BUSINESS BREAKFAST ONLINE

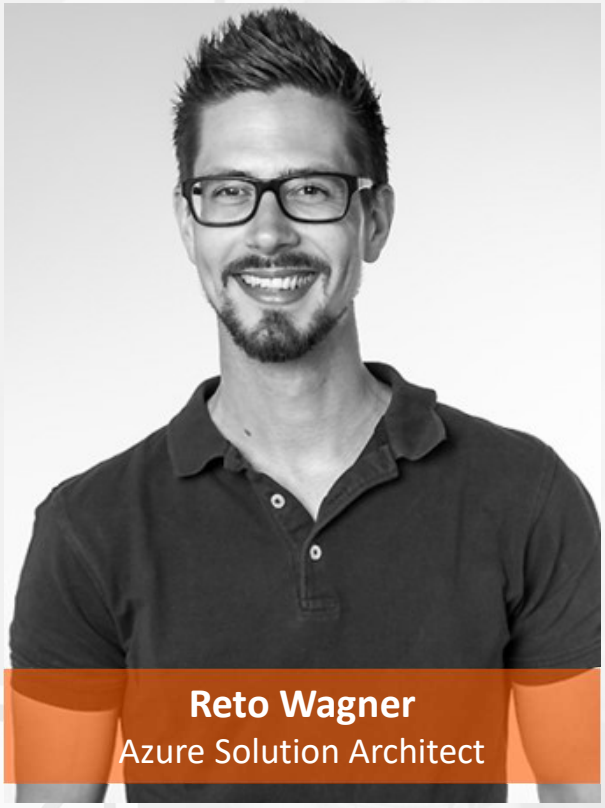
MULTI-FAKTOR-AUTHENTIFIZIERUNG MIT MICROSOFT AZURE

first frame networkers

IT, die Sie weiterbringt

NETWORKERS

first frame networkers
IT, die Sie weiterbringt



Reto Wagner
Azure Solution Architect

Timo Conradi
Accountmanager

AGENDA

first frame networkers
IT, die Sie weiterbringt

- Begrüssung
- Facts & Figures first frame networkers ag
- Kurzübersicht Microsoft Azure
- Multi-Faktor-Authentifizierung (MFA) mit Azure MFA
- Fragen

FIRST FRAME NETWORKERS AG

first frame networkers
IT, die Sie weiterbringt

- Inhabergeführte AG (seit 1997)
- Hauptsitz im Kanton Zug
- 74 Mitarbeitende (davon 10 Lernende)
- ISO 27001 & 9001 zertifiziert
- Über 400 Kunden (von klein bis gross, industrieneutral)
- Breites Portfolio im IT-Infrastrukturbereich
- Eigene Rechenzentren (first365) in Zürich & Bern

Microsoft Partner
Microsoft

- Silver Cloud Platform
- Silver Communications
- Silver Messaging
- Silver Application Development

Microsoft Partner
Microsoft

- Gold Datacenter
- Gold Cloud Productivity
- Gold Collaboration and Content
- Gold Small and Midmarket Cloud Solutions
- Gold Windows and Devices

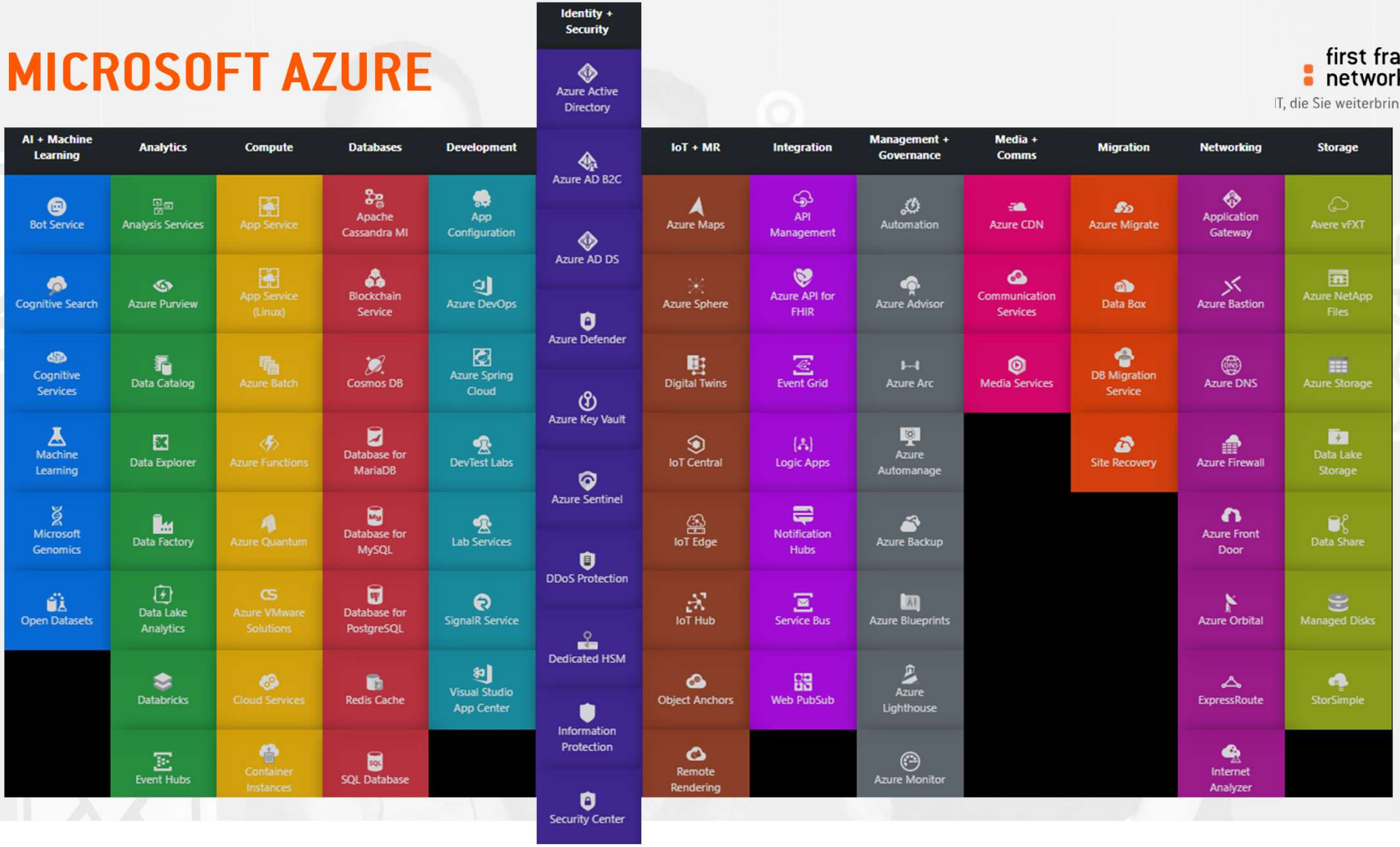
“Security is our top priority, and we are committed to working with others across the industry to protect our customers.”

Satya Nadella
Chief Executive Officer, Microsoft Corporation

«Sicherheit hat für uns oberste Priorität, und wir sind bestrebt, mit anderen in der Branche zusammenzuarbeiten, um unsere Kunden zu schützen.»

MICROSOFT AZURE

first frame networkers
IT, die Sie weiterbringt



08.06.2021


SICHERN SIE IHRE GERÄTE
SICHERN SIE IHRE APPS
SICHERN SIE IHRE DATEN
SICHERN SIE IHRE IDENTITÄTEN

SICHERN SIE DIE EINGANGSTÜR

first frame networkers
IT, die Sie weiterbringt

Werkzeuge:

- Risikobasierte Zugangskontrolle und Multi-Faktor-Authentifizierung
- Erweiterte Sicherheitsberichte
- Identifizieren von Bedrohungen vor Ort
- Identifizieren Sie die risikoreiche Nutzung von Cloud-Apps und verhindern Sie Bedrohungen.

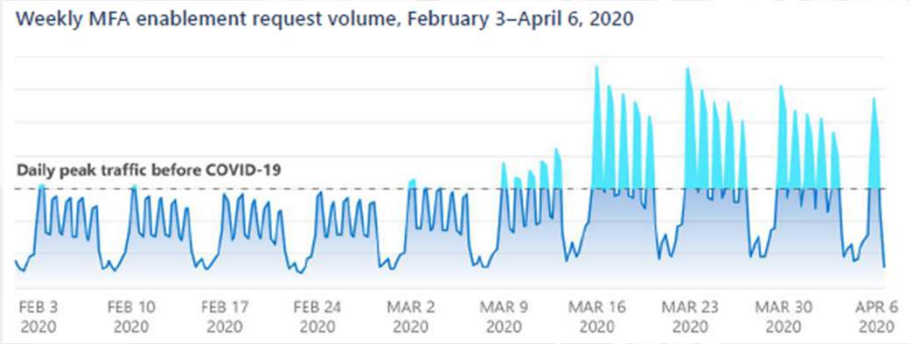
AZURE MFA

first frame networkers
IT, die Sie weiterbringt

WARUM MFA?

first frame networkers
IT, die Sie weiterbringt

- 80% aller erfolgreicher Hacking-Angriffe sind auf schwache Passwörter zurückzuführen.[2]
- Erhöhte Aktivität von Cyberkriminellen durch Covid-19 Pandemie / Home Office
- Vermehrte Nutzung von Cloud-Diensten verschiebt Sicherheitsperimeter
- Steigender Trend für Cloud & Home Office

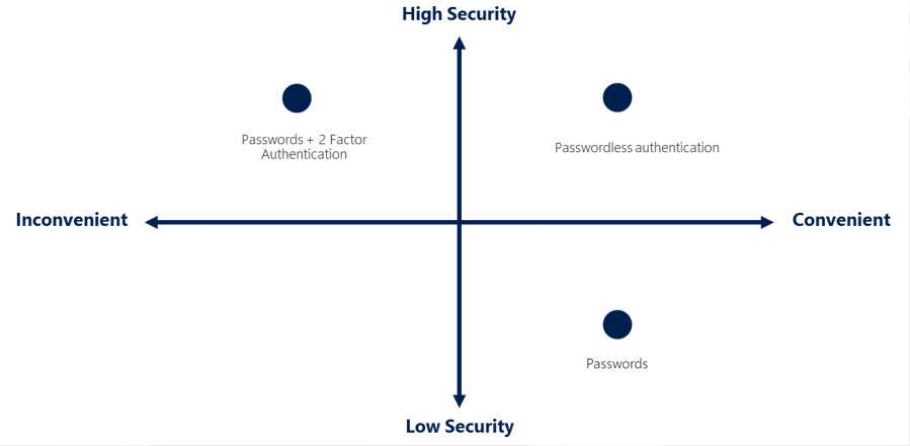


Quelle: Microsoft Digital Defense Report, September 2020

WARUM MFA?

first frame networkers
IT, die Sie weiterbringt

- Multi-Faktor-Authentifizierung (MFA) ist ein Prozess, bei welchem ein Benutzer während dem Login-Prozess dazu aufgefordert wird eine zusätzliche Form der Identifikation anzugeben.
  - Etwas, dass das der Benutzer weiss (typischerweise Passwort oder Code)
  - Etwas, dass der Benutzer besitzt, wie ein vertrauenswürdiges Gerät, dass nicht einfach kopiert werden kann (vertrauenswürdiges Gerät, welches nicht einfach dupliziert werden kann wie ein Telefon oder Security Key)
  - Etwas dass der Benutzer ist (Biometriedaten wie Fingerprint oder Gesichts-Scan)
- Implementation einer MFA-Lösung erhöht die Sicherheit, da Angreifer zweiten Faktor nicht ohne erhöhten Aufwand und hohes Risiko abfangen oder duplizieren kann.



Quelle: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

MFA LIZENZIERUNG & FEATURES

first frame networkers
IT, die Sie weiterbringt

Feature	Azure AD Free - Security defaults	Azure AD Free - Azure AD Global Administrators	Office 365 Apps for…	Azure AD Premium P1 or P2
Protect Azure AD tenant admin accounts with MFA	●	● (Azure AD Global Administrator accounts only)	●	●
Mobile app as a second factor	●	●	●	●
Phone call as a second factor		●	●	●
SMS as a second factor		●	●	●
Admin control over verification methods		●	●	●
Conditional Access				●
Fraud alert				●
MFA Reports				●
Custom greetings for phone calls				●
Custom caller ID for phone calls				●
Trusted IPs				●
Remember MFA for trusted devices		●	●	●
MFA for on-premises applications				●

Quelle: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

MFA LIZENZIERUNG & FEATURES

Empfehlung

first frame networkers
IT, die Sie weiterbringt

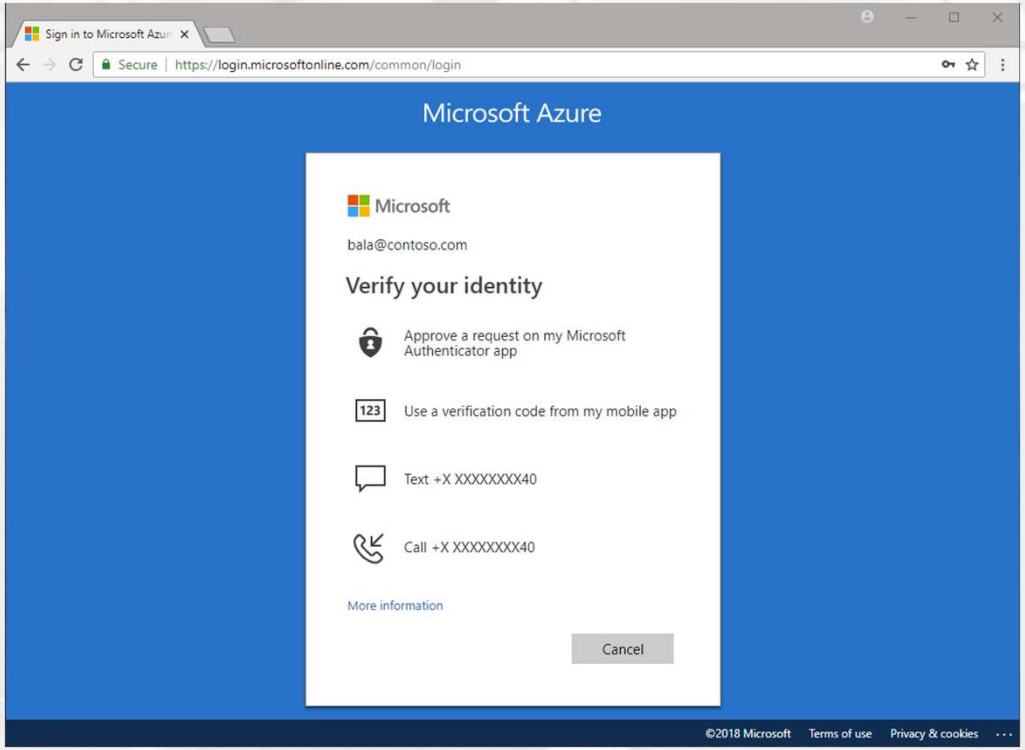
Security Defaults	Per-User MFA	Conditional Access
• Seit Q4/2019 standardmässig für neue Tenants verfügbar • Aktiviert MFA für alle Benutzer & Administratoren • Keine individuellen Konfigurationen möglich • Solange Feature aktiviert, kann Conditional Access nicht genutzt werden • Für Small Business ohne Azure AD P1 Lizenz sinnvoll, welche nicht in ein Lizenz-Upgrade investieren möchten (Azure AD Free) und keine Abhängigkeiten zu Legacy Authentication haben	• Ermöglicht Aktivierung von MFA pro Benutzer • Nur Trusted IPs konfigurierbar • Sollte bei Aktivierung von CA nicht mehr verwendet werden, da Verwaltung sonst in zwei Portalen erfolgt, was zu Verwirrung führen kann. • Für alle M365 Pläne sinnvoll, welche kein Azure AD P1/P2 enthalten, nicht in ein Lizenz-Upgrade investieren möchten und MFA User-spezifisch einsetzen möchten.	• Ermöglicht Aktivierung MFA auf Basis von Signalen (User/Gruppen, Apps, IPs, Devices…) • Nebst MFA können auch andere Signale mitberücksichtig werden • Individuelle Konfigurationen mit Policies & Aktionen möglich • Deckt erhöhte Sicherheitsanforderungen durch mehr Kontrolle & Granularität • In *M365 Business Premium* und *EMS* oder *M365 E3 und E5 (P2)* enthalten • Azure AD P1 / P2 auch als Add-On erwerbbar

Quelle: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

MFA AUTHENTIFIZIERUNGSMETHODEN

first frame networkers
IT, die Sie weiterbringt

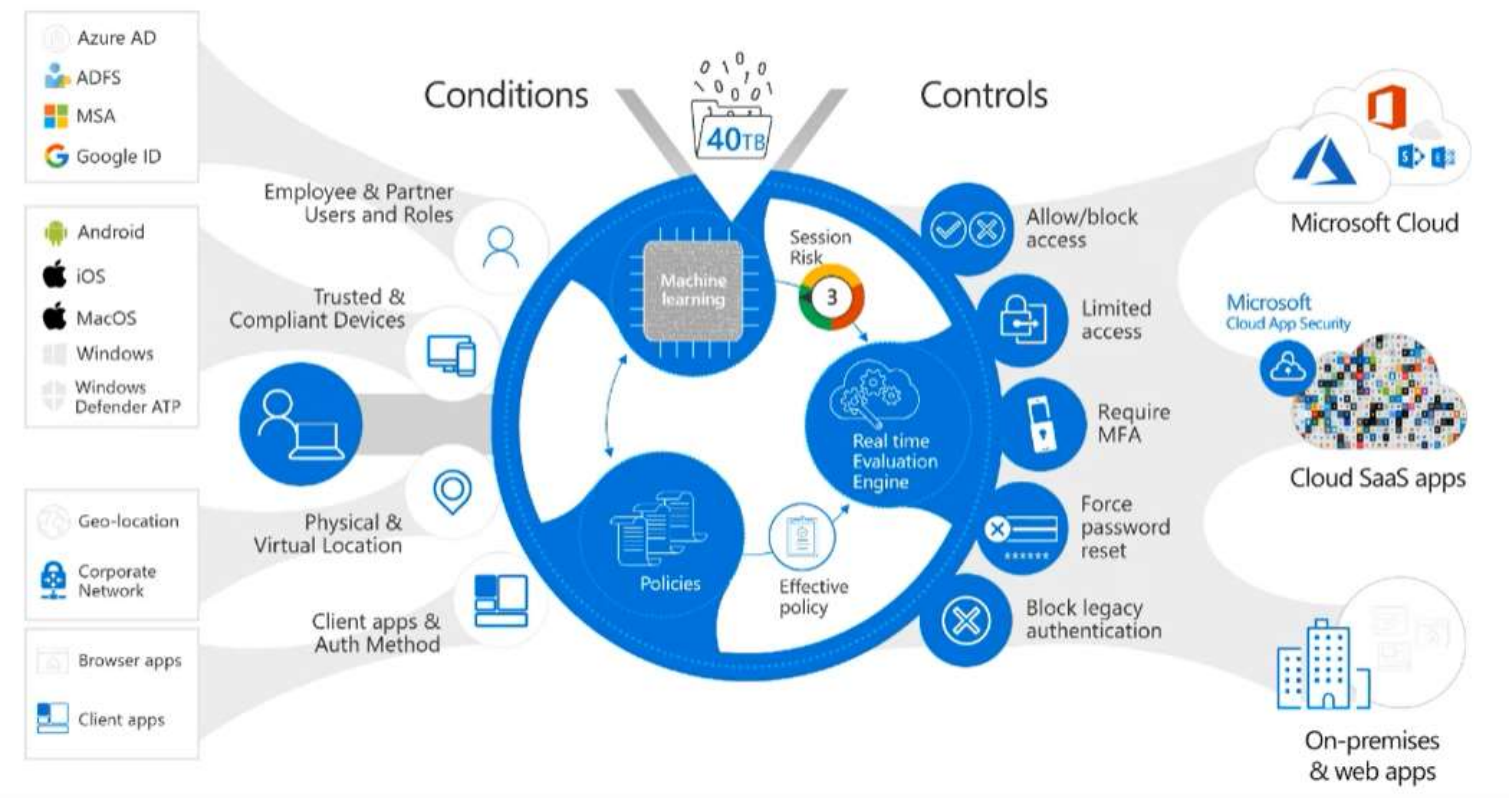
- Optionen
  - Microsoft Authenticator App (Benachrichtigung, Token oder Prüfcode)
  - SMS
  - Telefon-Anruf
  - FIDO2 Sicherheitsschlüssel
- Bei der Wahl der passenden Verifizierungsmethode sind folgende Themen zu berücksichtigen
  - Verfügbarkeit Mobilfunknetz / Internetverbindung (SMS, Voice Call, App-Benachrichtigung)
  - Privatsphäre (Microsoft Authenticator App auf privaten Geräten)
  - Sicherheit (Voice Call / SMS)



Quelle: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

MFA & CONDITIONAL ACCESS - ÜBERBLICK

first frame networkers
IT, die Sie weiterbringt



Quelle: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

MFA MIT CONDITIONAL ACCESS - VORTEILE

first frame networkers
IT, die Sie weiterbringt

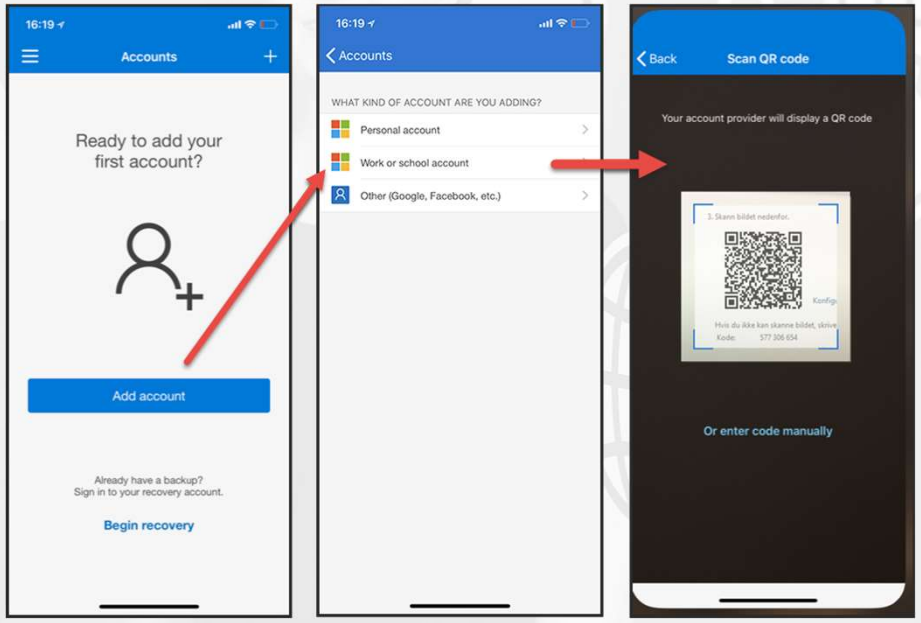
- Deckt erhöhte Sicherheits-Anforderungen
- Bietet mehr Kontrolle & Granularität
- Ermöglicht die Erstellung und Definition von Policies, die
  - auf Login-Events reagieren und
  - zusätzliche Aktionen anfordern, bevor einem Benutzer Zugriff zu einer Applikation oder einem Service gewährt wird.

- Ermöglicht Blockierung älterer Authentifizierungsprotokolle (Legacy Authentication) wie POP3, SMTP, IMAP, and MAPI, welche kein MFA unterstützen.
  - Mehr als 99 % von Password Spray Attacken und mehr als 97% von Credential Stuffing Attacken benutzen Legacy Authentication Protokolle
  - Das Risiko auf Kompromittierungen von Azure AD Accounts ist bei Deaktivierung / Blockierung von Legacy Authentication 67% tiefer

DEMO

first frame networkers
IT, die Sie weiterbringt

- MFA-Registrierung Verifikationsmethoden (kombinierte Registration)
- Browser-Login mit / ohne MFA
  - Authenticator App
  - Telefon
  - Trusted Location (ohne MFA)
- Passwordless Authentication FIDO2 Key



KEY POINTS 1/2

first frame networkers
IT, die Sie weiterbringt

- Kommunikation ist nebst der technischen Umsetzung das A & O in MFA-Projekten
- Azure AD Premium P1 bietet mit der Nutzung von Conditional Access Policies sowie der Integrierbarkeit in On-Premise-Lösungen die notwendige Flexibilität im geschäftlichen Umfeld
- Blockierung von Legacy Authentication sollte bei Einführung MFA erzwungen werden
- Client-Integration ins Azure AD (Hybrid Join) und in Microsoft Intune erlaubt die Nutzung von weiteren Signalen (Compliant / Hybrid Joined Device, Approved / Protected Apps) in Conditional Access und ermöglicht noch mehr Sicherheit

KEY POINTS 2/2

first frame networkers
IT, die Sie weiterbringt

- Parallele Einführung von Self-Service Password Reset (SSPR) mit kombinierter Registration ermöglicht eine einheitliche und einmalige Registrierung von Verifikationsmethoden, welche den Support-Aufwand reduziert und die Autonomie der Endbenutzer erhöht
- Passwortlose Authentifizierung ist im Vormarsch, es gibt jedoch teils noch Limitierungen (Unterstütze Geräte, Apps / Services, Windows vs. Browser…)
- Emergency Accounts ohne MFA minimieren das Risiko, sich aufgrund von Policy-Fehlkonfigurationen aus dem Azure Portal auszuschliessen und bei unwahrscheinlichem Ausfall des Azure MFA Dienstes noch arbeiten zu können

INTERESSE GEWECKT?

first frame networkers
IT, die Sie weiterbringt

- Azure MFA bietet als Cloud-Dienst bewährte, stetig weiterentwickelte Features mit vielfältigen Integrationsmöglichkeiten sowohl in Cloud wie auch On-Premise Applikationen
- Unsere zertifizierten Microsoft Engineers haben mehrjährige Erfahrung mit der Implementierung von Azure MFA-Lösungen
- Durch die von uns bereitgestellten, individualisierbaren Kommunikations- & Schulungsvorlagen erhöhen Sie die Akzeptanz bei der Einführung im Unternehmen

LINKS & QUELLEN

first frame networkers
IT, die Sie weiterbringt

1. Microsoft Digital Defense Report, September 2020
2. Email: Is the Digital Door Propped Open for Identity Hijackers? Multi-Factor Authentication Helps Shut Cyber Criminals Out
3. Wie MFA funktioniert
4. Was ist Conditional Access?
5. Was sind Security Defaults?
6. Legacy Authentication Protokolle
7. Self-Service Password Reset (SSPR)

DIE EINGANGSTÜR MIT AZURE MFA

first frame networkers
IT, die Sie weiterbringt

08.06.2021

FRAGEN

first frame networkers

IT, die Sie weiterbringt

KONTAKT & WEITERGEHENDE INFORMATIONEN

first frame networkers
IT, die Sie weiterbringt

first frame networkers ag
Haldenstrasse 1
Postfach 1338
CH-6340 Baar
Schweiz

+41 41 768 08 00
www.firstframe.net
www.firstframe.net/firstworkplace