WLAN-Sicherheit in Handwerksbetrieben

Einleitung
Nachfolgender Fachinformationstext informiert über technische Grundlagen zur WLAN-Technologie und hat insbesondere das Ziel, Schwachstellen und Gefährdungspotenziale aufzuzeigen. Weiterhin werden Optimierungsmethoden genannt sowie Hinweise zur Verbesserung der WLAN-Sicherheit gegeben.

Allgemeines
Die Abkürzung „WLAN“ steht für die englische Bezeichnung „wireless local area network“ (deutsch: „drahtloses lokales Netzwerk“) und bezeichnet ein lokales Funknetz, welches für die Übermittlung, den Empfang und den Austausch von Daten benutzt wird.

WLAN-Frequenzen liegen im lizenz- und genehmigungsfreien „ISM“-Band (wie z.B. auch Mikrowellengeräte und Babyphones).

Der im Juni 1997 festgelegte technische Standard nennt sich IEEE 802.11 und die WLAN-Technologie schaffte 1999 auch den Durchbruch im privaten Bereich.

Der Nachteil eines drahtlosen Netzwerkes ist aber dass sich die Informationen per Funk in alle Richtungen ausbreiten und ohne Schutzvorkehrungen von jedem mitgelesen werden können. Die Reichweiten sind vom jeweiligen technischen Standard sowie von der Frequenz abhängig. Meist liegen sie bei einigen Zehnermetern bis maximal einigen wenigen hundert Metern (nur auf freier Fläche).

WLAN safety quick check

Praxisnahe und schnelle Maßnahmen zur Verbesserung der WLAN-Sicherheit
1) Router per Passwort sichern (im Menü des Internet-Routers)
2) sicheres Passwort nutzen
3) WLAN bei Nichtgebrauch am Router ausschalten
4) Verschlüsselung aktivieren: WPA2 statt WEP oder WPA
5) Name des Funknetzes (SSID) ändern, also nicht z.B. „Maier-Netz“ o.ä.
6) Netzwerk unsichtbar machen im Router-Menü

Und diese Tipps für Spezialisten:
7) Abschalten des DHCP-Servers im Router. Nun können Router und Endgeräte nur miteinander kommunizieren wenn man im zu verbindenden Endgerät die notwendigen Informationen selbst einträgt. Die Folge ist allerdings ein umständlicher Verbindungsaufbau vom Endgerät zum Access Point Router.
8) Bei einem angeschalteten DHCP-Server im WLAN-Router muss man den Computern im Netzwerk feste IP-Adressen zuordnen.
9) Viele Router lassen sich so einstellen, dass sich nur bestimmte Geräte im Netzwerk anmelden können. Jede Netzwerkkarte eines PC´s oder Notebooks hat eine unverwechselbare Kennung, die Mac-Adresse. Diese wird pro Karte weltweit nur einmal vergeben. Trägt man also im Router die Mac-Adresse eines Endgerätes ein, dann bekommt (theoretisch) nur dieses Endgerät Zugriff auf das WLAN-Netzwerk.

WLAN-Optimierung / Sicherheitsmaßnahmen

Verschlüsselung
Das WLAN sollte nur mit der WPA2-Verschlüsselung betrieben werden. WPA2 steht für „WiFi-protected Access 2“. Falls technisch möglich, sollte man den WPS-Modus aktiv deaktivieren, um gänzlich auszuschließen, dass WPS-Signale gesendet werden.

Die VPN-Verschlüsselung
Virtual Private Networks (VPNs) leiten Internetdaten vom eigenen Gerät, zum Beispiel dem Smartphone, zuerst zu einem zwischengeschalteten Server (Proxy). Auf der Strecke zwischen Gerät und Proxy werden die Daten extra verschlüsselt. So können Dritte den Datenverkehr hier nicht mitlesen. Es ermöglicht also eine sichere Übertragung sensibler Daten über ein unsicheres Netzwerk. Vom Proxy gehen die Datenpakete dann zur eigentlichen Ziel-Adresse, zum Beispiel einer Webseite, die man gerade aufrufen möchte. Allerdings haben sie dann als Absender die IP-Adresse des Proxys und nicht mehr die eigene. So lässt sich die eigene IP-Adresse verschleiern.
Bisher gab es diesen VPN-Dienst nur bei Android-Geräten (einrichten über WLAN/sicheres WLAN am Smartphone). Nachteilig ist ein gewisser Geschwindigkeitsverlust.

Passwortschutz
Die Werkseinstellungen (login, Passwort) sind zu ändern, da die Zugangsdaten der Werkseinstellungen für nahezu alle Hersteller im Internet veröffentlicht sind. Fern- und Funkwartung sind abzuschalten. Viele Access Points bieten die Möglichkeit einer drahtlosen Konfiguration. Diese sollte vermieden werden, so dass der Angreifer die Einstellungen nicht über Funk verändern kann.

Leistungsanpassung
Die Sendeleistung eines WLAN´s ist auf die geringstmögliche Einstellung zu reduzieren.

WLAN-Empfang in den Betriebsräumen bzw. der Wohnung messen
So geht´s: den EKAHAU Heatmapper https://wifi.ekahau.com/heatmapper kostenlos downloaden, mit dem jeweiligen Endgerät (WLAN eingeschaltet) die Räume abschreiten und die Empfangsstärke der angezeigten WLAN-Systeme auf einem Raumplan notieren. Damit dann den optimalen Platz für den WLAN-Router bestimmen.

Der NetSurveyor (freier download aus dem Internet) dient dazu, für das eigene WLAN-Netz eine Optimierung durchzuführen, indem wenig belastete Kanäle identifiziert werden können.

Router-Platzierung
Stellen Sie den Router nicht auf den Boden – die Signale gehen nach unten und zur Seite. Besser: zentral an einer Wand befestigen.

Frequenzkanal ändern
Das Ausweichen auf von anderen WLAN-Nutzern in der Umgebung nicht oder weniger genutzte Frequenzkanäle kann die WLAN-Geschwindigkeit erheblich verbessern. Hierzu ist im WLAN-Menü des Routers der Funkkanal zu wechseln. Ggf. kann man sich mit Nutzern aus der näheren Umgebung (z.B. in einem Mehrfamilienhaus) absprechen.

Am Beispiel Fritzbox: unter WLAN/Funkkanal/WLAN-Umgebung findet sich eine grafische Darstellung, welches WLAN in der Nähe auf welchem Kanal arbeitet. Ähnliche Funktionalität bietet die App WiFi Analyzer (Android). Ebenso geeignet zur Kanaloptimierung: das sw tool „inSSIDer“ für Windows, macOS und Android.

Benachbarte Funkkanäle liegen in sehr geringen Abständen von je 5 MHz und können sich u.U. gegenseitig beeinflussen.

Firmware
Für Ihren Router gibt es regelmäßige Firmwareupdates. Ein Herunterladen dieser updates erhöht ganz allgemein die Sicherheit. Normalerweise werden Schwachstellen in den neuesten Versionen gepatcht.

Hacker-Angriffe und Sicherheitsüberprüfungen

Anzeichen für einen Hacker-Angriff sind:
- Unerklärliche Unterbrechung der Verbindung
- Die WLAN-Leuchte am Router leuchtet, obwohl das WLAN bei allen Endgeräten ausgeschaltet ist.

Prüfung auf Störungen
Wenn man bei allen WLAN-fähigen Geräten die Drahtlos-Verbindung ausschaltet und dann immer noch die WLAN-Leuchte am Router leuchtet wird vermutlich von außen ein Zugriffsversuch unternommen.

Zusätzlich kann man sih im Menü des Routers die Geräteliste anschauen und versuchen, die gelisteten Geräte zuzuordnen. Nicht zuordenbare Geräte deuten ebenfalls auf einen unautorisierten Zugriffsversuch hin.

Das Arbeiten im sogenannten „Hidden-Modus“ (SSID nicht sichtbar) bietet gegenüber professionellen Hackern keinen Schutz. Allerdings kann es nützlich sein gegenüber Gelegenheitstätern oder unabsichtlichen Kontakten. Hinweis: die „SSID“ steht auf der Rückseite des Routers auf einem label. Meist ist die Modellbezeichnung des Routers auch die SSID. Somit ist erklärbar, dass bei gleichlautenden SSID´s es zu Verwechslungen kommen kann, wenn die SSID´s nicht von ihren Betreibern umbenannt worden sind.

Geändertes Telemediengesetz
Die Haftung für Hotspot-Betreiber gibt es nicht mehr. Das vom Bundestag beschlossene WLAN-Gesetz gibt Betreibern öffentlicher hotspots in Zukunft mehr Rechtssicherheit. Die umstrittene Störerhaftung wurde abgeschafft. Bisher befanden sich Betreiber öffentlicher WLAN-Netze in einer rechtlichen Grauzone. Sie konnten dafür belangt werden, wenn hotspot-Nutzer urheberrechtlich geschützte Inhalte illegal darüber herunter geladen haben. Das Ziel der Reform ist es, mehr öffentliche hotspots entstehen zu lassen.

Die Suche nach hotspots in der Umgebung wird von

Gäste-WLAN
Das Gastnetzwerk kann am Router eingerichtet werden, ist vom Heimnetz getrennt und bietet zwar Zugriff auf das Internet, aber eben isoliert vom Heimnetzwerk. Wie der Name schon sagt, ist das Gast-WLAN ist ein spezielles Netzwerk nur für Gäste.

Es kann eine eigene SSID und ein separates Passwort (unter „WLAN-Netzwerkschlüssel“) vergeben werden.

Auch für dieses Gästenetz kann im Router-Menü eine Verschlüsselungsart gewählt werden, diese sollte ebenfalls WPA2 sein.

Alle IoT-Geräte mit einem korrekt konfigurierten Gastnetzwerk zu verbinden (NICHT mit Ihrem Hauptnetzwerk), bietet zusätzlichen Schutz vor Angriffen. Selbst wenn Cyberkriminelle eines Ihrer IoT-Geräte hacken sollten, können sie nicht in Ihr Hauptnetzwerk eindringen und die damit verbundenen Computer und Smartphones kompromittieren.

Die Sorglosbox

Die sorglosbox schützt sicher vor Abmahnungen und Gäste können das Internet so nutzen, wie sie es von ihrem eigenen Internetanschluss gewohnt sind. Die sorglosbox, ein separater Router baut ein komplett neues Netzwerk auf und trennt das Gäste-Netzwerk wirksam vom privaten Netzwerk, so dass Gäste keinen Zugriff auf das bestehende Netzwerk, private Geräte oder Daten haben können.

Die sorglosbox leitet den gesamten Datenverkehr des Gäste-Netzwerks zu den „sorglos Servern". Erst von dort aus gehen alle Datei- und Seitenaufrufe mit einer sorglos-IP-Adresse ins öffentliche Internet. Damit kann man im Ermittlungsfall nicht mehr als Anschlussinhaber herausgefunden werden. Die eigene IP-Adresse bleibt anonym.

Schutz in fremden WLAN-Netzen

Um den eigenen Computer in fremden WLAN-Netzen optimal zu schützen, muss man auf folgende Punkte achten:

- Aktiver und aktueller Virenscanner
- Aktive und aktuelle Firewall
- Ad-Hoc-Modus (Betriebsart von WLAN´s) immer deaktivieren

Angriffsmethoden

Nachfolgend aufgeführte Angriffstools (alles freeware) suchen aktiv nach Sicherheitslücken in WLAN-Netzen bzw. spüren Zugangspunkte auf:

- http://www.netstumbler.com/
- https://www.kismetwireless.net/
- https://www.wireshark.org/
- https://www.aircrack-ng.org/

Manchmal werden Hochleistungsantennen benutzt, um unentdeckt Zugänge aufzudecken.

Mac Spoofing: im Internet existieren Anleitungen, wie man die eigene Mac Adresse seines Rechners ändern kann. Hat der Angreifer nun eine Ziel-Mac-Adresse „ersnifft", kann er seinen eigenen Rechner mittels Mac Spoofing im fremden Netzwerk anmelden.

Man-in-the-middle-Attacken: durch Vorgabe, ein weiterer Router zu sein, kann ein Angreifer die Mac-Adresse des angegriffenen Computers erlangen. Gibt er Angreifer sich gegenüber dem Router dann mit der gleichen Mac-Adresse zu erkennen, gelangen zu ihm über den Router die gleichen Informationen wie zum angegriffenen Computer.

Denial-of-Service-Attacken („Verweigerung des Dienstes"): DoS-Attacken sind sehr effektiv und können einen Rechner innerhalb kurzer Zeit scheinbar bewegungslos machen, da er mit nichts anderem als der Beantwortung sinnloser Anfragen beschäftigt ist.

Serverbetreiber können dann zu einer Geldzahlung erpresst werden, damit ihr Internetangebot wieder erreichbar wird. Denial-of-Service-Attacken werden mittlerweile von Cyber-Kriminellen zum Kauf angeboten, um Konkurrenten zu schädigen.

War Driver: Hacker fahren ziellos mit dem Auto herum, um ungeschützte drahtlose LAN´s zu entdecken.

WLAN-Technik

WLAN-Mesh-Systeme
Ein WLAN-Mesh-System besteht aus einer Basis und mehreren Satelliten. Das Basisgerät wird mit einem LAN-Kabel an den Router angeschlossen. Die Satelliten werden im ganzen Gebäude verteilt. Diese Satelliten verbinden sich untereinander und stellen ein sogenanntes Mesh-Netzwerk her. Dieses Netzwerk kann alle Endgeräte, die sich per WLAN im Netzwerk befinden, verbinden. Mesh-Systeme besitzen Funktionen, welche die meisten Repeater nicht haben. Sie verbinden Geräte immer auf dem jeweils schnellsten Frequenzkanal und sie sollen Endgeräte immer mit demjenigen Satelliten verbinden, der gerade das beste Signal liefert.

WLAN-Repeater, RX/TX-Booster, Antennen
WLAN-Repeater sind Verstärker für das Funksignal und seit einiger Zeit schon recht preiswert. Die Übertragungsgeschwindigkeit wird dabei aber vom Router bestimmt und auch von einem Repeater nicht verbessert. Man kann nur Reichweiten vergrößern.

Nicht damit zu verwechseln sind sog. WLAN-RX-Booster. Sie sind mit dem empfangenden Gerät verbunden und steigern dessen Empfangsempfindlichkeit. Wieder etwas anders sind die sog. TX-Booster, die mit dem Router verbunden das WLAN-Signal verstärken.

WLAN-Antennen unterscheiden sich untereinander im Signalöffnungswinkel und können im 2,4 GHz-Frequenzband Signale gerichtet verstärken. Manche dieser Antennen sind durch ein Kabel an den Router anzuschließen.

Betriebsarten eines WLAN´s
Das Funknetz im Ad-Hoc-Modus besteht dabei aus einzelnen Komponenten, die sich selbst organisieren und direkt miteinander kommunizieren. Die Geräte müssen dabei den gleichen Funkkanal benutzen. Dabei muss man durch Drücken des WLAN icons am Computer ein neues drahtloses Netzwerk einrichten, dabei trennt man automatisch die Verbindung zum Router. An weiteren Computern dieses Netzwerkes muss der gleiche Netzwerkname gewählt werden. Die Reichweite im Ad-Hoc-Modus ist stark begrenzt.

Beim Infrastrukturmodus hingegen übernimmt der Router (Access Point) die Koordinierung des Datenverkehrs. Dies ist der üblicherweise verwendete Betriebsmodus bei einem WLAN-Netz.

WLAN auf größeren Flächen bzw. in größeren Räumen: um größere Flächen mit WLAN zu versorgen, gibt es die Möglichkeit, mehrere, räumlich verteilte Access Points mit dem lokalen Netzwerk zu verbinden. Hier ist dann ein Roaming zwischen den Zellen möglich. Der Benutzer wird dann beim Verlassen einer Zelle automatisch an die nächste Zelle weiter geleitet.

Haftungsausschluss
In unserem Fachinformationstext finden Sie externe Links auf die Internetseiten von Dritten. Auf den Inhalt dieser Webseiten haben wir keinen Einfluss und können daher keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist der jeweilige Betreiber verantwortlich. Zum Zeitpunkt der Link-Setzung wurde die verlinkte Seite auf mögliche Rechtsverstöße überprüft. Verstöße gegen geltendes Recht wurden nicht festgestellt. Eine ständige inhaltliche Kontrolle der verlinkten Internetseiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Sollten Rechtsverletzungen bekannt werden, entfernen wir unverzüglich derartige links.

Quellen

- Schulungsinhalte der Qualifizierung zum IT-Sicherheitsbotschafter: https://www.zdh.de/fachbereiche/zentralbereich/sicher-im-internet/it-sicherheitsbotschafter-im-handwerk/
- https://de.wikipedia.org/wiki/Wireless_Local_Area_Network
- https://www.computerbild.de/videos/cb-Tipps-DSL-WLAN-Mesh-Router-Infos-19656471.html
- https://www.e-recht24.de/news/telekommunikation/10976-wlan-hotspots-bgh-bestaetigt-aus-fuer-stoererhaftung.html
- https://www.computerbild.de/fotos/WLAN-Sicherheitstipps-2232051.html
- https://de.wikipedia.org/wiki/WPA2
- https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036
- https://de.wikipedia.org/wiki/Virtual_Private_Network
- https://www.elektronik-kompendium.de/sites/net/1712061.htm
- https://www.kaspersky.de/blog/guest-wifi/17693/
- http://www.spiegel.de/netzwelt/web/bgh-bestaetigt-ende-der-stoererhaftung-fuer-wlan-betreiber-a-1220278.html
- https://www.youtube.com/watch?v=ymaMgRATqUQ
- https://de.wikihow.com/Eine-MAC-Adresse-t%C3%A4uschen
- https://de.wikipedia.org/wiki/Denial_of_Service
- https://www.kaspersky.de/blog/was-ist-eine-man-in-the-middle-attacke/905/