Verlagsbeilage, Juli 2014

‹kes›
Die Zeitschrift für Informations-Sicherheit

special

Mobile Security

SecuMedia

Verschlüsselt kommunizieren mit Apps ab S. 24

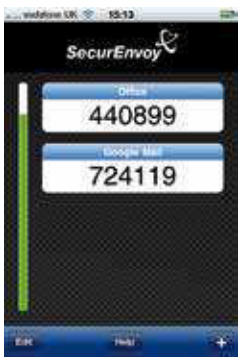
Zwei-Faktor-Authentifizierung per Smartphone

OTPs ohne Hardware-Token

Neue Lösungen zur Zwei-Faktor-Authentifizierung nutzen Mobiltelefone und Tablets zur sicheren Anmeldung und übernehmen so die Rolle von Hardware-Token. Der Beitrag beschreibt die Möglichkeiten solcher Produkte.

Von Robert Korherr, ProSoft

Bring Your Own Device (BYOD) bedeutet für Unternehmen eine höhere Produktivität und damit einen deutlichen Mehrwert. Andererseits steht der Begriff aber auch für alle Risiken, die durch die Nutzung von mobilen Devices entstehen. Zu den Risiken gehören unter anderem gehackte Passwörter für den Zugriff auf Unternehmensdaten über Web- und Cloud-Services. In diesem Jahr gab es bereits zwei große Vorfälle, in denen digitale Identitäten in großem Umfang gehackt wurden. Besonders ernst zu nehmen sind gestohlene Zugangsdaten, die unbemerkt weiter genutzt werden. Davor schützt eine Zwei-Faktor-Authentifizierung, die Remote-Zugriffe durch einmalig gültige Zusatzfaktoren wie Einmalpasswörter oder biometrische Merkmale absichert. Diese Art der doppelten Authentisierung ist auch im Alltag verbreitet: Kein Bankkunde würde sich sicher fühlen, wenn beim Bankautomaten die EC-Karte alleine genügen würde, um Bargeld abzuheben. Hier sichert die PIN als Faktor „Wissen" den Vorgang zusätzlich ab.



Das OTP lässt sich situationsgerecht über einen App oder auch per SMS generieren.

Unternehmen vertrauen bei Fernzugriffen aber häufig noch auf statische Login-Daten, also auf das klassische Passwort allein. Wenn eine Zwei-Faktor-Authentifizierung im Einsatz ist, handelt es sich noch vielfach um traditionelle Hardware-Token. Mit dieser Methode wird ein kurzfristig gültiges Einmalpasswort, auch One Time Password (OTP) genannt, generiert, zeitlich mit dem Unternehmen synchronisiert und bei Remote-Logins abgefragt. Die Sicherheit dieser Lösungen ist aber fragwürdig, deren Einsatz eher kostspielig und für Anwender umständlich. Hersteller dieser Technologie geben beispielsweise zu, mit nationalen Geheimdiensten zu kooperieren. Die sogenannten „Seed-Records" wurden bei einem Hersteller bereits im Jahr 2011 gehackt und in der Folge von Dritten für Spionagezwecke genutzt.

BYOT – Bring Your Own Token

Neue Lösungen wie SecurAccess setzen daher bereits vorhandene Devices wie Mobiltelefone und Tablets zur sicheren Authentifizierung ein. Das OTP wird hierbei situationsgerecht vorab oder in Echtzeit per SMS versandt, über eine App generiert, ein QR-Code als Photo-OTP abfotografiert oder über ein Telefonanruf-Verfahren per Tastatur übermittelt. Diese „tokenlosen" Verfahren bieten Anwendern und Unternehmen deutliche Vorteile. So müssen keine zusätzlichen Hardware-Token angeschafft und verwaltet werden.

Auch kann der Anwender mehrere Möglichkeiten der Authentifizierung nutzen, sodass er sich je nach Lokation, Netzverfügbarkeit oder Gebührensituation entscheidet, welches Verfahren kostengünstig oder gerade optimal für ihn ist. Im besten Fall darf er sich selbstständig über ein Webportal ein Verfahren aussuchen. Befindet sich ein Mitarbeiter beispielsweise kurzfristig im Ausland, kann er über sein Webportal den OTP-Empfang von Echtzeit-SMS auf die Soft-Token-App umstellen und damit Roaming-Gebühren sparen. Das Unternehmen wiederum kann die erlaubten Verfahren vorgeben.

Die neuen Verfahren punkten zudem bei der Sicherheit gegenüber den traditionellen Hardware-Token. Zwei-Faktor-Authentifizierungen, bei denen der Hersteller wesentliche Daten zur Berechnung von Einmalpasswörtern speichert, sind grundsätzlich zu vermeiden. Die Sicherheit der Lösung liegt dann nicht mehr im unternehmenseigenen Zugriff und stellt damit ein Sicherheitsrisiko dar. Bei Lösungen wie SecurAccess ist daher der Zufallsgenerator für die OTP-Berechnung vom Hersteller nicht nachvollziehbar.

Einmalpasswörter sollten an die ursprüngliche Session-ID gebunden sein. Dies schützt vor Phishing-Fallen. Werden der Login und der OTP-Empfang beziehungsweise dessen Generierung auf unterschiedliche Endgeräte aufgeteilt, ist das Mitlesen der Daten durch einen Hacker deutlich schwerer. Der zweite Faktor als E-Mail ist also auch als Fallback-Option wenig sinnvoll. Aktivierte Zugriffsperren über PIN-Codes bei Smartphones oder Tablets erschweren den physischen Zugriff auf Einmalkennwörter zusätzlich.

Letztendlich ist eine „tokenlose" Zwei-Faktor-Authentifizierung über Einmalpasswörter ein optimaler Kompromiss zwischen Sicherheit und Kosten und schützt Fernzugriffe aller Art.