Identity Security as a Service: Schützen Sie Ihre Identitäten immer und überall.

In der digitalen Welt wird der Schutz der Identität immer wichtiger. Haben Sie gewusst, dass sich mit den heutigen technischen Mitteln Identitäten problemlos fälschen lassen? Das klassische Identity Access Management (IAM) bildet die Basis und die organisatorischen Rahmenbedingungen für den Identitätsschutz. Mit Identity Security as a Service gehen wir einen Schritt weiter und schützen Ihre Identitäten immer und überall.

Identitätsmanagement stellt sicher, dass die richtige Person den passenden Zugriff auf die Ressourcen hat, für die sie berechtigt ist. Das ist einfach gesagt, aber lässt sich nicht so leicht umsetzen.

Es gibt eine Reihe von typischen Schwachstellen und Bedrohungen, die von Netzwerk- und Cloud-Security-Lösungen erkannt werden. Die folgenden drei Schwachstellen müssen zum Schutz von Identitäten speziell beachtet werden:

1. Nicht verwaltete Identitäten: Umgang mit privileged Access, lokalen Adminrechten, unpersönlichen Konten und generell dem Prozess der Identitäten (inaktive Identitäten etc.)
2. Falsch konfigurierte Identitäten: Dazu gehören Schattenadministratoren, Service Accounts, schwache Passwörter und schlechte Verschlüsselungspraktiken, welche den Zugriff in ein Netzwerk vereinfachen
3. Exponierte Identitäten: Dazu zählen in Speichern abgelegte Anmeldeinformationen sowie Zugriffs-Token, auf die Hacker zugreifen können

Wie funktioniert UMB Identity Security as a Service?

Identity Security as a Service überwacht permanent Ihre Identitäten und behält deren Angriffsfläche im Auge. Identity Security as a Service besteht aus Modulen, welche sich gegenseitig ergänzen. Folgende Funktionalitäten sind pro Modul enthalten:

- Aktive Überwachung und Härtung von onPrem und Azure Active Directories(AD)
- Konfigurationsänderungen auf den AD analysieren
- Unnötige Zugriffs-Rechte erkennen und beseitigen
- Kritische Schwachstellen auf Domain-, Computer- und Benutzerebene erkennen (AD und Azure AD)
- Regelmässiges Auditing von relevanten Cloud- und onPrem-Komponenten – wie Remote Access Lösungen, Firewall-Konfigurationen, Backup, Printer, Server, Fileserver und Datenbanken

Ihre Vorteile

- Kontinuierliche bzw. regelmässige Prüfung des Sicherheitsstands nach Best Practice
- Mögliche Angriffe werden im Ansatz verhindert
- Angreifer werden gestoppt und können einen Angriff nicht zu Ende führen

Servicebestandteile

- Kontinuierliches Überwachen des ADs
- Bei kritischen Identity-Schwachstellen sofortige Meldung an den Kunden
- Umfassender, monatlicher Servicebericht
- Regelmässige Auditberichte zu den definierten Audits
  - Handlungsempfehlungen zu Verbesserungsmöglichkeiten
  - Gegenüberstellung aktueller Zustand vs. letztem Zustand

Rundum sicher fühlen? Kontaktieren Sie uns!

Gerne beantworten wir Ihre Fragen zu Identity as Service

Kontakt

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch/security