Die Zukunft der starken Authentifizierung

Zwei-Faktor-Authentifizierung ist ein Gebot der Sicherheit – aber herkömmliche Lösungen sind für den Nutzer «kompliziert». Vasco DIGIPASS SecureClick macht den sicheren Zugang zu Webdiensten per Knopfdruck zur Realität.

Der sichere Zugriff auf öffentliche und unternehmensinterne Webanwendungen erfordert eine starke Benutzerauthentifizierung mit mindestens zwei Sicherheitsmerkmalen auf unterschiedlichen Kanälen. Aus dem E-Banking kennt man etwa das mTAN-Verfahren, bei dem ein zusätzlicher Sicherheitscode via SMS aufs Mobiltelefon geschickt wird.

Solche Zwei-Faktor-Authentifizierungslösungen sind sicher, für den Nutzer aber unbequem: Für jeden Zugang ist ein eigenes Passwort nötig – die Vernunft gebietet, nicht überall das gleiche zu verwenden oder Passwörter schriftlich zu notieren. Und für den zweiten Sicherheitsfaktor muss ein Code mit einem separaten Gerät empfangen und manuell in die Zielanwendung übertragen werden. Traditionell handelt es sich zudem um proprietäre Lösungen, die individuell in die Anwendungen integriert werden müssen.

DIGIPASS SecureClick von VASCO kommuniziert via Bluetooth Low Energy (BLE) drahtlos mit jedem BLE-fähigen Endgerät und ermöglicht mit einem Klick eine starke Authentifizierung.

Standard für bequeme Zwei-Faktor-Authentifizierung

Mit dem Ziel, einen Standard für eine allgemein anwendbare Zwei-Faktor-Authentifizierung zu schaffen, entwickelte Google zusammen mit Partnern die U2F-Spezifikation (Universal Second Factor). U2F dient dem Nachweis der Zugriffsberechtigung für beliebig viele webbasierte Dienste und verbindet hohe Sicherheit mit bequemer Bedienung und unmittelbarem Zugang. Eine zweite Spezifikation namens UAF (Universal Authentication Framework) beschreibt das Netzwerkprotokoll zur passwortlosen Authentifizierung.

Zusammen bilden beide Spezifikationen den FIDO-Standard, der im Dezember 2014 in Version 1.0 verabschiedet und seither von der Industrieallianz FIDO (Fast IDentity Online) vorangetrieben wird. FIDO-konforme Webdienste ersparen es den Nutzern, sich unzählige komplizierte Passwörter zu merken. Für den gesicherten und sofortigen Zugang zu einem Webdienst nutzt FIDO ein bei der Registrierung generiertes Schlüsselpaar, wobei der private Schlüssel auf dem Gerät des Nutzers verschlüsselt gespeichert und bei jeder Anmeldung mithilfe eines Sicherheitstokens oder biometrischen Verfahrens freigegeben wird.

Aktuell bieten die meisten Google-Dienste sowie Dropbox, GitHub, OpenSSH und Wordpress U2F-Unterstützung, und FIDO-basierte Lösungen lassen sich einfach in Unternehmensanwendungen integrieren.

Zugriff mit einem Klick

In der ersten Generation kamen FIDO-konforme Sicherheitstokens als USB-Dongles daher, die sich in erster Linie für Desktops und Notebooks eignen. Mit DIGIPASS SecureClick stellt Vasco jetzt eine moderne Generation vor, die via Bluetooth Low Energy (BLE) drahtlos und verschlüsselt mit dem Computer, Tablet oder Smartphone kommuniziert. DIGIPASS SecureClick funktioniert sofort mit jedem BLE-fähigen Endgerät: Für die Authentifizierung genügt – nach der Eingabe des für alle Dienste identischen Passworts – ein Klick auf den «Go»-Button.

Das kreisrunde Sicherheitstoken in Form eines eleganten Schlüsselanhängers misst 25 mm im Durchmesser und ist 3,9 mm dünn. Die auswechselbare CR2012-Batterie reicht bei 10 Anmeldungen pro Tag für mehr als zwei Jahre. Für kundenspezifische Anwendungen lässt sich das Token mit Logo und Farben der Firmenidentität anpassen. Für Geräte ohne BLE-Unterstützung ist von Vasco ein USB-Dongle mit SecureClick-Funktion erhältlich.

VASCO

Vasco gehört zu den Weltmarktführern bei Authentifizierung, digitaler Unterschrift und Identitätsmanagement und liefert jeden Tag über 100 000 Sicherheitstokens aus. Die Lösungen von Vasco kennt das Publikum vor allem vom E-Banking her, zum Beispiel CrontoSign: Dabei wird ein grafisches Kryptogramm aus Farbpunkten mit der Smartphone-Kamera eingescannt und darauf ein Einmalpasswort generiert. Auch der bekannte gelbe PostFinance-Kartenleser stammt von Vasco.

Vasco DIGIPASS SecureClick: die Highlights

- Starke Authentifizierung mit einem Klick
- Sofortiger Zugang
- Ein einziges Passwort für alle unterstützten Webdienste
- FIDO-konformes BLE-Device
- BLE-Dongle für ältere PCs mitgeliefert
- Batterie reicht für zwei Jahre (auswechselbar)
- In Form eines eleganten Schlüsselanhängers

BOLL
IT Security Distribution

BOLL ENGINEERING AG

Jurastrasse 58
5430 Wettingen

Tel. 056 437 60 60,
info@boll.ch
www.boll.ch