

## WLAN ohne Risiko: Drahtlose Netze sicher konfigurieren

**Einfach, schnell und kabellos: Kein Notebook oder PC wird heute ohne WLAN-Schnittstelle ausgeliefert. Doch wo Daten per Funk übertragen werden, treten auch Sicherheitsprobleme auf. Wir wollen Ihnen zeigen, wie Sie sich schützen können.**

Der kabellose Internetzugang über das heimische WLAN-Netz ist an Komfort kaum zu überbieten. Doch ebenso schnell wie Access Point, Notebook und PC über die Luftschnittstelle verbunden sind, werden oft die einfachsten Sicherheitsmaßnahmen außer Acht gelassen. Das belegen immer wieder entsprechende Studien diverser Sicherheitsunternehmen, denen zufolge bis zu 70 Prozent der privaten Funknetzwerke Daten unverschlüsselt und somit für jeden mitlesbar durch den Äther funken.

Wer bei seinem WLAN-Netz keine oder nur unzureichende Sicherheitsvorkehrungen trifft, setzt sich gleich mehreren Gefahren aus. Ungebetene und kriminell motivierte Gäste können aus ungeschützt übertragenen Funkpaketen persönliche Daten wie Login-Informationen und Passwörter ausspähen - mit allen bekannten Folgen.



Ferner lassen sich offene Internetzugänge über ungesicherte WLAN-Netze für beliebige Zwecke missbrauchen, etwa für das Herunterladen von illegalen Inhalten, den Massenversand von Spam oder das Ausführen von Denial-of-Service-Attacken<sup>1</sup>, um nur einige Beispiele zu nennen. Sollten sich später Ermittlungsbehörden für die illegalen Vorgänge interessieren, ist selbstredend der Besitzer des Anschlusses der Hauptverdächtige, auch wenn der sich keiner Schuld bewusst ist.

Folglich ist das Abschotten von drahtlosen Heimnetzwerken vor WLAN-Piraten und sonstigen Eindringlingen von äußerster Wichtigkeit. ZDNet stellt auf den nächsten Seiten die entscheidenden Maßnahmen für die WLAN-Absicherung vor.

### Access Points sicher verwalten

Die Konfiguration von drahtlosen Heimnetzwerken wird grundsätzlich über einen Browser und der Administrationsoberfläche des WLAN-Access-Points getroffen. Insbesondere bei der ersten Inbetriebnahme empfiehlt es sich, das Gerät ausschließlich über eine Kabelverbindung zu verwalten. Dies verhindert, dass ein unsichtbarer Datenspion das Kennwort des Access Points über die noch ungeschützten Funkwellen abfangen kann. Sollte eine Konfiguration über Kabel nicht möglich sein, ist zumindest sicherzustellen, dass eine mit HTTPS beziehungsweise SSH verschlüsselte Funkverbindung zum Verwaltungs-Tool besteht.

### Standard-Passwort ändern

WLAN-Access-Points sind im Auslieferungszustand grundsätzlich mit einem Standard-Passwort für die Administration versehen. Findige Cracker nutzen im Internet frei verfügbare, nach Hersteller und Modell sortierte Listen von werkseitig eingestellten Kennungen, um in nachlässig administrierte WLAN-Hardware einzubrechen. Aus naheliegenden Gründen sollte jeder Access Point zuallererst mit einem neuen, individuellen Passwort versehen werden.

---

<sup>1</sup> Als Denial of Service (DoS, zu Deutsch etwa: *Dienstverweigerung*) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service). Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dem Angreifer durch solche Botnetze weitere Wirte zum Ausführen seiner Angriffe bringen.

Dabei spielt die Wahl eines qualitativ hochwertigen Passworts für die Sicherheit eine entscheidende Rolle. Im Idealfall sollte der gewählte Begriff aus Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen, und eine Länge von mindestens zehn Zeichen besitzen. Zudem ist es ratsam, auch solche "sicheren" Passwörter in regelmäßigen Zeitabständen zu ändern.

Hilfe bei der Erstellung guter Passwörter bieten kostenlose Programme wie Zebu's Passwort Generator oder die Javascript-Browser-Anwendung von Security-Gui.de.

### **Fernkonfiguration deaktivieren**

In diesem Zusammenhang ist auch die von manchen Access Points angebotene Möglichkeit der Fernkonfiguration (Remote Administration) erwähnenswert. Während die Funktion im Unternehmensbereich durchaus Verwendung findet, wird sie in privaten Netzwerken nur selten benötigt. Da die Fernkonfiguration eine weitere potenzielle Angriffsfläche bietet, sollte sie bei Nichtgebrauch deaktiviert werden.

### **Firmware und Software aktualisieren**

So gut wie keine Software ist fehlerfrei, was natürlich auch für die Firmware von Access Points und WLAN-Netzwerkkarten gilt. Um bekannte Sicherheitslücken in der Betriebssoftware der Geräte zu schließen, lohnt es sich, in regelmäßigen Zeitabständen die Support-Seiten der Hersteller zu besuchen. Nicht selten stehen bereits wenige Wochen nach der Markteinführung eines Geräts Firmware-Sicherheitsupdates zum Download bereit.

- AVM
- Belkin
- Buffalo
- D-Link
- Lancom
- Linksys
- Netgear
- Siemens
- SMC
- Zyxel

Webseiten bekannter WLAN-Gerätehersteller:

Auch Hardware-Treiber und proprietäre WLAN-Software der Gerätehersteller werden oft aktualisiert, um Sicherheitslücken zu schließen. Dies gilt sowohl für Windows als auch für den Mac.

### **Bestmögliche Verschlüsselung einsetzen**

Um den Datenverkehr vor unbefugtem Zugriff zu schützen, ist der Einsatz einer effektiven Funkverschlüsselung unabdingbar. Auf Basis der in diesem Artikel beschriebenen Maßnahmen kann die Verschlüsselung als der mit Abstand wichtigste Faktor genannt werden. Anders ausgedrückt: Wenn die Verschlüsselung nicht stimmt, nutzen die anderen Tipps nur noch wenig.

Die drei gängigen Verschlüsselungsverfahren für drahtlose Netzwerke sind

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access 2)

Die WEP-Verschlüsselung ist die älteste und aufgrund diverser Schwachstellen die unsicherste der drei Standards. WEP gilt schon seit längerem als geknackt, und stellt für einen Cracker, der mit Bestimmtheit in das Funknetz eindringen möchte, kein echtes Hindernis dar. Bei älterer WLAN-Hardware wird oft nur WEP unterstützt. In diesem Fall ist es dringend anzuraten, die veralteten Geräte durch neuere zu ersetzen, die mit den moderneren und deutlich verbesserten Standards WPA und WPA2 zurechtkommen. Bis dahin gilt: Ist WEP die einzige verfügbare Verschlüsselungsoption, legt das Verfahren nach dem "besser als gar nichts"-Prinzip potenziellen Einbrechern zumindest einen Stolperstein in den Weg.

Der Verschlüsselungsstandard WPA bietet deutlich mehr Sicherheit. Der WEP-Nachfolger ergänzt den alten Standard um dynamische Schlüssel, die es einem potenziellen Angreifer erheblich erschweren, den Datenverkehr zu dechiffrieren. Da aber seit Ende 2004 Wörterbuchangriffe auf WPA mittels Cracker-Tools gang und gäbe sind, ist der von WPA gebotene Schutzgrad stark von der verwendeten Passphrase abhängig. So sollte auch für den WPA-Key ein Passwort mit mindestens zehn Stellen gewählt werden, das aus zufälligen Zahlen, Buchstaben und Sonderzeichen besteht. Je länger das Passwort, desto besser.

WPA2 bietet von den drei Verfahren derzeit den besten Schutz. Der in der Weiterentwicklung von WPA verwendete Verschlüsselungsalgorithmus basiert auf dem Advanced Encryption Standard (AES), der sich auch im VPN-Bereich fest etabliert hat.

Es ist wichtig, darauf zu achten, dass auch alle Geräte das gewählte Verschlüsselungsverfahren unterstützen. Beherrscht nur ein Modell im WLAN ausschließlich das unsichere WEP, stuft der Router möglicherweise die Verschlüsselung für alle angeschlossenen Einheiten herunter.

### **SSID ändern und Broadcast unterbinden**

Der so genannte Service Set Identifier (SSID) ist der Name des einzurichtenden drahtlosen Netzwerks. Im Auslieferungszustand ist die SSID auf einen Standardnamen eingestellt, der sich je nach Access-Point-Hersteller oder -Modell unterscheidet.

Aus Sicherheitsgründen sollte die voreingestellte SSID geändert werden, wobei der neue Netzwerkname keine Rückschlüsse auf den Betreiber, Nutzungszweck oder Standort des WLANs erlauben sollte.

Zudem ist die "SSID-Broadcast"-Option zu deaktivieren. Diese Einstellung verhindert, dass der Access Point den Namen des WLAN-Netzes andauernd, oftmals bis zu zehn Mal pro Sekunde, in den Äther aussendet.

Beide Maßnahmen erschweren die Erkennung dieses ersten Angriffspunkts für etwaige Übeltäter. Mit speziellen Tools lässt sich die SSID zwar leicht ausspähen, leichtherzig verschenken sollte man die Information aber dennoch nicht.

### **Reichweite des WLAN-Funksignals beschränken**

Wenn die Sendeleistung des Access Points über die räumlichen Grenzen des geplanten Nutzungsbereichs hinausgeht, ist das nur für diejenigen gut, die nichts im Netz zu suchen haben. Kann der Hacker kein Signal empfangen, kommt er auch nicht in die Versuchung, den Zugang zu knacken.

Die Stärke des WLAN-Funksignals lässt sich oft mit dem Administrations-Tool einstellen. Bei Access Points mit Richtfunkantennen kann der abgedeckte Sendebereich zusätzlich durch gezielte Positionierung maßgeblich beeinflusst werden.

## **DHCP deaktivieren und MAC-Filter einsetzen**

Eine weitere Möglichkeit, den unbefugten Zugriff auf das WLAN zu erschweren, bietet der MAC-Filter<sup>2</sup>. Hier geht es nicht darum, Apple-Systeme auszusperrern, sondern nur ausgewählten Rechnern mit bestimmten Netzwerk-Hardware-Adressen die Anmeldung im Netz zu erlauben.

Auch diese Maßnahme stellt kein größeres Hindernis für versierte Angreifer dar, da aus abgefangenen Datenpaketen die im WLAN versendeten MAC-Adressen herausgelesen und anschließend fingiert werden können. Für Gelegenheitshacker bedeutet der MAC-Filter aber zumindest einen weiteren Arbeitsschritt, der sie womöglich dazu bewegt, ein einfacheres Ziel ins Visier zu nehmen.

Darüber hinaus sollte die automatische Zuweisung von IP-Adressen per DHCP<sup>3</sup> deaktiviert werden. Nur Rechner mit Netzwerkkarten, die in der MAC-Filtertabelle eingetragen sind, sollten eine IP-Adresse erhalten.

## **Firewall, Paketfilter, Logbücher**

Die Mehrzahl der heute erhältlichen Access Points hat eine Firewall und Paketfilter an Bord. Wenn vorhanden, sind beide unbedingt zu aktivieren, um das Schutzniveau des Netzwerks anzuheben. Typische Funktionen sind die Abwehr von Denial-of-Service-Attacken, Ping-Anfragen, RIP-Requests und fragmentierten Datenpaketen.

## **Logbücher regelmäßig auswerten**

Auch wer die Grundsätze eines sicheren drahtlosen Heimnetzwerks befolgt, sollte sich nicht allzu sehr in Sicherheit wiegen. Es lohnt sich, die Speicherung von Statusinformationen (Logs) zu aktivieren und die erstellten Berichte regelmäßig auszuwerten. Geben die Log-Dateien Aufschluss über häufige Einbruchsversuche oder gar erfolgreiche Netzwerkanmeldungen von unbefugten Nutzern, ist es an der Zeit, strengere Sicherheitsvorkehrungen zu treffen.

---

<sup>2</sup> Die MAC-Adresse (Media Access Control, Ethernet-ID oder bei Apple Airport-ID und Ethernet-ID genannt) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Die MAC-Adresse wird der Sicherungsschicht, Schicht 2 des OSI-Modells, zugeordnet. Um die Sicherungsschicht mit der Vermittlungsschicht zu verbinden, wird zum Beispiel bei Ethernet das Address Resolution Protocol verwendet. Netzwerkgeräte brauchen dann eine MAC-Adresse, wenn sie auf Schicht 2 explizit adressiert werden sollen, um Dienste auf höheren Schichten anzubieten. Leitet das Gerät wie ein Repeater oder Hub die Netzwerkpakete nur weiter, ist es auf der Sicherungsschicht nicht sichtbar und braucht folglich keine MAC-Adresse. Bridges und Switches untersuchen zwar die Pakete der Sicherungsschicht, um das Netzwerk physikalisch in mehrere Kollisionsdomänen aufzuteilen, nehmen aber selbst nicht aktiv an der Kommunikation teil, brauchen also ebenfalls keine MAC-Adresse. Ein Switch benötigt nur dann eine MAC-Adresse, wenn er managebar ist bzw. Monitoring-Dienste anbietet (zum Beispiel über Telnet, SNMP oder HTTP). Bridges verwenden die MAC-Adresse für den Spanning Tree Algorithmus.

<sup>3</sup> Das Dynamic Host Configuration Protocol (DHCP) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computer in einem Netzwerk (z. B. Internet oder LAN). Das Dynamic Host Configuration Protocol wurde definiert im RFC 2131 und bekam von der Internet Assigned Numbers Authority (IANA) die UDP-Ports 67 und 68 zugewiesen.