Intel stellt eigenen Passwortmanager vor

Intel Security (ehemals McAfee) hat einen Passwortmanager vorgestellt, der schwer merkbare Passwörter durch biometrische Merkmale ablösen soll. Momentan befindet sich True Key noch in der Entwicklung. Interessenten können sich auf eine Warteliste setzen lassen, um den Dienst vor dem offiziellen Start auszuprobieren.

True Key funktioniert Hand in Hand mit einem Cloud-Speicher, dem man seine Zugangsdaten anvertrauen muss. Als Masterpasswort dienen Merkmale wie ein Fingerabdruck oder ein Webcam-Schnappschuss – hat man sich auf diese Weise gegenüber der App authentifiziert, übernimmt TrueKey das Ausfüllen von Login-Formularen. Man soll den Cloud-Speicher aber auch durch weitere Faktoren absichern können. Intel führt als Beispiel das Smartphone auf: Ist es mit dem True-Key-Account verknüpft, muss der Nutzer beim Zugriffsversuch über das Display streichen. So wäre sichergestellt, dass die Person, die sich gerade einzuloggen versucht, auch Zugriff auf das Handy des legitimen Account-Inhabers hat. Wer will, kann auch ein Masterpasswort als einen der Faktoren nutzen. Laut Intel wird die Passwortdatenbank lokal mit AES-256 verschlüsselt, ehe sie in die Cloud wandert. Der Hersteller gibt an, keine Möglichkeit zu haben, die Daten zu entschlüsseln.

True Key unterstützt Windows, OS X, Android und iOS. Das Speichern von bis zu 15 Passwörtern ist gratis; wer mehr Speicherplatz benötigt, soll ihn sich „verdienen“ können – vermutlich ist damit ein Empfehlungssystem gemeint, wie es auch Dropbox betreibt. Darüber hinaus will Intel einen Premium-Zugang für 20 US-Dollar im Jahr anbieten. (rei)

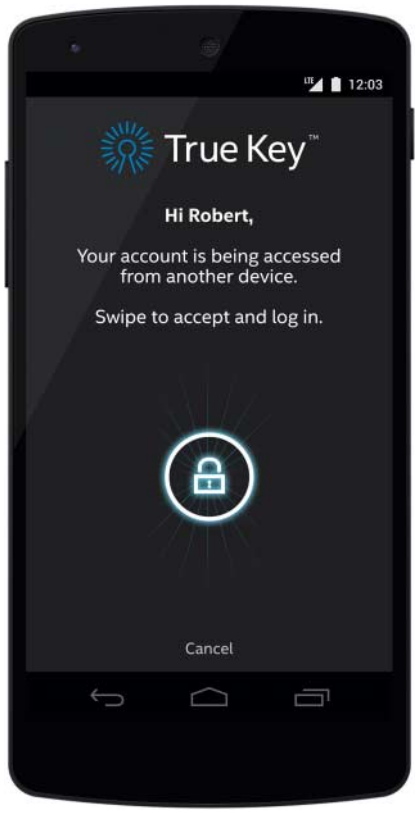

Bild: Intel

True Key setzt auf Mehrfaktor-Authentifizierung. Auf Wunsch fragt der Passwortmanager per Handy bei jedem Login nach.

BSI-Präsident fordert Zwangstrennung für infizierte Rechner

Unternehmen in Deutschland müssen nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ihre Anstrengungen für die digitale Sicherheit deutlich verstärken. Trotz einer erheblichen Bedrohung gebe es eine „digitale Sorglosigkeit“, so BSI-Präsident Michael Hange. Seiner Einschätzung nach sind bis zu einer Milliarde Schadprogramme weltweit im Umlauf, vor allem für Windows-PCs.

Hange setzte sich auf dem Berliner Forum zu Cyber-Sicherheit dafür ein, mit Trojanern und anderen Schadprogrammen infizierte Rechner zwangsweise durch die Internet-Provider vom Netz zu nehmen. In Deutschland seien rund eine Million PCs Bestandteil von sogenannten Bot-Netzen, die von Computer-Kriminellen mithilfe von Viren und Trojanern aufgebaut wurden und oft für fadenscheinige Zwecke verwendet werden. Häufig ignorierten die Besitzer der infizierten PCs Warnhinweise der Provider, wenn beispielsweise von ihren Rechnern aus Attacken auf andere Rechner im Netz laufen. (axk/fab)

Google veröffentlicht Zeroday-Lücken und erzürnt Microsoft

Googles Sicherheitsteam hat mehrere bisher unbekannte Sicherheitslücken in Windows veröffentlicht. Das Timing der Veröffentlichungen erzürnte Microsoft, da Google eine Lücke zwei Tage vor dem Januar-Patchday offengelegt hatte. Sein Unternehmen sei kurz davor gewesen, die Lücken zu schließen, klagte ein hochrangiger Mitarbeiter von Microsofts Security Response Center. Microsoft hatte einen weiteren Patch wegen Kompatibilitätsgründen auf den Februar-Patchday verschoben und Google informiert, aber auch diese Sicherheitslücke legte Google offen.

Microsoft wünscht sich, dass Sicherheitsforscher die Details zu Lücken erst herausgeben, wenn ein Patch allgemein verfügbar ist. Google hingegen gibt anderen Firmen routinemäßig genau 90 Tage Zeit, einen Patch zu entwickeln – dann wird die Lücke automatisch offengelegt. (fab)

HTTP-Header als Supercookie

Eigentlich soll der HSTS-Header dazu dienen, Lauschangriffe auf HTTPS-Verbindungen zu vereiteln. Jetzt hat ein Sicherheitsforscher allerdings gezeigt, wie Tracking-Firmen diese Schutzfunktion missbrauchen können, um das Nutzerverhalten im Netz zu überwachen.

HTTP Strict Transport Security (HSTS) verhindert, dass Nutzer eine gesicherte Webseite wie https://paypal.com über eine ungesicherte Verbindung wie http://paypal.com aufrufen. Dann merkt sich der Browser, dass ein Server grundsätzlich nur über gesichertes HTTPS kommuniziert. So kann auch ein Angreifer den Nutzer nicht auf die ungesicherte URL umleiten und dann den Datenverkehr mitschreiben. Leider lässt sich das aber auch gegen den Nutzer wenden. Um eine Art Supercookie zu erzeugen, füttert ein Server den Browser mit HSTS-Werten für bestimmte Subdomains. Beim nächsten Besuch kann er testen, für welche Subdomains der Browser HSTS aktiviert hat und den Besucher wiedererkennen.

Während das HSTS-Supercookie momentan ein rein akademischer Angriff ist, der noch nicht aktiv ausgenutzt wird, erfreuen sich andere unlöschbare Cookies reger Beliebtheit. So schiebt zum Beispiel der US-Mobilfunkanbieter Verizon seinen Kunden standardmäßig bei sämtlichen Web-Anfragen zusätzliche HTTP-Header unter. Damit sind die Kunden eindeutig identifizierbar, und zwar nicht nur durch Verizon selbst, sondern durch alle Unternehmen, die den Header auslesen (siehe S. 50). (fab)

c't HSTS-Supercookies im Detail: ct.de/yz4f

Sicherheits-Notizen

Momentan versenden Unbekannte verstärkt Schadcode per E-Mail, der über Microsoft-Office-Makros ausgeführt wird. Die **Macro-Trojaner** fordern Nutzer auf, die Funktionen zum Ausführen von Makros in Word oder Excel zu aktivieren – bleiben diese deaktiviert, ist der Angriff wirkungslos.

Microsoft hat den Mainstream-Support von **Windows 7** eingestellt. Für die kommenden fünf Jahre liefert die Firma allerdings weiterhin Sicherheits-Updates.

Androids **WebView** hat gravierende Sicherheitslücken, die laut Google nicht mehr geschlossen werden sollen. Betroffen sind alle Geräte bis einschließlich Android 4.3, die noch den alten Standard-Browser des Betriebssystems nutzen.