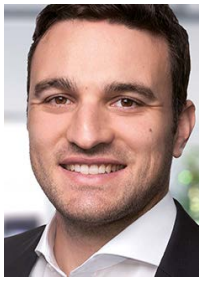
Sichere Transaktionen – so haben Betrüger keine Chance

Spätestens mit dem Inkrafttreten von PSD2 müssen Banken die Absicherung ihrer digitalen Transaktionen überdenken. Denn die neue EU-Richtlinie verlangt ab 2018 eine „starke" Authentifizierung. Mechanismen wie Passwörter reichen dann nicht mehr aus, um in Zeiten massiver Hackerangriffe und Betrugsversuche auf der sicheren Seite zu sein.



Autor:
Dr. Amir Alsbih,
COO/CTO von KeyIdentity

Gestohlene oder schwache Passwörter sind heute in über 80 Prozent aller Fälle die Ursache für einen Hack. Dazu kommt, dass viele Nutzer ihre Passwörter mehrfach für unterschiedliche Anwendungen verwenden – von SAP im Unternehmen über den privaten Facebook- oder Amazon-Account bis hin zur Steuerung ihres Smart-Home.

Durch die Mehrfachverwendung von Passwörtern wird dann nicht nur ein Dienst kompromittiert, sondern sehr wahrscheinlich gleich mehrere. So probieren Angreifer die erbeuteten Daten systematisch und automatisiert bei diversen anderen Portalen aus. Haben diese sich erst einmal einen Zugang verschafft, erbeuten sie umso mehr Daten, je länger sie dabei unerkannt bleiben.

Passwörter versagen bei Transaktionen

Der kurze Einblick in die aktuellen Bedrohungsszenarien zeigt, dass Passwörter heute keine geeignete Methode mehr für die Authentifizierung digitaler Identitäten sind. Dies gilt insbesondere für Logins und Transaktionen im Finanzsektor. Diese Schwachstelle hat inzwischen auch Regulierungsbehörden der EU auf den Plan gerufen, die eine erweiterte Zahlungsdienste-Richtlinie entwickelt haben: Laut PSD2 muss die digitale Authentifizierung bei Banken künftig auf mindestens zwei der drei folgenden Faktoren basieren:

- Wissen: Passwörter, PINs oder Identifizierungsnummern, die nur der autorisierte Kunde oder Mitarbeiter kennt
- Besitz: Token, Smartphone-Apps oder Smartcards, die nur der berechtigte Nutzer besitzen kann oder darf
- Eigenschaft: biometrische Eigenschaften des Anwenders, beispielsweise sein Fingerabdruck

Die Bestätigung eines Logins oder einer Transaktion durch mindestens zwei voneinander unabhängige Berechtigungsnachweise wird als 2-Faktor- (2FA) oder auch Multi-Faktor-Authentifizierung (MFA) bezeichnet.

Soll im Investment-Banking beispielsweise eine außergewöhnlich hohe oder durch ihre Häufigkeit auffallende Überweisung getätigt werden, löst das System beispielsweise eine Verifikation via Push-Authentifizierung aus. Dabei wird automatisch eine Push-Nachricht auf das Smartphone eines Vorgesetzten oder eines anderen berechtigten Mitarbeiters gesendet. Dieser muss die Transaktion bestätigen – oder eben ablehnen, wenn sie nicht rechtens ist. Dafür genügt ein Klick auf „OK" oder „Abgelehnt". Einfacher geht es kaum. Analog können die Push-Token zur sicheren Authentifizierung von Kunden im Onlinebanking eingesetzt werden. Diese bestätigen ihren Login am Bank-Portal anschließend einfach mit einem „OK".

Kryptographisch sichere Push-Token verschlüsseln die Nachrichten mit einem Public-Private-Key und signieren die enthaltenen Informationen zusätzlich. Auf diese Weise wird sowohl die Vertraulichkeit als auch die Integrität unabhängig vom Transportmedium gewährleistet. Das ermöglicht zudem eine Nicht-Abstreitbarkeit, was in manchen Fällen die Haftungsfrage eindeutig klärt. Unwissenheit vorzutäuschen ist dann keine Option mehr.

Sichere Multi-Faktor-Authentifizierung

Banken können aus einer großen Bandbreite an Token für die Multi-Faktor-Authentifizierung wählen – je nach Sicherheitslevel der Nutzer und deren Einsatzszenario. So sind für PSD2-Szenarien neben Push-Token auch QR-Token denkbar, bei denen die Authentifizierung per Scan des QR-Codes mittels Smartphone-Kamera und -App durchgeführt wird.

Durch den zweiten Faktor Token erhalten Angreifer nicht mehr den Schlüssel zum Königreich, wenn sie Passwörter erbeuten. Aus diesem Grund und weil Passwörter sehr häufig für die Kompromittierung von Diensten verantwortlich sind (ca. 80 Prozent), sollten Systeme mit einem hohen Schutzbedarf immer mittels einer 2FA / MFA Lösung abgesichert werden.