WLAN

Ob zuhause, am Arbeitsplatz oder im öffentlichen Raum: Mit mobilen Geräten ist es heute fast überall und zu jeder Zeit möglich online zu sein. Oft wird dabei ein WLAN genutzt.

Schützen Sie sich, indem Sie...

- unbekannte WLANs nur eingeschränkt nutzen resp. nach Möglichkeit ganz meiden.
- kein E-Banking über öffentliche WLANs betreiben und über diese prinzipiell keine vertraulichen Daten senden.
- sich, wenn immer möglich, nur mit verschlüsselten WLANs verbinden.
- bei Ihrem eigenen Access Point eine aktuelle Verschlüsselungsmethode (WPA) mit einem starken Passwort verwenden.

Funktionsprinzip

Dank der Nutzung der Funktechnik bieten WLANs eine äusserst flexible, komfortable Möglichkeit, sich von einem mobilen Gerät aus mit einem Netzwerk und dem Internet zu verbinden. Dies ohne die Notwendigkeit sich über eine lästige Verkabelung Gedanken machen zu müssen. Für mobile Geräte, wie z. B. Tablets, ist es oft gar die einzige Möglichkeit, sich mit dem Netzwerk zu verbinden. Auch bei Smartphones ist dieser Verbindungstyp häufig aktiviert.

Die Nutzung und der Betrieb von solchen Funknetzwerken bergen aber auch gewisse Risiken, welche vielen nicht immer bewusst sind.

WLAN sicher Nutzen

Haben Sie ein «gesundes» Mass an Misstrauen, wenn Sie ein unbekanntes WLAN nutzen.

Wenn immer möglich, verbinden Sie sich nur mit (WPA2 oder WPA3) verschlüsselten WLANs.

Betreiben Sie kein E-Banking und senden Sie keine vertraulichen Daten über öffentliche Funknetzwerke, z. B. «Hotspots» in öffentlichen Räumen (Städten, Bahnhöfen etc.) oder Hotels.

Setzen Sie für vertrauliche Daten unabhängig von der gewählten Übertragungstechnik End-zu-End-Verschlüsselung ein.

Deaktivieren Sie falls möglich für unbekannte und nicht geschützte WLANs die Funktion «automatisch verbinden» bei ihrem mobilen Gerät.

WLAN sicher Betreiben

Aktivieren Sie eine starke Verschlüsselung, mindestens WPA, besser WPA2 oder WPA3, und wählen Sie unbedingt einen starken Netzwerkschlüssel bzw. Passwort.

Ändern Sie die SSID des Netzwerkes, sofern diese Angaben zu einer Person, z. B. Familiennamen, oder Informationen zum Router, z. B. dessen Typ, enthält.

Ersetzen Sie die werkseitig voreingestellten Router-Passwörter durch eigene, starke.

Aktivieren Sie den MAC-Filter.

Falls möglich reduzieren Sie die Sendeleistung Ihres WLAN-Routers und schalten Sie diesen aus, wenn das lokale Funknetzwerk nicht gebraucht wird.

Treffen Sie entsprechende Vorkehrungen auch beim Betreiben von eigenen Hot-Spots auf Ihren Handy, um einem Missbrauch Ihrer mobilen Internetverbindung vorzubeugen.

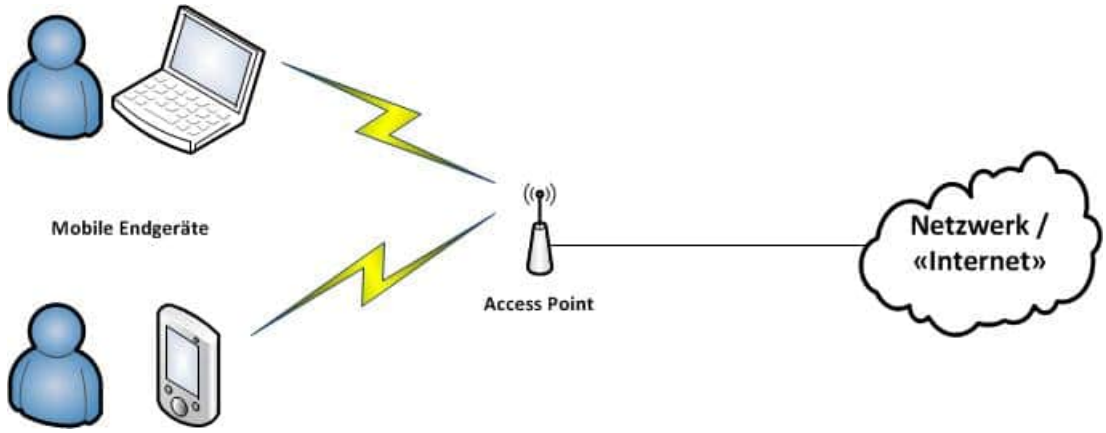
WLAN steht für Wireless Local Area Network, zu Deutsch etwa «lokales Funknetzwerk». Die drahtlose Kommunikation ist äusserst flexibel, komfortabel und deshalb heute weit verbreitet.

Die Nutzung und der Betrieb von WLANs bergen aber auch gewisse Risiken. Mit den richtigen Massnahmen können sie die Sicherheit wesentlich erhöhen.

Weiterführende Informationen für Interessierte

Aufbau eines WLAN

Die zentrale Komponente in einem WLAN stellt der Access Point dar. Er ist das Bindeglied zwischen der Luftschnittstelle zu den mobilen Endgeräten auf der einen Seite und dem kabelgebundenen Netzwerk und dem Internet auf der anderen Seite. Der Access-Point «erzeugt» das WLAN, indem er über seine Antenne Funksignale in alle Raumrichtungen aussendet.



Damit die Endgeräte das WLAN «sehen» können, sendet der Access Point normalerweise eine Netzwerkkennung - die sogenannte SSID (Service Set Identifier) - aus. Darüber kann der Nutzer die an einem Ort verfügbaren WLANs unterscheiden und die gewünschte Verbindung auswählen.

Verschlüsselung

Die Nutzung einer Funkübertragung hat den Nachteil, dass es relativ einfach ist, die übertragenen Daten mitzulesen. Grundsätzlich bekommt jedes Gerät, das sich im Sendebereich eines WLANs befindet den gesamten Datenverkehr mit. Deshalb sollte die Verbindung zwischen den mobilen Endgeräten und dem Access Point verschlüsselt werden. Damit kann zwar nicht verhindert werden, dass die Kommunikation mitgelesen wird – aber wenigstens kann niemand etwas damit anfangen.

Es existieren verschiedene Verschlüsselungsverfahren:

- **WEP**
  Wired Equivalent Privacy war das erste Verschlüsselungsprotokoll, das standardmässig in WLANs genutzt wurde. Es gilt aber mittlerweile als unsicher und kann relativ einfach geknackt werden. Deshalb sollte es nicht mehr eingesetzt werden.
- **WPA**
  WiFi Protected Access ist die Weiterentwicklung des WEP-Protokolls. Verbesserte Sicherheitsmechanismen garantieren einen höheren Schutz. So wurde die Authentifizierung der Teilnehmenden im Netzwerk verbessert sowie dynamische Schlüssel für die Übertragung eingeführt.
- **WPA2**
  WPA2 baut auf WPA auf, nutzt aber den starken AES-Algorithmus für das Chiffrieren der Datenübertragung.
- **WPA3**

WPA3 stellt den aktuell jüngsten Verschlüsselungsstandard für drahtlose Netze dar. Damit werden gegenüber WPA2 insbesondere Attacken auf das Verschlüsselungspasswort wesentlich erschwert.

Wenn immer möglich, sollte heute nur noch WPA2 resp. wo verfügbar WPA3 in WLANs zum Einsatz kommen. Der Preshared Key, also gewissermassen das Passwort zum Netzwerk, muss genügend stark gewählt werden. Er sollte mindestens 16 Zeichen lang sein und die Eigenschaften eines starken Passwortes (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) aufweisen.

In diesem Zusammenhang muss zudem festgehalten werden, dass damit nur die Strecke zwischen dem Endgerät und dem Access Point geschützt ist. Diese Verschlüsselung wird auf dem Access Point jedoch terminiert, weshalb ab hier die Daten wieder ungeschützt unterwegs sind. Vertrauliche Inhalte sollten daher unabhängig von der gewählten Übertragungstechnik End-zu-End verschlüsselt werden, z.B. beim Surfen im Internet oder beim E-Banking mit einer TLS/SSL-Verschlüsselung (https, Schlosssymbol).

MAC-Filter

Jedes Netzwerkgerät, also auch alle mobilen Endgeräte, besitzen eine MAC-Adresse, über welche sie grundsätzlich eindeutig identifiziert werden können. Access Points bieten die Möglichkeit, einen MAC-Filter zu nutzen. Dadurch dürfen nur registrierte mobile Geräte mit bekannter MAC-Adresse auf das Netzwerk zugreifen.

Die MAC-Adressen der Geräte sind jedoch nicht fälschungssicher. Mit entsprechenden Werkzeugen kann eine berechtigte MAC-Adresse «vorgegaukelt» und der Filter damit umgangen werden. Um einem potenziellen Angreifer aber eine weitere Hürde in den Weg zu stellen, sollte die MAC-Filter Option trotzdem genutzt werden.