# Wenn das Handy den Körper analysiert: Von der Gesichtserkennung bis zum Iris-Scanner

Veröffentlicht am 14.04.2018 von EpochTimes

**Experten warnen davor, dass die 2D-Gesichtserkennung leicht überlistet werden kann. So reicht ein Bild, egal ob ausgedruckt oder digital, um das System auszutricksen.**

Fingerabdruck, Gesichtserkennung, Iris-Scanner: Heutzutage lassen sich Handys und Tablets nicht nur mit PIN oder Passwort entsperren. Wie funktionieren die Methoden – und wie sicher sie?

### ► Der Fingerabdruck

Es gibt halbautomatische Scanner, bei denen die Fingerkuppe über eine Fläche gezogen werden muss, und automatische, bei denen das Auflegen reicht. Die Strukturen der Fingerkuppe werden dann über Sensoren abgetastet und mit dem gespeicherten Abbild verglichen. Stimmt alles überein, wird das Gerät entsperrt. Da Fingerabdrücke einzigartig sind, ist es schwer, diese Methode zu überlisten, erklärt das Portal Teltarif.

*Klotzkopf: Ein sogenannter Cosplayer ist bei der Spielemesse Gamescom völlig in sein Handy vetieft.*
Foto: Marius Becker/dpa

Mit großem Aufwand geht es aber: So verschafften Experten sich Zugang zu einem Smartphone, indem sie einen Fingerabdruck von einer Glasoberfläche abfotografierten, bearbeiteten und auf eine Folie druckten. Dann wurde das Imitat mit Holzkleber oder Latexmilch bestrichen, die von Maskenbildnern benutzt wird, und angefeuchtet. Diese Imitation eines Fingers reichte, um das Gerät zu überlisten.

Andere Experten erstellten aus 800 Fingerabdrücken rund 8.200 Teilabdrücke. Ähnlich wie bei Codes wurden dann verschiedene Kombinationen probiert, bis sich der Scanner überlisten ließ.

### ► Die Gesichtserkennung

Bei der Gesichtserkennung wird die Frontkamera des Geräts benötigt, es werden die 2D-Erkennung und die sicherere 3D-Erkennung unterschieden. Bei beiden Verfahren wird das Gesicht des Nutzers nach ovalen Formen, Farben und geometrischen Anordnungen analysiert, etwa dem Abstand der Augen.

Das 3D-System tastet das Gesicht dreidimensional ab. Stimmen die registrierten Ebenen mit dem Referenzfoto überein, klappt das Entsperren.

Experten warnen davor, dass die 2D-Gesichtserkennung leicht überlistet werden kann. So reicht ein Bild, egal ob ausgedruckt oder digital, um das System auszutricksen; das gilt auch für neuere Kameras.

Die 3D-Gesichtserkennung bietet deutlich mehr Sicherheit. Hier benötigten Sicherheitsexperten zum Knacken der Sperrung einen 3D-Drucker, mit dem sie eine Maske des Nutzers erstellten, außerdem brachten sie unterschiedliche Perspektiven der Augen an der Maske an.

**► Der Iris-Scanner**

Auch die Iris eines Menschen ist einzigartig, deshalb eignet sie sich gut zur Identifizierung. Um sie zu erkennen, scannt die Kamera unterstützt von Infrarotlicht rund 260 optische Eigenschaften und Muster der Regenbogenhaut. Allerdings funktioniert die Erkennung bei Brillenträgern nicht so gut wie ohne Brille.

Dafür ist die Iris-Erkennung nicht so leicht zu knacken wie die Gesichtserkennung. Ein Foto reicht nicht aus, um das System zu überlisten, weil plastische Informationen des Auges nötig sind.

Austricksen konnten Experten die Iris-Erkennung nur mit einem hochauflösenden Bild, das in eine Kontaktlinse eingebettet wurde.

**► Das Passwort als Alternative**

Den besten Schutz bietet derzeit die 3D-Gesichtserkennung, wie die Experten von Teltarif betonen. Als unsicher gilt die 2D-Gesichtserkennung. Der Fingerabdruck und der Iris-Scanner liegen im Mittelfeld.

Wer das alles nicht möchte oder nicht bezahlen will, sollte zum Entsperren des Bildschirms auf ein gut durchdachtes Passwort zurückgreifen – und dabei gängige Wörter und Namen vermeiden.

(afp)