

# CONDITIONAL ACCESS

Sicherung des Cloud- und Device Zugriffs, um an **jedem Ort** und zu **jeder Zeit** produktiv sein zu können. Bedingter Zugriff mithilfe von Richtlinien über Conditional Access.

- Die **Sicherheit der Login Kombination** aus z.B. E-Mail und Passwort alleine ist gefährlich und veraltet. Durch Phishing Angriffe wird diese Kombination oft gestohlen. Durch den Einsatz einer **Multifaktor-Authentifizierung** werden weitere Parameter wie Standort und Endgerät in einer KI-basierten Risikoerkennung ausgewertet und weitere Identifikationsfaktoren bei Bedarf zum Login abgefragt.
- Das Paket basiert auf Conditional Access AD Richtlinien im Gegensatz zu alternativen Intune Richtlinien.

## Konfiguration

von Conditional Access Best Practice Richtlinien und Rollout

## Implementierung

eines Conditional Access Monitoring Dashboards und des Azure AD Hybrid Join

## Übergabe

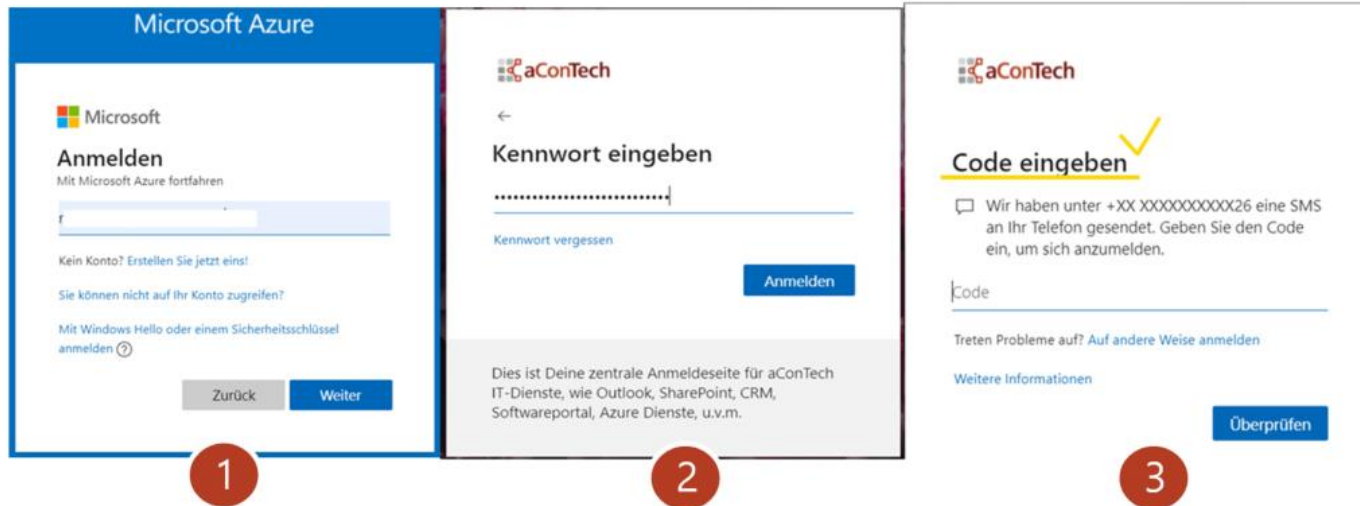
sowie Dokumentation



# CONDITIONAL ACCESS

## Praxisbeispiel

Multifaktor-Authentifizierung (MFA) über Conditional Access:



The image shows three sequential screenshots of the authentication process:

- 1. Microsoft Azure Login:** A Microsoft Azure login page with the title "Anmelden" and a "Weiter" button.
- 2. aConTech Password Entry:** A page titled "Kennwort eingeben" with a password input field and an "Anmelden" button.
- 3. aConTech MFA Code Entry:** A page titled "Code eingeben" with a checkbox for SMS verification, a code input field, and an "Überprüfen" button.

ZULASSUNG ODER BLOCKIERUNG DES ZUGRIFFS VON M365-APPS  
AUF WINDOWS, MAC-OS, IOS- UND ANDROID-GERÄTEN  
MIT EXTRA PASSWORT ODER BIOMETRIE  
ZUM SCHUTZ SENSIBLER UNTERNEHMENSINFORMATIONEN.

