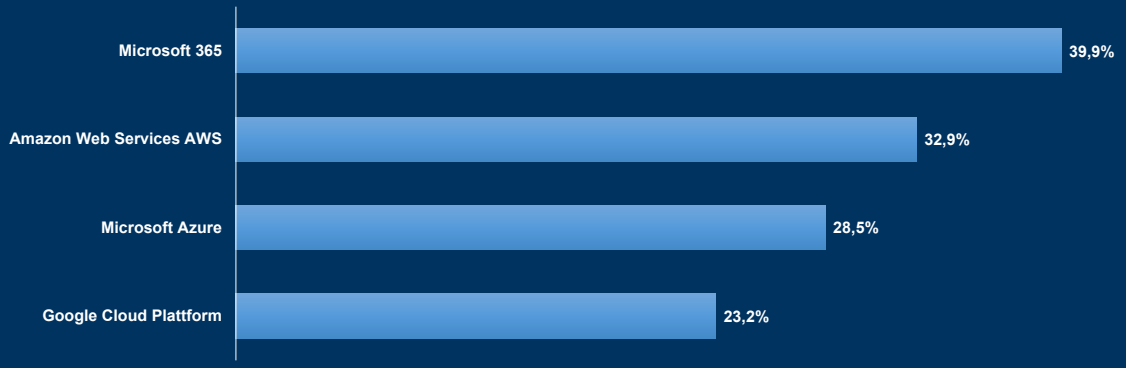

heise online › Microsoft Teams › Sicherheitslücke in Teams: Microsoft-Token im Klartext gespeichert

Sicherheitslücke in Teams: Microsoft-Token im Klartext gespeichert

Die Windows-, Linux- und macOS-Version von Teams speichert Token im Klartext, mit dem Angreifer die Microsoft-Dienste der Nutzer abgreifen können.

Quelle: Heise

Public Cloud Nutzung Jänner-März 2022



meistverwendete Cloud Services in Unternehmen, Quelle: Statista

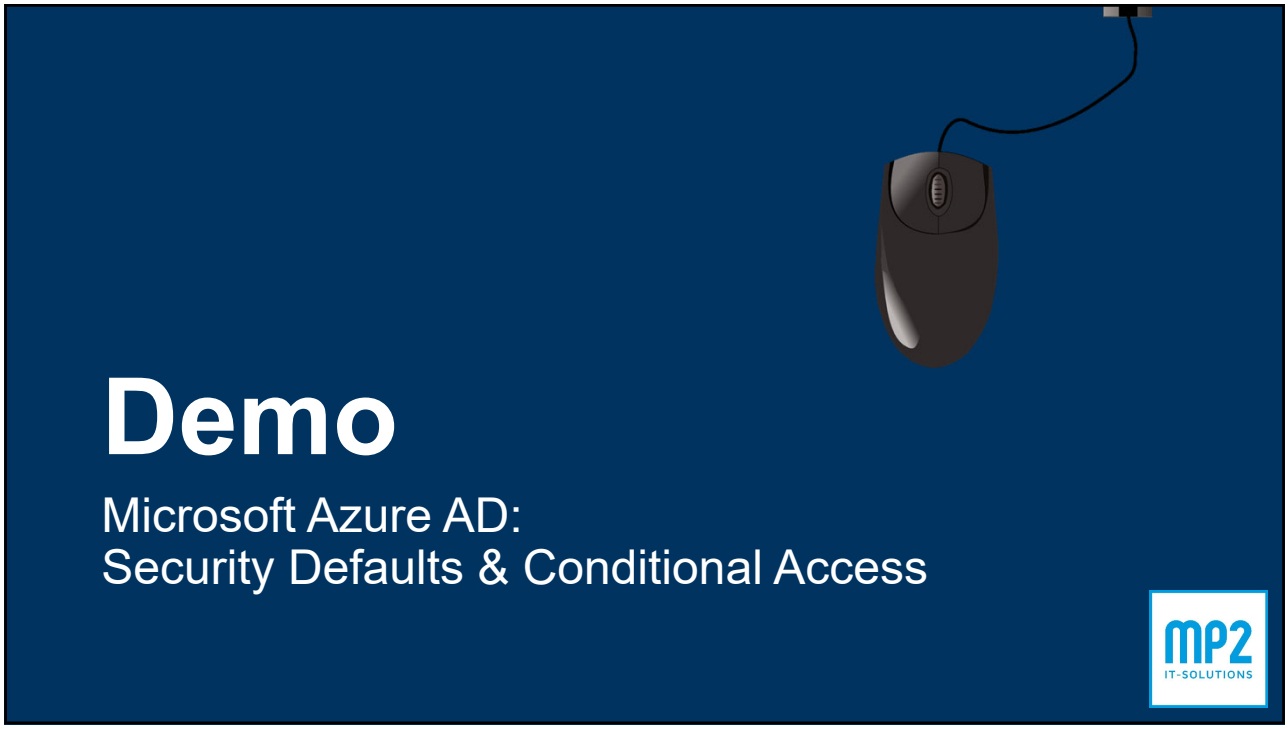
Security-Kennzahlen 2021

- 9,75 Mio. DDoS Attacken
- 25,6 Milliarden abgewehrte Brute-Force-Attacken auf Microsoft Azure
- 35,7 Milliarden gefilterte Phishing-Mails in Microsoft 365
- 58 Zero-Day-Exploits

Quellen: Netscout, Microsoft, Google

10 empfohlene Einstellungen I

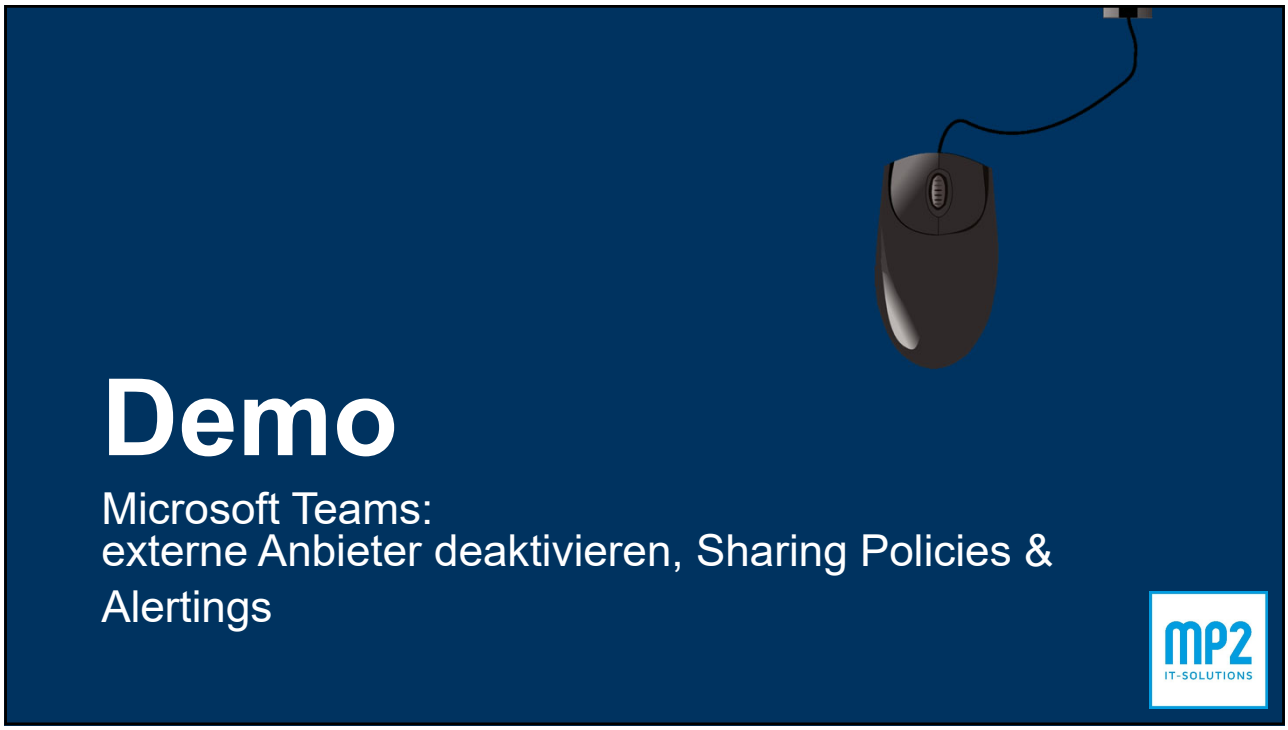
1. Multi-Faktor-Authentifizierung (MFA)
2. inaktive Benutzer automatisch abmelden
3. unsichere Protokolle deaktivieren



Demo

Microsoft Azure AD:
Security Defaults & Conditional Access


10 empfohlene Einstellungen II
10
4. Benutzerkennwörter sollen nicht ablaufen
5. Liste nicht erlaubter Kennwörter führen
6. Externe Freigaben gezielt planen
7. Applikationen von Drittanbietern beachten
TOP 10


Demo
Microsoft Teams:
externe Anbieter deaktivieren, Sharing Policies & Alertings
MP2
IT-SOLUTIONS

Externen Zugriffen absichern

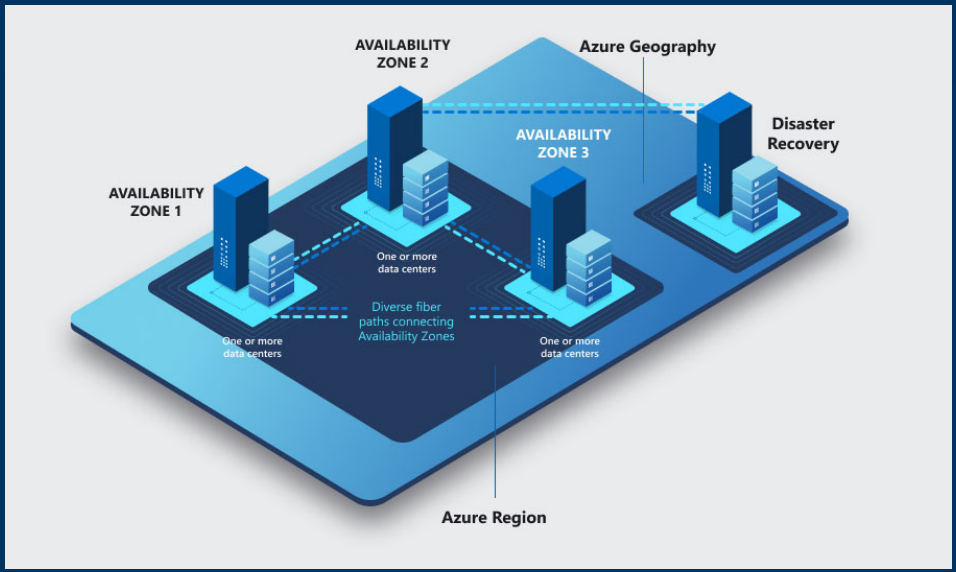
- Sharing Policies anpassen
  - Domain- & Group whitelist
- Data Loss Prevention Policies
- Gast-Zugriffe nutzen

Hybride Cloud-Architektur

- Nur notwendige Objekte synchronisieren / für die Kommunikation erlauben
- Netzwerktechnisch absichern
- Dedizierte Administratoren-Konten für Cloud- & onPremise AD
- Least-Privilege Administrative Model

Datensicherung & Redundanz

Archivierung, Alertings & Ausfallszenarien



https://learn.microsoft.com/en-us/azure/availability-zones/az-overview

Aufbewahrungszeiten

- Gelöschte Benutzer: 30 Tage
- OneDrive, Teams & SharePoint: 93 Tage
- Gelöschte Mailbox-Elemente: 14-30 Tage

Redundanz, Datensicherung, Archivierung

- Verfügbarkeit der Cloud-Dienste meist hoch - Redundanz
- Anders bei Datensicherung und Archivierung
- Oft kurze Aufbewahrungszeiten, kein Archiv-Backup
- Archivierungsmöglichkeiten der Dienste nutzen

Sicherheit Archive

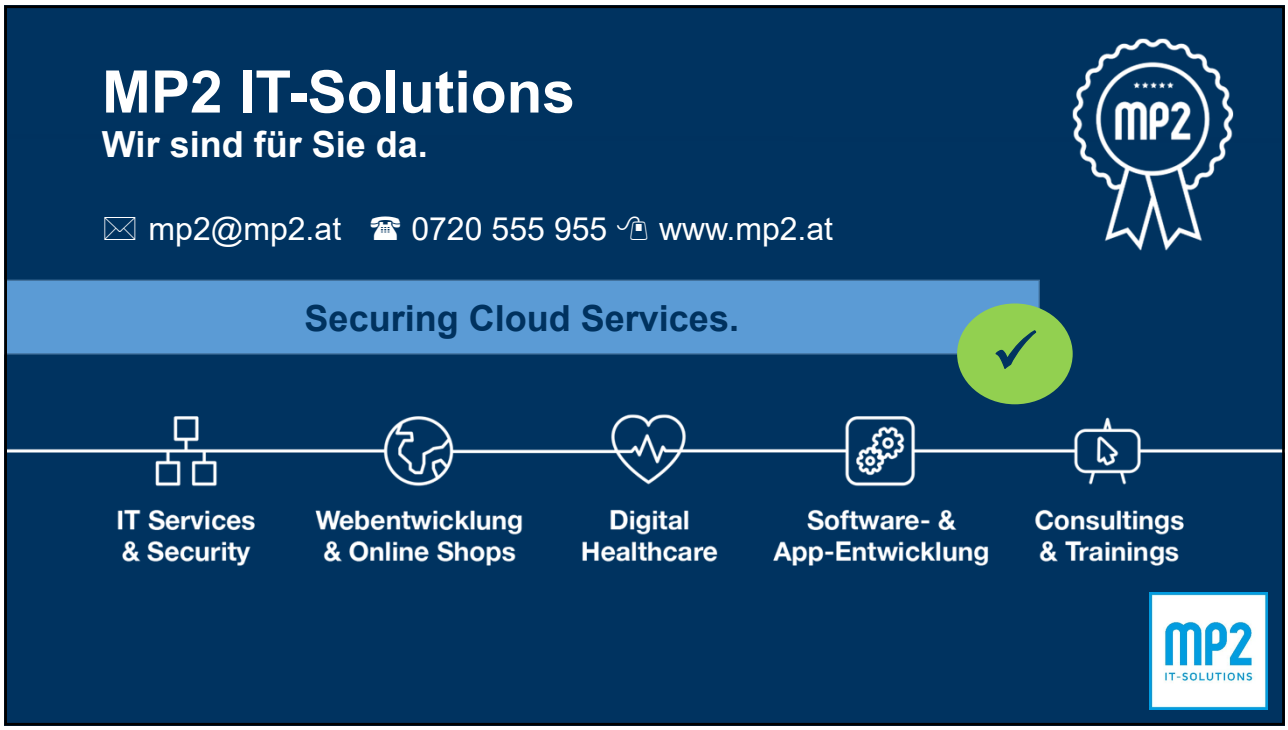
- Berechtigte Benutzer können meist sämtliche Daten löschen – auch Archive
- Änderungen an Archivdaten oft nicht überwacht oder nachvollziehbar
- Fehlende Archivdaten oder überschrittene Aufbewahrungszeiten oft spät bemerkt

Gegenmaßnahmen

- Datensicherung und Archivierung zu anderem Anbieter mit eigener Authentifizierung
- Sicherung lokal und Bandsicherung
- Gruppe administrativ Berechtigter, speziell „globale Administratoren“, sehr klein halten
- Überwachung für spezielle Operationen aktivieren

Zusammenfassung

- Zahlen & Fakten
- 10 empfohlene Security-Einstellungen
- Hybride Cloud-Architektur
- Redundanz, Datensicherung, Datenarchivierung


MP2 IT-Solutions
Wir sind für Sie da.
mp2@mp2.at
0720 555 955
www.mp2.at
Securing Cloud Services.
IT Services & Security
Webentwicklung & Online Shops
Digital Healthcare
Software- & App-Entwicklung
Consultings & Trainings
MP2 IT-SOLUTIONS