3.11 Sicherheit im WLAN

WLAN muss besonders gut abgesichert werden, weil die Datenübertragung per Funk erfolgt.

Bei einem kabelgebundenen Netzwerk muss man meistens physischen Zugang zu einer Netzwerkdose oder einem Kabel haben.

Bei WLAN kann das Funksignal je nach Reichweite auch außerhalb des Gebäudes empfangbar sein.

Deshalb gilt:

> WLAN ohne ausreichende Verschlüsselung ist ein Sicherheitsrisiko.

Warum ist WLAN-Sicherheit wichtig?

WLAN ist ein Funknetz.

Das bedeutet:

> Die Daten werden über elektromagnetische Wellen übertragen.

Diese Funkwellen können sich über Räume, Wände und teilweise auch über Gebäudegrenzen hinaus ausbreiten.

Mögliche Risiken:

> - unbefugter Zugriff auf das Netzwerk
> - Mitlesen unverschlüsselter Daten
> - Nutzung des Internetanschlusses durch Fremde
> - Zugriff auf interne Systeme
> - Angriffe auf Clients oder Server
> - Missbrauch des Netzwerks für illegale Aktivitäten

Merksatz:

> WLAN endet nicht automatisch an der Wand.

Begriff: WLAN-Verschlüsselung

WLAN-Verschlüsselung schützt die Funkverbindung zwischen Client und Access Point.

Ziel:

> Daten sollen nicht im Klartext über Funk übertragen werden.

Vereinfacht gesagt:

> Nur berechtigte Geräte mit passenden Zugangsdaten sollen das WLAN nutzen können.

Wichtig:

> WLAN-Verschlüsselung schützt die Funkstrecke.
> Sie ersetzt keine Firewall,
> keine Benutzerrechte
> und keine sichere Anwendungskommunikation.

Merksatz:

> WLAN-Verschlüsselung schützt die drahtlose Verbindung.

WEP

WEP steht für:

> Wired Equivalent Privacy

WEP ist ein alter WLAN-Sicherheitsstandard.

WEP gilt heute als unsicher und sollte nicht mehr verwendet werden.

Problem:

> WEP kann mit heutigen Mitteln relativ leicht angegriffen werden.

Für die Prüfung wichtig:

> WEP ist veraltet und unsicher.

Merksatz:

```
WEP nicht mehr verwenden.
```

WPA

WPA steht für:

```
Wi-Fi Protected Access
```

WPA wurde als Nachfolger von WEP eingeführt.

WPA war sicherer als WEP, gilt heute aber ebenfalls als veraltet.

Für moderne WLANs sollte WPA nicht mehr als bevorzugter Sicherheitsstandard verwendet werden.

Merksatz:

```
WPA war ein Zwischenschritt,
ist heute aber nicht mehr Stand der Technik.
```

WPA2

WPA2 steht für:

```
Wi-Fi Protected Access 2
```

WPA2 ist lange Zeit der wichtigste Sicherheitsstandard für WLAN gewesen.

WPA2 verwendet in der Praxis meistens AES zur Verschlüsselung.

AES steht für:

```
Advanced Encryption Standard
```

Wichtig:

WPA2 gilt deutlich sicherer als WEP und WPA.
Für viele Netze ist WPA2 weiterhin verbreitet.
Wenn möglich, sollte WPA3 verwendet werden.

Merksatz:

WPA2 ist der ältere moderne Mindeststandard.

WPA3

WPA3 steht für:

Wi-Fi Protected Access 3

WPA3 ist der neuere WLAN-Sicherheitsstandard.

Er verbessert die Sicherheit gegenüber WPA2.

Vorteile:

- besserer Schutz bei schwachen Passwörtern
- moderneres Authentifizierungsverfahren
- verbesserte Sicherheit in offenen Netzen
- stärkerer Schutz gegen bestimmte Angriffe

Wichtig:

Access Point und Client müssen WPA3 unterstützen.

Merksatz:

WPA3 ist aktueller und sicherer als WPA2.

WPA2 versus WPA3

Merkmal	WPA2	WPA3
Alter	älter	neuer

Merkmal	WPA2	WPA3
Sicherheit	gut, wenn korrekt konfiguriert	besser
Geräteunterstützung	sehr weit verbreitet	abhängig von Gerät und Betriebssystem
Passwortschutz	abhängig von Passwortstärke	besser gegen bestimmte Angriffe
Empfehlung	Mindeststandard	bevorzugt, wenn verfügbar

Prüfungstauglich:

```
WLAN sollte mindestens mit WPA2,
besser mit WPA3 abgesichert werden.
```

Begriff: Pre-Shared Key

Pre-Shared Key bedeutet:

```
vorab geteilter Schlüssel
```

Abkürzung:

```
PSK
```

Bei WPA2-Personal oder WPA3-Personal verwenden alle berechtigten Nutzer dasselbe WLAN-Passwort.

Beispiel:

```
SSID: Firma-Gast
Passwort: gemeinsames WLAN-Passwort
```

Vorteil:

```
einfach einzurichten
```

Nachteil:

```
Das Passwort wird mit mehreren Personen geteilt.
```

Merksatz:

```
PSK = gemeinsames WLAN-Passwort.
```

WPA-Personal

WPA-Personal wird häufig in kleinen Netzen oder Heimnetzen verwendet.

Dabei wird ein gemeinsames WLAN-Passwort verwendet.

Typische Einsatzbereiche:

```
- Heimnetz
- kleines Büro
- Gast-WLAN
- einfache WLAN-Umgebung
```

Wichtig:

```
Das Passwort muss ausreichend lang und sicher sein.
```

Merksatz:

```
WPA-Personal = WLAN-Zugang mit gemeinsamem Passwort.
```

WPA-Enterprise

WPA-Enterprise wird häufig in Unternehmen, Schulen und größeren Organisationen verwendet.

Dabei meldet sich jeder Benutzer oder jedes Gerät individuell an.

Häufige Technik:

```
802.1X
RADIUS-Server
```

Vorteile:

```
- individuelle Benutzerkonten
- zentrale Verwaltung
- einzelne Benutzer können gesperrt werden
- besser für größere Umgebungen
- keine gemeinsame Passwortweitergabe nötig
```

Merksatz:

```
WPA-Enterprise = individuelle Anmeldung statt gemeinsamem WLAN-Passwort.
```

Begriff: 802.1X

802.1X ist ein Standard für portbasierte Netzwerkzugangskontrolle.

Er wird bei kabelgebundenen und drahtlosen Netzwerken eingesetzt.

Im WLAN-Kontext ermöglicht 802.1X eine Anmeldung mit individuellen Benutzerdaten oder Zertifikaten.

Typischer Zusammenhang:

```
Client
Access Point
RADIUS-Server
```

Merksatz:

```
802.1X = kontrollierter Netzwerkzugang mit Authentifizierung.
```

Begriff: RADIUS

RADIUS steht für:

```
Remote Authentication Dial-In User Service
```

RADIUS ist ein Dienst zur zentralen Authentifizierung.

Im WLAN kann ein RADIUS-Server prüfen, ob ein Benutzer oder Gerät Zugang erhalten darf.

Typische Aufgabe:

```
Benutzername und Passwort oder Zertifikat prüfen.
```

Merksatz:

```
RADIUS = zentrale Prüfung von Zugangsdaten.
```

Begriff: Authentifizierung

Authentifizierung bedeutet:

```
Nachweis der Identität
```

Beispiel:

```
Ein Benutzer meldet sich mit Benutzername und Passwort an.
Ein Gerät weist sich mit einem Zertifikat aus.
```

Im WLAN bedeutet Authentifizierung:

```
Der Client muss nachweisen,
dass er das WLAN nutzen darf.
```

Merksatz:

```
Authentifizierung = Wer bist du?
```

Begriff: Autorisierung

Autorisierung bedeutet:

```
Festlegen, was ein Benutzer oder Gerät darf.
```

Beispiel:

```
Ein Mitarbeiter darf ins interne WLAN.
Ein Gast darf nur ins Internet.
Ein IoT-Gerät darf nur bestimmte Server erreichen.
```

Merksatz:

```
Authentifizierung = Wer bist du?
Autorisierung = Was darfst du?
```

Begriff: SSID

SSID steht für:

```
Service Set Identifier
```

Die SSID ist der Name eines WLANs.

Beispiele:

```
Firma-Mitarbeiter
Firma-Gast
Firma-IoT
```

Wichtig:

```
Die SSID ist nicht das Passwort.
Die SSID ist nur der Name des WLANs.
```

Merksatz:

```
SSID = WLAN-Name.
```

SSID-Trennung

Es ist sinnvoll, verschiedene WLANs für verschiedene Zwecke zu verwenden.

Beispiele:

SSID	Zweck
Firma-Mitarbeiter	interne Geräte und Benutzer
Firma-Gast	Besucher und private Geräte
Firma-IoT	Kameras, Sensoren, Smart-Geräte
Firma-Admin	administrative Geräte

Vorteil:

Unterschiedliche Nutzergruppen können voneinander getrennt werden.

Wichtig:

Die Trennung erfolgt nicht nur durch verschiedene Namen,
sondern technisch durch VLANs und Firewall-Regeln.

Merksatz:

Mehrere SSIDs helfen bei der Trennung von Nutzergruppen.

Gast-WLAN

Ein Gast-WLAN ist ein separates WLAN für Besucher.

Ziel:

Gäste erhalten Internetzugang,
aber keinen Zugriff auf interne Systeme.

Typische Eigenschaften:

- eigene SSID
- eigenes VLAN
- getrennte Firewall-Regeln
- kein Zugriff auf Server oder Clients im internen Netz
- häufig zeitlich begrenzter Zugang
- oft mit Captive Portal

Merksatz:

> Gast-WLAN vom internen Netzwerk trennen.

Begriff: VLAN

VLAN steht für:

> Virtual Local Area Network

Ein VLAN ist ein logisch getrenntes Netzwerk innerhalb einer physischen Netzwerkinfrastruktur.

Im WLAN kann jede SSID einem VLAN zugeordnet werden.

Beispiel:

SSID	VLAN	Zweck
Firma-Mitarbeiter	VLAN 10	internes Netzwerk
Firma-Gast	VLAN 20	Gastzugang
Firma-IoT	VLAN 30	Geräte-Netz

Merksatz:

> SSID = WLAN-Name.
> VLAN = logische Netztrennung.

Firewall-Regeln für WLAN

Eine Firewall kann festlegen, welche Kommunikation erlaubt oder blockiert wird.

Beispiele:

> Mitarbeiter-WLAN darf auf interne Server zugreifen.
> Gast-WLAN darf nur ins Internet.
> IoT-WLAN darf nur zu bestimmten Diensten.
> Admin-WLAN darf auf Netzwerkgeräte zugreifen.

Wichtig:

Ein separates WLAN ohne passende Firewall-Regeln ist keine vollständige Sicherheitslösung.

Merksatz:

VLAN trennt logisch.
Firewall regelt den Zugriff.

Begriff: Captive Portal

Ein Captive Portal ist eine Anmeldeseite für Netzwerke.

Es wird häufig bei Gast-WLANs eingesetzt.

Beispiel:

Ein Gast verbindet sich mit dem WLAN.
Danach öffnet sich eine Webseite.
Dort muss er Nutzungsbedingungen akzeptieren oder Zugangsdaten eingeben.

Merksatz:

Captive Portal = Anmeldeseite für Netzwerkzugang.

Sichere WLAN-Passwörter

Bei WPA-Personal ist ein sicheres Passwort sehr wichtig.

Ein gutes WLAN-Passwort sollte:

- lang sein
- nicht leicht zu erraten sein
- keine Wörterbuchbegriffe enthalten
- nicht mehrfach verwendet werden
- regelmäßig überprüft werden
- bei Verdacht geändert werden

Wichtig:

Ein kurzer oder einfacher Schlüssel schwächt auch moderne Verschlüsselung.

Merksatz:

Starkes WLAN-Passwort = wichtiger Sicherheitsfaktor.

MAC-Filter

Ein MAC-Filter erlaubt oder blockiert Geräte anhand ihrer MAC-Adresse.

Problem:

MAC-Adressen können gefälscht werden.

Deshalb gilt:

MAC-Filter können eine kleine Zusatzhürde sein,
ersetzen aber keine echte WLAN-Sicherheit.

Wichtig für die Prüfung:

MAC-Filter sind kein ausreichender Schutz.

Merksatz:

MAC-Filter ist Zusatz,
aber keine starke Sicherheit.

SSID verstecken

Manche WLANs verstecken ihre SSID.

Das bedeutet:

Der WLAN-Name wird nicht aktiv sichtbar ausgesendet.

Problem:

Versteckte SSIDs können trotzdem erkannt werden.

Deshalb gilt:

SSID verstecken ist keine echte Sicherheitsmaßnahme.

Merksatz:

Versteckte SSID ersetzt keine Verschlüsselung.

WPS

WPS steht für:

Wi-Fi Protected Setup

WPS soll das Verbinden von Geräten erleichtern.

Beispiele:

Verbindung per Taste
Verbindung per PIN

Problem:

Besonders WPS-PIN kann ein Sicherheitsrisiko sein.

Empfehlung:

WPS deaktivieren,
wenn es nicht benötigt wird.

Merksatz:

WPS ist bequem,
kann aber ein Sicherheitsrisiko sein.

WLAN und Updates

Access Points, WLAN-Router und Controller sollten aktuell gehalten werden.

Gründe:

```
- Sicherheitslücken schließen
- Stabilität verbessern
- Kompatibilität verbessern
- neue Funktionen erhalten
- bekannte Angriffe erschweren
```

Wichtig:

```
Auch Netzwerkgeräte benötigen regelmäßige Sicherheitsupdates.
```

Merksatz:

```
WLAN-Sicherheit braucht auch aktuelle Firmware.
```

WLAN und Gerätesicherheit

Nicht nur der Access Point ist wichtig.

Auch die Endgeräte müssen sicher sein.

Dazu gehören:

```
- aktuelles Betriebssystem
- aktuelle Treiber
- aktuelle Sicherheitsupdates
- sichere Benutzerkonten
- Virenschutz bzw. Endpoint-Schutz
- keine unsicheren gespeicherten WLANs
```

Merksatz:

```
WLAN-Sicherheit betrifft Access Point und Clients.
```

Offene WLANs

Ein offenes WLAN hat keine Verschlüsselung auf der Funkstrecke.

Risiken:

- Daten können leichter mitgelesen werden
- fremde Geräte können sich verbinden
- höhere Missbrauchsgefahr
- Nutzer verlassen sich eventuell fälschlich auf Sicherheit

Wichtig:

Auch wenn Anwendungen HTTPS nutzen,
sollte das WLAN selbst trotzdem sicher konfiguriert werden.

Merksatz:

Offenes WLAN ist nur mit zusätzlicher Absicherung sinnvoll.

WLAN und HTTPS

HTTPS verschlüsselt die Verbindung zwischen Browser und Webserver.

Das ist wichtig, aber:

HTTPS ersetzt keine WLAN-Verschlüsselung.

Warum?

WLAN-Verschlüsselung schützt die Funkstrecke.
HTTPS schützt die Anwendungskommunikation zwischen Client und Server.

Beide schützen unterschiedliche Bereiche.

Merksatz:

```
WPA schützt WLAN.
HTTPS schützt Webkommunikation.
```

Rogue Access Point

Ein Rogue Access Point ist ein unerlaubter oder nicht autorisierter Access Point im Netzwerk.

Beispiele:

```
- Mitarbeiter steckt privaten WLAN-Router ins Firmennetz
- Angreifer stellt ein gefälschtes WLAN bereit
- falsch konfigurierte WLAN-Hardware wird angeschlossen
```

Risiko:

```
Sicherheitsregeln können umgangen werden.
Benutzer können sich mit falschen WLANs verbinden.
```

Merksatz:

```
Rogue Access Point = unerlaubter Access Point.
```

Evil Twin

Ein Evil Twin ist ein gefälschter Access Point, der eine bekannte SSID nachahmt.

Ziel:

```
Benutzer sollen sich versehentlich mit dem falschen WLAN verbinden.
```

Beispiel:

```
echtes WLAN: Firma-WLAN
gefälschtes WLAN: Firma-WLAN
```

Schutz:

```
- WPA-Enterprise mit Zertifikatsprüfung
- Benutzer sensibilisieren
- WLAN-Monitoring
- keine automatischen Verbindungen zu unbekannten Netzen
```

Merksatz:

```
Evil Twin = gefälschtes WLAN mit bekanntem Namen.
```

Client-Isolation

Client-Isolation bedeutet, dass WLAN-Clients nicht direkt miteinander kommunizieren dürfen.

Das ist besonders sinnvoll bei Gast-WLANs.

Beispiel:

```
Gast A kann nicht auf Gerät von Gast B zugreifen.
```

Vorteil:

```
weniger Risiko durch Angriffe zwischen verbundenen Clients
```

Merksatz:

```
Client-Isolation trennt WLAN-Clients voneinander.
```

WLAN-Sicherheit in Unternehmen

In Unternehmen sollte WLAN-Sicherheit geplant und dokumentiert werden.

Wichtige Punkte:

```
- WPA2 oder besser WPA3
- bei größeren Umgebungen WPA-Enterprise
- getrennte SSIDs
- VLAN-Trennung
```

- Firewall-Regeln
- Gast-WLAN getrennt vom internen Netz
- regelmäßige Updates
- sichere Passwörter oder Zertifikate
- Monitoring
- Dokumentation
- Deaktivierung unsicherer Altstandards

Merksatz:

WLAN-Sicherheit besteht aus Verschlüsselung, Trennung und Kontrolle.

Einordnung in das Schichtenmodell

WLAN-Sicherheit betrifft mehrere Ebenen.

Thema	Einordnung
Funkübertragung	OSI-Schicht 1
WLAN-Zugriff und MAC	OSI-Schicht 2
WPA2 / WPA3	WLAN-Sicherheitsverfahren im Zugangsbereich
VLAN	OSI-Schicht 2
IP-Netztrennung	OSI-Schicht 3
Firewall mit Ports	OSI-Schicht 3 / 4
HTTPS	OSI-Schicht 7 mit Sicherheitsbezug

Wichtig:

WLAN-Sicherheit ist nicht nur ein Passwort.
Sie besteht aus mehreren technischen Maßnahmen.

Merksatz:

WLAN-Sicherheit betrifft Funk, Zugang, Netztrennung und Dienste.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum muss WLAN verschlüsselt werden?
- Warum ist WEP unsicher?
- Was ist der Unterschied zwischen WPA2 und WPA3?
- Was bedeutet WPA-Personal?
- Was bedeutet WPA-Enterprise?
- Was ist ein Pre-Shared Key?
- Was ist eine SSID?
- Warum ist ein Gast-WLAN sinnvoll?
- Warum sollte ein Gast-WLAN vom internen Netz getrennt werden?
- Was ist der Unterschied zwischen SSID und VLAN?
- Warum ist MAC-Filter kein ausreichender Schutz?
- Warum ersetzt HTTPS keine WLAN-Verschlüsselung?
- Was ist ein Rogue Access Point?
- Was ist ein Evil Twin?

Typische Prüfungsfallen

WLAN ohne Verschlüsselung ist unsicher.

WEP gilt als veraltet und unsicher.

WPA ist ebenfalls nicht mehr Stand der Technik.

WPA2 ist Mindeststandard,
WPA3 ist besser.

SSID ist der WLAN-Name,
nicht das Passwort.

Eine versteckte SSID ist keine echte Sicherheitsmaßnahme.

MAC-Filter ersetzt keine Verschlüsselung.

HTTPS ersetzt keine WLAN-Verschlüsselung.

Ein Gast-WLAN braucht Trennung vom internen Netz.

Mehrere SSIDs allein reichen nicht,

wenn VLANs und Firewall-Regeln fehlen.

WPA-Enterprise ist für größere Umgebungen besser geeignet als ein gemeinsames Passwort.

WPS kann ein Sicherheitsrisiko sein.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
WLAN-Verschlüsselung	Schutz der Funkverbindung zwischen Client und Access Point
WEP	alter und unsicherer WLAN-Sicherheitsstandard
WPA	älterer Nachfolger von WEP
WPA2	moderner verbreiteter WLAN-Sicherheitsstandard
WPA3	neuerer WLAN-Sicherheitsstandard
PSK	Pre-Shared Key, gemeinsames WLAN-Passwort
WPA-Personal	WLAN-Zugang mit gemeinsamem Passwort
WPA-Enterprise	WLAN-Zugang mit individueller Authentifizierung
802.1X	Standard für Netzwerkzugangskontrolle
RADIUS	zentraler Dienst zur Authentifizierung
Authentifizierung	Nachweis der Identität
Autorisierung	Festlegung erlaubter Zugriffe
SSID	Name eines WLANs
VLAN	logische Netztrennung
Gast-WLAN	separates WLAN für Gäste
Captive Portal	Anmeldeseite für Netzwerkzugang
MAC-Filter	Zugriffskontrolle anhand von MAC-Adressen
WPS	vereinfachtes WLAN-Verbinden, kann Sicherheitsrisiko sein
Rogue Access Point	unerlaubter Access Point
Evil Twin	gefälschtes WLAN mit bekanntem Namen
Client-Isolation	Trennung von WLAN-Clients untereinander

IHK-sichere Kurzformulierung

WLAN muss abgesichert werden, weil die Datenübertragung per Funk erfolgt und das Signal auch außerhalb des direkten Raumes empfangbar sein kann. Veraltete Verfahren wie WEP gelten als unsicher und sollten nicht mehr verwendet werden. WLAN sollte mindestens mit WPA2, besser mit WPA3 verschlüsselt werden. In größeren Umgebungen ist WPA-Enterprise mit 802.1X und RADIUS sinnvoll. Gast-WLANs sollten vom internen Netzwerk getrennt werden, zum Beispiel durch eigene SSIDs, VLANs und Firewall-Regeln. MAC-Filter oder versteckte SSIDs sind keine ausreichenden Sicherheitsmaßnahmen.

Merksätze

WLAN braucht Verschlüsselung.

WEP ist unsicher.

WPA ist veraltet.

WPA2 ist Mindeststandard.

WPA3 ist besser.

PSK = gemeinsames WLAN-Passwort.

WPA-Personal = gemeinsames Passwort.

WPA-Enterprise = individuelle Anmeldung.

802.1X = Netzwerkzugangskontrolle.

RADIUS = zentrale Authentifizierung.

SSID = WLAN-Name.

VLAN = logische Netztrennung.

Gast-WLAN vom internen Netz trennen.

MAC-Filter ist kein ausreichender Schutz.

Versteckte SSID ist keine echte Sicherheit.

WPS kann ein Risiko sein.

HTTPS ersetzt keine WLAN-Verschlüsselung.

WPA schützt die Funkstrecke.

Firewall-Regeln steuern den Zugriff.

WLAN-Sicherheit besteht aus Verschlüsselung, Trennung und Kontrolle.