# WPA3 ist fertig: Neuer WLAN-Standard löst nervige Probleme

Eine gravierende Sicherheitslücke in der WLAN-Verschlüsselung WPA2 schreckte im vergangenen Herbst die Anwender auf. Jetzt gibt es den Nachfolger: Die Wi-Fi Alliance hat damit begonnen, erste Geräte gemäß WPA3 zu zertifizieren.
Ein neues Protokoll für die Verschlüsselung von drahtlosen Datennetzwerken soll die Sicherheit in WLANs deutlich erhöhen. Das Firmenkonsortium Wi-Fi Alliance, das Geräte mit Funkschnittstellen zertifiziert, hat nun offiziell damit begonnen, Geräte mit dem WPA3-Standard auszuzeichnen. Die Technologie war Anfang des Jahres auf der Technikmesse CES in Las Vegas vorgestellt worden. WPA3 soll WLANs nicht nur sicherer machen, sondern auch den Umgang mit ihnen vereinfachen.
In dem neuen Standard wurden vier neue Funktionen definiert. WPA3 soll erstens einen robusten Schutz bieten, selbst wenn Benutzer einfache Passwörter wählen, die den typischen Empfehlungen von Sicherheitsexperten nicht entsprechen. Zweitens soll der Prozess der Konfiguration der Sicherheit für Geräte vereinfacht werden, die über keinen Bildschirm verfügen. Ein weiteres Feature soll die Privatsphäre der Nutzer in offenen Netzwerken durch eine individualisierte Datenverschlüsselung stärken.
Schließlich soll WPA3 ermöglichen, Wi-Fi-Netzwerke auch in Bereichen zu betreiben, in den erhöhte Sicherheitsanforderungen bestehen, etwa bei Regierungseinrichtungen, dem Militär oder in sensiblen Bereichen in Unternehmen. Geräte, die das neue Protokoll WPA3 unterstützen, sollen noch 2018 auf den Markt kommen. Bis WPA3 in neuen Geräten zum Standard wird, wird es aber bis mindestens 2019 dauern. Flächendeckend wird WPA3 erst in einigen Jahren eingesetzt werden.

## WPA3 - Die Antwort auf die "Krack"-Sicherheitslücke

Neues Verschlüsselungsprotokoll WPA3 soll WLANs sicherer machen. Bild: Andrea Warnecke/dpa
Im vergangenen Herbst hatte eine vom belgischen Sicherheitsforscher Mathy Vanhoef entdeckte Sicherheitslücke im Vorgängerprotokoll WPA2 das Thema der Sicherheit in WLANs in den Blick der Öffentlichkeit gerückt. Inzwischen haben zwar etliche Hersteller die "Krack"-Sicherheitslücke geschlossen, etliche betroffene Geräte werden aber wohl niemals ein Update bekommen. Bei dem "Krack"-Angriff war es möglich, die WLAN-Verschlüsselung auszuhebeln und damit den Datenverkehr in einem WLAN zu belauschen und zu manipulieren.