Daten schützen

Passwort erklären

OTP

2 Faktor Authentifizierung

Android oder IOS

Voraussetzung:

Der Zugriff zum Smartphone (Handy) muss mit einem Code (PIN) gesichert sein.

Was ist ein Einmal-Passwort (OTP)? Quelle: **Tools4ever Informatik GmbH**

Ein **Einmal-Passwort**, Einmal-PIN oder auch **One-Time-Password** (Abkürzung OTP) genannt, ist ein Passwort, das für eine bestimmten Zeitraum gültig ist, wenn eine einzelne Login-Sitzung oder Transaktion abgeschlossen wird.

Ein Einmal-Passwort hilft, einige der Nachteile traditioneller, vom Benutzer erstellter, statischer oder fester Passwörter zu umgehen. Einmal-Passwörter können allein oder in Verbindung mit einer Multi-Faktor-Authentifizierung verwendet werden, um z.B. eine zusätzliche Sicherheitsstufe hinzuzufügen.

Einmal-Passwörter werden automatisch generiert und laufen nach einem bestimmten Zeitraum ab (z.B. alle 60 Sekunden). Wenn nach Ablauf der Zeit ein neues OTP generiert wird, bleibt es der einzige gültige Code vor dem nächsten Zurücksetzen.

OTP-Anwendungsbereiche

Ist die Nutzung unabhängig, wird ein Benutzer aufgefordert, einige persönliche Informationen einzugeben, wie z.B. eine E-Mail-Adresse, eine Telefonnummer oder einen Benutzernamen. Das zufällig generierte Einmal-Passwort wird dann per E-Mail, SMS, Push-Benachrichtigung oder auf anderem Wege an den Benutzer gesendet. **Da der Benutzer die einzige Person sein sollte, die es erhält, kann er sicher sein, dass er exklusiven Zugriff hat. Anschließend kann er sich dann einloggen.**

Wenn das Einmal-Passwort in Verbindung mit einem üblichen Passwort verwendet wird, wird der Benutzer aufgefordert, sich normal anzumelden. Erst nach erfolgreicher Eingabe seines regulären Anmeldekennworts wird das OTP gesendet oder angefordert. In vielen Fälle erhalten die Benutzer kleine Geräte, wie z.B. einen Schlüsselanhänger oder einen Token, um das Einmal-Passwort zu generieren, welches sie für den Zugang zu ihrem Konto verwenden würden. Alternativ kann ein Benutzer ein OTP- oder „Authenticator“-Client (z.B. Google Authenticator) auf sein Smartphone herunterladen, der ein mit einem bestimmten Anmeldeverfahren verknüpftes OTP anzeigt.

OTP-Tokens können entweder ereignis- oder zeitbasiert sein.

- Ereignisbasierte Token generieren auf Knopfdruck neue Codes und bleiben bis zur Verwendung gültig.
- Zeitbasierte Token generieren Codes, die nur für eine bestimmte Zeitspanne (normalerweise weniger als eine Minute) gültig sind, wonach ein neuer Code generiert wird. Diese Token sind in beim Online-Banking recht beliebt, um sicherzustellen, dass die sensiblen Bankinformationen der Benutzer sicher aufbewahrt werden und um das Risiko eines unbefugten Zugriffs auf die Benutzerkonten zu verringern oder zu eliminieren.

Passwörter mindestens 12 Zeichen lang oder länger.

Verwenden werden Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen.

Niemals Zahlenreihen, Geburtstage, Namen usw. die allesamt leicht zu knacken sind.

2 Faktor Authentifizierung (2FA)

User ID

PW

1.Faktor

User ID -> öffentlich

PW-> geheim (muss stark sein)

SMS (OTP)

PIN (OTP)

Authenticator (OTP)

Email (OTP)

Push Nachricht (OTP)

Fingerabdruck

Gesichtserkennung

Andere

2. Faktor

Beispiele

Bezahl-Terminal an Supermarkt-Kasse

Bankkarte (EC) 1.Faktor

PIN oder Unterschrift sind 2. Faktor

Online- Banking

Bank-App 1.Faktor

Bank-Secure App 2.Faktor