

# MICROSOFT 365 FEST IM GRIFF

Volker Steltenkamp

DIGITALE SICHERHEIT  
ANPACKEN

**#umsetzungstag**



# EINFÜHRUNG



# MICROSOFT 365 KURZ ZUSAMMENGEFASST

- Suite von cloudbasierten Produktivitäts- und Kollaborationstools
- Microsoft Office-Anwendungen (wie Word, Excel, PowerPoint)
- Services:
  - Exchange Online (E-Mail)
  - SharePoint Online (Dokumentenfreigabe und Zusammenarbeit)
  - Teams (Kommunikation und Zusammenarbeit)
  - Forms (Formulare einfach erstellen und auswerten)
  - Viva Suite (Plattform für Mitarbeitererfahrung, Lernen, Wohlbefinden etc.)
  - Power Plattform (Low-Code-/No-Code-Umgebung für das Erstellen von Workflows und Unternehmensapplikationen für Mitarbeitende ohne Programmierkenntnisse)

# DARUM SOLLTEN SIE SICH MIT DEM SICHEREN BETRIEB VON M365 BEFASSEN

- Schutz sensibler Informationen:  
Microsoft 365 enthält oft sensible Unternehmensdaten, wie Kundendaten, geistiges Eigentum, Finanzinformationen und interne Kommunikation.
- Datenschutz und Compliance:  
Erfüllen von rechtlichen Bestimmungen und Vorschriften in Bezug auf den Datenschutz und die Datensicherheit.
- Prävention von Cyberangriffen:  
Microsoft 365 ist ein attraktives Ziel für Cyberkriminelle, da es Zugriff auf sensible Daten bietet.
- Vermeidung von Datenverlust:  
Implementierung von Backups und Notfallwiederherstellungsplänen

# DARUM SOLLTEN SIE SICH MIT DEM SICHEREN BETRIEB VON M365 BEFASSEN

- Schutz vor Phishing- und Malware-Angriffen:  
Phishing-E-Mails und bösartige Anhänge sind häufige Methoden, um Schadsoftware in Systeme einzuschleusen.
- Gewährleistung der Verfügbarkeit und Leistung:  
Überwachung der Systemleistung, um sicherzustellen, dass die Dienste kontinuierlich verfügbar sind und reibungslos funktionieren.
- Default-Einstellungen sind möglicherweise unzureichend.

# WELCHE ROLLE SPIELT DIE AZURE ACTIVE DIRECTORY (AAD)?

- Bereitstellung von Identitäts- und Zugriffsmanagementfunktionen
- zentralisierte Plattform für das Identitäts- und Zugriffsmanagement für
  - cloudbasierte Dienste wie Microsoft 365
  - lokale Dienste und Anwendungen
- Azure AD ist das Identitätsverwaltungssystem, das Microsoft 365 zur Authentifizierung und Autorisierung von Benutzerinnen und Benutzern verwendet.
- Bereitstellung einer Single Sign-On-Funktionalität (SSO) für Microsoft 365
  - Zugriff auf verschiedene Microsoft-365-Anwendungen und -Dienste, ohne sich mehrfach authentifizieren zu müssen.










Nahezu alle sicherheitsrelevanten Einstellungen müssen daher im Azure AD vorgenommen werden. Viele dieser Einstellungen können aber auch über das M365 Admin Center erreicht werden.

# MASSNAHMEN UND GEEIGNETE TOOLS DES M365/AAD BAUKASTENS



# IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

Das sicherste Passwort ist gar kein Passwort!

<b>Bad:</b> Password	<b>Good:</b> Password and...	<b>Better:</b> Password and...	<b>Best:</b> Passwordless
123456 qwerty password iloveyou Password1	 SMS   Voice	 Authenticator (Push Notifications)   Software Tokens OTP   Hardware Tokens OTP (Preview)	 Authenticator (Phone Sign-in)   Window Hello   FIDO2 security key   Certificates



# IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

## Privileged Identity Management

- Prinzip der geringstmöglichen Berechtigungen
- Idee: Nur die Rechte holen, die für die aktuelle Aufgabe benötigt werden.
- Just-in-Time Aktivierung von Azure AD Rollen
- Möglichkeiten der Kontrolle und Überwachung

The screenshot shows the Microsoft Azure portal interface for Privileged Identity Management. The main navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'admin\_volker@volkerst... VOLKERS DEMO TENANT (VOLKE...)'.

The breadcrumb trail is: Home > Privileged Identity Management | Meine Rollen > Meine Rollen | Azure AD-Rollen. The 'Meine Rollen | Azure AD-Rollen' section is highlighted in yellow.

On the left sidebar, the 'Aktivieren' section is active, with 'Azure AD-Rollen' selected. Other options include 'Gruppen (Vorschau)', 'Azure-Ressourcen', 'Problembehandlung + Support', 'Problembehandlung', and 'Neue Supportanfrage'.

The main content area shows the 'Aktivieren' page for the role 'Administrator für Angriffssimulation'. The role is listed in a table with columns 'Rolle', 'Bereich', and 'Mitgliedschaft'. The role name is highlighted in yellow.

Rolle	Bereich	Mitgliedschaft
Administrator für Angriffssimulation	Verzeichnis	Direkt

Below the table, there are tabs for 'Berechtigte Zuweisungen', 'Aktive Zuweisungen', and 'Abgelaufene Zuweisungen'. A search bar 'Nach Rolle suchen' is present.

The right-hand panel shows the 'Aktivieren' configuration for the selected role. It includes a 'Startzeit der benutzerdefinierten Aktivierung' checkbox, a 'Dauer (Stunden)' slider set to 8, and a 'Begründung (max. 500 Zeichen) \*' text area, which is highlighted in yellow.

# IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

## Bedingter Zugriff / Conditional Access

- Alle verfügbaren Datenpunkte werden in die Authentifizierung und Autorisierung einbezogen – Identität, Standort, Geräteintegrität, Datenklassifizierung, Anomalien, Dienst oder Workload.
- Möglichkeiten der Kontrolle und Überwachung

# IDENTIFIZIERUNG VON SICHERHEITSANFORDERUNGEN

- Kategorisieren von Informationen hinsichtlich des Schutzbedarfs:
  - E-Mails
  - Teams in MS Teams
  - Sharepoint Online Sites
  - Office- und PDF-Dokumente
- Nutzung von „Sensitivity Labels“ zur Datenklassifizierung
- Darauf basierend können Richtlinien zur Data Loss Prevention (DLP) erstellt werden.

# DATENBACKUP UND WIEDERHERSTELLUNG

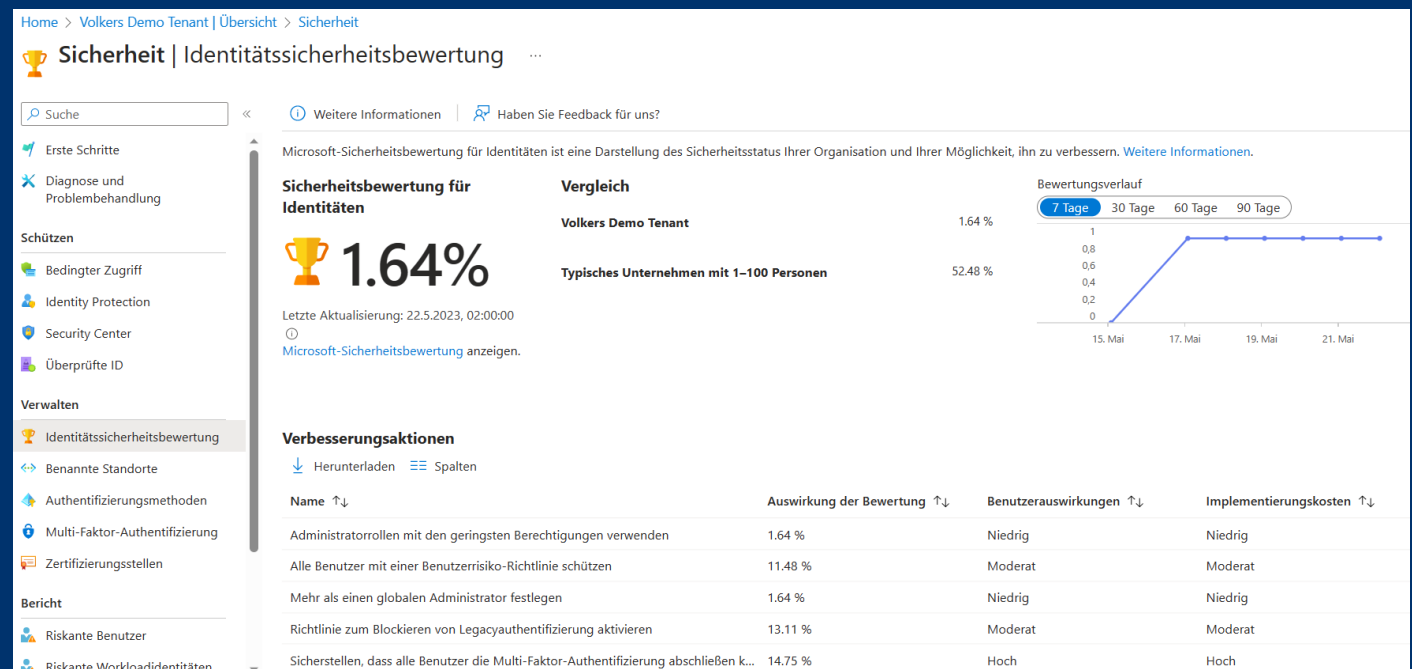
- Etablierung eines Cloud-Datensicherungsplans
  - Auswahl eines geeigneten Software-Anbieters
  - Nutzung von Backup-Szenarien in Azure
  - Verschlüsselung der Backups
  - Aufbewahrung an sicherem Ort
- Mindestens genauso wichtig ist die regelmäßige Überprüfung der Wiederherstellung.
- Kein Backup? Kein Mitleid!

# IDENTITÄTS- SICHERHEITS- BEWERTUNG – DER MS SECURE SCORE



# IDENTITÄTSSICHERHEITSBEWERTUNG

- Bewertung und Verbesserung der Sicherheit ihrer Microsoft-365-Umgebung
- bietet konkrete Empfehlungen und Maßnahmen
- Priorisierung der erforderlichen Maßnahmen
- Vergleich zu anderen Unternehmen Ihrer Größe



**FAZIT**



# FAZIT

Microsoft bietet eine Vielzahl von Möglichkeiten, die Sicherheit und Compliance Ihres Tenants zu erhöhen. Nutzen Sie die bereits vorhandenen Tools und Methoden. Viele davon haben Sie bereits bezahlt!

- Planen Sie Ihre eigene Microsoft Cloud Security Road Map:  
Der MS Secure Score unterstützt Sie dabei.
- Führen Sie eine Risikobewertung aller Ihrer Informationen durch:
  - Was sind die „Kronjuwelen“ des Unternehmens?
  - Sind bereits hochriskante Daten in der Cloud?



# Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

Die Grundlagen der Digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer Digitalen Daten und Wertgegenstände.

Besuchen Sie unsere Website: [www.digital-sicher.nrw](http://www.digital-sicher.nrw)

## Adresse

**Standort Bochum**  
Lise-Meitner-Allee 4  
44801 Bochum

**Standort Bonn**  
Rheinwerkallee 6  
53227 Bonn

## Kontakt

 +49 234 - 5200 7334

 [info@digital-sicher.nrw](mailto:info@digital-sicher.nrw)

## Social Media



**DIGITAL  
SICHER  
NRW**