Microsoft

Identity Management
mit Azure Active Directory

Benutzerkonten sind die Grundlage der heutigen Sicherheitskonzepte. Durch eine stetig steigende Anzahl an erforderlichen Anwendungen und Diensten, werden immer wieder neue Benutzerkonten für einen Mitarbeiter angelegt. Somit steigt auch das Risiko eines Identitätsdiebstahls und dem damit verbundenen Zugriff von Dritten auf Unternehmensdaten.

Was bedeutet das konkret für Sie?

- Sie benötigen eine zentrale Plattform, in der alle Mitarbeiter einen zugewiesenen Benutzer besitzen
- Diese Plattform muss auch für Cloud-Dienste von extern erreichbar sein und eine hohe Verbreitung besitzen

Unsere Empfehlung:

- Für Ihre On-Premises Infrastruktur kann das etablierte Active Directory von Microsoft genutzt werden
- Um die Authentifizierung an ausgewählten Online-Diensten zu ermöglichen kann das Azure Active Directory eingerichtet werden
- Verbinden Sie Ihr On-Premises Active Directory mit dem cloudbasierten Azure Active Directory um eine Synchronisierung Ihrer Identitäten zu ermöglichen und somit redundante Benutzerkonten zu vermeiden

Hier können wir Sie aktiv unterstützen:

- Erweiterung Ihrer On-Premises Infrastruktur, mit dem Cloud-Dienste Azure Active Directory
- Absicherung der Zugriffe auf Ihre Unternehmensdaten
- Einrichtung einer zentralen Identitätsverwaltung, die auch an ausgewählten herstellerübergreifenden Diensten authentifiziert

Wussten Sie, dass...

- ... die Premium-Funktionen von Azure Active Directory auch in der Enterprise Mobility and Security Suite und somit auch im Microsoft 365 Bundle enthalten sind!
- Unsere Experten prüfen gerne, welche Features Sie haben und wie diese am besten eingesetzt werden können.

value – inspired by people

Das Azure Active Directory bietet eine Vielzahl an Funktionen, um die administrativen Tätigkeiten zu optimieren. Hierbei lassen sich die Lösungen auch flexibel auf Ihre Anforderungen anpassen und einrichten. Damit Sie mögliche Einsatzszenarien evaluieren können, geben wir Ihnen eine KLEINE Übersicht der Funktionen.*

Funktion	Basic	Premium 1	Premium 2
Single Sign–On	✓	✓	✓
Anwendungsproxy	✓	✓	✓
Self-Service Passwort Portal	✓	✓	✓
Multi-Faktor Authentifizierung		✓	✓
Conditional Access		✓	✓
Identity Protection			✓

*Eine vollständige Übersicht erhalten Sie hier: https://azure.microsoft.com/en-us/pricing/details/active-directory/

Single Sign–on

- Vermeiden Sie die Erstellung von zusätzlichen Benutzerkonten für Ihre Mitarbeiter. Ein Mitarbeiter der mehrere Benutzerkonten für seine Arbeit benötigt, verwendet entweder ein gemeinsames Passwort oder viele schwache Passwörter.
- Mit einer Identität aus Ihrem Active Directory können sich die Mitarbeiter an einer steigenden Zahl von Online-Diensten authentifizieren
- Hierbei erfolgt die Anmeldung vollständig im Hintergrund. Somit ist es nicht erforderlich, dass der Mitarbeiter sein Kennwort erneut eingibt.
- Dies gilt auch für einen domänenübergreifenden Zugriff im B2B Bereich.
- Sie müssen nicht mehr für externe Dienstleister zusätzliche Benutzerkonten anlegen und pflegen.

Anwendungsproxy

- Richten Sie einen Azure Anwendungsproxy in Ihrer DMZ ein, um den Zugriff auf interne Ressourcen schnell und sicher extern bereitzustellen
- Gruppieren Sie mehrere Anwendungsproxys, um ein Lastenausgleich zu erhalten sowie die Verfügbarkeit zu erhöhen.
- Webseiten die über den Azure Anwendungsproxy bereitgestellt werden können durch den Conditional Access abgesichert werden.
- Somit lässt sich der Zugriff sowohl auf Cloud als auch auf On-Premise Anwendungen mit einem Regelwerk einheitlich absichern.

Self-Service Passwort Portal

- Entlasten Sie Ihre IT-Abteilung im täglichen Betrieb, in dem Sie den Mitarbeitern Mittel zur Selbstorganisation bereitstellen.
- Ein Beispiel hierfür, ist das eigene Benutzerkonto selbst zu verwalten, in dem Passwörter eigenständig zurückgesetzt oder erneuert werden können.
- Durch die Abfrage von weiteren Faktoren, kann die Authentizität des Mitarbeiters sichergestellt werden.

Multi-Faktor Authentifizierung

- Erhöhen Sie die Zugriffssicherheit, in dem Sie zusätzliche Faktoren bei der Anmeldung prüfen.
- Ermöglichen Sie somit, dass ausschließlich autorisierte Personen Zugriff auf Ihre geschäftlichen Daten erhalten.
- Skalieren Sie die Sicherheit je nach Sensibilität der Informationen auf die zugegriffen werden soll.
- Nutzen Sie hierfür verschiedene Faktoren zur Authentifizierung:
  - Token
  - Anruf
  - Smartcard
  - SMS

Conditional Access

- Definieren Sie Voraussetzungen, die für einen erfolgreichen Zugriff erfüllt werden müssen
- Kombinieren Sie hierbei die verschiedenen Cloud-Produkte von Microsoft, um flexibel Ihre Anforderungen zu erfüllen
- Schützen Sie neben den Cloud-Diensten auch die externen Zugriffe auf Anwendungen in Ihrer Unternehmensinfrastruktur
- Fordern Sie bei auffälligen Anmeldungen einen zusätzlichen Faktor zur Authentifizierung an.

Identity Protection

- Stellen Sie sicher, dass Ihre Benutzerkonten nicht von unautorisierten Dritten verwendet werden.
- Identifizieren Sie einen möglichen Missbrauch von Benutzerkonten oder auffälliges Anmeldeverhalten
- Reduzieren Sie die Reaktionszeit, in dem Sie Maßnahmen definieren, die bei der Erkennung einer missbräuchlichen Verwendung durchgeführt werden

Gängige Beispiele für Unternehmensrichtlinien

CONDITIONAL ACCESS

Der Zugriff auf Unternehmensdaten darf ausschließlich von bekannten Geräten erfolgen. Alle bekannten Gerät sind entweder:

- Domänenintegriert (Windows)
- Per Microsoft Intune registriert (Windows 10, iOS, Android, MacOS)

IDENTITY PROTECTION

Wenn bei einer Anmeldung, eine unmögliche Reise erkannt wird (z. B. Deutschland -> China in 5 Sekunden), soll der Benutzer deaktiviert oder eine Multi-Faktor Authentifizierung angefordert werden

Die Benutzerkonten innerhalb Ihres Unternehmens sind das erste Ziel von Angreifern. Mittlerweile gibt es ausreichend Lösungen, um Pishing-Mails oder bösartige Dateien zu identifizieren und zu beseitigen, bevor diese über Ihre Unternehmensinfrastruktur an den Mitarbeiter bereitgestellt werden.

Mit einer zunehmenden Auslagerung wichtiger Dienste in die Cloud, ist es für Angreifer nicht mehr erforderlich, in Ihre Unternehmensinfrastruktur einzudringen. Während Ihre Mitarbeiter den Zugriff auf die geschäftlichen Daten lediglich 8x5 Stunden in der Woche benötigen, können Hacker versuchen die Passwörter jederzeit (24x7) zu ermitteln.

Unsere Empfehlung

- Entscheiden Sie, wann und wer auf Ihre Unternehmensdaten Zugriff erhält!
- Fragen Sie bei unseren Experten eine vollständige Übersicht der Funktionen des Azure Active Directorys an und besprechen Sie mit Ihnen die Anwendungsgebiete.
- Erhalten Sie einen Überblick über die modernen Sicherheitsmechanismen und wie diese mit anderen Diensten zusammenarbeiten.

Key Facts

- Single-Point-of-Control für alle Benutzerkonten und alle Dienste

- Keine redundanten Konten

- 1 Mitarbeiter = 1 Benutzer für eine Vielzahl an Diensten

- Synchronisierung der Benutzereigenschaften

- Skalierbarkeit der Sicherheitsanforderung, je nach Sensibilität

- Beschränkung der Zugriffe auf Unternehmensressourcen. Sowohl On-Premise als auch in der Cloud

---

msg services gmbh – Ihr Partner: Als IT-Service- und Consultingpartner entwickelt die msg services gmbh innovative Lösungen von hoher Leistungsqualität, mit denen unsere Kunden einen dauerhaften Mehrwert in ihrem Business erzielen. Wir gehören zur msg-Gruppe, einem der bedeutendsten IT-Beratungs- und Systemintegrationsunternehmen im deutschsprachigen Raum. Herstellerunabhängig und branchenübergreifend ausgerichtet, reichen unsere Kernkompetenzen von der Prozessberatung über Infrastrukturlösungen bis zu Betriebs- und Anwendungsservices.

msg services gmbh | Robert-Bürkle-Straße 1 | 85737 Ismaning/München
Telefon: +49 89 96101-2500 | www.msg-services.de | sales.services@msg.group