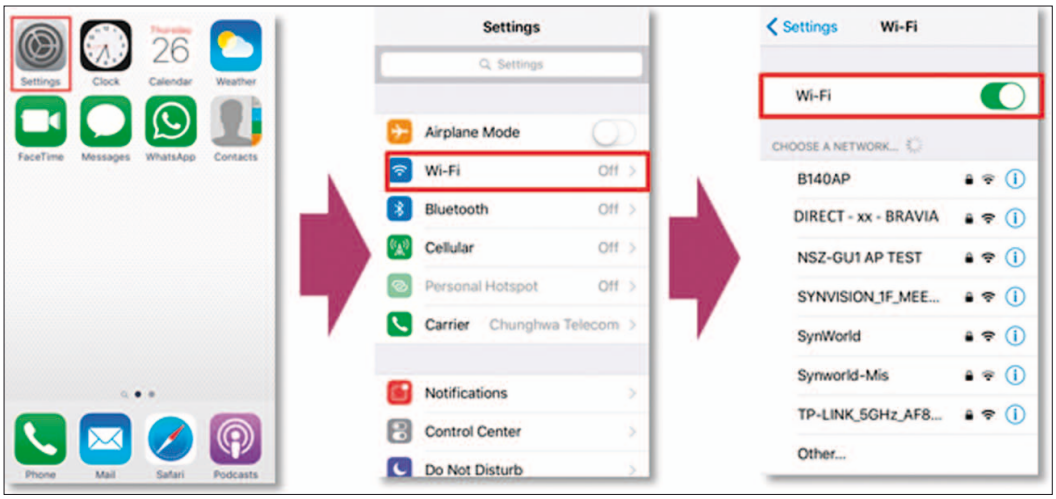
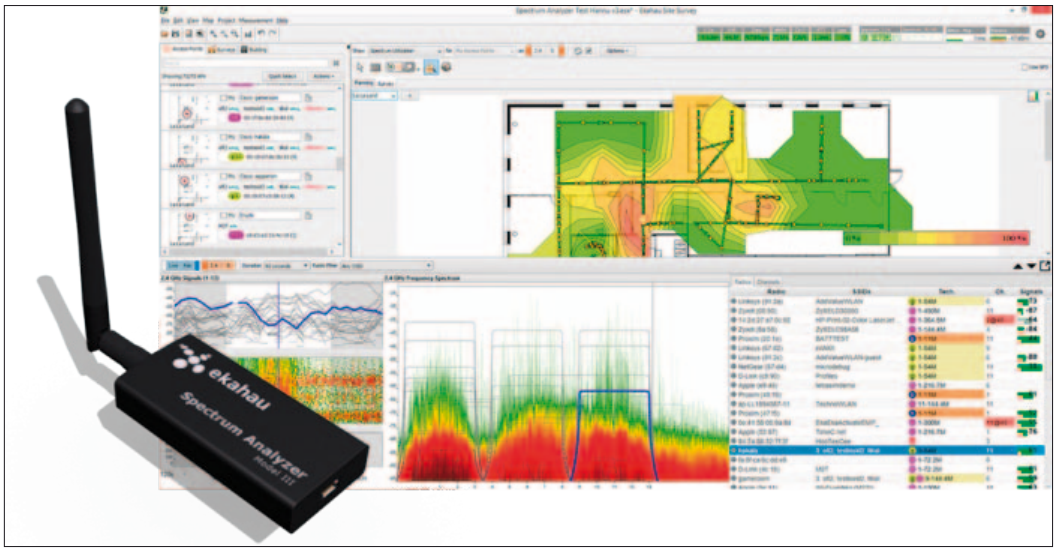
WiFi, WLAN, WPA & Co.



WiFi und Mobilfunk verschmelzen: Verwenden der WiFi-Direct-Funktion mit einem iPhone (Sony)

Die Begriffe hängen eng miteinander zusammen. Der ganze Themenbereich ist immer noch im Wandel. Aktuelle Neuerungen sind WPA3 und WiFi 4 bis 6. Ein Überblick



Entdecken, orten und beseitigen von WiFi-Interferenzen mit dem Ekahau WiFi Spectrum Analyzer (Werksbild)

WiFi bezeichnet sowohl ein Firmenkonsortium, das Geräte mit Funkschnittstellen zertifiziert, als auch den zugehörigen Markenbegriff. In Analogie zu HiFi gebildet, ist WiFi ist ein für Vermarktungszwecke erfundener Kunstbegriff. Das Wi steht sicher für Wireless, das Fi für Fidelity. Oft dient WiFi als Synonym für WLAN, doch das Wireless Local Area Network bezeichnet das Funknetzwerk, WiFi hingegen die Zertifizierung durch die WiFi-Alliance anhand des Standards IEEE-802.11. WPA schließlich steht für WiFi Protected Access und ist ein Sicherheitsstandard für Computer mit einer WiFi-Funkverbindung. WPA ist die Verbesserung des ursprünglichen Security-Standards für Wi-Fi WEP (Wired Equivalent Privacy), der als nicht mehr sicher gilt.

Die WiFi Alliance wurde 1999 unter dem Namen Wireless Ethernet Compatibility Alliance (WECA) gegründet und 2002 umbenannt. Die WiFi Alliance zertifiziert die Produkte verschiedener Hersteller auf der Basis des IEEE-802.11-Standards, sodass der Betrieb untereinander gewährleistet ist (Interoperabilität). Diese Produkte erhalten das WiFi-Zertifikat und dürfen das entsprechende Logo tragen. Allerdings stellt ein fehlendes WiFi-Logo nicht zwangsläufig eine Abweichung vom Standard dar. Ein standardkonformes Produkt ohne Logo wurde nur nicht zur Prüfung eingereicht. Die WiFi-Alliance umfasst über 300 Unternehmen als Mitglieder.

Bedrohungen für die WLAN-Sicherheit

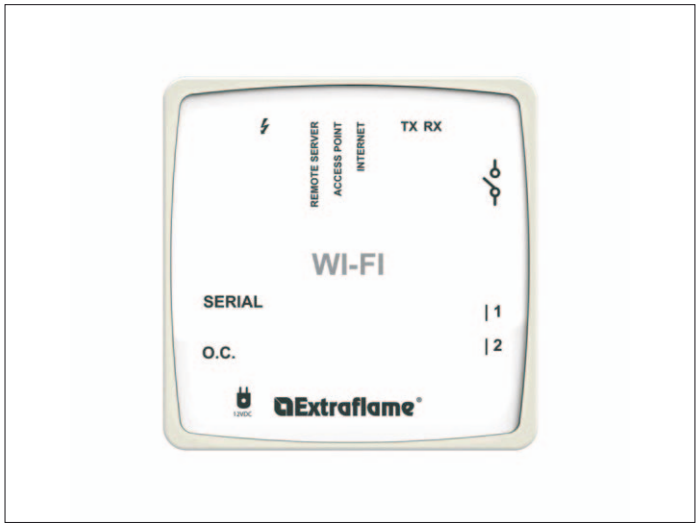
Die unzureichende Sicherheit im internen Unternehmens-WLAN ist ein Grund, sich Sorgen zu machen. Neben neuen Bedrohungen, vor allem aus dem Mobilbereich, sind natürlich auch die alten Angriffsmethoden eine latente Gefahr. Ein E-Handbook bietet dazu Information und Tipps. Es ist erreichbar über:

www.searchnetworking.de/definition/WPA-WPA2-WiFi-Protected-Access

Zum Thema „WLAN absichern und neue Bedrohungen abwehren“ finden sich Links auf:

www.elektronik-kompendium.de/sites/net/2009011.htm

Ein WiFi Audio Streaming Receiver (Werksbild)



Modul für die Fernsteuerung via WiFi-System (Werksbild). Das Gerät nutzt den Internet-Anschluss am Aufstellungsort

WiFi Protected Access (WPA)

beruht auf einer fortschrittlichen Datenverschlüsselung und bietet die Authentifizierung für Anwender. Nach der Verabschiedung von IEEE 802.11i erweiterte die WiFi Alliance den Standard WPA um eine zweite Version WPA2. Der wesentliche Unterschied ist die Verschlüsselungsmethode. Während WPA das weniger sichere TKIP (Temporary Key Integrity Protocol) verwendet, kommt in WPA2 das sichere AES zum Einsatz. Der Advanced-Encryption-Standard ist ein Algorithmus für die symmetrische Blockverschlüsselung (Blockchiffre) wichtiger Informationen. AES ist weltweit in Soft- und Hardware implementiert, um sensible Daten zu verschlüsseln.

Die Version WPA2 ist selbst bei Heimanwendern Standard. Jeder Heim-Router wird per Voreinstellung mit WPA2 als Verschlüsselung ausgeliefert. Im professionellen Bereich ist WPA2 praktisch vollständig etabliert.

Die starke Anwender-Authentifizierung basiert auf dem Standard 802.1x und dem EAP (Extensible Authentication Protocol). WPA hängt von einem zentralen Authentifizierungsserver wie zum Beispiel RADIUS (Remote Authentication Dial-In User Service) ab.

WPA2 lässt sich derzeit nur mit sogenannten Brute-Force-Angriffen knacken. Das Passwort kann auch per Wörterbuchangriff erraten werden (Dictionary Attack). Um diesen Angriffen zu begegnen, sollte man ein möglichst langes und komplexes Passwort verwenden. Selbst Heim-Router bieten eigentlich stets die Möglichkeit von WPA2-PSK (Pre-Shared Key) an. In diesem Fall meldet sich das Client-Gerät mithilfe eines Passworts am drahtlosen Netzwerk an.

Das Sicherheitskonzept von WPA beruht auf der Trennung von Benutzer-Authentifizierung, Nachrichtenverschlüsselung und Integritätssicherung. Schlüssel werden regelmäßig neu erstellt. Verschiedene Schlüssel gibt es für verschiedene Anwendungen. Der Master Key bildet nur die Grundlagen für die Schlüsselerzeugung.

Im Jahr 2018 wurde der Nachfolger WPA3 spezifiziert, der einige Fehler, die bei der Implementierung entstehen können, beseitigt. Außerdem wurde WPA3 an die aktuelle Sicherheitslage angepasst. WLAN ist nun auch in besonders geschützten Bereichen wie Regierungseinrichtungen oder dem Militär möglich. Bis der WPA3-Standard flächendeckend zum Einsatz kommt, wird allerdings noch etwas Zeit vergehen. Die komplette Umstellung der Produktion erfolgt vermutlich ab 2019.

Im Oktober 2018

gab die WiFi Alliance bekannt, dass die Funknetze in Zukunft WiFi 4, WiFi 5 und WiFi 6 genannt werden sollen, um den Nutzern die unterschiedlichen Standards einfacher zu machen. WiFi 4 steht dabei für den IEEE 802.11n-Standard, WiFi 5 für den Standard 802.11ac und WiFi 6 für den neuen Standard 802.11ax. Die dahinter stehende Absicht ist, Anwendern den optimalen Einsatz zu erleichtern. Jede der neuen Generation bietet neue Features und bessere Eigenschaften als der Vorgänger, wie höhere Geschwindigkeit, gesteigerten Durchsatz oder bequemere Anwendung. Hierzu gehört auch ein verbessertes User Interface (UI).

Mit dem Beginn von Wi-Fi 6 hat die WiFi Alliance ein überarbeitetes Zertifikationsprogramm angekündigt, WiFi Certified 6™, um auch hier eine hohe Qualität und problemlose Interoperabilität sicherzustellen. ***FS***

Die Mini HD WiFi Camera DCS 8000LH (dlink)