HEIMNETZWERK VOR ANGRIFFEN SCHÜTZEN

Im heimischen Netzwerk haben Außenstehende nichts zu suchen. Damit das auch so bleibt, gibt es einige einfache Tipps, mit denen Sie Ihr Heimnetzwerk schützen können.

Auf Ihrem heimischen Rechner liegen meist persönliche Daten, die Sie in einem Heimnetzwerk zum Beispiel auch auf einem NAS-Laufwerk sichern. Theoretisch ist dieses Netzwerk mit dem Internet verbunden, was Ihnen einige Komfortfunktionen bringt, das Netzwerk aber auch anfällig gegen Angriffe von außen macht. Damit Ihre Daten sicher bleiben, können Sie das Netzwerk aber mit einfachen Handgriffen wirkungsvoll schützen.

1. Betriebssystem und Firmware immer aktualisieren

Die größten Angriffspunkte auf das Heimnetzwerk sind die Geräte, die direkt mit dem Internet verbunden sind. Das ist zum einen Ihr Router, aber auch alle daran angeschlossenen PCs, Laptops, Tablets und Smartphones. Jedes dieser Geräte besitzt ein Betriebssystem, zum Beispiel Windows, MacOS, iOS, Linux und Android.

Auch Ihr Router besitzt eine solche Basis-Software, die bei solchen Geräten als Firmware bezeichnet wird. In jedes Betriebssystem sind bereits viele Schutzmechanismen gegen Angriffe von außen eingebaut. Weil die Systeme aber sehr komplex sind, können Entwickler nicht jede Eventualität von vorneherein einplanen. Die Folge sind Sicherheitslücken, über die Angreifer doch auf Geräte oder zumindest bestimmte Teile davon zugreifen können.

Diese Lücken schließen die Hersteller von Betriebssystem meist schnell, wenn sie davon erfahren. Das geschieht in Form von Software-Updates. Das Wichtigste, um alle bekannten Sicherheitslücken zu schließen, ist also, immer die neueste Version des jeweiligen Betriebssystems zu installieren. Windows, MacOS und mobile Betriebssysteme auf Handys und Tablets aktualisieren sich meist automatisch.

Schlimmstenfalls poppt hier ein Fenster auf, auf dem Sie die Aktualisierung bestätigen müssen. Bei Ihrem Router können Sie über das Router-Interface manuell ein Firmware-Update auslösen. Das sollten Sie vielleicht einmal im Monat machen, um zu prüfen, ob es eine Aktualisierung für die Software gibt.

Kabelverbindungen nutzen, wo es nur geht

2. Das WLAN sichern – oder wenig benutzen

Jeder, der in Reichweite Ihres WLANs ist, kann sich mit diesem theoretisch auch verbinden. Deswegen sollten Sie hier besondere Vorsicht walten lassen. Der erste Schritt ist ein sicheres WLAN-Passwort. Das muss keine wirre Buchstaben-Zahlen-Sonderzeichen-Kombination sein, die Sie sich niemals merken können.

Es muss nur lang genug sein. Verwenden Sie als Passwort zum Beispiel den Satz "KönnenPinguine23Elcheaufeinmalessen?" haben Sie darin sowohl Buchstaben als auch Zahlen und ein Sonderzeichen verwendet, ihr Passwort ist 36 Zeichen lang und Sie können es sich trotzdem einfach merken. Ein Mensch oder ein Algorithmus, der ohne Anhaltspunkt versucht, dieses Passwort zu knacken, wird es nie schaffen.

Noch sicherer ist Ihr WLAN aber natürlich dann, wenn Sie es gar nicht erst benutzen. Wo Sie können, sollten Sie deswegen Kabelverbindungen zwischen dem Router und Ihren Endgeräten anschließen. Das kann aber schnell im Kabelsalat enden oder gerade in großen Wohnungen und Häusern sehr unpraktisch sein, weil Sie lange Kabel verlegen müssen.
In dem Fall kann es schon helfen, das WLAN oder gleich den ganzen Router auszuschalten, wenn Sie Ihn nicht benutzen – also zum Beispiel nachts, wenn Sie tagsüber auf der Arbeit sind oder in Urlaub fahren. Zwingend notwendig ist ausschalten für die Sicherheit nicht – wer sich damit sicher fühlt, kann sich so aber noch besser schützen.

3. Voreingestellte Netzwerkdaten sofort ändern

Wenn Sie einen neuen Router anschließen, kommt der mit einigen Voreinstellungen. So gibt es einen Standard-Benutzernamen und ein Standard-Passwort, mit dem Sie auf das Router-Interface gelangen. Das WLAN enthält im Werkszustand oft den Namen Ihres Routers und das Passwort ist auf der Rückseite aufgedruckt.

Alle Daten sollten Sie deswegen sofort nach dem Anschluss des Routers ändern. Vergeben Sie einfach einen neuen Benutzernamen und ein neues Passwort für den Router (oft geschieht das beim Einrichtungs-Assistenten automatisch), benennen Sie das WLAN um und vergeben Sie dafür ein eigenes Passwort.

Das Problem an den Voreinstellungen ist, dass diese je nach Hersteller ähnlich oder gleich auf mehreren Geräten sein können, was versierte Hacker wissen. Die Angabe des Router-Modells im WLAN-Namen verrät einem Angreifer womöglich, nach welchen Sicherheitslücken er Ausschau halten muss.

Unsichere Geräte sollten in ein eigenes Netzwerk

Nutzen Sie wenn möglich https.

Imago

4. Nutzen Sie https, aber nicht WPS

Zwei kleine Tipps zum Schluss: Wenn Sie Einstellungen an Ihrem Router vornehmen, öffnen Sie das Interface meist über einen Browser, indem Sie in die Adressleiste entweder die IP-Adresse des Routers oder eine Standard-Adresse wie zum Beispiel "fritz.box" eingeben. Die Verbindung mit dem Router geschieht dann wie bei einer Webseite über das "Hypertext Transfer Protocol", kurz http. Das erkennen Sie an den ersten vier Buchstaben jeder Web-Adresse. http ist ein Protokoll, was für Angriffe von außen anfällig ist.

Sicherer ist die Verwendung von https, was schlicht für "Hypertext Transfer Protocol Secure" steht. Daten werden hierbei abhörsicher übertragen. Um dieses Protokoll für die Datenübertragung zwischen Ihrem Endgerät und Ihrem Router zu benutzen, müssen Sie lediglich darauf achten, dass die Adresse in der Adresszeile des Browsers mit "https" statt nur mit "http" beginnt. Beispielsweise müssten Sie dann https://192.168.0.1 eingeben, wenn Sie Ihren Router per IP-Adresse aufrufen.

WPS steht für "Wi-Fi Protected Setup". Das ist eine Funktion, mit der Sie ein Gerät ins WLAN hinzufügen können. Meist geschieht das, indem Sie auf Ihrem Router und dem entsprechenden Endgerät einen WPS-Knopf drücken. Beide Geräte stellen dann automatisch eine Verbindung her. Die muss noch über eine PIN bestätigt werden, die meist auf der Rückseite Ihres Routers aufgedruckt ist. Das ist unsicher, denn irgendwo aufgeschriebene PINs und Passwörter sind am einfachsten zu klauen. In der Regel werden Sie die WPS-Funktion des Routers selten nutzen. Da empfiehlt es sich, Sie über das Router-Interface zu deaktivieren und nur dann zu aktivieren, wenn Sie sie tatsächlich benötigen.

5. Packen Sie unsichere Geräte in ein eigenes Netzwerk

Neben den klassischen Endgeräten wie PCs, Laptops, Smartphones und Tablets sind auch immer mehr Haushaltsgeräte netzwerk- oder gar internetfähig. Jedes dieser Geräte ist damit ein zusätzlicher Angriffspunkt, aber Sie dürfen vom Hersteller einer Kaffeemaschine nicht den gleichen Sicherheitsstandard erwarten wie von einem Router-Hersteller.

Damit Angreifer nicht über schlecht gesicherte Smart-Home-Geräte Zugriff auf Ihr Heimnetzwerk erhalten, gibt es einen Trick. Verbinden Sie diese Geräte nicht mit dem WLAN, das Sie auch mit Ihren anderen Endgeräten nutzen, sondern mit einem zweiten WLAN-Netzwerk. Jeder Router bietet mittlerweile meist ein Gast-Netzwerk an, das eigentlich wie der Name sagt für Gäste gedacht ist.

Das lässt sich im Router-Interface so konfigurieren, dass hiermit verbundene Geräte zwar Zugang zum Internet haben, nicht aber auf alle anderen Geräte im Netzwerk. So kann Ihre smarte Kaffeemaschine vielleicht angegriffen werden, Angreifer kommen von dort aber nicht weiter auf Ihren Heimserver oder PC.

Eine Ausnahme gibt es allerdings: Wenn Sie eine Smart-Home-Zentrale besitzen, die sich per WLAN steuern lässt, muss diese mit Endgeräten verbunden sein (sonst ließe sie sich darüber nicht steuern) und mit den Smart-Home-Geräten (sonst ließen sich diese darüber nicht steuern). Diese muss also so eingestellt werden, dass Sie mit beiden Netzwerken kommunizieren kann. Allerdings sind Smart-Home-Zentralen als Herzstücke meist auch gut gegen Angriffe abgesichert.