Europas größtes IT- und Tech-Magazin

c't magazin für computer technik

27.3.2021 8

Vergleichstest
High-End-Kopfhörer

Test: WhatsApp vs. Signal, Threema, Telegram …

Jetzt weg von WhatsApp

Verschlüsselung, Umstiegshilfe, Datenschutz

IM TEST

- SSDs mit PCIe 3.0 und 4.0
- Fotohandys versus Kamera
- Günstige Allround-PCs fürs Homeoffice
- DJI-Drohne für Video und Racing

Ängste, Depression, Schlafstörung

Apps für die Psyche

Praxis: Maximaler Datenschutz

MS Office ohne Cloud

Exchange-Angriff: Microsofts Versagen
Windows-Spiele unter Linux
Switches für Kleinbüros und Zuhause
Günstige Prepaid-Tarife fürs Handy

€ 5,50
AT € 6,10 | LUX, BEL € 6,50
NL € 6,70 | IT, ES € 6,90
CHF 8.10 | DKK 60,00

Praxiseinstieg in Low Code und No Code

Programmieren ohne Code

Workflows automatisieren, Projekte im Team organisieren

4 199748 405504 08

Reiner Schutz

2FA-Generator Reiner SCT Authenticator

Der Reiner SCT Authenticator sichert Online-Accounts als zweiter Faktor ab. Das ist komfortabler und leichter verständlich als per Smartphone-App.

Von Ronald Eikenberg

Ein zweiter Faktor ist das Beste, was Ihren Online-Accounts passieren kann: Haben Sie die Zwei-Faktor-Authentifizierung (2FA) aktiviert, dann ist Ihr Account auch dann noch geschützt, wenn ein Hacker Ihr Passwort kennt. Der zweite Faktor ist zum Beispiel ein Einmalcode, den Ihnen der Dienst per SMS zuschickt oder den eine Authenticator-App generiert. Das Einloggen gelingt mit 2FA nur dann, wenn sowohl das Passwort als auch der aktuell gültige Einmalcode stimmen. Damit der Schutz wirksam ist, darf der Hacker nicht die Chance bekommen, den Einmalcode abzurufen oder zu generieren.

Würde der Code-Generator einfach nur als Software auf dem Rechner laufen, mit dem Sie sich einloggen, könnte ein Trojaner nicht nur das eingetippte Passwort, sondern auch den Code-Generator mit allen Geheimnissen abgreifen. Daher ist es sinnvoll, den Code mit einer separaten Hardware zu generieren. Das kann im einfachsten Fall das Smartphone mit Authenticator-App sein, aber auch ein USB-Stick wie ein YubiKey.

Der deutsche Kartenleser-Hersteller Reiner SCT bietet nun auch eine dritte Option an, die bei näherer Betrachtung durchaus sinnvoll ist: Der Reiner SCT Authenticator ist ein autarkes Gerät mit Zifferntastatur und Farbdisplay. Er besitzt keine Schnittstellen zur Außenwelt. Somit ist gewährleistet, dass ein Trojaner, der eventuell auf ihrem Rechner oder Smartphone lauert, keinen Zugriff darauf hat und keine Einmalcodes generieren kann.

Der Authenticator arbeitet nach dem zeitbasierten TOTP-Verfahren (Time-based One-time Password), das die meisten Online-Dienste unterstützen, die Zwei-Faktor-Authentifizierung anbieten, darunter Google, Facebook und Twitter. Das Gerät ist mit einem Display und einer Zifferntastatur ausgestattet und erinnert äußerlich an einen Taschenrechner. Neue Accounts fügt man jedoch nicht umständlich über die Zifferntasten hinzu, sondern über die kleine Kamera auf der Rückseite: Sie scannt das für TOTP nötige Krypto-Geheimn is einfach als QR-Code vom Webdienst.

PIN-Sperre mit Selbstzerstörung

Nach dem Einschalten drückt man zwei Mal auf den OK-Knopf, um das Gerät in den Scanmodus zu versetzen und den Code zu scannen. Das hat im Test zuverlässig funktioniert, das Scannen dauerte lediglich eine Sekunde. Anschließend generiert der Authenticator einen passenden TOTP-Code, wenn man den gewünschten Account in der Liste auswählt. Der Zugriff lässt sich durch eine bis zu 12-stellige PIN

Reiner SCT Authenticator

OTP-Generator	
Hersteller	Reiner SCT, www.reiner-sct.de
Anschlüsse	–
OTP-Verfahren / Accounts	OATH-TOTP (SHA 1, SHA 256, SHA 512) / 60
Display / Auflösung	1,77"-TFT / 128 × 160 Pixel
Größe / Gewicht	102 mm × 62,5 mm × 19 mm / 80 g
Stromversorgung	4 × AAA-Batterien
Preis	40 €

Auf der Rückseite des Authenticators befindet sich eine Kamera, mit der man QR-Codes fotografiert. So kann man Online-Accounts leicht mit dem Gerät verknüpfen.

schützen. Ist der PIN-Schutz aktiv, führt das Gerät nach fünf Fehlversuchen einen Reset auf Werkseinstellungen durch.

Damit ist der Funktionsumfang auch schon fast erzählt. Über das zweckmäßige Menü kann man die PIN-Sperre konfigurieren, Account-Einträge umsortieren und löschen sowie Batteriestatus und Seriennummer abfragen. Hier lässt sich zudem eine Komfortansicht aktivieren, die sich jedoch kaum von der Standardansicht unterscheidet. Der Authenticator ist mit einer Uhr ausgestattet, die er benötigt, um die zeitbasierten OTP-Codes zu erzeugen. Sie kann über das Menü oder das Scannen eines QR-Codes gestellt werden. Eine Pufferbatterie sorgt dafür, dass man sich circa eine Minute mit dem Wechseln der vier AAA-Batterien Zeit lassen kann, ohne dass die eingestellte Uhrzeit verloren geht. Laut Hersteller halten die Batterien fünf Jahre, wenn pro Jahr 500 TOTP-Codes generiert werden.

Firmware-Update über YouTube

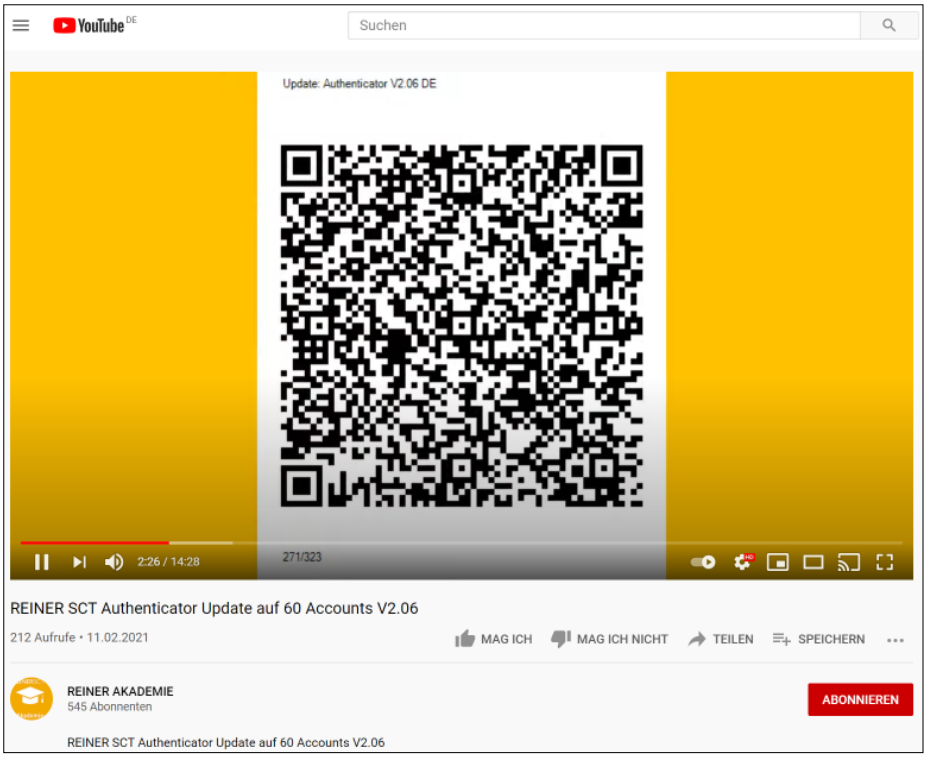
Ursprünglich konnte sich der Reiner SCT Authenticator lediglich zehn Accounts merken, inzwischen hat der Hersteller jedoch mit der neuen Firmware-Version 2.06 auf 60 aufgestockt. Wer das Gerät mit der alten Firmware gekauft hat, kann das Update nachträglich installieren – das ist ziemlich interessant, weil der Authenticator keine der üblichen Datenschnittstellen wie USB hat. Der Hersteller hat dieses Problem kreativ gelöst: Das Update erfolgt per YouTube-Video. Im Video flimmern einige Minuten QR-Codes über den Bildschirm, in die das Firmware-Update kodiert ist. Versetzt man den Authenticator in den Scan-Modus und filmt den Bildschirm einige Minuten ab, während im Hintergrund beruhigende Musik läuft, ist das Gerät anschließend auf dem aktuellen Firmware-Stand. Das klingt seltsam, funktioniert aber. Der Hersteller empfiehlt, das Video mit der 360p-Auflösung abzuspielen, damit das Update reibungslos über die Bühne geht.

Im Alltagstest hat sich der Authenticator erstaunlich gut bewährt. Liegt das quietschgelbe Gerät neben der Tastatur, hat man den geforderten TOTP-Code schnell parat. Das geht schneller von der Hand, als etwa das Smartphone aus der Hosentasche zu ziehen, zu entsperren und den Google Authenticator zu starten. Wer bereits eine Authenticator-App mit allen Accounts eingerichtet hat, kann diese mit etwas Glück schnell auf den Reiner Authenticator übertragen: Mit der Android-App andOTP konnten wir einfach QR-Codes zu den hinterlegten Accounts anzeigen lassen, die sich mit dem Reiner-Gerät einlesen ließen. Der bei andOTP eingestellte „Aussteller“ wurde anschließend auf dem Reiner Authenticator als Dienstname angezeigt. Mit dem Google Authenticator klappte der Export jedoch nicht, das Gerät wusste mit den angezeigten QR-Codes nichts anzufangen. Es ist problemlos möglich, den von einem Webdienst angezeigten QR-Code mit mehreren Authentifikatoren zu scannen und das Reiner-Gerät parallel mit einer App zu nutzen.

Fazit

Die Zwei-Faktor-Authentifizierung ist mit dem Reiner SCT Authenticator zugänglicher als per Smartphone-App oder USB-Stick. Durch seinen reduzierten Funktionsumfang ist das Gerät intuitiv bedienbar, die Nutzung hat Parallelen zu TAN-Verfahren beim Online-Banking. Damit ist es auch für Personen verständlich, die mit der Nutzung einer Authenticator-App überfordert wären. *(rei@ct.de)* c't

Produktseite, Update-Video: ***ct.de/y3k8***



Ungewöhnlich, aber effektiv: Der Reiner-Authenticator zieht sein Firmware-Update, indem er ein YouTube-Video abfilmt. Die Update-Daten sind in die flimmernden QR-Codes kodiert.