CHUBB®

Multi-Faktor-Authentifizierung (MFA)

MFA unterstützt Sie bei der Abwehr von Cyberkriminellen

Cyberangriffe setzen in vielen Fällen den Zugriff der Hacker auf das Netzwerk oder die E-Mails Ihres Unternehmens voraus. Mit einem herkömmlichen Nutzer-Login und Passwort-Zugang auch 1-Faktor-Authentifizierung (1FA) genannt können Angreifer unter Umständen problemlos auf das IT-System eines Unternehmens zugreifen.

Hat ein Angreifer erst einmal Zugriff auf Ihre Mails, kann er vorgeben, Sie zu sein, und Fake-E-Mails verschicken oder, sofern er Zugriff auf Ihr Netzwerk hat, Ihre Umgebung auskundschaften, Privilegien ausweiten, Backups löschen und Ransomware einschleusen.

Hacker können hierzu verschiedene Verfahrensweisen anwenden:

- Anwendung einer sogenannten „Brute Force"-Vorgehensweise oder Einsatz eines Tools, mit dem durch das Ausprobieren einer Vielzahl häufig verwendeter Passwörter diese automatisiert geknackt werden können.
- Abfangen von Berechtigungsnachweisen oder Ausnutzung der Tatsache, dass Mitarbeiter für ihre verschiedenen Konten häufig dieselben ID- und Passwortkombinationen verwenden.
- Phishing oder Versenden einer Fake-E-Mail-Aufforderung zum Zurücksetzen eines Passworts, wodurch die geschäftlichen E-Mail-Daten des jeweiligen Mitarbeiters abgegriffen werden können.

Eine der effektivsten Methoden, um Tätern den Zugang zu Ihren Systemen zu verwehren, ist die Multi-Faktor-Authentifizierung (MFA), da sie im Grunde eine zweite Authentifizierungs-/Abwehrstufe bietet.

Was ist MFA?

MFA erfordert mindestens zwei Authentifizierungsfaktoren oder Identitätsnachweise, um sicherzustellen, dass Personen, die auf Ihre Unternehmens-E-Mails oder andere wichtige Computersysteme Ihres Unternehmens zugreifen möchten, auch diejenigen sind, die sie vorgeben zu sein.

Beispiel einer dreistufigen Authentifizierung:

1. 

Eine Ihnen bekannte Information
(normalerweise ein Passwort oder ein Verifizierungscode)

2. 

Ein in Ihrem Besitz befindliches Objekt
(ein vertrauenswürdiges Gerät, das nicht ohne Weiteres dupliziert werden kann, z. B. ein Telefon oder ein Sicherheitsschlüssel)

3. 

Eines Ihrer persönlichen Merkmale
(Biometrie)

> ***Zwei oder mehr Authentifizierungsfaktoren zu kompromittieren, ist für Angreifer nicht einfach, sodass sich hierdurch das Risiko einer Manipulation erheblich verringert.***

Warum ist MFA so wichtig?

Das Konzept der mehrstufigen Authentifizierung beruht darauf, dass es, wenn es Cyberkriminellen tatsächlich gelingt, etwas zu stehlen, das den berechtigten Nutzern bekannt ist, viel weniger wahrscheinlich ist, dass sie auch im Besitz derselben Objekte sind. Im Falle eines E-Mail-Kontos besitzt dessen Nutzer das entsprechende Soft-Token oder das Gerät, mit dem ein eindeutiger, nur kurze Zeit gültiger Code erzeugt werden kann.

Implementierung einer MFA

Eine mehrstufige Authentifizierung kann eine der schnellsten und wirkungsvollsten Maßnahmen sein, um die Identität von Nutzern zu schützen. Viele, wenn nicht gar die Mehrzahl, der gängigen Webservices verfügen über eine MFA, die allerdings häufig standardmäßig deaktiviert ist.

Lassen Sie sich von Experten beraten, wie Sie die für Ihr Unternehmen bestgeeignete MFA implementieren können.

Chubb. Insured.℠

DE0426-MD 06/22