Netz abschotten

Sicherheits-Checkliste WLAN-Router

Der Einrichtungsassistent bringt den neuen WLAN-Router binnen Minuten online. Doch damit ist längst nicht alles für optimale Sicherheit Ihres Netzes getan. Besonders das WLAN-Passwort braucht heute Aufmerksamkeit: Wegen eines neuen Angriffs auf WPA2 genügen 8 Zeichen bei Weitem nicht mehr.

Von Ernst Ahlers

Webinterface schützen

Moderne Router lassen sich dank cleverer Helfer im Handumdrehen einrichten. Leider übersehen manche dieser Assistenten, dass Sie auch das im Werk eingestellte Konfigurationspasswort ändern sollten. Denn dieses steht – wie auch die vorgegebenen WLAN-Einstellungen – üblicherweise auf dem Typenschild. Ein unauffälliger Knips mit der Smartphone-Kamera genügt.

Geben Sie also Ihrer Bequemlichkeit nicht nach und ändern Sie die Vorgabe: Wer an das Webinterface herankommt, kann sich nicht nur an Internet-Zeitbeschränkungen für die Sprösslinge vorbeimogeln, sondern sich oft auch unbemerkt einen VPN-Zugang von außen in Ihr Netz legen.

Stellen Sie bei der Gelegenheit auch sicher, dass automatische Firmware-Updates aktiviert sind. So holt sich der Router von selbst seine neue Software, falls der Hersteller sie wegen neuer Sicherheitslücken überarbeitet hat.

WLAN richtig sichern

Selbst wenn Ihr Router ab Werk schon mit individuellen WLAN-Einstellungen versehen ist, setzen Sie trotzdem einen eigenen Funknetznamen und einen neuen Schlüssel. Denn diese Voreinstellungen stehen üblicherweise auf dem Router und oft auch auf einem beiliegenden Merkzettel. Wer da herankommt, erhält auch Zugang zum internen Netz, und wenn es nur die Putzhilfe ist.

Das Verstecken des WLANs und eine eventuelle Positivliste für die Clients (MAC-Filter) erhöhen die Sicherheit nicht, sie machen nur zusätzliche Arbeit.

Bei einigen WLAN-Basen lässt sich das Knacken der Verschlüsselung über ein spezielles Steuerpaket abkürzen. Dann ist immer noch ein zeitintensiver Brute-Force-Angriff mit massiver Rechenkraft nötig. Erst der frisch eingeführte WPA2-Nachfolger WPA3 verhindert die Attacke. Wie viel Zeit der Angreifer investieren muss, hängt von der Länge Ihres WLAN-Passworts ab. Nutzen Sie 20 bis 30 Zeichen, bis alle Ihre Geräte WPA3 können.

Gastnetz nutzen

Verbannen Sie Besucher oder verdächtige Smart-Home- beziehungsweise IoT-Geräte ins Gast-WLAN. Schützen Sie auch dieses mit einem langen WPA2-Passwort. Ändern Sie dieses Passwort gelegentlich, denn es könnte sich über Ihren Nachwuchs in der Nachbarschaft ausbreiten.

Falls Ihr Router die Funktion bietet, schränken Sie das Gast-WLAN auf bestimmte Dienste ein, beispielsweise Surfen und Mailen. Das beugt Ärger etwa wegen Filesharings vor.

Freigaben checken

Falls Sie einen von außen erreichbaren Heimserver betreiben, etwa für die eigene Cloud, oder PCs fernwarten, achten Sie darauf, nur sichere, also TLS-verschlüsselte Protokolle per Portweiterleitung oder Portfreigaben zu erlauben. Das gilt auch für die Konfiguration des Routers selbst: Wenn Sie ihn von außen steuern wollen, tun Sie das nur über ein sicheres Protokoll, also HTTPS. Wenn möglich, ändern Sie den Port dafür vom Standardwert 443 auf einen hohen, damit Ihr Router nicht schon bei den simpelsten Portscans aufleuchtet.

WPS und UPnP aus

Nicht erst bei langen, komplexen WLAN-Passwörtern ist das Koppeln der Clients per Tastendruck (WPS) bequem. Nutzen Sie diese Funktion, aber schalten Sie sie hinterher wieder aus. Sonst kann sich jeder Zugang verschaffen, der an den Router herankommt – auch neue Freunde Ihrer Kinder, denen Sie noch nicht trauen.

Manche Anwendungen und Smart-Home-Geräte wollen sich Portweiterleitungen mittels UPnP automatisch einrichten. Wenn das verzichtbar ist, deaktivieren Sie diese Funktion oder beschränken Sie sie auf einzelne Hosts, falls Ihr Router das unterstützt. Denn sie nützt nicht nur den bewusst installierten Programmen, sondern auch eingeschleppter Malware.

Nachdem Sie die Netzzentrale abgedichtet haben, sorgen Sie auch dafür, dass die Arbeit nicht vergebens war. Exportieren Sie die Router-Konfiguration und speichern Sie die Datei unverlierbar ab. Sie lässt sich zwar nicht auf beliebigen Routern zurückladen, aber auf jeden Fall bei einem baugleichen Ersatz und oft auch bei anderen Geräten desselben Herstellers. *(ea@ct.de)* c't