ROUTER-HACKING – WIE SCHÜTZE ICH MICH

Kann ein Router gehackt werden?

Bei einem gehackten Computer sind die Gefahren klar: Die Eindringlinge können sich all Ihrer sensiblen persönlichen Dateien bedienen und sie sogar löschen. Und wenn Hacker sich erst einmal Zugriff auf Ihren Computer oder Ihr Smartphone verschafft haben, können sie darauf Malware installieren, um Ihre Internetaktivitäten auszuspionieren, Ihre Dateien mit Ransomware zu verschlüsseln oder anderen Schaden anzurichten.

Leider sind auch Router anfällig für Hackerangriffe.

Welche Gefahr geht von einem gehackten Router aus?

Ein gehackter Router kann zu einer ganzen Reihe neuer Bedrohungen führen, von scheinbar harmlosen bis hin zu sehr ernsten. Hacker haben auf Ihrem Router folgende Möglichkeiten:

- Einschränken der Bandbreite: Das ist zwar eher lästig als gefährlich, aber dennoch: Wenn jemand Ihr WLAN unbemerkt mitbenutzt und zum Streamen von Spielen und Filmen (oder sogar zum Schürfen von Kryptowährungen) einsetzt, bleibt erheblich weniger Bandbreite für Ihre eigene Nutzung übrig.
- Ausspionieren des Internetverkehrs: Eine Person, die sich in Ihr WLAN-Netzwerk eingeklinkt hat, kann den gesamten Datenverkehr in Ihrem Netzwerk ausspionieren, und zwar von jedem Gerät, das damit verbunden ist. Dazu gehören Ihr Computer, Ihr Smartphone, die Computer und Smartphones Ihrer Familie, Ihre Videospielkonsole, Ihre Smart-Home-Geräte und mehr. Hacker können auch einen Paket-Sniffer verwenden, um Ihren Internetverkehr in Echtzeit zu überwachen und die ein- und ausgehenden Daten zu erfassen.
- Zugreifen auf illegale Inhalte: Sie selber haben vielleicht einen blitzsauberen Internetverlauf, aber das hält die WLAN-Hacker nicht davon ab, sich anders zu verhalten. Sie können Ihre Internetverbindung nutzen, um illegale Medien anzusehen oder hochzuladen, raubkopierte Inhalte zu streamen oder herunterzuladen, im Darknet einzukaufen und viele andere unschöne Dinge zu tun – alles unter Ihrem Namen.
- Erfassen Ihrer persönlichen Daten: Router-Hacker können alles abfangen, was Sie auf einer Website mit einer unverschlüsselten Verbindung eingeben – also auf einer Website, die nur HTTP verwendet. Und das gilt auch für alle, die mit Ihrem gehackten WLAN verbunden sind. Geben Sie niemals sensible Daten, wie z. B. ein Passwort, auf einer Website ohne HTTPS-Verschlüsselung ein.
- Installieren von Malware: Ja, es gibt Router-Malware. Hacker mit Zugriff auf Ihren Router können auch die Router-Firmware hacken und mit Malware infizieren, was die Voraussetzungen für weitere Angriffe und Spionage-Aktivitäten in der Zukunft schafft.
- Analysieren der Struktur des WLAN-Netzwerks: Jemand, der Ihren Router angezapft hat, kann alle Geräte in Ihrem Netzwerk sehen und diese Informationen nutzen, um weitere Angriffe zu planen. Router-Angriffe auf Smart-Home-Geräte und andere Geräte im Internet der Dinge (IoT) können besonders gefährlich sein, da viele Menschen der Sicherheit des IoT nicht so viel Aufmerksamkeit schenken wie dem Schutz ihres Computers und Telefons.
- Angreifen anderer Personen: Cyberkriminelle können Ihren gehackten Router für einen massiven DDOS-Angriff nutzen.
- Ändern Ihrer DNS-Einstellungen: Ein häufiges Ziel bei einem WLAN-Router-Hack sind die DNS-Einstellungen des Routers. Hacker können die DNS-Einstellungen des Routers so ändern, dass der Internetverkehr auf Websites ihrer Wahl umgeleitet wird – in der Regel auf Pharming-Websites, die Sie zur Herausgabe persönlicher Daten verleiten, oder auf schädliche Websites, durch die Malware auf Ihre Geräte heruntergeladen wird.

Von einem gehackten Router gehen zahlreiche Sicherheitsbedrohungen aus

Wir wissen jetzt also, was WLAN-Hacker alles anstellen können, und sehen uns nun an, was Sie dagegen tun können.

So schützen Sie Ihr WLAN vor Hackern

Mit nur ein paar einfachen Vorsichtsmaßnahmen für Ihren WLAN-Router können Sie Hackern das Leben erschweren. Wie oft im Leben ist das Verhindern eines WLAN-Hacks billiger und einfacher als das Auseinandersetzen mit einem gehackten Router. Denn dieses Problem wird erheblich schwieriger, wenn auch nicht unmöglich, zu lösen sein.

So blockieren Sie WLAN-Hacker mit intelligenter Router-Sicherheit:

Ändern der Admin-Anmeldeinformationen Ihres Routers

Alle Router verfügen über einen Benutzernamen und ein Passwort, mit denen auf die Einstellungen zugegriffen werden kann. Wenn Sie einen Router bekommen, egal ob neu oder gebraucht, sollten Sie sofort den Benutzernamen und das Passwort ändern.

WLAN-Hacker kennen die standardmäßigem Admin-Anmeldedaten fast aller gängigen Router auf dem Markt. Wenn sich eine Person in der Nähe Ihres WLAN-Netzwerks befindet, kann sie versuchen, sich mit diesen Informationen bei Ihrem Router anzumelden. Haben Sie die Anmeldedaten nicht nach dem Erwerb Ihres Routers aktualisiert, machen Sie Ihr WLAN zur leichten Beute für einen Router-Hacker. Und wenn Sie den Router von einer anderen Person gekauft haben, wissen Sie nicht, wer die alten Anmeldeinformationen noch alles haben könnte. In jedem Fall sollten Sie sie so schnell wie möglich ändern.

Legen Sie ein neues Router-Passwort fest, indem Sie sich an die Richtlinien zur Erstellung sicherer Passwörter halten – oder erstellen Sie ein wirklich „unknackbares“ Passwort mit zufälligen Zeichenfolgen –, um zu verhindern, dass WLAN-Hacker zu leicht in Ihren Router eindringen können.

Aktivieren von WPA2- (oder WPA3-) Verschlüsselung

WPA2 und WPA3 – die zweite und dritte Version des Sicherheitsprotokolls „Wi-Fi Protected Access“ – schützen Ihren Router mithilfe von AES-Verschlüsselung vor unerwünschten Zugriffen. Die gleiche Art der Verschlüsselung nutzen wir für unser supersicheres Avast SecureLine VPN, also können Sie sicher sein, dass sie gut ist. Jeder ernstzunehmende Router ist WPA2-fähig, und einige neuere Modelle unterstützen WPA3.

Aktivieren Sie die WPA2- oder WPA3-Verschlüsselung, damit jeder, der eine Verbindung zu Ihrem geschützten Router herstellen möchte, Ihr WLAN-Passwort benötigt. Und legen Sie ein sicheres Passwort fest, indem Sie sich an bewährte Leitlinien für die Erstellung von Passwörtern halten. Mit diesen einfachen

Schritten stellen Sie jeden Möchtegern-WLAN-Hacker vor eine ernsthafte Herausforderung.

Ändern Sie den Router-Netzwerknamen (SSID)

Bei der Konfiguration Ihres Routers – bei der Sie die Admin-Anmeldedaten ändern und ein sicheres Passwort festlegen – sollten Sie auch die SSID ändern. SSID steht für *Service Set Identifier* und ist im Prinzip ganz einfach der Name Ihres WLAN-Netzwerks.

SSIDs neuer Router enthalten oft die Marke des Routers, und WLAN-Hacker könnten diese Informationen nutzen, um Ihr Passwort zu knacken. Legen Sie stattdessen einen benutzerdefinierten Netzwerknamen fest, damit die Hacker nicht wissen, welchen Routertyp Sie haben. Je mehr Anhaltspunkte Sie Hackern geben, desto einfacher machen Sie es ihnen.

Seien Sie beim Festlegen des WLAN-Netzwerknamens kreativ: Denken Sie sich am besten einen langen und komplexen Namen aus. Bei der WPA-Verschlüsselung wird die SSID als Teil des Algorithmus verwendet. Wenn Sie also standardmäßige oder gängige Netzwerknamen meiden, machen Sie Ihr Netzwerk auch widerstandsfähiger gegenüber Passwort-Cracking wie durch Rainbow Tables. Außerdem freuen sich Ihre Nachbarn sicher über einen besonders kreativen Netzwerknamen.

Deaktivieren von WPS

Neben WPA2 oder WPA3 verfügen viele Router auch über WPS (Wi-Fi Protected Setup): Das bedeutet, dass Sie zur Verbindungsherstellung nicht das Passwort eingeben müssen, sondern nur eine Taste drücken oder eine PIN eingeben können. Obwohl das natürlich bequemer ist, sinkt das Sicherheitsniveau, wenn keine Passwörter verwendet werden.

Jeder, der physischen Zugang zu Ihrem Router hat, kann die WPS-Taste drücken und eine Verbindung herstellen. Und eine kurze PIN ist viel leichter mit einem Brute-Force-Angriff zu knacken als ein langes und komplexes Passwort.

Leider unterstützen nicht alle Router die Deaktivierung von WPS-Funktionen, aber wenn dies bei Ihrem Router der Fall ist, schalten Sie WPS aus und legen Sie ein Passwort fest.

Deaktivieren von kabelloser oder Remoteadministration

Mithilfe der Remoteadministration können Sie sich von jedem Ort der Welt in die Admin-Einstellungen Ihres Routers einloggen. Aber wenn Sie nicht gerade Entwickler sind, brauchen Sie diese Funktion sehr wahrscheinlich nicht. Wenn Sie sie deaktivieren, können Sie nur dann auf die Einstellungen zugreifen, wenn Ihr Computer physisch über ein Ethernet-Kabel mit Ihrem Router verbunden ist. Das Deaktivieren der Remoteadministration ist eine gute Möglichkeit, Hackern ihr Handwerk zu legen.

Aktualisieren der Firmware Ihres Routers

Firmware ist die Bezeichnung für Software zur Steuerung von Hardware – in diesem Fall Ihr Router. Wie das Betriebssystem Ihres Computers oder Programme und Apps kann auch die Firmware aktualisiert werden.

Durch Firmwareaktualisierungen können Schwachstellen Ihres Routers geschlossen werden, die in älteren Versionen der Firmware entdeckt wurden. Einige Router suchen automatisch nach Firmwareaktualisierungen, aber Sie können auch selbst in den Admin-Einstellungen Ihres Routers die Firmware-Infos prüfen.

Verwenden eines Tools für die Cybersicherheit, das auch Ihr WLAN-Netzwerk schützt

Eine der einfachsten und sichersten Möglichkeiten zur Absicherung Ihres WLAN-Netzwerks ist die Verwendung eines WLAN-Überwachungstools, das Ihr Netzwerk automatisch im Auge behält, sodass Sie es nicht selbst manuell überwachen müssen.

Avast Free Antivirus verfügt über einen integrierten WLAN-Inspektor, der Ihr Netzwerk ständig auf verdächtige Aktivitäten oder Geräte überprüft, sodass Sie jederzeit genau wissen, was in Ihrem WLAN vor sich geht. Schützen Sie Ihr WLAN-Netzwerk, entfernen Sie alle Geräte, die dort nicht dazugehören, und erhalten Sie die Gewissheit, dass Sie sofort Bescheid wissen, sollten sich WLAN-Hacker in Ihr Netzwerk

eingenistet haben.