Image-Backup für APFS

Acronis hat die Mac-Variante seiner Backup-Software namens True Image Ende November in der Fassung 22.5 herausgebracht. Unter den diversen kleinen Neuigkeiten sticht hervor, dass True Image nun Partitionen von APFS-basierten Systemen ohne Behelfs-Skripte wiederherstellen kann.

Für Cloud-Backups auf Datei-Ebene gibt es eine neue Nonstop-Backup-Planungseinstellung und eine neue Standardeinstellung verhindert, dass ein Computer in den Energiesparmodus geht, während ein Mobilgerät (iOS oder Android) Backup-Daten zu ihm sendet (dafür sind separate Smartphone-Apps erforderlich). Acronis True Image für macOS ist in Varianten mit und ohne Cloud-Funktionen ab 50 Euro erhältlich und setzt mindestens macOS 10.10 voraus (Yosemite), spielt aber auch mit dem aktuellen 10.13 (High Sierra). Außerdem eignet es sich für die Dateisysteme APFS, HFS+, FAT32, exFAT und mit kleinen Einschränkungen auch für NTFS. *(dz@ct.de)*

Sichert nicht nur APFS und diverse weitere Partitionen auf dem Mac, sondern nimmt auch Backups von Smartphones entgegen: Acronis True Image für macOS.

Apple Watch misst Herzrhythmus

Apple und die Universität Stanford untersuchen zusammen, wie zuverlässig sich Vorhofflimmern allein mit dem Pulssensor der Apple Watch erkennen lässt. Belege dafür hatte zuvor schon die University of California in San Francisco in einer eigenen Studie geliefert. Vorhofflimmern verursache häufig Blutgerinnsel und Schlaganfälle und in den USA jedes Jahr rund 130.000 Todesfälle, schreibt Apple. Außerdem betreffe Vorhofflimmern Millionen von Menschen, von denen jedoch viele keine Symptome spüren, sodass die Erkrankung oft undiagnostiziert und somit unbehandelt bleibt.

Die Apple Watch misst den Blutdurchfluss fortlaufend am Handgelenk. Aus den durch den Herzschlag resultierenden Schwankungen leitet die Uhr zunächst nur den Puls ab. In der Studie setzen die Forscher zusätzliche Algorithmen ein, um daraus den Herzrhythmus zu ermitteln.

Dazu erfasst die „Apple Heart Study"-App die Daten und sendet sie zur Auswertung an Apple und die Universität. Teilnehmer erhalten bei Unregelmäßigkeiten einen Warnhinweis und können einen an der Studie beteiligten Arzt konsultieren.

Die Studie läuft zurzeit nur in den USA. Teilnehmer müssen mindestens 22 Jahre alt sein und eine Apple Watch ab dem Modell Series 1 besitzen. Die allererste Generation der Computer-Uhr eignet sich nicht für den Zweck. In dieselbe Richtung zielt das seit 2016 in Deutschland erhältliche Apple-Watch-Armband „Kardia Band". Es kostet 230 Euro und nimmt ein komplettes EKG auf, das sich etwa als PDF-Datei exportieren lässt. *(dz@ct.de)*

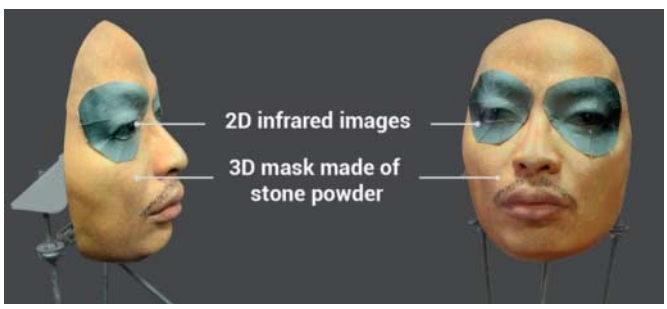
Face-ID-Überlistung lässt Fragen offen

Die Sicherheitsfirma Bkav hat eine Methode vorgestellt, die Apples im iPhone X verwendete Gesichtserkennungstechnik Face ID überlisten soll. Face ID soll nur dem Nutzer den Zugang zum iPhone X gewähren, dessen Gesicht es zweifelsfrei identifiziert.

Die Firma Bkav hatte bereits kurz nach Erscheinen des iPhone X von ersten erfolgreichen Versuchen berichtet, die Face-ID-Authentifizierung mit einer Maske zu überwinden, die dem Nutzer ähnlich sieht. Die Prozedur dauerte rund neun bis zehn Stunden, wie die Sicherheitsforscher später einräumten. Bkav warnte, dass besonders gefährdete Personen wie Spitzenpolitiker auf Face ID verzichten sollten.

Nun hat Bkav die Warnung auf alle iPhone-X-Nutzer ausgeweitet, denn mit dem neuen Verfahren lasse sich ein iPhone X sofort entsperren. Bkav zeigt die Methode in einem Video und erklärt, dass es sehr simpel sei, eine solche Maske anzufertigen. Sie setzt lediglich eine Handvoll Fotos aus bestimmten Winkeln voraus, die zu einem 3D-Modell zusammengesetzt werden. Die Kosten für den 3D-Druck belaufen sich auf rund 200 US-Dollar. Bkav verwendet unter anderem Steinmehl, das Face ID besser austricksen soll als das in der ersten Maske verwendete Papierklebeband.

Wie gravierend die Face-ID-Schwäche ist, bleibt zunächst jedoch unklar, denn die maximale Zuverlässigkeit erreicht Face ID erst nach einer Trainingsphase – welche die Sicherheitsforscher aber weggelassen haben. Stattdessen attackierten sie die Zugangstechnik gleich nach der erstmaligen Einrichtung. Dennoch sollte man Face ID bis auf Weiteres möglichst nicht in sicherheitskritischem Umfeld verwenden und stattdessen nur die Passwortauthentifizierung nutzen. *(dz@ct.de)*



Sicherheitsforscher haben Apples Face-ID-Technik zwar geknackt, aber noch ist offen, wie gravierend die Methode in der Praxis ist.