iTentity erklärt:

Multi-Faktor-Authentifizierung (MFA)

Cyber Security Awareness Month

iTentity erklärt:

Was ist Multi-Faktor-Authentifizierung (MFA)?

In einer Zeit, in der Cyberangriffe immer häufiger und raffinierter werden, ist es entscheidend, vorhandene Online-Konten bestmöglich zu schützen. Die Multi-Faktor-Authentifizierung (MFA) bietet eine effektive Lösung, um die Sicherheit zu erhöhen.

Multi-Faktor-Authentifizierung ist ein Sicherheitsprozess, bei dem zwei oder mehr Authentifizierungsfaktoren verwendet werden, um die Identität eines Benutzers zu überprüfen.

iTentity erklärt:

Was ist Multi-Faktor-Authentifizierung (MFA)?

Diese Faktoren können umfassen:

- Etwas, das man weiß – wie ein Passwort oder eine PIN.
- Etwas, das man hat – wie ein Smartphone oder ein spezielles Authentifizierungsgerät.
- Etwas, das man ist – wie ein Fingerabdruck oder Gesichtserkennung.

iTentity erklärt:

Warum ist MFA wichtig?

Erhöhte Sicherheit:
Selbst wenn ein Angreifer das Passwort herausfindet, reicht das allein nicht aus, um Zugang zu dem Konto zu erhalten.

Schutz vor Phishing:
MFA schützt vor Phishing-Angriffen, da Angreifer zusätzlich zur Kenntnis des Passworts auch Zugriff auf den zweiten Authentifizierungsfaktor benötigen.

Vertrauen:
Durch den Einsatz von MFA signalisiert man Nutzern und Kunden, dass einem Sicherheit am Herzen liegt.

iTentity erklärt:

Wie implementiert man MFA?

Wählen eines MFA-Dienstes:
Es gibt viele zuverlässige MFA-Dienste, wie Google Authenticator, Microsoft Authenticator oder Authy.

Aktivieren von MFA auf den Konten:
Die meisten Online-Dienste bieten die Möglichkeit, MFA in den Kontoeinstellungen zu aktivieren.

Regelmäßige Überprüfung:
Regelmäßige Überprüfung der MFA-Einstellungen und bei Bedarf Aktualisierung der Authentifizierungsmethoden.