Webinar: Microsoft 365 Tenant Security – Verstehen. Anwenden. Absichern. – Q&A

Wo findet sich die Aufrufhistorie der Shared Links? Gibt es eine Übersicht über alle Shared Links (von wem an wen)?

Die Nutzung von Shared Links ohne aktiviertes Entra B2B, wie in der ersten Demo gezeigt, findet man nur mit passendem Such-Parameter ("SharingLinkUsed"). Eine Gesamtübersicht lässt sich mit Bordmitteln nur mit Powershell-Scripting realisieren. Alternativ gibt es sehr gute 3rd Party-Tools die dies und mehr managebar machen, wie von unserem Partner AvePoint

Wie kann ich einem Admin-Account nur bestimmte Funktionen innerhalb von Intune freigeben? Zur Zeit bekommen bestimmte Admins den "Intune-Administrator", aber damit kann man ja alles machen. Ich würde gerne z.B. nur, dass er Geräte im Enrollment hinzufügen kann, aber sonst nur lesend.

Intune unterstützt Role Based Access Control (RBAC) direkt aus dem Intune Adminportal. Dort gibt es eine vorgefertigte Anzahl an Rollen, die von Entra-Rollen abgeleitet wurden. Es ist aber auch die Erstellung von Custom Roles möglich.

Funktionieren die Risiko-basierten Loginbeschränkungen nur mit Entra ID P2?

Das ist korrekt, für die risk based Funktionen ist die Entra ID P2 Lizenz erforderlich.

Wie löst man folgende Situation: Wenn ein Abteilungshandy nur an einem festen Firmenstandort von mehreren Personen verwendet werden soll und diese auf dem Handy auf eine Shared Mailbox zugreifen soll? Ist es am besten die Shared Mailbox zu einem User Account umzuwandeln, passwortlose Anmeldung einzurichten + MFA, CA erstellen damit man sich nur an dem Standort anmelden kann (hat eine feste IP Adresse)?

Technisch ist es möglich, die Login-Sperre des automatisch erstellten Benutzers der Shared Mailbox herauszunehmen. Dann könnte man diesen verwenden. Generell sollten die Benutzer von Shared Mailbox Accounts geblockt sein. In der CA Policy wäre die Empfehlung, die Network Location nicht IP-basiert zu hinterlegen, sondern via WLAN SSID. Grund hierfür ist, dass man dann auch mit einem VPN nicht vorgeben kann, am Standort zu sein.

Was ist mit MFA über Conditional Access erzwingen genau gemeint? MFA täglich für den normalen Benutzer oder erst wieder bei Kennwortablauf?

Über CA können wir generell erst einmal festlegen, dass MFA gefordert wird, um überhaupt Zugriff auf den Tenant zu erhalten. Über die Session Controls lässt sich dann explizit festlegen, wie oft bzw. nach welcher Zeit eine Re-Authentifizierung erfolgen muss. Hier empfiehlt es sich, jeweils eine Policy für Admins und User anzulegen.