SCALTEL

ZERO TRUST

Access Management

ZERO TRUST

Was bedeutet Zero Trust im Access Management?

Zero Trust gewährleistet, dass berechtigte Nutzer nur über korrekte Kanäle auf angemessene Daten zugreifen können – unter Einbeziehung des passenden Devices, Netzwerks und der Applikationen.

Die Identität steht im Mittelpunkt, da sie den Ausgangspunkt der Sicherheitskette bildet. Im Zero Trust-Modell erfolgt die Identifizierung ausschließlich durch Computer, wobei herkömmliche Benutzername-Kennwort-Kombinationen durch zusätzliche Faktoren wie Chipkarten, Tokens und biometrische Daten ersetzt werden.

Digitale Identitäten können Attribute wie Benutzername und Passwort, Chipkarten, Tokens oder biometrische Daten umfassen. Diese Entwicklung ist essenziell, da herkömmliche Passwörter nicht mehr ausreichen und durch Multi-Faktor-Authentifizierung (MFA) ergänzt werden müssen. Die Verifizierung digitaler Identitäten wird zu einem zentralen Aspekt im Zero Trust-Ansatz, der den Gap in der Identitätsprüfung schließt und die Sicherheit durch zuverlässige Authentifizierung stärkt.

MASSNAHMEN

Die wichtigsten Zero-Trust-Maßnahmen

Multifaktor-Authentifizierung für Mitarbeiter:

- Push-OTP

Privileged Access Management für Cloud-Infrastrukturen:

- Schutz privilegierter Zugriffe auf Cloud-Ressourcen.
- Verbesserung der Sicherheit durch kontrollierte Berechtigungen.

Sicherer Zugriff auf APIs:

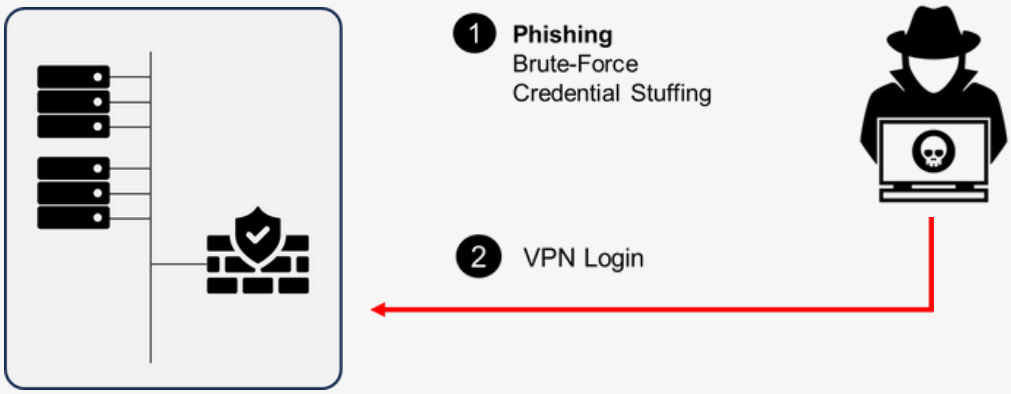
- Gewährleistung sicherer Verbindungen zu Anwendungsprogrammierschnittstellen.
- Schlüsselmaßnahme für den Schutz von Daten und Systemen.

In diesem Kontext sollte das Identitätsmanagement fest in den Verantwortungsbereich der Sicherheitsteams eingebunden werden, um eine proaktive und ganzheitliche Herangehensweise zu gewährleisten.

Der Schutz vor Phishing, als eines der populärsten Angriffsszenarien, erfordert daher nicht nur technologische Abwehrmechanismen, sondern auch eine kontinuierliche Schulung und Sensibilisierung der Nutzer, um die menschliche Komponente in der Sicherheitsstrategie zu stärken.

ANGRIFFSSZENARIEN

Phishing bleibt trotz Multi-Faktor-Authentifizierung eine ernste Bedrohung. Obwohl sich MFA weiterentwickelt, sind Kundenumgebungen oft unzureichend geschützt, und Phishing-Angriffe sind weiterhin häufige Ursachen für den Verlust von Kennwörtern. Unternehmen sollten neben fortschrittlichen MFA-Methoden gezielte Maßnahmen ergreifen, um Phishing-Risiken zu minimieren.



Unerlaubte Zugriffe beim VPN-Login sind ernstzunehmende Bedrohungen durch Phishing, Brute-Force oder Credential Stuffing. Diese können zu vollem Netzwerkzugriff führen, was Sensibilisierung für umfassende Identitätsverwaltung und starke Authentifizierungsmechanismen erfordert, um effektiv vorzubeugen.

Brute-Force

Brute-Force ist eine Methode, bei der ein Angreifer systematisch verschiedene Benutzerkennwortkombinationen ausprobiert, um Zugang zu einem System oder Konto zu erhalten.

Durch die schiere Rechenkraft von Computern werden alle möglichen Kombinationen durchprobiert. Systeme verwenden Maßnahmen wie Sperrzeiten und Captchas, um den Erfolg zu minimieren.

Starke Passwörter und Multi-Faktor-Authentifizierung sind entscheidend zur Verteidigung gegen Brute-Force-Angriffe.

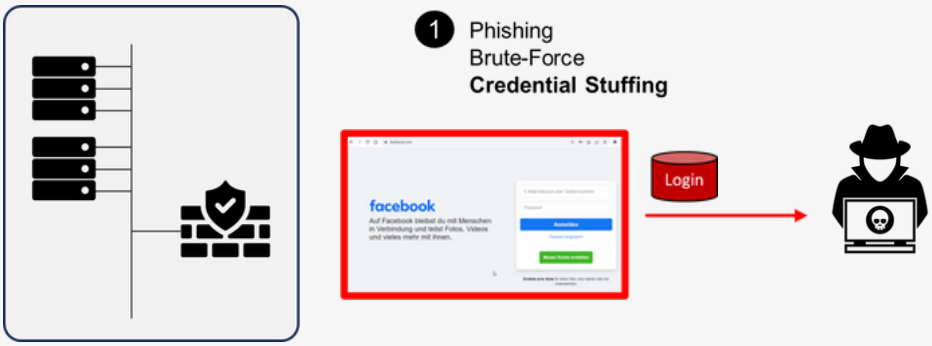
ANGRIFFSSZENARIEN

Credential Stuffing

Credential Stuffing ist eine Angriffsmethode, bei der gestohlene Benutzername-Passwort-Kombinationen aus früheren Datenlecks wiederverwendet werden.

Die kompromittierten Zugangsdaten werden im Darknet oder auf anderen Plattformen verkauft, und Angreifer versuchen, sich mit diesen Informationen in anderen Online-Diensten anzumelden. Dieser Ansatz ist besonders gefährlich, da viele Menschen dieselben Passwörter für mehrere Konten verwenden.

Unternehmen können sich gegen Credential Stuffing schützen, indem sie starke Passwörter, Multi-Faktor-Authentifizierung und regelmäßige Überprüfungen auf verdächtige Aktivitäten fördern.



Angriffe auf SaaS

Angriffe auf SaaS-Applikationen wie Microsoft 365 stellen eine ernsthafte Bedrohung dar. Häufig erfolgt der Zugang zu einem Konto ohne Multi-Faktor-Authentifizierung (MFA).

Opfer erhalten betrügerische Zahlungsaufforderungen nach einem erfolgreichen Hack, was zu Dilemmas führt. Die Nutzung von MFA bietet eine zusätzliche Sicherheitsebene.

Da Microsoft 365 oft Ziel von Angriffen ist, betont dies die Notwendigkeit von MFA und proaktiven Sicherheitsmaßnahmen, um Datenlecks zu verhindern oder frühzeitig zu erkennen.

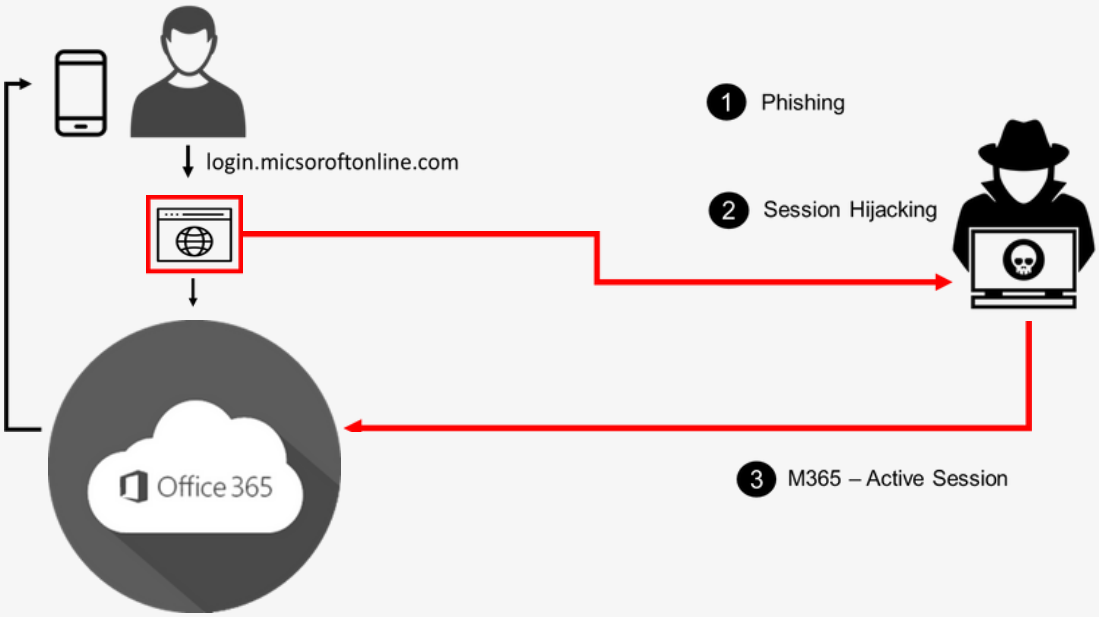
ANGRIFFSSZENARIEN

Session Hijacking

Einige Kunden setzen bereits auf Multi-Faktor-Authentifizierung (MFA) für SaaS-Applikationen.

Jedoch haben verstärkte Sicherheitsmaßnahmen auch neue Angriffsmethoden wie Session Hijacking hervorgebracht. Dabei lenkt ein Angreifer einen Mitarbeiter über einen Reverse Proxy auf externe Ressourcen, um Standard MFA-Mechanismen zu umgehen. Mitarbeiter könnten so unwissentlich einem Angreifer vollen Zugriff gewähren.

Dies betont die Bedeutung der Sensibilisierung von Mitarbeitern für mögliche Angriffsszenarien und die Überprüfung verdächtiger Links oder Anfragen, zusätzlich zur MFA-Implementierung.



GEGENMASSNAHMEN

Um die genannten Angriffsszenarien zu verhindern, sind verschiedene Gegenmaßnahmen erforderlich:

Brute-Force

Anwender muss starke Kennwörter wählen

Phishing

Anwender muss wissen welche Links er klicken darf und welche nicht

Credential Stuffing

Anwender muss für unterschiedliche Dienste unterschiedliche Kennwörter wählen

Multi-Faktor-Authentifizierung (MFA) ist eine wirksame Schutzmaßnahme gegen Brute-Force- und Phishing-Angriffe.
Die Nutzung von zweiten Faktoren wie Push-OTP oder Hardware-Token erhöht die Sicherheit, erfordert jedoch bewusste Benutzerinteraktion und Schulungen.

Für den Schutz vor Session Hijacking kommen moderne Methoden wie Webauthn zum Einsatz, die zusätzliche Faktoren wie Fingerabdruck und Gesichtserkennung nutzen.

Gegen Credential Stuffing ist Single Sign On (SSO) bedeutend. Ein zentraler Identity Provider ermöglicht sichere Anmeldungen, komplexe Zugriffsdaten und MFA, minimiert das Risiko von Credential Stuffing und steigert die Benutzerfreundlichkeit.

Brute-Force / Phishing

Zweiter Faktor

Push-OTP

Hardware Token

Session Hijacking

MFA (Phishing resistent)

FIDO 2
(Webauthn)

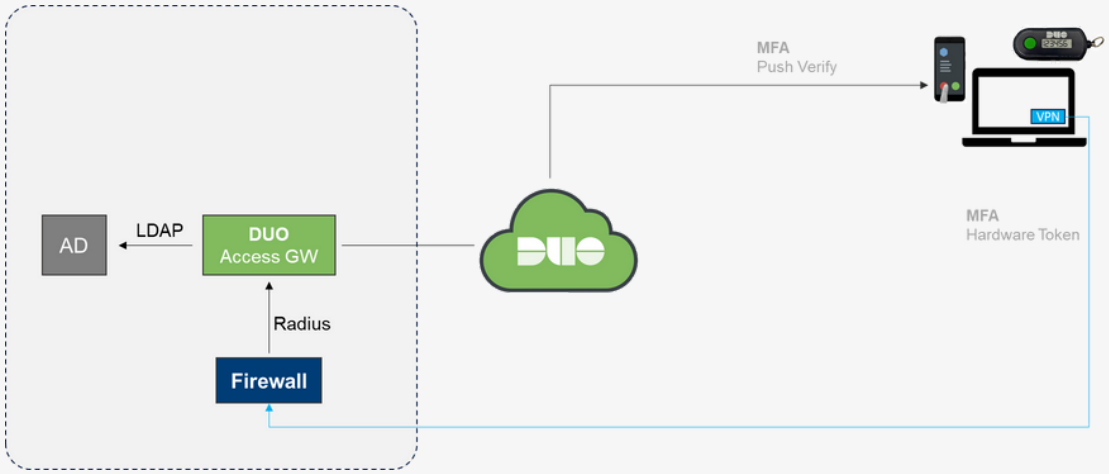
Credential Stuffing

SSO – Möglichst wenige Applikationen, die jeweils lokale Accounts benötigen

ARTEN VON MFA

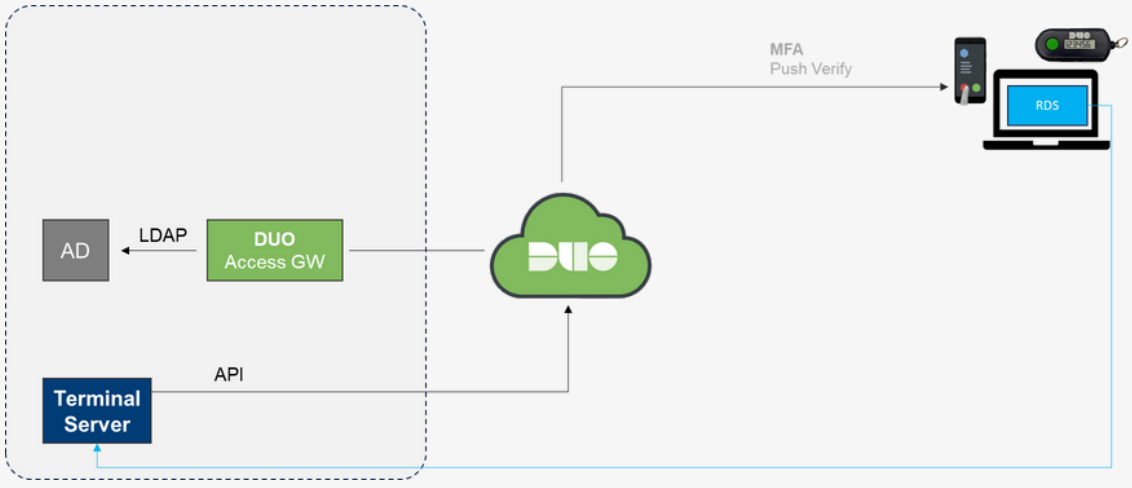
MFA per Radius

Die Integration von Multi-Faktor-Authentifizierung (MFA) über Radius ist entscheidend für den Schutz von VPN-Zugriffen. Bei herkömmlichen VPN-Zugriffen erfolgt die Übermittlung einer Benutzername-Kennwort-Kombination mit möglicher LDAP-Anbindung für die Zugriffsbestätigung. Cisco Duo, Teil unseres Portfolios, bietet eine effiziente MFA-Lösung über Radius mit Standards wie Push OTP, Token oder Zertifikat. Unternehmen ohne diese MFA-Technologien laufen Gefahr, den aktuellen Sicherheitsstandard zu verpassen.



MFA per Agent/APII

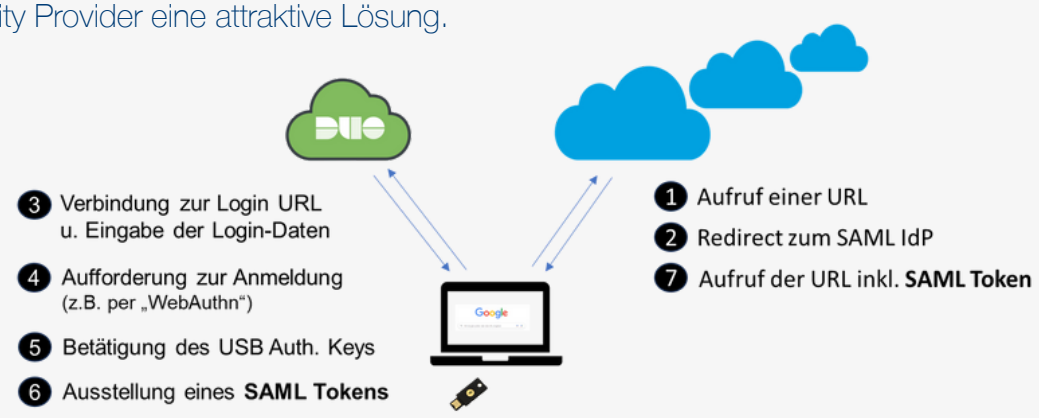
MFA über Agents oder APIs schafft wirksame Sicherheitsschichten in bestimmten Anwendungs- und Systemumgebungen. Durch Installation auf Geräten wie Windows Servern wird MFA nach herkömmlicher Anmeldung aktiviert. In Szenarien wie Remote Desktop Services triggert der Server-Agent die MFA-Bestätigung sofort nach der Anmeldung, und weitere Aktionen sind erst nach Bestätigung möglich. Obwohl wenig genutzt, bietet diese Methode starken Schutz in administrativen Umgebungen durch einen zusätzlichen Sicherheitsschritt.



ARTEN VON MFA

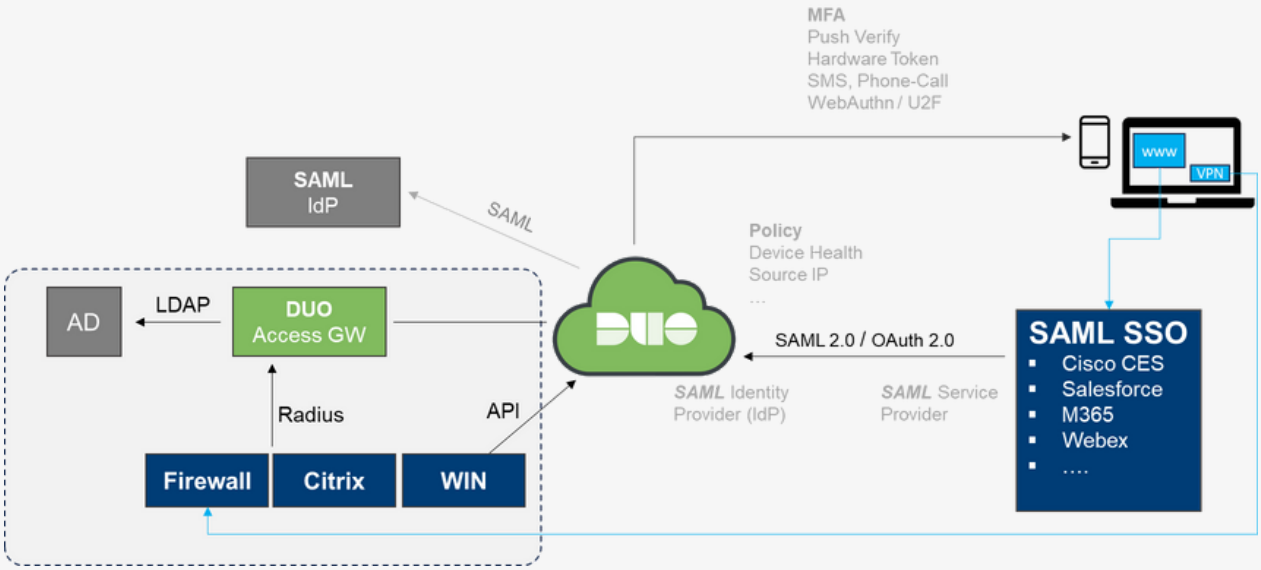
SSO mit Webapplikationen

Single Sign-On (SSO) mit Webanwendungen vereinfacht den Zugang zu verschiedenen Diensten erheblich.
Bei der Authentifizierung durch einen Identity Provider für SaaS-Dienste wie Salesforce wird nach erfolgreicher Identitätsprüfung ein SAML-Token erstellt. Dieses Token ermöglicht den Zugriff auf verschiedene SaaS-Anbieter. SSO verbessert die Usability durch eine einmalige Anmeldung für verschiedene Anwendungen. Für Administratoren erleichtert es die Zugangssperre von Mitarbeitern mit einer einzigen Maßnahme, statt jede SaaS-Anwendung separat zu verwalten.
Trotz Risiken bietet die einfache Steigerung von Usability und Sicherheit über einen zentralen Identity Provider eine attraktive Lösung.



Access Management mit Cisco DUO

Cisco Duo verschiedene Webanwendungen über SSO an und ermöglicht Administratoren die zentrale Verwaltung und Sperrung von Zugriffen. Das Duo Access Gateway bietet eine Lösung für Legacy VPN-Zugänge, während die zentrale Erfassung von Logindaten Anomalieerkennung und Alarmgenerierung ermöglicht. Der Einsatz von Cisco Duo bietet insgesamt eine effiziente Kontrolle über Identitäts- und Authentifizierungsmechanismen.



UNSER WEG ZU ZERO TRUST

Zusammenfassend - Access Management

Welche Maßnahmen gibt es für die verschiedenen Angriffsszenarien?

Kennen Sie die unterschiedlichen Angriffsszenarien?

Haben Sie passenden Gegenmaßnahmen getroffen?

Haben Sie MFA implementiert?

Kennen Sie die verschiedenen MFA Arten?

Welches MFA passt zu Ihnen und schützt Sie am effizientesten?

Gerne begleiten wir sie auf Ihrem Weg zu Zero Trst