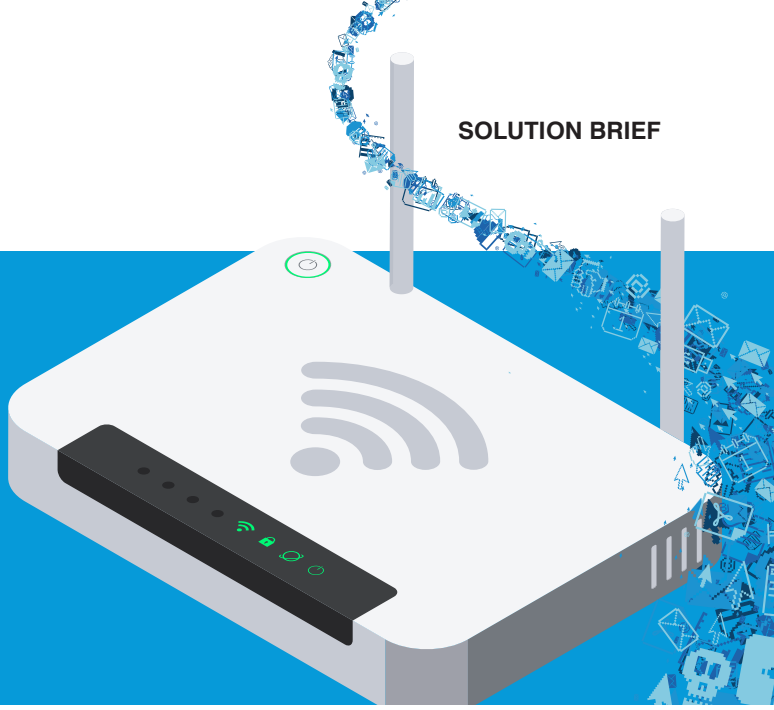
proofpoint.

SOLUTION BRIEF

In 3 Schritten zu aktuellen Sicherheitseinstellungen für das heimische WLAN-Netzwerk



Möglicherweise haben Sie schon davon gehört, dass die Anmeldung bei kostenlosen, offenen WLAN-Netzwerken Gefahren birgt. Wissen Sie aber auch, dass selbst Ihr heimisches Netzwerk für persönliche Daten gefährlich sein kann? Ohne die richtigen Sicherheitsmaßnahmen ist Ihr Heim-WLAN genauso anfällig wie das offene WLAN im Café um die Ecke. Ohne angemessenen Schutz kann Ihr Netzwerk auch von Personen mit geringen IT-Kenntnissen ausgespäht werden.

Unsere Sicherheitsexperten haben deshalb die drei wichtigsten Schutzmaßnahmen für typische Heim-WLAN-Netzwerke zusammengestellt. Nach ihrer Einschätzung „sollten sich damit 99,99 % aller Probleme von 99,99 % aller Anwender lösen lassen."[1]

Lesen Sie sich die nachfolgenden Tipps gut durch und machen Sie Ihr Netzwerk damit sicherer. Der Gedanke, Standardkennwörter und die WLAN-Einstellungen zu verändern, klingt im ersten Moment vielleicht sehr technisch. Es ist aber einfacher, als Sie glauben. Wenn Sie schon einmal einen Festplattenrekorder (oder in grauer Vorzeit einen Videorekorder) programmiert haben, können Sie das auch.

1. Ändern Sie das Standard-Administratorkennwort und deaktivieren Sie die Fernverwaltung

Das „Admin"-Kennwort für Ihren Router unterscheidet sich von dem Kennwort, mit dem Sie sich im WLAN-Netzwerk anmelden. Das WLAN-Kennwort dient dazu, sich über Ihren Router mit dem Internet zu verbinden. Mit dem Kennwort des Routers erhalten Sie hingegen Zugriff auf die Konfigurationseinstellungen des WLAN-Netzwerks selbst. (Die Schritte zum Festlegen oder Ändern Ihres WLAN-Kennworts finden Sie unter Tipp 3.)

Standardkennwörter bergen die Gefahr, dass sie von Amateur-Hackern ebenso wie von erfahrenen Cyberkriminellen im Internet gefunden werden können. Damit ist Ihr Netzwerk dann offen. Mit dem Ändern der Standardkennwörter schließen Sie also eine Schwachstelle.

So ändern Sie Ihr Standardkennwort:

- → Suchen Sie das Etikett auf Ihrem Router, auf dem Standard-IP-Adresse sowie Benutzername und Kennwort für den Administrator stehen.
- → Öffnen Sie im Browser Ihrer Wahl eine neue Registerkarte oder ein neues Fenster.
- → Geben Sie in die Adressleiste die Standard-IP-Adresse ein. Sie hat das Format 123.456.7.8.
- → Geben Sie im Anmeldebildschirm den Standardbenutzernamen und das Standardkennwort ein.
- → Navigieren Sie zum Administratorbereich und ändern Sie das Administratorkennwort. Dabei gilt: Je länger, desto besser und möglichst einschließlich Sonderzeichen. Richtig toll ist ein Satz, mit dem Sie etwas anfangen können, der für andere jedoch schwierig zu erraten ist (z. B. Ich<3CurryWurst).
- → Im nächsten Schritt müssen Sie die Fernverwaltung deaktivieren, da diese Funktion das Einwählen von außen bei Ihrem Router ermöglicht. Sie sollte nur aktiviert werden, wenn sie auch wirklich benötigt wird. Andernfalls stellt sie ein Einfallstor für Angriffe dar.
- → Um die Funktion zu deaktivieren, suchen Sie nach einer Schaltfläche oder einem Kontrollkästchen mit der Kennzeichnung „Fernverwaltung aktivieren" bzw. eben „Fernverwaltung deaktivieren". Legen Sie fest, dass die Fernverwaltung abgeschaltet ist.

Hinweis: Falls Sie die Stelle zum Ändern des Administratorkennworts auf der Benutzeroberfläche nicht finden, geben Sie in die Suchmaske Ihres Browsers „Kennwort ändern <Router-Marke> <Modellnummer>" ein. Dann sollten Sie recht schnell eine entsprechende Anleitung finden.

1 Wie bei den meisten Netzwerken können WLAN-Systeme aus verschiedenen Gerätetypen und Konfigurationen bestehen. Für diesen Artikel sind wir von relativ üblichen Einstellungen für das Netzwerk in einem Haushalt ausgegangen, mit einem einzelnen WLAN-Router und integriertem Zugangspunkt.

2. Aktualisieren Sie die Firmware Ihres Routers

Wenn Sie gerade im Administratorbereich sind, sollten Sie auch gleich die Firmware Ihres Routers auf den neuesten Stand bringen. Wie bei allen elektronischen Geräten finden auch die Hersteller von Routern noch Fehler, nachdem die Geräte schon ausgeliefert und in Betrieb genommen wurden. Ein Update der Firmware Ihres Routers ist das Gegenstück zur Aktualisierung des Betriebssystems auf Ihrem Smartphone oder Tablet. Damit lassen sich Schwachstellen beseitigen und die Leistung verbessern.

Um das Update vorzunehmen, suchen Sie im Administratorbereich nach einer Option wie „Firmware-Update“, „Router-Update“ (oder ähnlich). Sollten Sie auf eine Möglichkeit stoßen, automatische Firmware-Updates zu erlauben (die entsprechende Funktion heißt dann „Automatische Router-Updates“ oder ähnlich), aktivieren Sie diese. Damit erhalten Sie künftig automatische Sicherheits-Updates und neue Funktionen.

Wie bereits unter Tipp 1 erwähnt, kann Ihnen gegebenenfalls eine Internetsuche helfen, die Stelle auf der Benutzeroberfläche zu finden, von der aus Sie die Aktualisierung vornehmen können.

3. Konfigurieren Sie die Sicherheitseinstellungen für das WLAN

Bei der Konfiguration des WLAN-Netzwerks sollten Sie vor allem drei Einstellungen überprüfen (und gegebenenfalls ändern): Ihre SSID (das ist der Name Ihres drahtlosen Netzwerks), Ihre Verschlüsselungsmethode und Ihr WLAN-Kennwort. Gehen Sie dazu wie folgt vor:

- → Suchen Sie nach einer Registerkarte mit der Bezeichnung „Drahtlosnetzwerk einrichten“ (oder ähnlich). (Auch hier hilft Ihnen eine Internetsuche, wenn Sie sich nicht sicher sind, wo genau Sie Ihren Router im Netzwerk finden.)
- → Überprüfen Sie dann die Verschlüsselung des Drahtlosnetzwerks. Der neueste Verschlüsselungsstandard ist WPA3, aber er steckt noch in den Kinderschuhen. Die meisten Router und andere Geräte wie Smartphones oder Laptops unterstützen WPA3 noch nicht. Wahrscheinlich steht diese Verschlüsselung also nicht zur Auswahl, sofern Sie nicht einen ausdrücklich WPA3-kompatiblen Router verwenden. Bis WPA3 weiter verbreitet ist, wählen Sie die WPA2-Verschlüsselung. Diese ist ein Muss, da frühere WLAN-Verschlüsselungsprotokolle viel anfälliger sind. Sollte es bei WPA2 mehrere Optionen geben, wählen Sie WPA2-PSK, WPA2-PSK (AES) oder WPA2-Personal aus. Alle drei Verschlüsselungsmethoden sind im Wesentlichen gleich und bieten nach WPA3 den besten Schutz für Privatanwender.
- → Legen Sie ein Kennwort für Ihr Drahtlosnetzwerk fest oder ändern Sie es. (Ein von Ihrem Anbieter vergebenes Kennwort sollten Sie ändern.) Wie zuvor schon beim neuen Administratorkennwort für den Router, sollten Sie nach Möglichkeit einen längeren Satz mit persönlicher Bedeutung wählen, der (durch Sonderzeichen, Ziffern usw.) zudem eine gewisse Komplexität hat. Verwenden Sie Ihr Administratorkennwort NICHT ein zweites Mal.
- → Ändern Sie die Standard-SSID in einen Namen Ihrer Wahl. (Mit „Polizeiüberwachung 1“ etwa können Sie bei Ihren Nachbarn wahlweise für Belustigung oder Nervosität sorgen.) Wenn Sie die Standard-SSID behalten, machen Sie damit mit einiger Wahrscheinlichkeit Marke und Typ des von Ihnen verwendeten Routers öffentlich. Diese Informationen wissen Cyberspione zu nutzen.

Sollten Sie sich in diesem Zusammenhang übrigens Sorgen machen, dass Fremde Ihr WLAN-Netzwerk für ihren Internetzugang nutzen, anstatt selbst dafür zu bezahlen, deaktivieren Sie einfach die SSID-Broadcast-Funktion. (Unbefugte Nutzung von Drahtlosnetzwerken ist eher in dichtbesiedelten Gebieten wie Häusern mit mehreren Mietparteien ein Problem.)

Bei abgeschaltetem SSID-Broadcast ist der Name Ihres WLAN-Netzwerks für andere Geräte unsichtbar, die die Gegend nach verfügbaren Drahtlosnetzwerken abtasten. Das bietet den Vorteil, dass Fremde sich nur schwer in Ihr Netzwerk einwählen können, weil sie dazu sowohl Ihre SSID als auch Ihr Kennwort erraten müssen. Der Nachteil ist, dass Ihre Geräte die SSID auch nicht finden. Sie müssen den Netzwerknamen also manuell in jedes Gerät eingeben, das sich verbinden soll.

Um diese Funktion abzuschalten, suchen Sie im Bereich für die Einrichtung des Drahtlosnetzwerks nach „SSID Broadcast” (oder ähnlich). Aktivieren oder deaktivieren Sie das Kontrollkästchen oder die Schaltfläche entsprechend, um diese Funktion zu deaktivieren.