



**Hochschule  
Albstadt-Sigmaringen**  
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

# Die 10 größten Bedrohungen für Computer-Netzwerke

## ECSM

# Tobias Scheible, M.Eng.

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, ...



## Die 10 größten Bedrohungen für Computer-Netzwerke

.....  
06.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 32 Bachelor- und Masterstudiengänge

Fakultät  
Engineering



Fakultät  
Business Science  
and Management



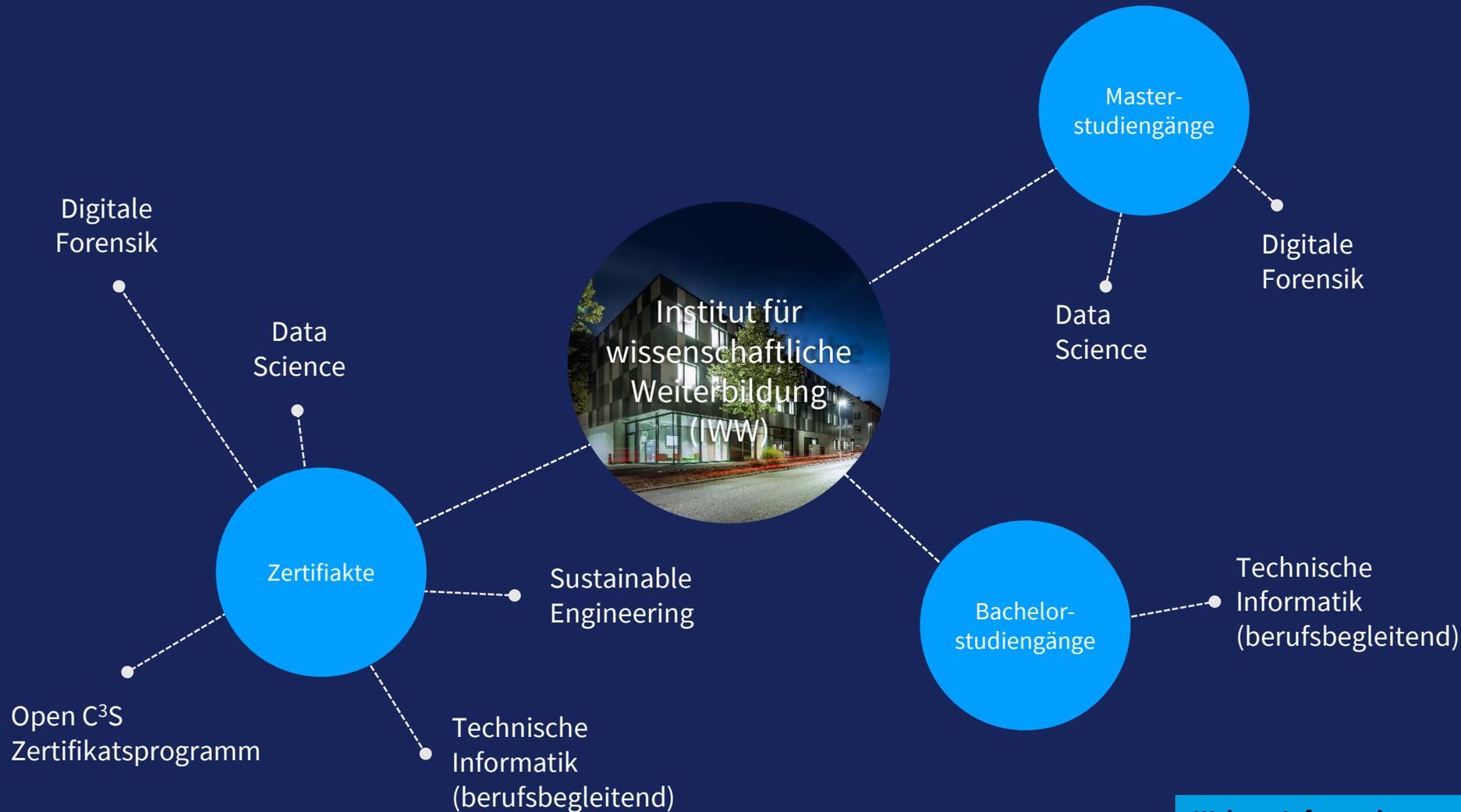
Fakultät Life  
Sciences



Fakultät  
Informatik

Die 10 größten Bedrohungen  
für Computer-Netzwerke

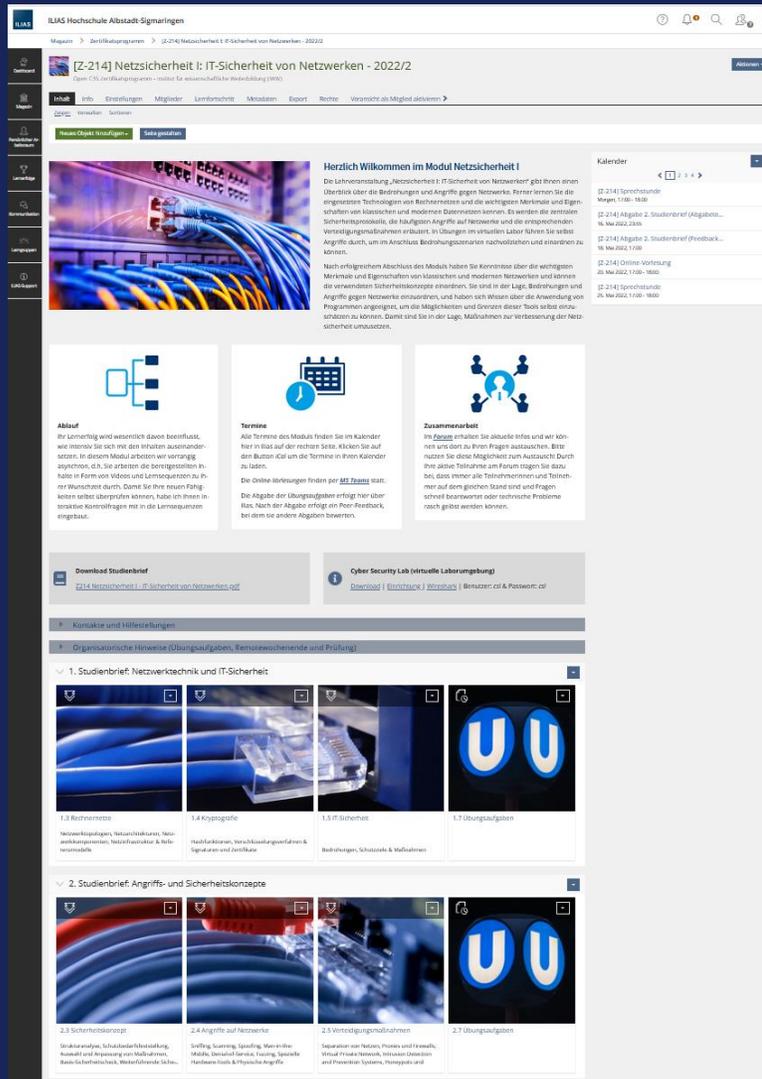
# Institut für wissenschaftliche Weiterbildung



**Weitere Informationen:**  
[www.hs-albsig.de/iww](http://www.hs-albsig.de/iww)

## Die 10 größten Bedrohungen für Computer-Netzwerke

# Netzwerkssicherheit I: IT-Sicherheit von Netzwerken



ILIAS Hochschule Albstadt-Sigmaringen  
 [Z-214] Netzwerkssicherheit I: IT-Sicherheit von Netzwerken - 2022/2

**Herzlich Willkommen im Modul Netzwerkssicherheit I**  
 Die Lehrveranstaltung „Netzwerkssicherheit I: IT-Sicherheit von Netzwerken“ gibt Ihnen einen Überblick über die Bedrohungen und Angriffe gegen Netzwerke. Ferner können Sie die eingesetzten Technologien von Betriebssystemen und die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Datennetzen kennen. Es werden die aktuellen Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Vorstellungsmaßnahmen erläutert. Im Übergang ins virtuelle Labor führen Sie selbst Angriffe durch, um im Anschluss Bedrohungsszenarien nachvollziehen und einordnen zu können.

**Ablauf**  
 Ihr Lernfortschritt wird wesentlich davon beeinflusst, wie intensiv Sie sich mit den Inhalten auseinandersetzen. In diesem Modul arbeiten wir vorwiegend gegenseitig, d.h. Sie arbeiten die Lerninhalte in Form von Videos und Lernsequenzen zu Phasen zusammen. Gerne Sie Ihre neuen Fähigkeiten selbst überprüfen können, haben wir Ihnen interaktive Kontrollfragen mit in den Lernsequenzen eingebaut.

**Termine**  
 Alle Termine des Moduls finden Sie im Kalender hier in ILIAS auf der rechten Seite. Klicken Sie auf den Button „Kal“ um die Termine in Ihren Kalender zu laden. Die Online-Vorlesungen finden per [MS Teams](#) statt. Die Abgabe der Übungsaufgaben erfolgt hier über ILIAS. Nach der Abgabe erfolgt ein Peer-Feedback, bei dem Sie andere Aufgaben bewerten.

**Zusammenarbeit**  
 Im [Forum](#) erhalten Sie aktuelle Infos und wir können uns dort zu Ihren Fragen austauschen. Bitte nutzen Sie diese Möglichkeit zum Austausch! Durch Ihre aktive Teilnahme am Forum tragen Sie dazu bei, dass immer alle Teilnehmerinnen und Teilnehmer auf dem gleichen Stand sind und Fragen schnell beantwortet oder technische Probleme rasch gelöst werden können.

**Download Studienbrief**  
[Z14 Netzwerkssicherheit I: IT-Sicherheit von Netzwerken.pdf](#)

**Cyber Security Lab (virtuelle Laborumgebung)**  
[Download](#) | [Einrichtung](#) | [Werkzeuge](#) | Benutzer: cid & Passwort: cid

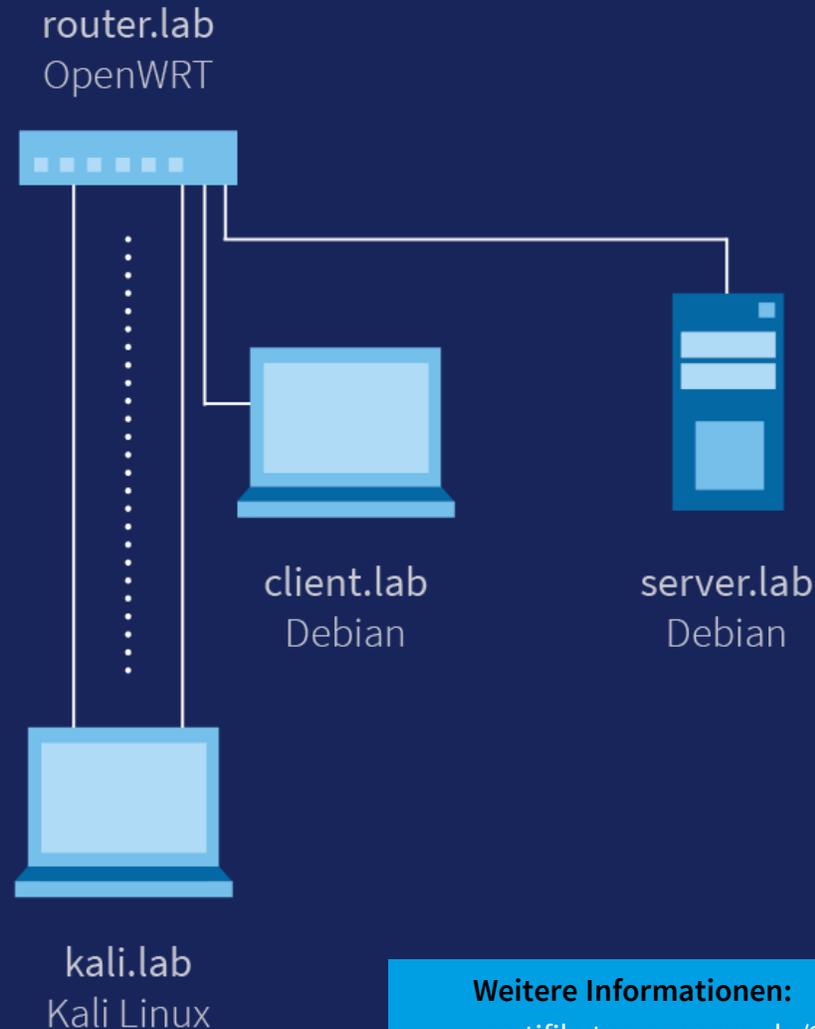
**Kontakt und Hilfestellungen**  
 Organisatorische Hinweise (Übungsaufgaben, Remotewochenende und Prüfung)

**1. Studienbrief: Netzwerktechnik und IT-Sicherheit**

- 1.3 Netzwerke
- 1.4 Kryptografie
- 1.5 IT-Sicherheit
- 1.6 Übungsaufgaben

**2. Studienbrief: Angriffs- und Sicherheitskonzepte**

- 2.3 Sicherheitskonzepte
- 2.4 Angriffe auf Netzwerke
- 2.5 Vorstellungsmaßnahmen
- 2.7 Übungsaufgaben



**Weitere Informationen:**  
[www.zertifikatsprogramm.de/214](http://www.zertifikatsprogramm.de/214)

## Die 10 größten Bedrohungen für Computer-Netzwerke

06.10.2022 | ECSM

Tobias Scheible, M.Eng.

# Agenda

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

## Hinweis

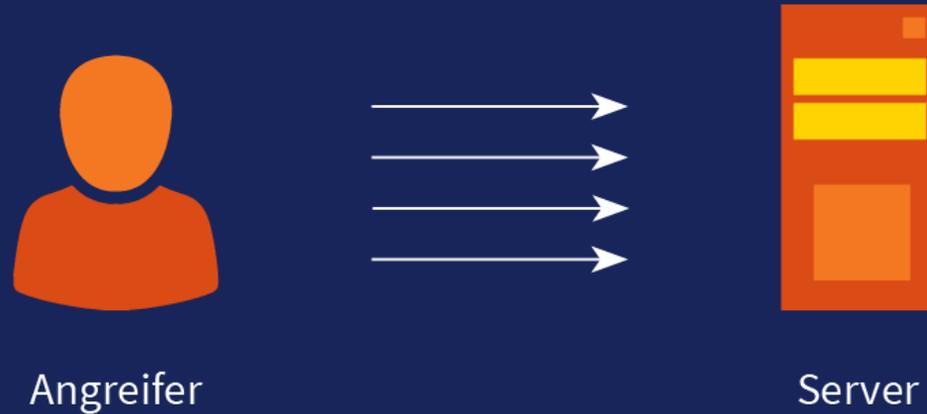
Die komplette Präsentation wird im Anschluss unter [www.scheible.it](http://www.scheible.it) bereitgestellt.

## Die 10 größten Bedrohungen für Computer-Netzwerke

A close-up photograph of a network switch or patch panel. The device is illuminated with a strong blue light, and several green LEDs are glowing, indicating active connections. Numerous blue cables are plugged into the ports, creating a dense array of lines. The background is dark, making the glowing lights and blue tones stand out.

# 10 Bedrohungen für Computer-Netzwerke

# Scanning



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

Scanning

Sniffing

Spoofing

Man-in-the-Middle

Denial-of-Service

Physical Attacks

Replay Attack

Jamming

Deauthentication

Evil Twin AP

# PRAXIS Scanning



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

Scanning

Sniffing

Spoofing

Man-in-the-Middle

Denial-of-Service

Physical Attacks

Replay Attack

Jamming

Deauthentication

Evil Twin AP

# Scanning

Sobald sich ein Angreifer innerhalb eines Netzwerkes befindet, verschafft er sich als Erstes mit einem Scan einen Überblick über das Netzwerk. Dies wird auch als Recognition (dt. Erkundung oder Aufklärung) bezeichnet. Als Erstes wird eine Übersicht erstellt, welche Rechner im Netzwerksegment aktiv sind. Dann wird analysiert, welche Dienste genutzt werden. Dabei werden alle Ports auf eine Reaktion überprüft. Ist ein Port gefunden, wird versucht, herauszufinden, welche Software auf diesem Port einen Dienst bereitstellt. Wurde dies auch erfolgreich durchgeführt, wird als Nächstes versucht, die Version herauszufinden.

## ■ Gegenmaßnahmen

Nur notwendige Ports sollten nach außen geöffnet sein und Versionsnummern dürfen niemals kommuniziert werden. Aggressive Scans sollten erkannt und der Urheber geblockt werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

Scanning

Sniffing

Spoofing

Man-in-the-Middle

Denial-of-Service

Physical Attacks

Replay Attack

Jamming

Deauthentication

Evil Twin AP

# Sniffing

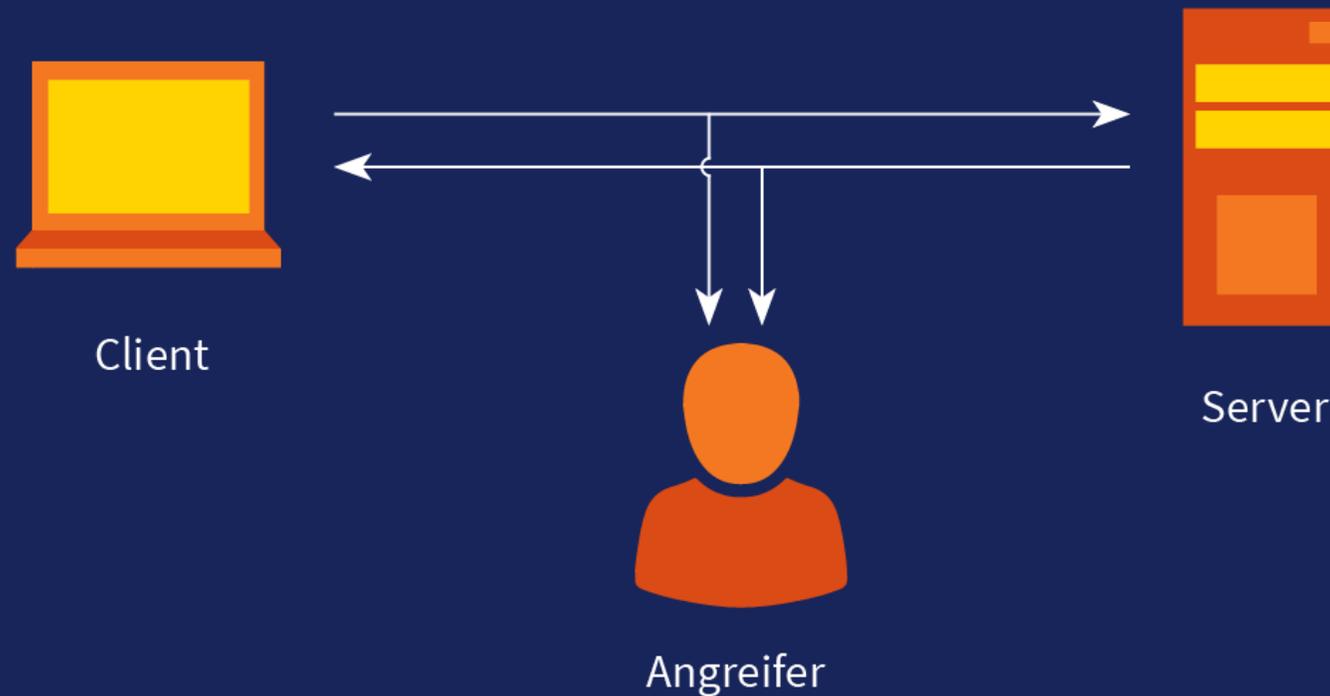


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Sniffing



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# EXKURS Sniffing



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Sniffing

Sniffing (dt. schnüffeln) bezeichnet das Mitschneiden oder Mitlesen des Datenverkehrs einer Netzwerkverbindung. Dabei handelt es sich um einen passiven Angriff, da der Datenverkehr nur abgehört und nicht verändert wird. Der Zugriff auf die Kommunikation erfolgt dabei je nach Netzwerkart auf unterschiedliche Art und Weise. Zum Beispiel kann ein Notebook mit zwei Netzwerkadaptern genutzt und zwischen einer Verbindung platziert und somit ein Sniffer realisiert werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Spoofting



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

Scanning

Sniffing

Spoofting

Man-in-the-Middle

Denial-of-Service

Physical Attacks

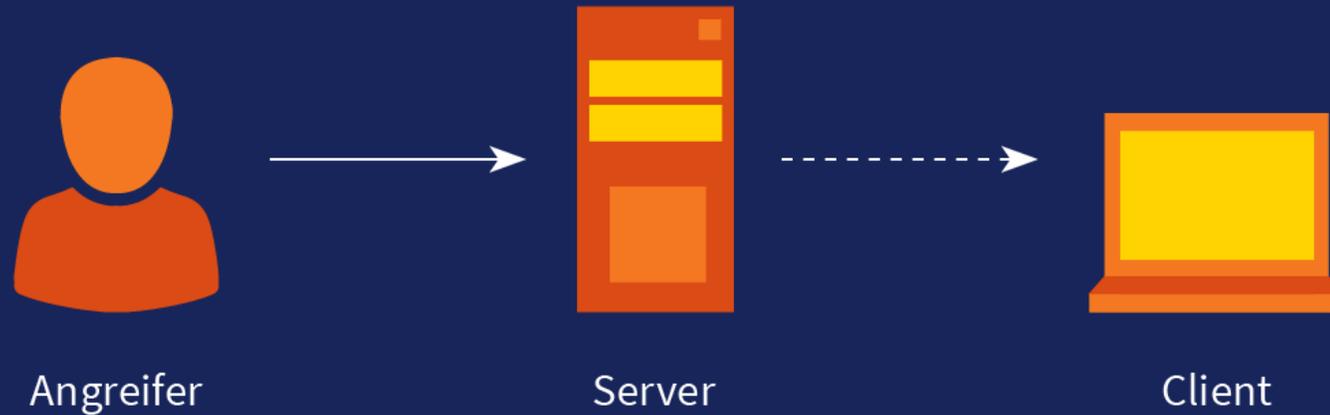
Replay Attack

Jamming

Deauthentication

Evil Twin AP

# Spoofting



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofting
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# PRAXIS Spoofing



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Spoofing

Spoofing (dt. Manipulation, Verschleierung oder Vortäuschung) werden in der Informationstechnik verschiedene Täuschungsmethoden genannt, bei denen ein Angreifer entweder seine eigene Identität verschleiern möchte oder eine andere Identität vortäuscht, welcher der Empfänger vertraut. Im Bereich Netzsicherheit gehört dazu etwa ARP-Spoofing, IP-Spoofing und DNS-Spoofing.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Man-in-the-Middle

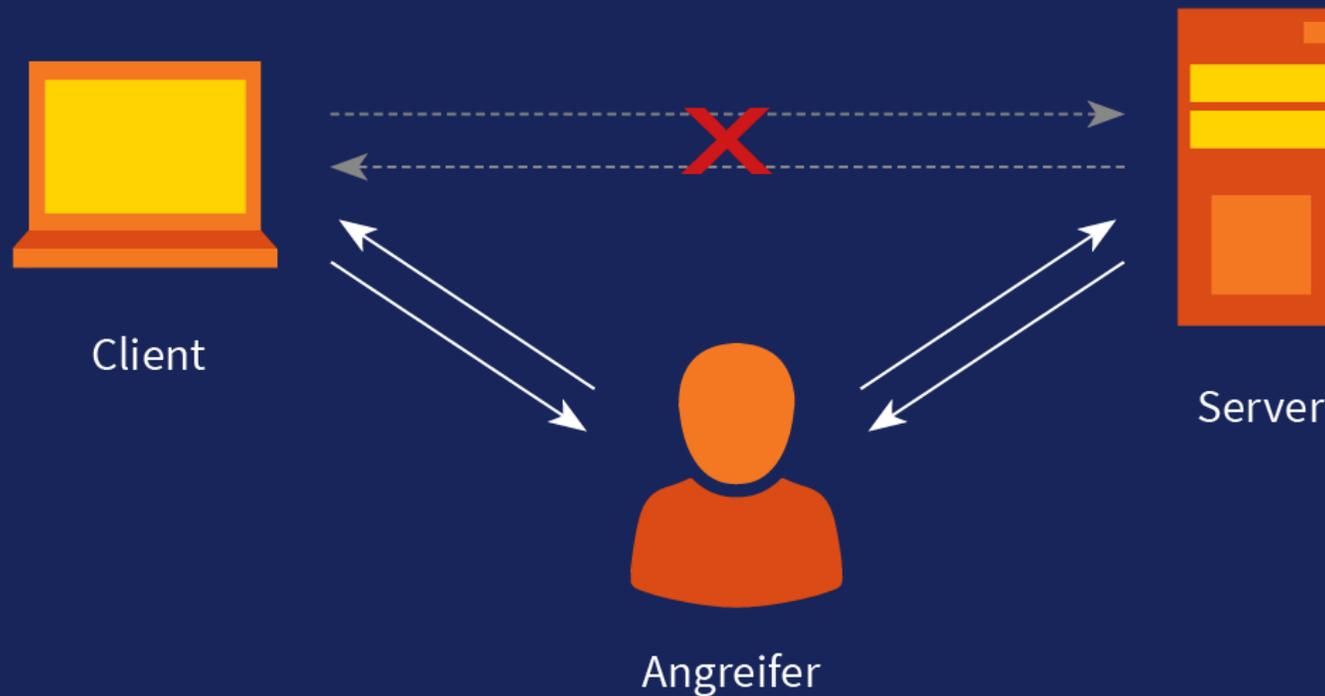


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Man-in-the-Middle



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Man-in-the-Middle

Bei einem Man-in-the-Middle-Angriff (MitM-Angriff) oder auch Person-in-the-Middle-Angriff positioniert sich ein Angreifer zwischen zwei Kommunikationspartnern. In dieser Position können Nachrichten abgehört, manipuliert, geblockt oder gefälscht werden. Es gibt verschiedene Arten, wie ein Angreifer in eine Verbindung eingreifen kann, etwa den Spoofing-Angriff. In der Netzsicherheit wird das Umleiten eines Datenstroms auch als Redirect- oder Routing-Angriff bezeichnet.

## ■ Gegenmaßnahmen

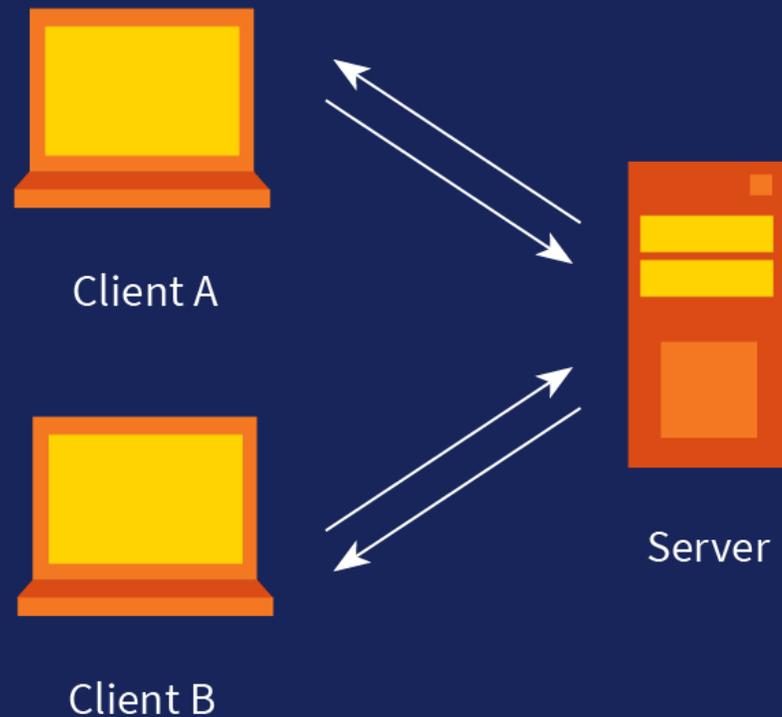
Um Kommunikationsverbindungen dagegen zu schützen, müssen mittels kryptografischer Funktionen sichere Verschlüsselungen realisiert werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Denial-of-Service

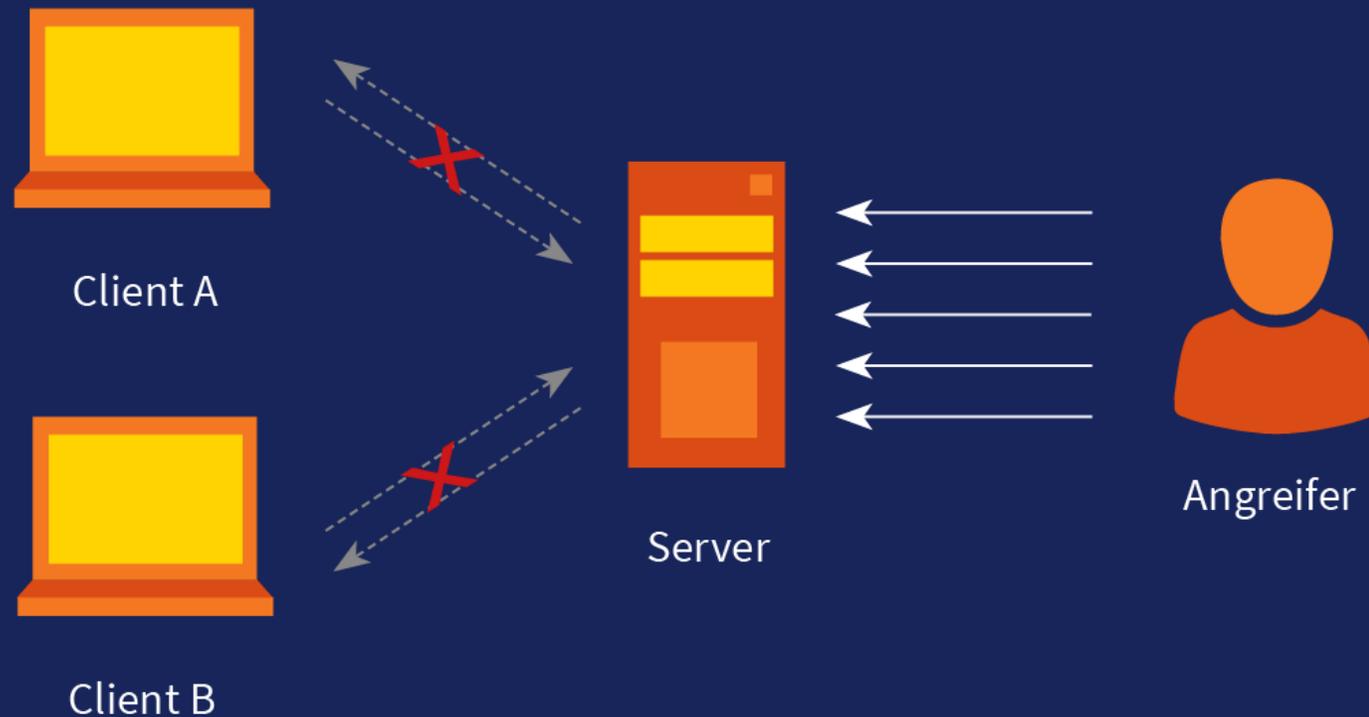


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Denial-of-Service



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# PRAXIS Denial-of-Service



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Denial-of-Service

Eine Denial-of-Service-Attacke (auch als DoS-Attacke abgekürzt) ist ein Angriff, der dazu führen soll, dass ein Server temporär oder in besonders extremen Fällen auch über einen längeren Zeitraum hinweg nicht mehr erreicht werden kann. DoS-Attacken sind häufig nichts weiter als Cyber-Vandalismus, die bei Unzufriedenheit mit einer Situation eingesetzt werden. Dies kommt häufig vor, da viele Tools existieren, die ohne tieferes Know-how bedient werden können. Es werden auch illegale Dienstleistungen angeboten, bei denen DoS-Angriffe eingekauft werden können.

## ■ Gegenmaßnahmen

Systeme müssen gegen DDoS-Attacke gehärtet und präventive Maßnahmen vorab initiiert werden. Die Netzwerkinfrastruktur muss vorbereitet werden, damit Angriffe gefiltert und geblockt werden können.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Physical Attacks

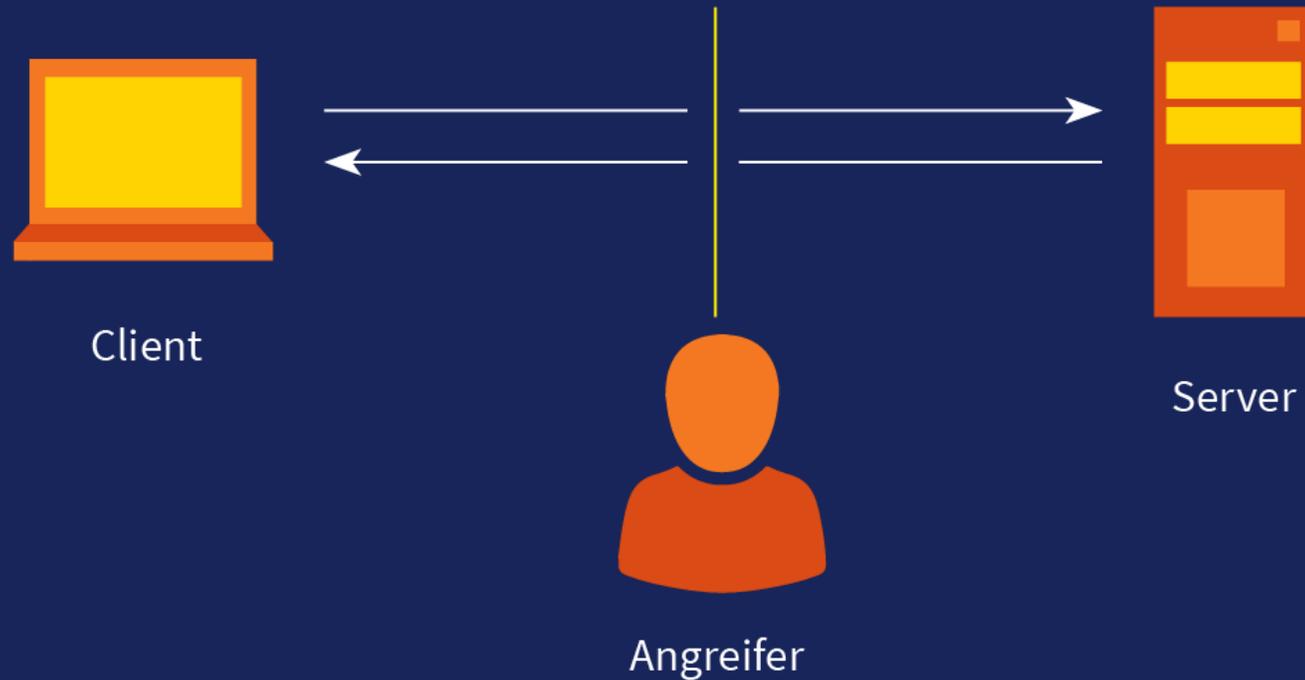


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Physical Attacks



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Physical Attacks

Physische Angriffe auf Netzwerke haben eine reine Zerstörung zum Ziel, um Verbindungen zu unterbrechen. Das reicht im einfachsten Fall vom Durchtrennen eines Kabels bzw. Lichtwellenleiters bis hin zur Manipulation mit Stromstößen. Dabei wird eine offene Netzwerkbuchse gezielt einem starken Stromimpuls ausgesetzt. Hier hat ein Angreifer das Ziel, dass mehrere angeschlossene Komponenten im Netzwerk durch Überlastung zerstört werden.

## ■ Gegenmaßnahmen

Daher muss auch die Netzwerkinfrastruktur mit baulichen Maßnahmen gegen Angriffe und Manipulationen geschützt werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Replay Attack

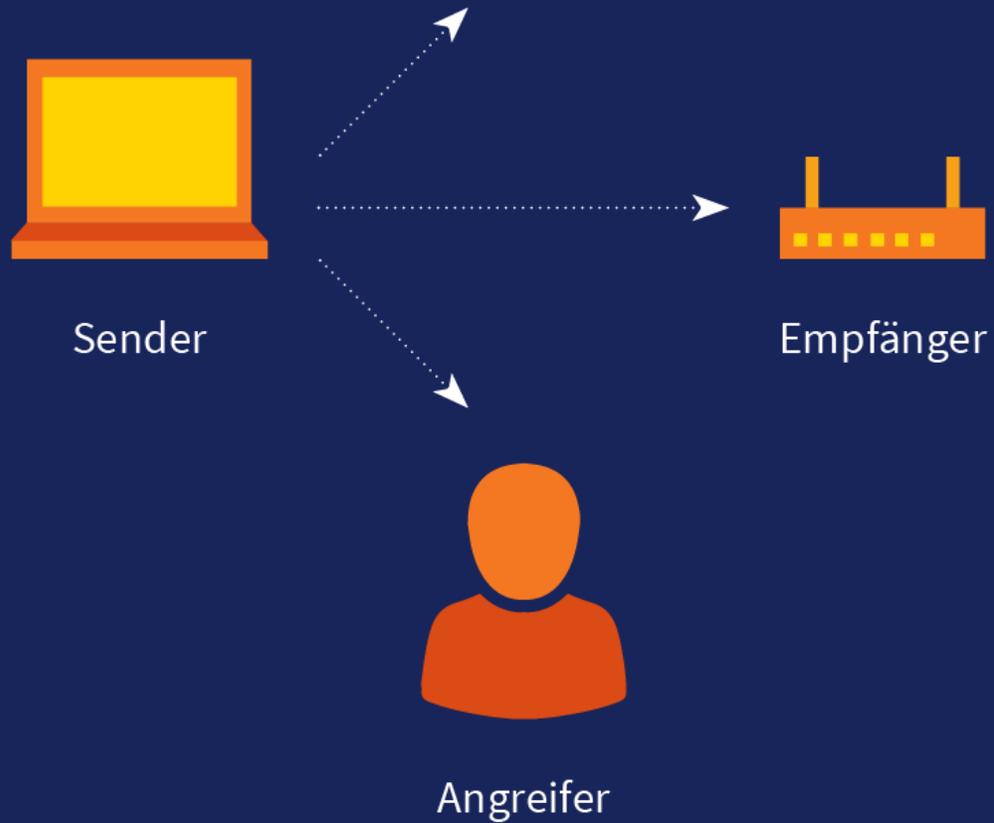


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Replay Attack

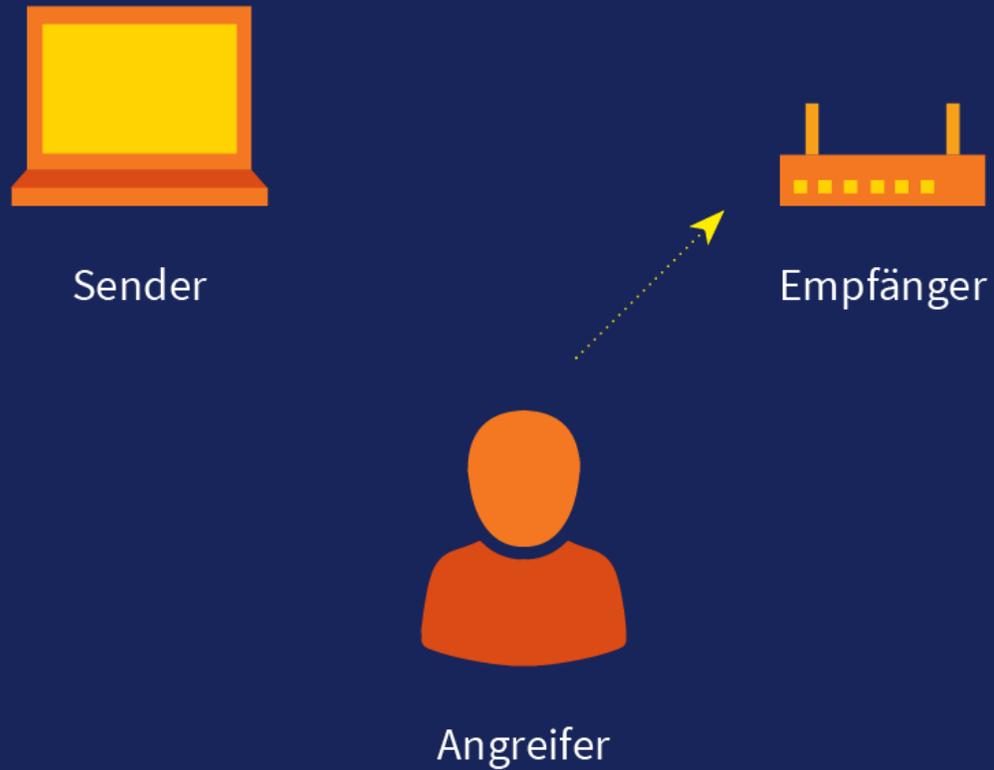


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Replay Attack



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# EXKURS Replay Attack



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Replay Attack

Bei einem Replay Attack wird ein Signal mit keiner oder nur schwacher Schutzmaßnahme aufgezeichnet und erneut gesendet. Findet hier auf der Empfängerseite keine Validierung statt, wird diese Übertragung einfach verarbeitet. Damit ist es einem Angreifer möglich, eine Übertragung mit etwa einem Befehl erneut einzuschleusen, ohne dass das eigentliche Signal dekodiert werden muss. Dies funktioniert zum Teil, auch wenn eine symmetrische Verschlüsselung mit immer dem gleichen Code verwendet wird.

## ■ Gegenmaßnahmen

Um diese zu verhindern, können Techniken wie eine Nonce, Sequenznummern, Message Authentication Code oder das Rolling-Code-Verfahren eingesetzt werden. Damit wird jede Übertragung so verändert, dass sie einmalig ist und erneut gesendete Übertragungen erkannt und geblockt werden können.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Jamming

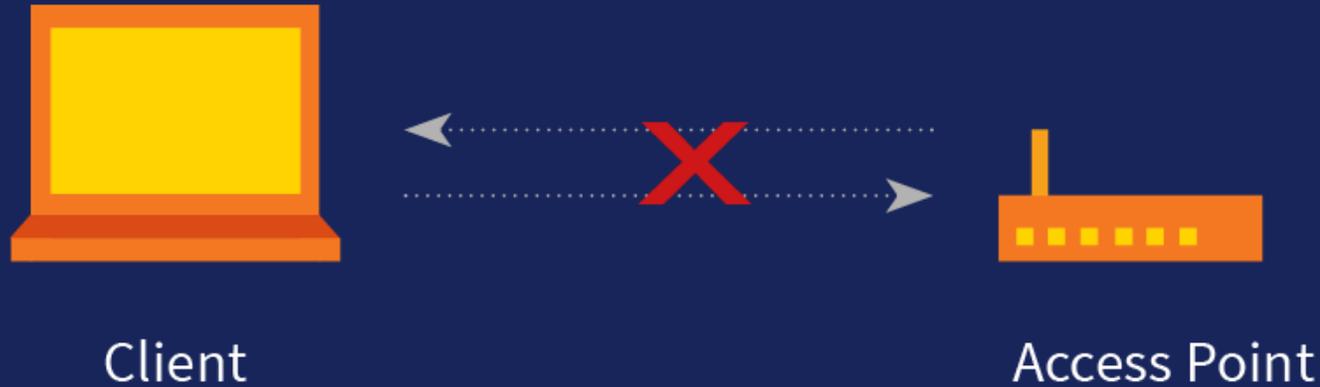


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Jamming

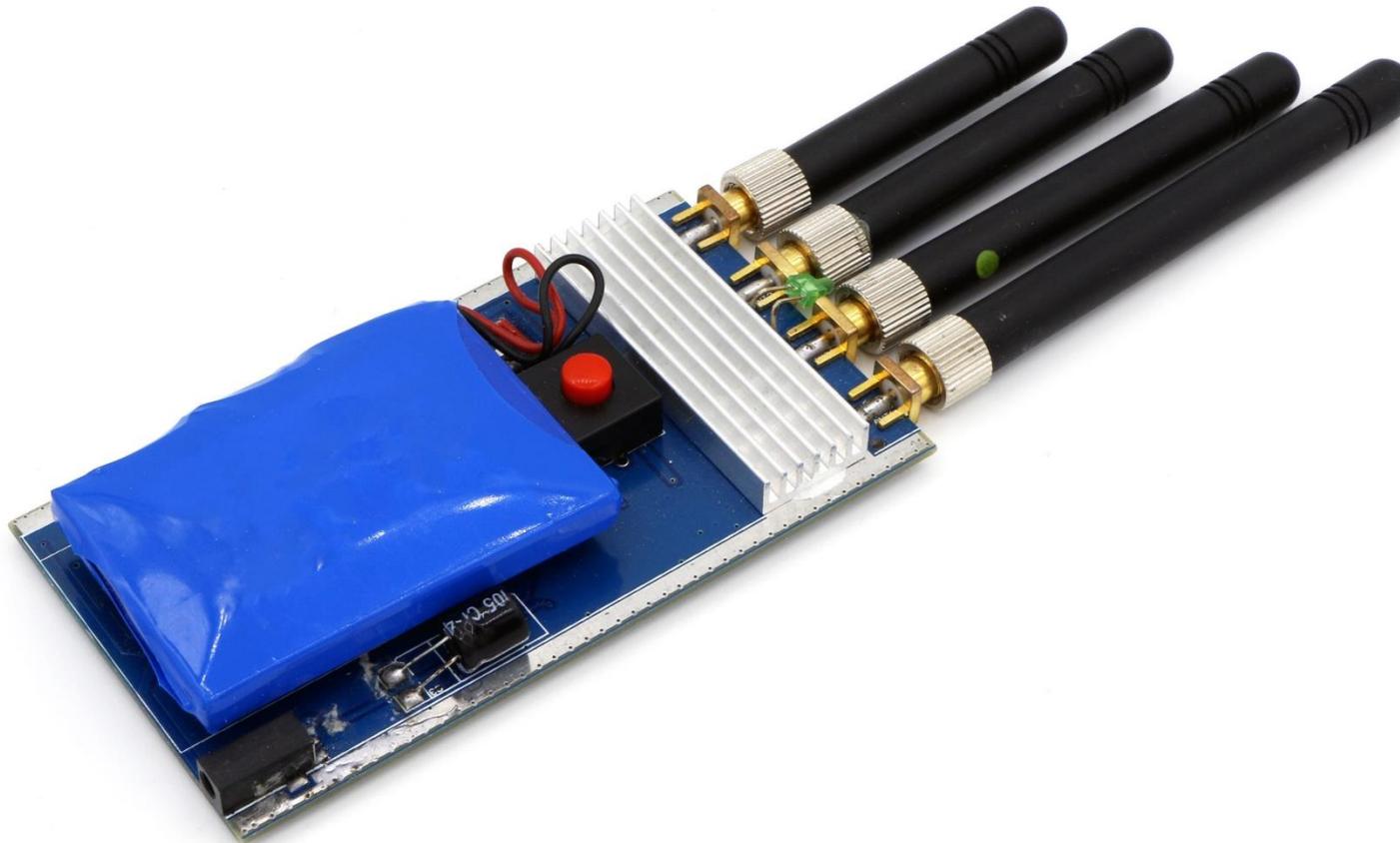


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# EXKURS Jamming



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Jamming

Per Jamming werden kabellose Übertragungen gestört, so dass der Empfang eines Signals nur noch schwer oder gar nicht möglich ist. Ein Störsender sendet etwa auf einer bestimmten Frequenz ein zufälliges Signal mit möglichst großer Stärke und überlagert so andere Übertragungen. Dadurch ist keine Kommunikation mehr möglich und eine WLAN-Verbindung bricht zum Beispiel zusammen. Störsender gibt es für verschiedene Funkprotokolle bzw. -frequenzen wie Bluetooth, WLAN, GSM, UMTS, LTE und GPS.

## ■ Gegenmaßnahmen

Gegenmaßnahmen gegen das Stören eines Signals lassen sich nur schwer umsetzen. Grundsätzlich sollte bei der Unterbrechung eines Signals ein Alarm ausgelöst und solche Vorgänge dokumentiert werden. Systeme sollten in einen definierten Status schalten, wenn keine Verbindung mehr vorhanden ist.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Deauthentication

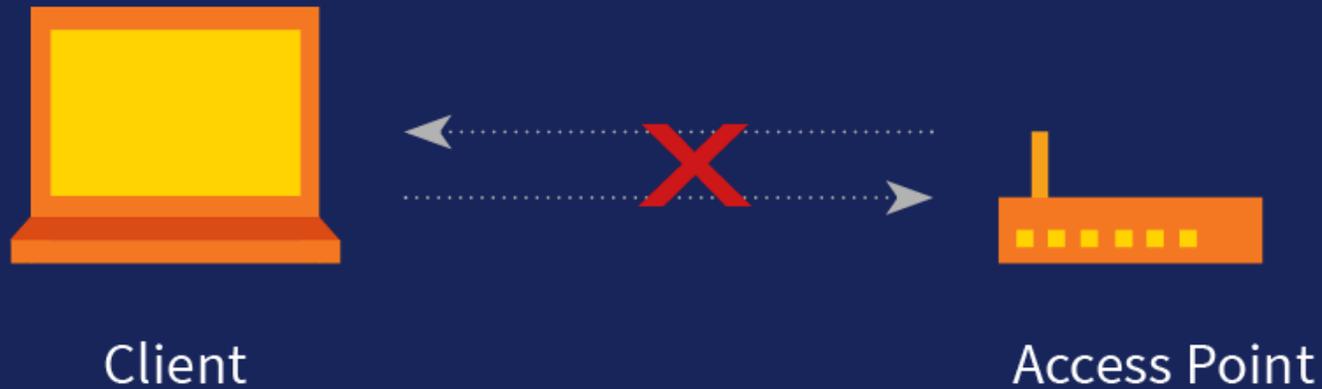


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Deauthentication

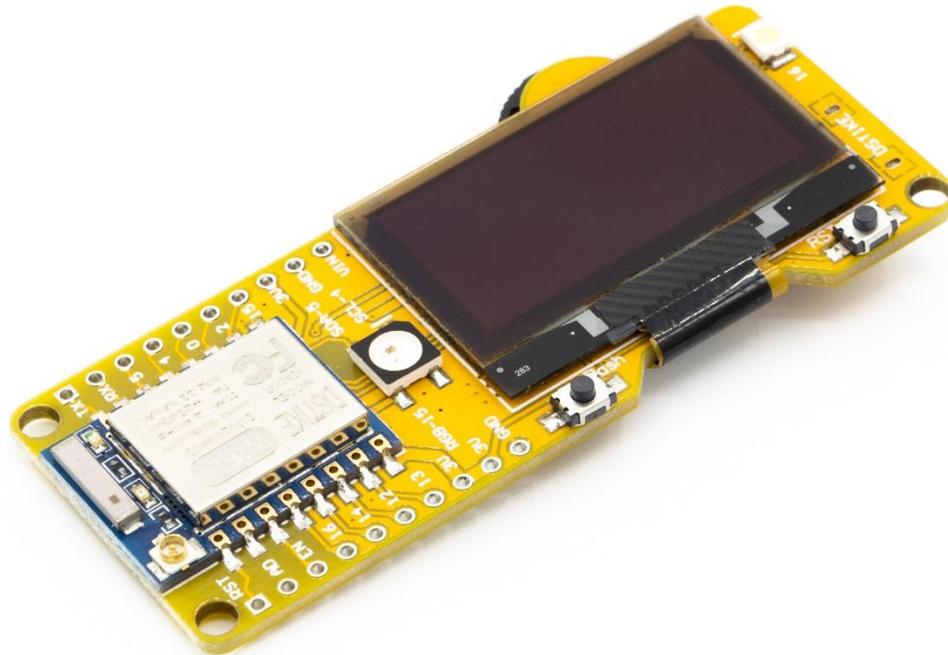


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# EXKURS Deauthentication



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Deauthentication

In kabellosen Netzwerken (WLAN) kann ein Angreifer einen Client vom Netzwerk abmelden. Dabei wird das Deauthentication-Signal des Access-Points (AP) imitiert und damit dem Endgerät fälschlicherweise eine Beendigung der Verbindung signalisiert. Die Deauthentication-Funktion ist eigentlich dazu gedacht, dass ein Teilnehmer an einem System aus mehreren Access-Points von einer überlasteten Station abgemeldet wird und sich dann mit einem anderen Access-Point verbindet. Dieses Signal kann jedoch ohne großen Aufwand gefälscht werden – und damit kann man gezielt die WLAN-Verbindung unterbrechen. Um das Deauthentication-Signal zu senden, muss der Angreifer nicht die Zugangsdaten zum WLAN kennen, da es sich um einen Management-Frame handelt und nur die Datenübertragung verschlüsselt wird.

## ■ Gegenmaßnahmen

Der WLAN-Standard IEEE 802.11w kennt bereits Gegenmaßnahmen, um einen Schutz zu realisieren, dies wird als Protected Management Frames (PMF) bezeichnet. Allerdings wird die Funktion nicht von allen Geräten unterstützt und muss manuell aktiviert werden. Der Sicherheitsstandard WPA3 bietet ebenfalls eine Schutzmaßnahme und sollte daher aktiviert werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Evil Twin AP

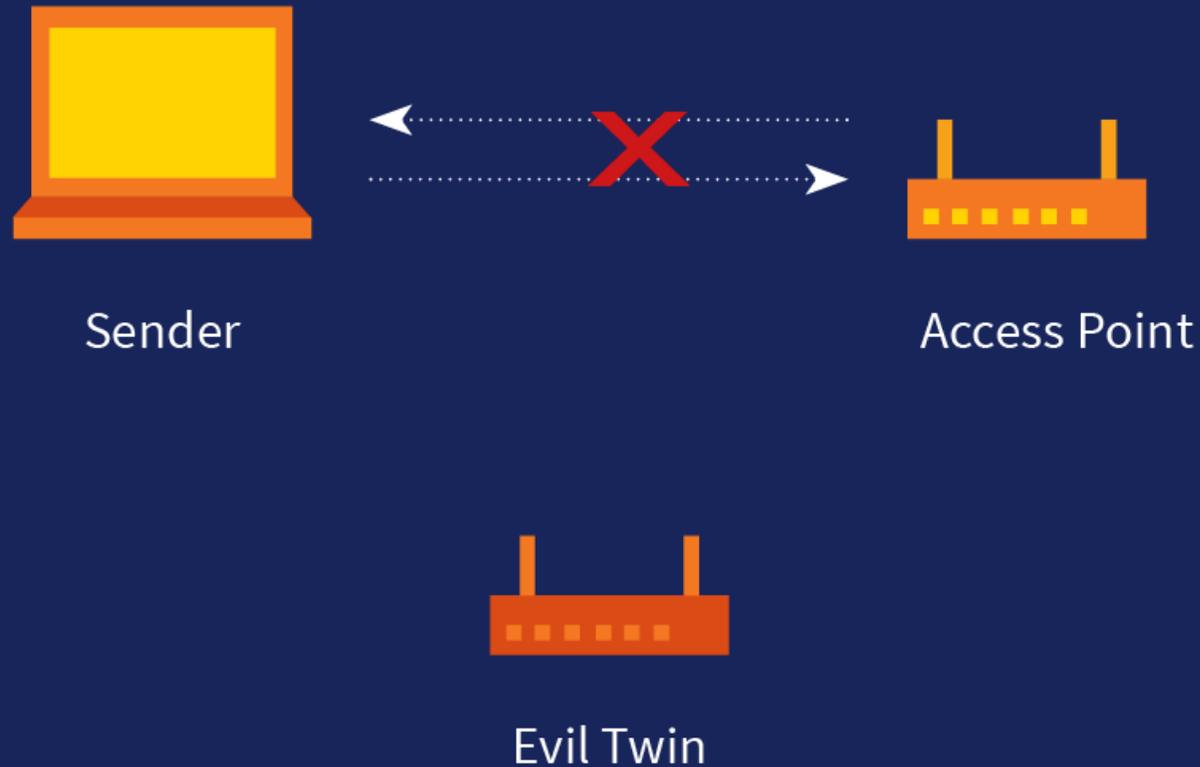


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Evil Twin AP

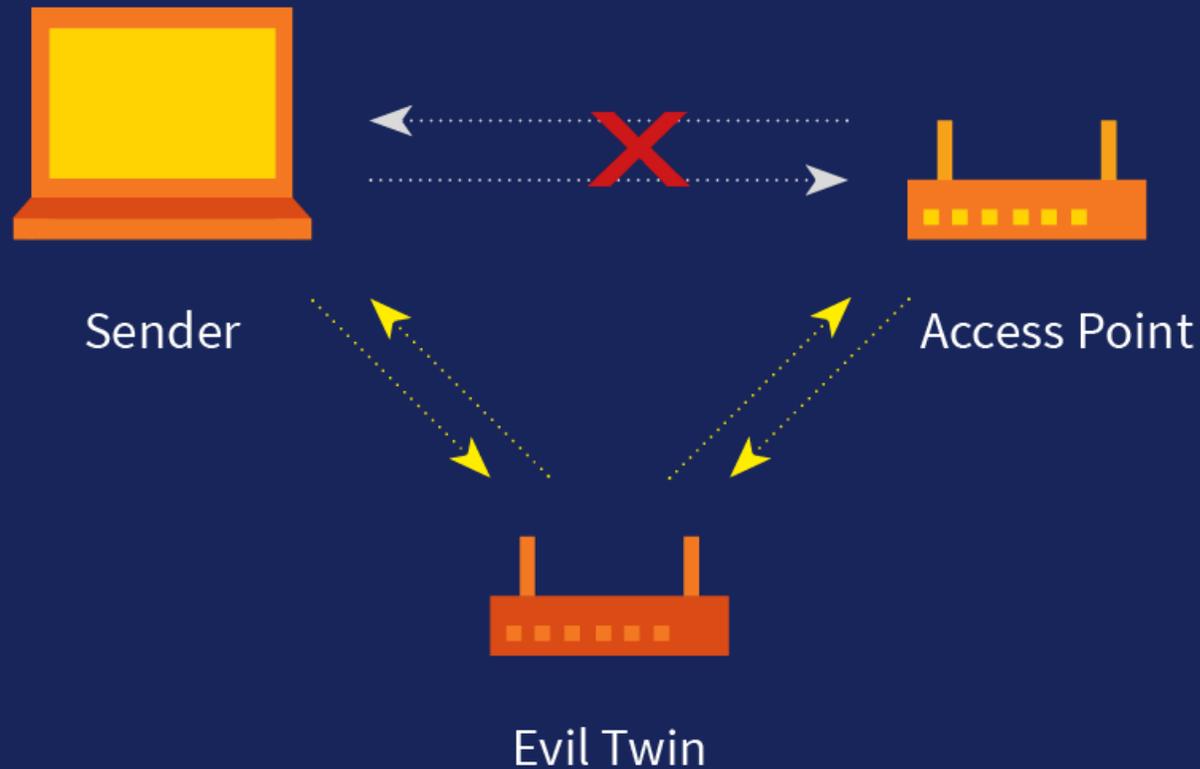


## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# Evil Twin AP



## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

# EXKURS Evil Twin AP

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP



# Evil Twin AP

Angreifer versuchen mit einem Access Point ein WLAN zu erstellen, das den gleichen Namen trägt wie das ursprüngliche WLAN. Dabei wird eine Verbindung mit dem ursprünglichen Netzwerk durch den Angreifer hergestellt und der gesamte Datenverkehr weitergeleitet. Verbindet sich nun ein Opfer mit dem gefälschten Zwillings-WLAN, daher der Name Evil Twin AP, kann der Angreifer unverschlüsselten Datenverkehr mitschneiden und manipulieren.

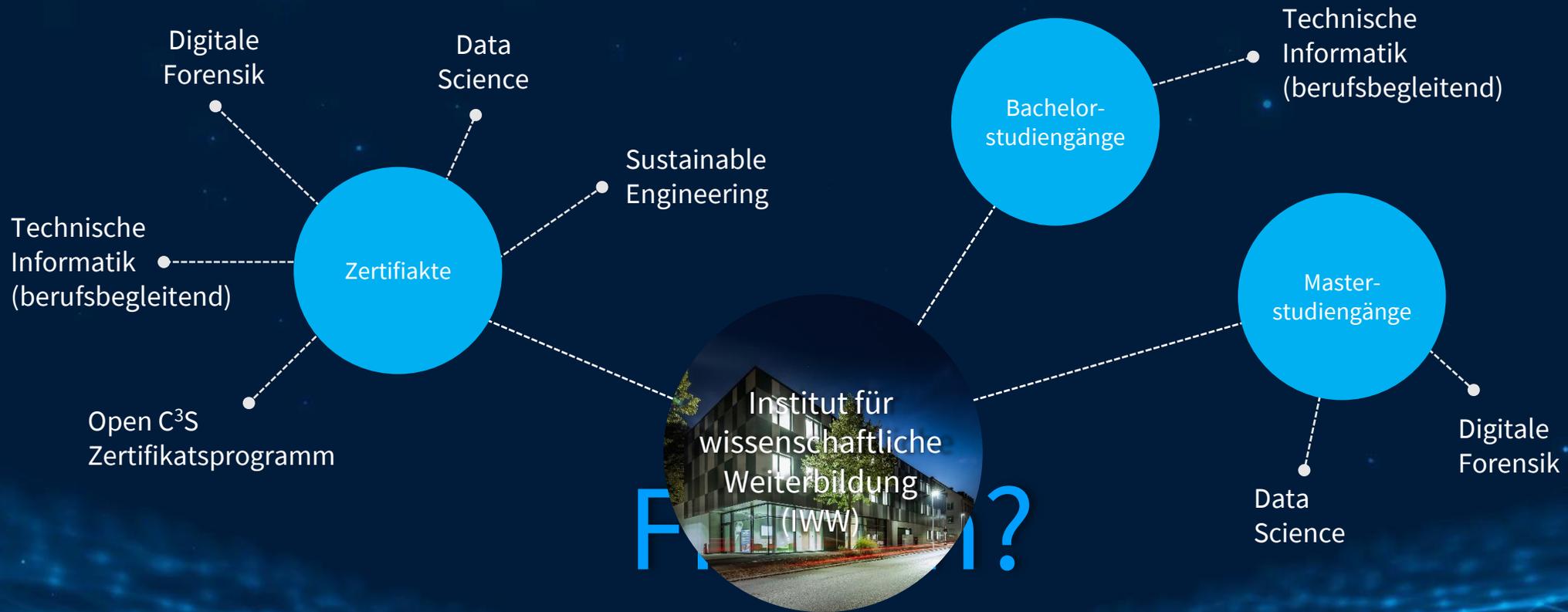
## ■ Gegenmaßnahmen

Im Unternehmensumfeld sollte für die Authentifizierung die Variante WPA2 Enterprise eingesetzt und bei fremden WLANs immer zusätzlich eine VPN-Verbindung verwendet werden.

## Die 10 größten Bedrohungen für Computer-Netzwerke

### Angriffe gegen Netzwerke

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP



# Vielen Dank für Ihre Aufmerksamkeit

Weitere Vorträge: [weiter-bildung.info](http://weiter-bildung.info) | Präsentation online unter: [scheible.it](http://scheible.it)