Passwortlose Authentisierung in Klein- und Mittelbetrieben

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Gerhard Hassenstein
Experte: Dr. Igor Metz (GLUE Software Engineering AG)

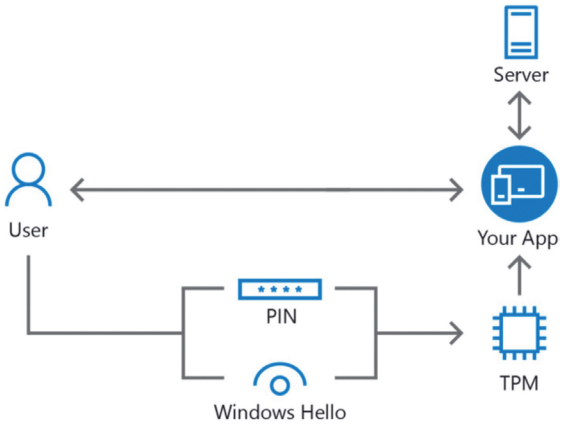
Die Verwendung eines Benutzernamens kombiniert mit einem Passwort ist seit geraumer Zeit als Authentisierungsmittel etabliert. Die Sicherheitsrisiken bei Verwendung und auch der serverseitigen Speicherung von Passwörtern sind weitgehend bekannt. Das Zurücksetzen wie auch die Verwendung von zu einfachen Passwörtern verursachen in Unternehmen hohe finanzielle Schäden.

Einleitung

Die Authentisierung mittels Benutzernamen und Passwort wird bei Microsoft vor allem seit der Veröffentlichung von Windows 10 weiterführend behandelt. Das, mit dem Namen «Windows Hello», enthaltene Funktionspaket bietet den Benutzern die Authentisierung am eigenen Gerät mittels PIN oder biometrischen Merkmalen wie Fingerabdruck oder Iris. Die erfassten Daten bleiben lokal auf dem Gerät des Benutzers gespeichert und werden nicht auf Serverdienste weiterverarbeitet.
Zuständig für die sichere Ablage der Daten ist das Trusted Platform Module (TPM). Die Verwendung von biometrischen Merkmalen unter Windows Hello sowie die Sicherheitsvorkehrungen eines TPM erschaffen ein weitaus sichereres Authentisierungssystem als die Verwendung von Benutzernamen und Passwort.

Passwortlose Authentisierung

Als Erweiterung von «Windows Hello» stellt Microsoft für den Einsatz in einem Unternehmen «Windows Hello for Business» zur Verfügung. Ergänzt werden die Funktionen in Windows 10 mit Server- und Clouddienste zur Verwaltung und Überwachung der Authentisierung. Microsoft gibt für die Umsetzung von «Windows Hello for Business» die drei nachfolgenden Szenarien vor:



Authentisierung mit Windows Hello (Quelle: docs.microsoft.com)

Cloud

Die eingesetzten Dienste befinden sich ausschliesslich in der Cloud.

Hybrid

In einer Hybrid-Lösung werden Dienste sowohl in der Cloud bezogen, wie auch On-Premises betrieben.

On-Premises

Im On-Premises-Ansatz befinden sich die eingesetzten Dienste ausschliesslich intern im Unternehmen. Die Geräte der Benutzer sind Teil der lokalen Domäne. Sowohl beim hybriden wie auch beim On-Premises-Szenario wird zwischen einem schlüsselbasierenden (Key-Trust) und einem zertifikatsbasierenden (Certificate-Trust) Ansatz unterschieden. Beide Ansätze unterscheiden sich nur durch eingesetzte Serverkomponenten. Die gewährleistete Sicherheit bleibt in beiden Ansätzen jedoch gleich.

Bring your own Device (BYOD)

Bei Bring your own Device (BYOD) handelt es sich um private Geräte, die der Benutzer sowohl für den Zugriff auf private wie auch auf Daten seines Unternehmens verwendet. Solche Geräte sind kommerziell erhältlich. Der Zugriff auf geschäftliche Daten bringt Sicherheitsrisiken mit sich. Der Schutz der Daten sowie die Steuerung des Zugriffes ist bei der Freigabe von BYOD zentral. Microsoft ist bestrebt in Windows 10 zusammen mit den Geräteverwaltungsdiensten die Zugriffe auf sensible Daten zu kontrollieren und einzuschränken.

Ergebnis

Der Informationsgehalt zur passwortlosen Authentisierung mittels «Windows Hello for Business» ist gross. Sobald es aber an die Umsetzung geht, bleibt es eher oberflächlich. Die langsame Vorangehensweise bei der Standardisierung beteiligter Standards setzt hinter die passwortlose Authentisierung heute noch ein Fragezeichen. Die angekündigten Erweiterungen seitens Microsoft sowie eine mögliche nahtlose Integration von Diensten und Webseiten, lassen aber spannende Grundgedanken für die Zukunft offen.

Fabian Hutzli