

WLAN GEHACKT – WAS TUN?

Trotz aller Vorsicht kann es passieren, dass sich Hacker Zugriff auf Ihr Heimnetzwerk verschaffen. Das bedeutet aber nicht, dass Sie deren Tun hilflos ausgeliefert sind. So werden Sie unberechtigte WLAN-Gäste wieder los.

Was bedeutet es, wenn das heimische WLAN "gehackt" ist?

Ein System oder Netzwerk gilt als gehackt, wenn sich ein Unberechtigter Zutritt dazu verschafft hat. Im Falle Ihres heimischen WLANs würde das also bedeuten, dass jemand, dem Sie keine Zugangsdaten dafür gegeben haben, Ihr WLAN nutzt.

Je nachdem, welche Schutzmaßnahmen Sie vorher angewandt haben, kann das einfacher oder schwerer sein. Haben Sie ein unsicheres Passwort, können Hacker das mit simplen Algorithmen knacken, die etwa alle Wörter aus dem Duden mit oder ohne Zahlenkombinationen durchprobieren. Wie immer jemand Ihr WLAN knackt, er kann darin dann alles machen, was auch Sie tun können – also etwa auf alle angeschlossenen Computer und Geräte zugreifen und die je nach Fernzugriffsmöglichkeiten steuern.

Wie merke ich, dass jemand mein WLAN gehackt hat?



Ein gehacktes WLAN bemerkt man vor allem an den Auswirkungen.

Imago

Es ist nicht leicht, herauszufinden, ob jemand Ihr WLAN gehackt hat. Am ehesten merken Sie es an der Netzwerkliste im Adminbereich Ihres Routers. Hier sind alle Geräte aufgeführt, die derzeit mit dem Router verbunden sind.

Allerdings tragen Sie oft kryptische Namen, die Sie aber editieren können. Wenn Sie auf diese Weise alle Ihnen bekannten Geräte identifizieren, müssen alle anderen, die noch verbunden sind, unberechtigterweise Ihr WLAN nutzen.

Nun können Sie regelmäßig diese Liste checken, aber erstens ist das umständlich und wird in 99 Prozent der Fälle zu keinem Ergebnis führen. Zweitens ist es verwirrend, denn meist sind mehr Geräte mit dem WLAN verbunden, als man denkt.

Nur an der Typbezeichnungen im Adminbereich des Routers lässt sich oft schwer sagen, ob etwas ein Gerät aus Ihrem Haushalt oder ein unberechtigter Zugriff ist – gerade dann, wenn viele Menschen in

Ihrer Wohnung leben, von denen jeder wiederum mehrere Geräte besitzt.

In der Regel werden Sie ein gehacktes WLAN deswegen eher an den Auswirkungen bemerken. Das kann sein, dass Ihr Internetzugang plötzlich lahm (weil ein Hacker Ihre Bandbreite mitnutzt), Endgeräte verrückt spielen, also etwa ohne Ihr Zutun an und aus gehen (weil eben ein Hacker sie fernsteuert) oder Ihre Daten verschwinden und Sie damit eventuell auf die ein oder andere Weise erpresst werden.

Was kann ich gegen ein gehacktes WLAN machen?



Im schlimmsten Fall sollten Sie ihren Router auf Werkseinstellungen zurücksetzen.

Imago

Jemanden, der unberechtigt im eigenen WLAN mitmisch, wieder zu entfernen, ist nicht schwer. Der erste Schritt sollte sein, im Router-Adminbereich alle Geräte zu entfernen, die Sie nicht zuordnen können. Damit sich ein Hacker, der Ihr Passwort geknackt hat, dies nicht einfach wieder eingeben kann, sollten Sie es ändern.

In schwereren Fällen, in denen ein Hacker etwa das Router-Passwort geändert hat und Sie so nicht mehr auf die Oberfläche zugreifen können, oder wenn Sie nicht sicher sind, welche Geräte berechtigter- oder unberechtigterweise in Ihrem WLAN sind, können Sie den Router einfach auf Werkseinstellungen zurücksetzen.

Wie das geht, erfahren Sie im Routerhandbuch. In der Regel müssen Sie eine bestimmte Taste oder Tastenkombination für 10 Sekunden drücken. Im Werkszustand gelangen Sie mit einem voreingestellten Passwort auf die Router-Oberfläche und können das Gerät dort neu konfigurieren – inklusive besserer Passwörter.

In jedem Fall sollten Sie auch die Firmware des Routers dabei aktualisieren. Geknackte Passwörter sind nur ein Weg für Hacker in Ihren Router und Ihr WLAN. Auch Sicherheitslücken in der Software des Routers können ein Einfalltor sein. Sofern bekannt, werden diese durch Firmware-Updates geschlossen.