

Praxisvorträge

Dozent: Jürgen Kraft

- 2017: Sicheres Surfen in öffentlichen WLAN-Hotspot Netzen
- 2018: Sichere Tunnelverbindung (VPN) von Notebook und Smartphone zum Heimnetzwerk und ins Internet über unsichere Übertragungswege, wie z.B. WLAN-Hotspots

Dozent: Jürgen Kraft

Definition WLAN Hotspot

(WLAN) Hot Spots sind öffentliche drahtlose Internetzugangspunkte. Sie sind sowohl in öffentlichen Räumen (Bibliotheken, Krankenhäusern, Flughäfen, Bahnhöfen usw.) als auch in privaten wie z. B. Gastronomie, Hotels etc. installiert.

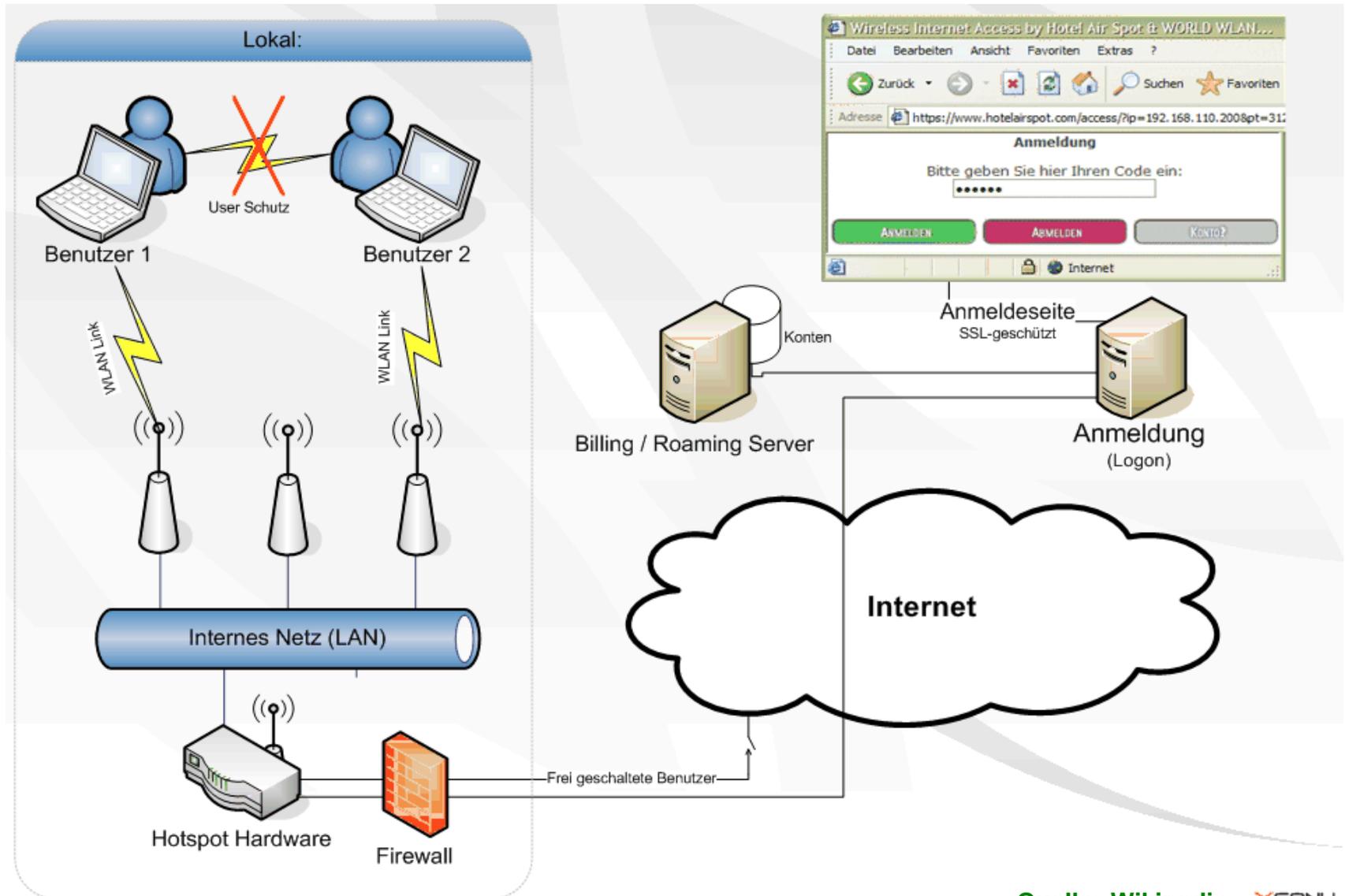
(Quelle: Wikipedia)

WLAN Hotspot technisch gesehen

Ein WLAN Hotspot basiert auf einem oder mehreren WLAN-Accesspoints. Der Name des Netzwerkes (SSID) wird stets gesendet und die Datenübertragung in der Regel nicht auf Netzwerkprotokollebene verschlüsselt.

Eine Authentifikation der Nutzer findet nicht auf WLAN-Protokollebene statt, sondern in einem dahinterliegenden Backend-System. Freie Hotspots verzichten auf Authentifikationsmechanismen.

Aufbau eines Hotspot-Systems



WiFi Pineapple Nano

Specifications:

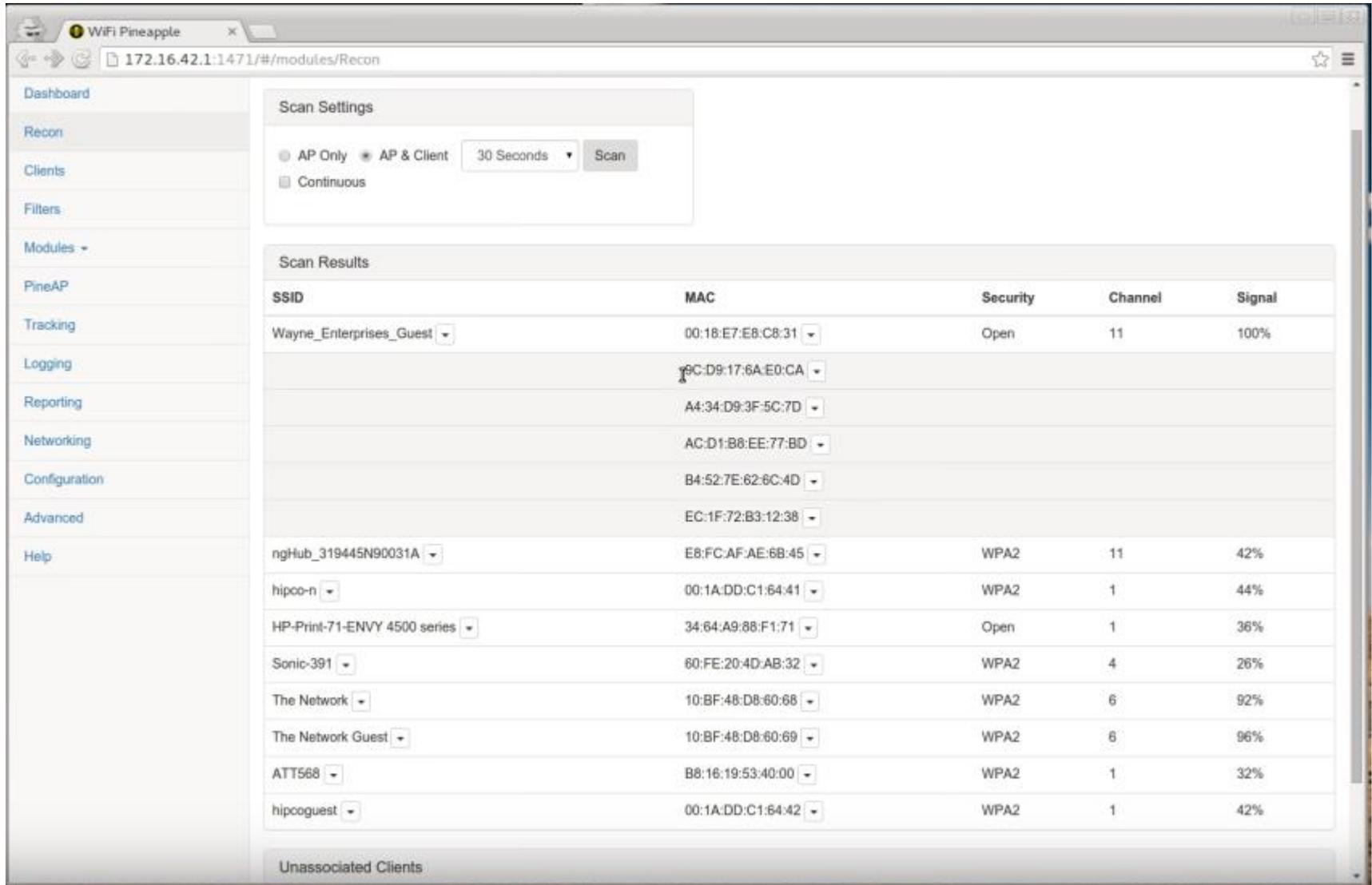
- **CPU:** 400 MHz MIPS Atheros AR9331 SoC
- **Memory:** 64 MB DDR2 RAM
- **Disk:** 16 MB ROM + Micro SD (not included)
- **Wireless:** Atheros AR9331 + Atheros AR9271, both IEEE 802.11 b/g/n
- **Ports:** (2) RP-SMA Antenna, Ethernet over USB (ASIX AX88772A), USB 2.0 Host, Micro SD
- **Power:** USB 5V 1.5A
- **Software:** PineAP Suite, Web Interface or Command Line, <100 additional Modules

<https://www.wifipineapple.com>



Preis: ca. 150 €
z.B Amazon

WiFi Pineapple Nano - Webinterface



The screenshot displays the WiFi Pineapple Nano web interface. The browser address bar shows the URL `172.16.42.1:1471/#/modules/Recon`. The left sidebar contains navigation links: Dashboard, Recon, Clients, Filters, Modules, PineAP, Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area is titled "Scan Settings" and includes radio buttons for "AP Only" (selected) and "AP & Client", a "30 Seconds" dropdown menu, and a "Scan" button. Below the settings is a "Scan Results" table with columns for SSID, MAC, Security, Channel, and Signal. The table lists several detected networks, including "Wayne_Enterprises_Guest" (Open security, 100% signal) and "ngHub_319445N90031A" (WPA2 security, 42% signal). At the bottom, there is a section for "Unassociated Clients".

SSID	MAC	Security	Channel	Signal
Wayne_Enterprises_Guest	00:18:E7:E8:C8:31	Open	11	100%
	9C:D9:17:6A:E0:CA			
	A4:34:D9:3F:5C:7D			
	AC:D1:B8:EE:77:BD			
	B4:52:7E:62:6C:4D			
	EC:1F:72:B3:12:38			
ngHub_319445N90031A	E8:FC:AF:AE:6B:45	WPA2	11	42%
hipco-n	00:1A:DD:C1:64:41	WPA2	1	44%
HP-Print-71-ENVY 4500 series	34:64:A9:88:F1:71	Open	1	36%
Sonic-391	60:FE:20:4D:AB:32	WPA2	4	26%
The Network	10:BF:48:D8:60:68	WPA2	6	92%
The Network Guest	10:BF:48:D8:60:69	WPA2	6	96%
ATT568	B8:16:19:53:40:00	WPA2	1	32%
hipcoguest	00:1A:DD:C1:64:42	WPA2	1	42%

WiFi Pineapple Nano - Modules

NANO				
TETRA				
MK5				
MK4				
Name	Version	Author	Description	Type
DWall	1.1	sebkinne	Display's HTTP URLs, Cookies, POST DATA, and images from browsing clients as a stream. Wall of Sheep style.	GUI
SSLSplit	1.0	whistlemaster	Perform man-in-the-middle attacks using SSLSplit	GUI
EvilPortal	2.1	newbi3	An Evil Captive Portal.	GUI
Deauth	1.4	whistlemaster	Deauthentication attacks of all devices connected to APs nearby	GUI
SiteSurvey	1.2	whistlemaster	WiFi site survey	GUI
nmap	1.4	whistlemaster	GUI for security scanner nmap	GUI
ettercap	1.4	whistlemaster	Perform man-in-the-middle attacks using ettercap	GUI
wps	1.2	whistlemaster	WPS brute force attack using Reaver, Bully and Pixiewps	GUI
Occupineapple	1.5	whistlemaster	Broadcast spoofed WiFi SSIDs	GUI
urlsnarf	1.4	whistlemaster	Output all requested URLs sniffed from http traffic using urlsnarf	GUI
Status	1.1	whistlemaster	Display status information of the device	GUI
tcpdump	1.4	whistlemaster	Dump traffic on network using tcpdump	GUI
PortalAuth	1.4	sud0nick	Captive portal cloner and payload distributor.	GUI
DNSspooF	1.3	whistlemaster	Forge replies to arbitrary DNS queries using DNSspooF	GUI
SignalStrength	1.0	r3dfish	Displays signal strength for wireless cells that are within range. Can be used to physically locate cells.	GUI
RandomRoll	1.1	foxtrot	This module allows you to troll unsuspecting clients connected to your WiFi Pineapple.	GUI
Cabinet	1.0	newbi3	A file manager for the Web Interface	GUI
ConnectedClients	1.4	r3dfish	Shows currently connected clients, DHCP leases and blacklist management.	GUI
OnlineHashCrack	1.1	whistlemaster	Submit Hash and WPA Handshake to www.onlinehashcrack.com web service	GUI
get	1.2	dustbyter	Profile clients through the browser plugins supported by their browser	GUI
Papers	1.4	sud0nick	A TLS/SSL and SSH certificate generator/manager.	GUI

Auswahl an möglichen Angriffsarten

- **Stören der WLAN Verbindung zwischen Client und Accesspoint**
 - **Störsender**
 - **Deauthentication Pakete aussenden und somit eine bestehend WLAN-Verbindung beenden.**
- **Abhören des WLAN-Datenstroms**
- **Honeypot**
 - **Verwenden einer fremden SSID für eigenen Hotspot**
z.B. Ich betreibe einen Accesspoint mit der SSID „Telekom“
- **Man in the middle Attacke**
 - **Verbindung wird über WLAN-AP des Angreifers geleitet und dann zum regulären AP weitergereicht.**

Man in the middle Attacke



**WLAN
Client**

Verbindung 1



**WLAN Hotspot
SSID: Telekom_ICE**

Man in the middle Attacke



**WLAN
Client**

Verbindung 1



**WLAN Hotspot
SSID: Telekom_ICE**



**Angreifer
z.B. WiFi Pineapple Nano**

Man in the middle Attacke



**WLAN
Client**

Verbindung 1



**WLAN Hotspot
SSID: Telekom_ICE**



**Angreifer
z.B. WiFi Pineapple Nano**

Man in the middle Attacke



**WLAN
Client**

Verbindung 1



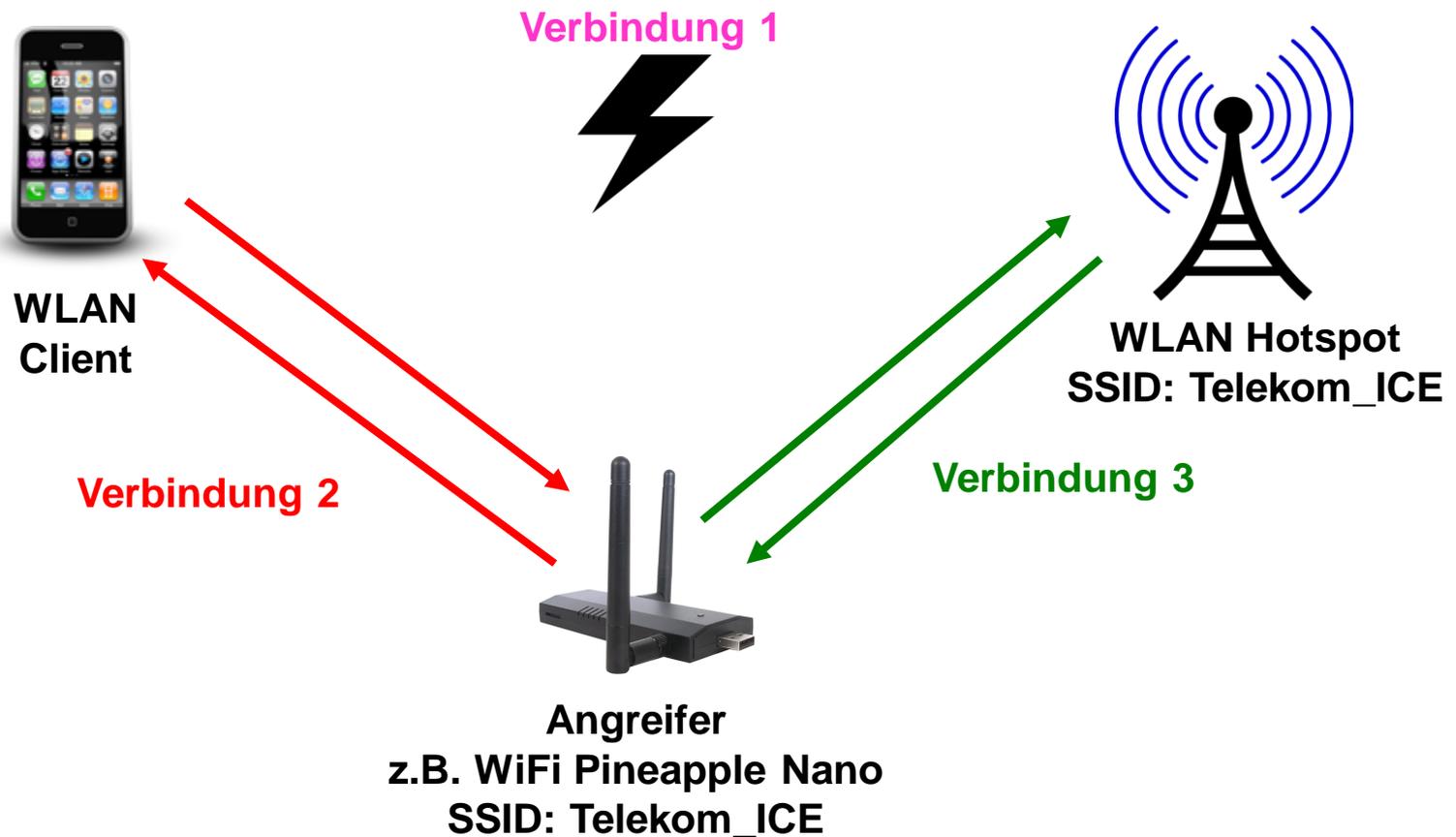
**WLAN Hotspot
SSID: Telekom_ICE**

Verbindung 2

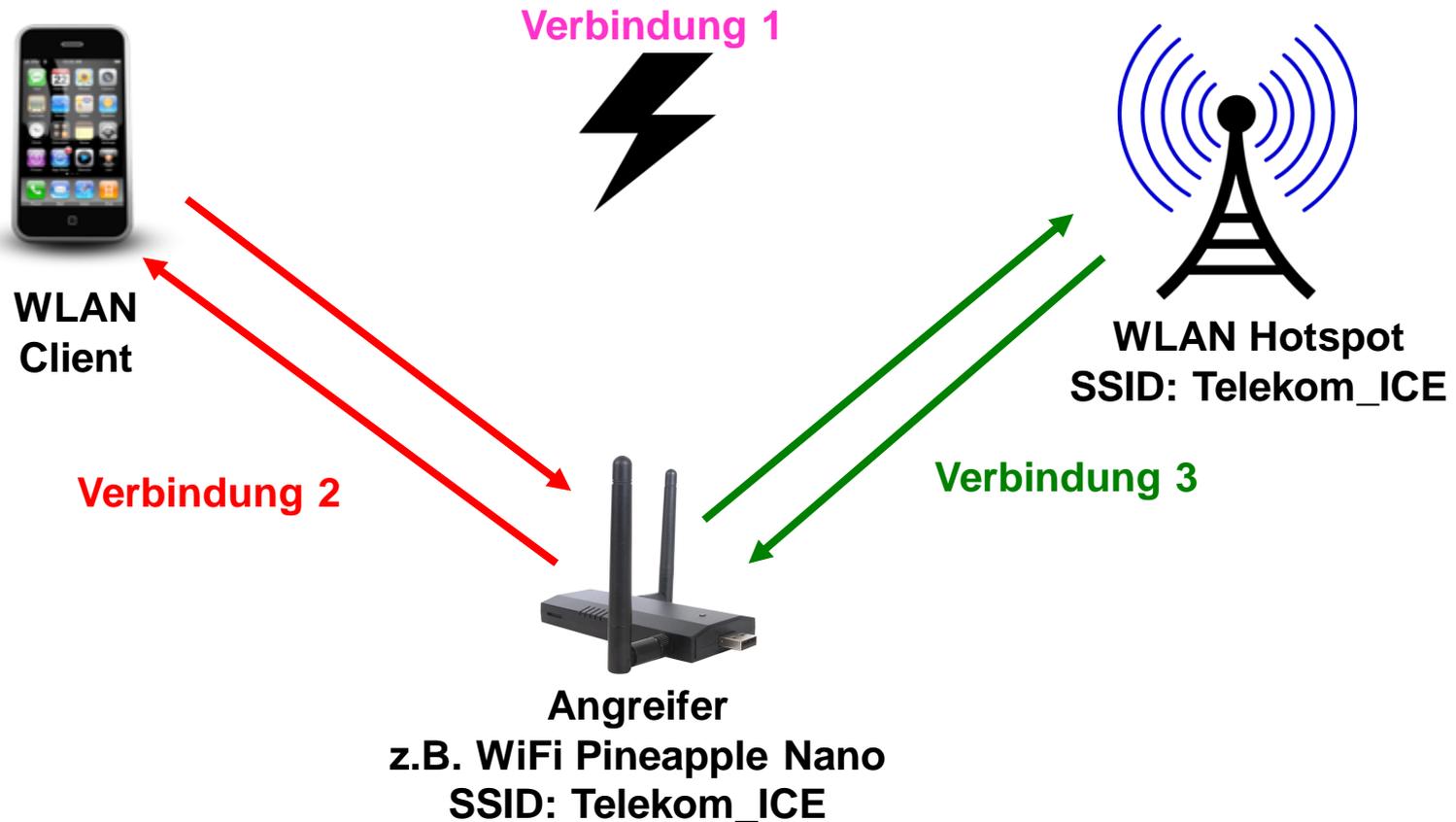


**Angreifer
z.B. WiFi Pineapple Nano
SSID: Telekom_ICE**

Man in the middle Attacke



Man in the middle Attacke



Ergebnis: WLAN Client nutzt aus seiner Sicht weiterhin den WLAN Hotspot von der Telekom im ICE. Angreifer kann jedes Datenpaket mitlesen und ggf. auch verändern ohne, dass Hotspot noch Client was mitbekommen

Möglichkeiten für den Angreifer durch die „Man in the middle Attacke“

- **Direktes Mitlesen und ggf. Veränderung von unverschlüsseltem Datenverkehr, z.B.**
 - **Webseiten, die über HTTP-Protokoll angesurft werden**
 - **E-Mails, die unverschlüsselt über SMTP, IMAP oder POP3 übertragen werden**
 - **DNS-Spoofing (Adressauflösung von Domains verändern)**
 - **Phishing (Fälschen von Webseiten)**

Möglichkeiten für den Angreifer durch die „Man in the middle Attacke“

- **Direktes Mitlesen und ggf. Veränderung von unverschlüsseltem Datenverkehr, z.B.**
 - Webseiten, die über HTTP-Protokoll angesurft werden
 - E-Mails, die unverschlüsselt über SMTP, IMAP oder POP3 übertragen werden
 - DNS-Spoofing (Adressauflösung von Domains verändern)
 - Phishing (Fälschen von Webseiten)
- **Zugriff auf Serverdienste, die auf dem WLAN Client laufen, z.B.**
 - Windows Dateifreigabe
 - Remote Desktop Dienst
 - Lokale Webserver (mache Programme liefern diese mit)
 - Dateiaustausch Apps

Schutz vor Zugriff auf Serverdienste am WLAN Client



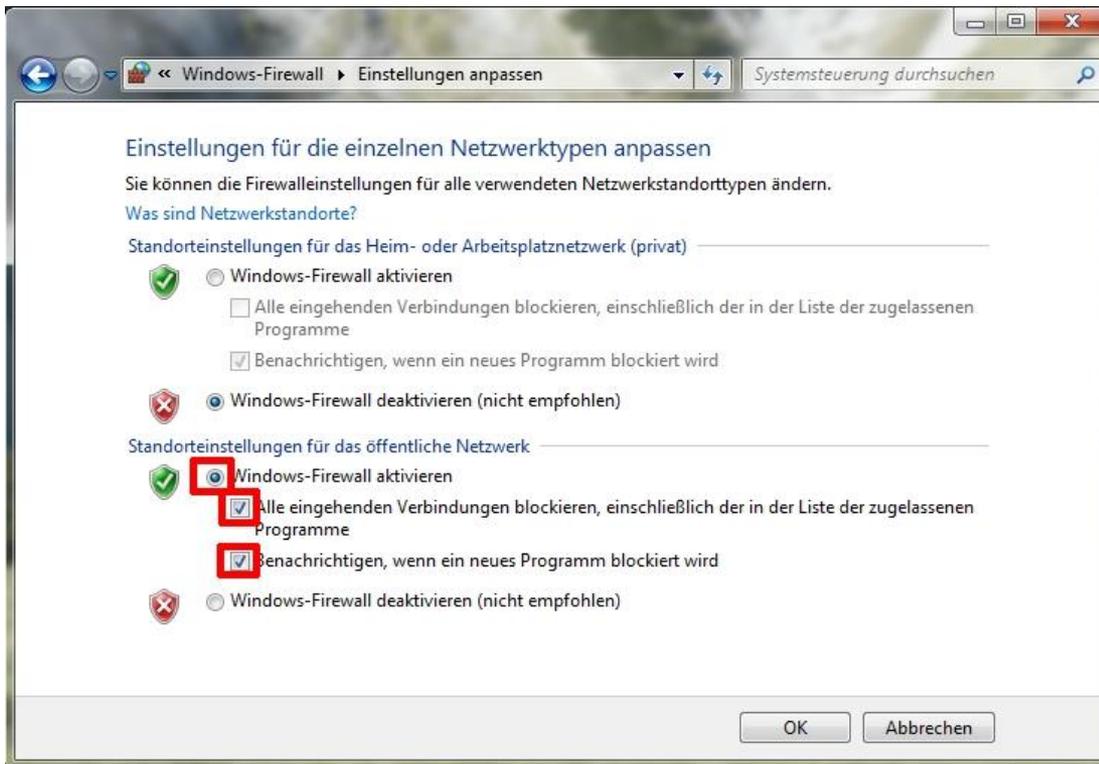
- neue WLAN-Netze grundsätzlich als öffentliche Netze einstufen bei Windows Netzerkennungsfraage



Schutz vor Zugriff auf Serverdienste am WLAN Client



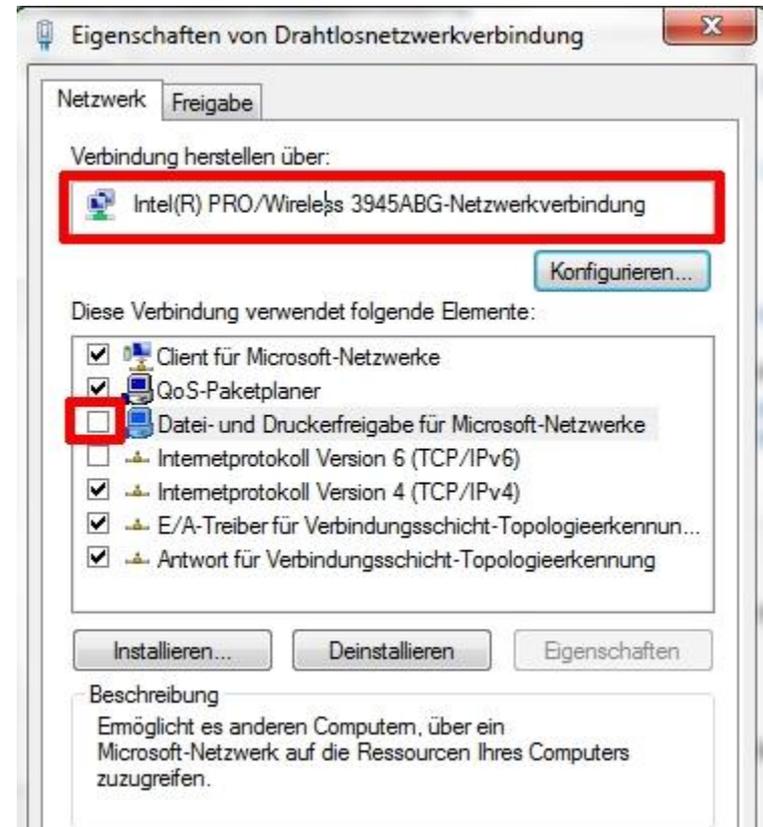
- **Windows Firewall** zumindest für öffentliche Netze aktivieren und keine eingehenden Verbindungen zulassen.



Schutz vor Zugriff auf Serverdienste am WLAN Client



- „*Datei und Druckerfreigabe*“ für WLAN-Interface abschalten, wenn diese über WLAN nicht verwendet
- Wer keine Windows Serverdienste nutzt kann die Option „*Client für Microsoft-Netzwerke*“ auch deaktivieren

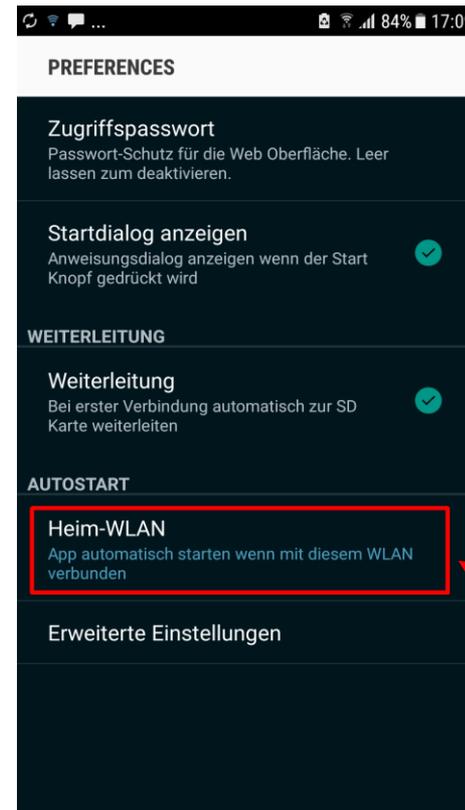
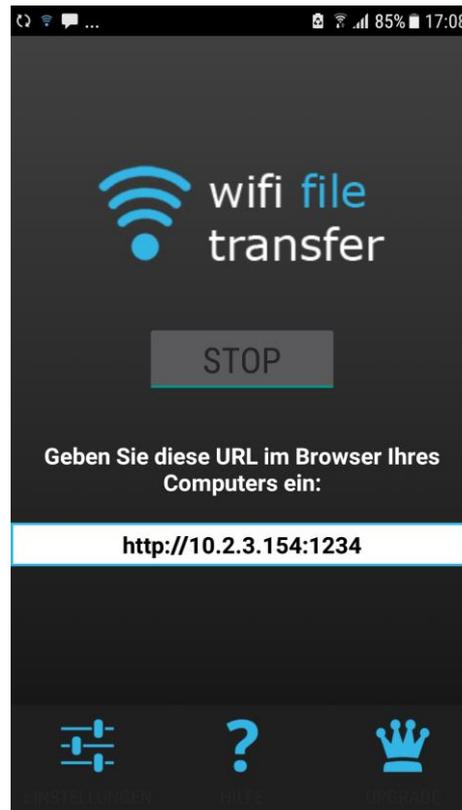


Schutz vor Zugriff auf Serverdienste am WLAN Client



- Keine dauerhaftes Aktivieren von Apps, die Serverdienste bereithalten

Beispiel App:
WiFi File Transfer



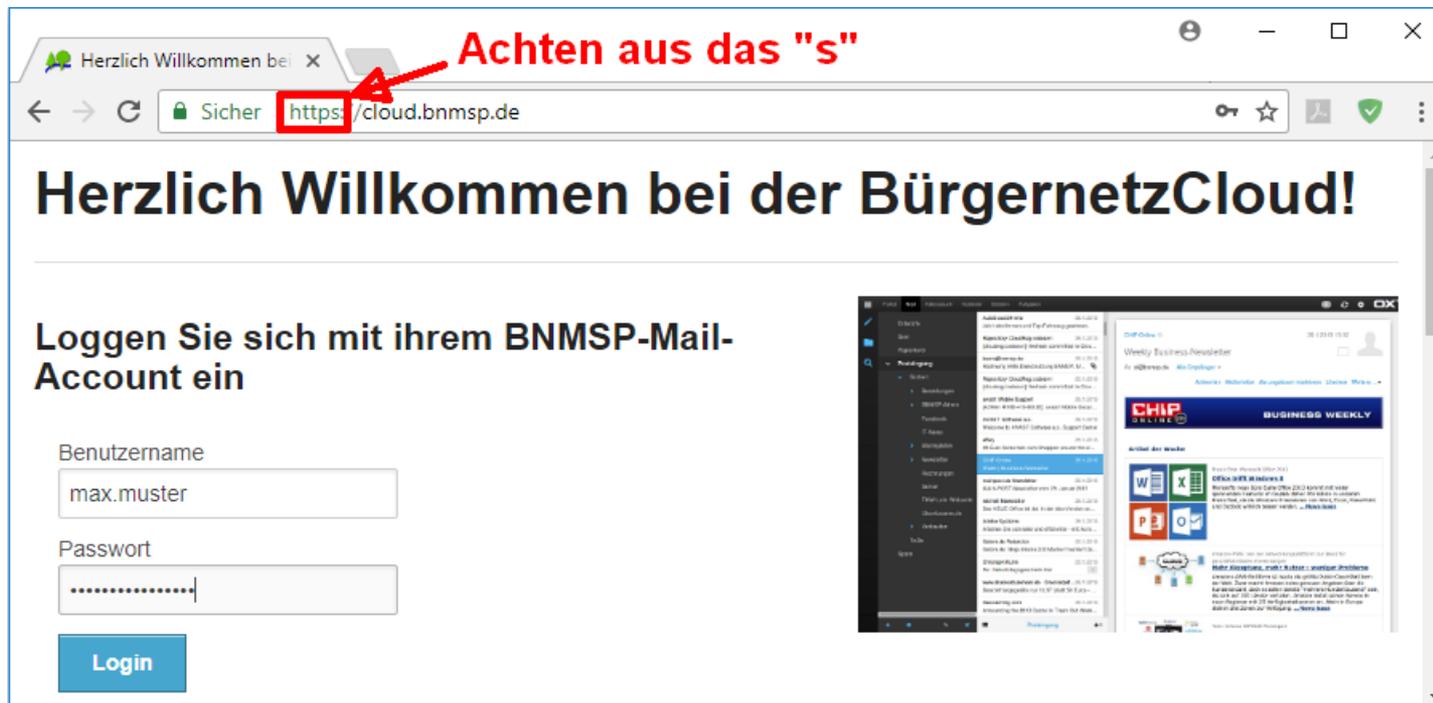
Kritisch !!

Schutz vor Mitlesen und Veränderung von Daten, die über WLAN-Hotspot ausgetauscht werden

- **Nutzung von Verschlüsselung auf Dienst- und Applikationsebene**
 - **Keine Verwendung von unverschlüsselten Protokollen, wie HTTP**
 - **Webseiten, die über HTTPS-Protokoll aufrufen**
 - **E-Mail Client nur mit verschlüsselten Protokollen nutzen**

Schutz vor Mitlesen und Veränderung von Daten, die über WLAN-Hotspot ausgetauscht werden

- Webseiten nur über HTTPS aufrufen



Herzlich Willkommen bei x

Sicher **https**://cloud.bnmosp.de

Achten auf das "s"

Herzlich Willkommen bei der BürgernetzCloud!

Loggen Sie sich mit ihrem BNMSP-Mail-Account ein

Benutzername

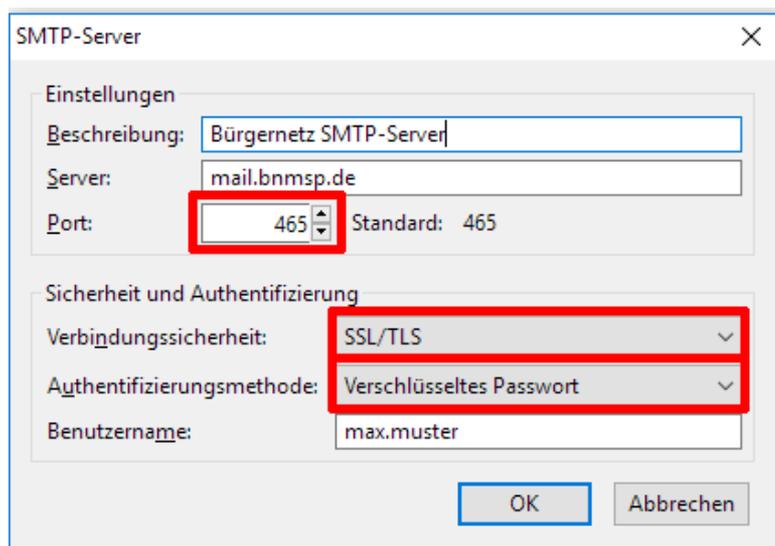
Passwort

Login

- bei kritische Webseiten entweder Server URL mit ***https://meine-bank.de*** immer direkt eingeben oder aus vorher gespeicherten Bookmarks aufrufen
- Aufruf nicht über den Vorschlag einer Suchmaschine

Schutz vor Mitlesen und Veränderung von Daten, die über WLAN-Hotspot ausgetauscht werden

Richtige Einstellung am E-Mail Client



SMTP-Server

Einstellungen

Beschreibung: Bürgernetz SMTP-Server

Server: mail.bnmsp.de

Port: 465 Standard: 465

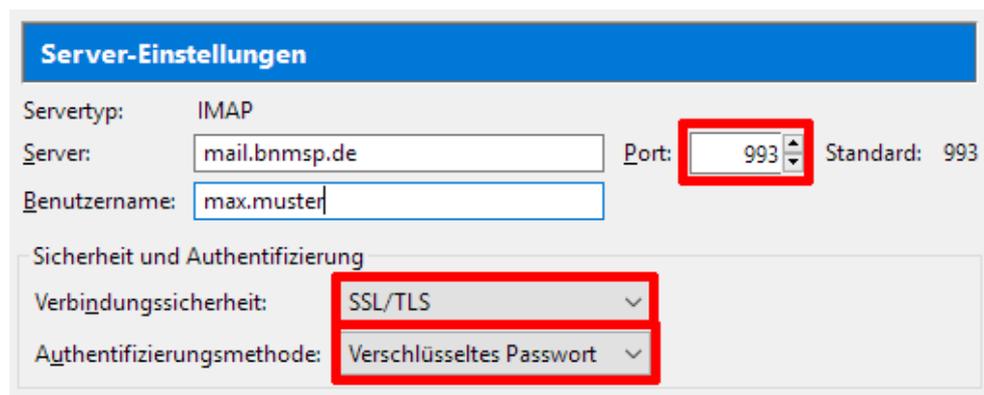
Sicherheit und Authentifizierung

Verbindungssicherheit: SSL/TLS

Authentifizierungsmethode: Verschlüsseltes Passwort

Benutzername: max.muster

OK Abbrechen



Server-Einstellungen

Servertyp: IMAP

Server: mail.bnmsp.de Port: 993 Standard: 993

Benutzername: max.muster

Sicherheit und Authentifizierung

Verbindungssicherheit: SSL/TLS

Authentifizierungsmethode: Verschlüsseltes Passwort

Für Postausgang Port 465 (SMTPS)

Für Posteingang Port 993 (IMAPS)

Nach Möglichkeit immer SSL/TLS anstelle von STARTTLS verwenden

Schutz vor Mitlesen und Veränderung von Daten, die über WLAN-Hotspot ausgetauscht werden

Apps ohne Verschlüsselung nicht über WLAN-Hospots nutzen

**Frage: Wie erkenne ich, dass eine App ihre Daten
verschlüsselt überträgt?**

**Antwort: Als Nutzer kann man das nicht erkennen, ohne
dass man selber oder ein anderer die
Kommunikation überprüft hat**

**Viele Anbieter werben heute mit Schlagworten,
wie AES265 Verschlüsselung, Ende-zu-Ende Verschlüsselung, etc**

Als Nutzer muss man dem vertrauen

**Beispiele: - WhatsApp (Ende-zu-Ende Verschlüsselung) -> Hohe Reputation -> OK
- DropBox (Transportveschlüsselung) -> Hohe Reputation -> OK**

Schutz vor Mitlesen und Veränderung von Daten, die über WLAN-Hotspot ausgetauscht werden

Phishing Fälschen von Webseiten

Schutz:

- Steht die richtige Domain des Anbieters in der URL-Zeile vom Browser?
(auch Schreibweise beachten!)
- Virens Scanner mit Websecurity
- 2 Faktor Authentisierung bei kritischen Diensten
(PIN als SMS für zweiten Bestandteil des Loginvorgangs)



Angriffe auf SSL / TLS Verschlüsselung

Sicherheitsfeature: Verschlüsselung auf Dienstebene

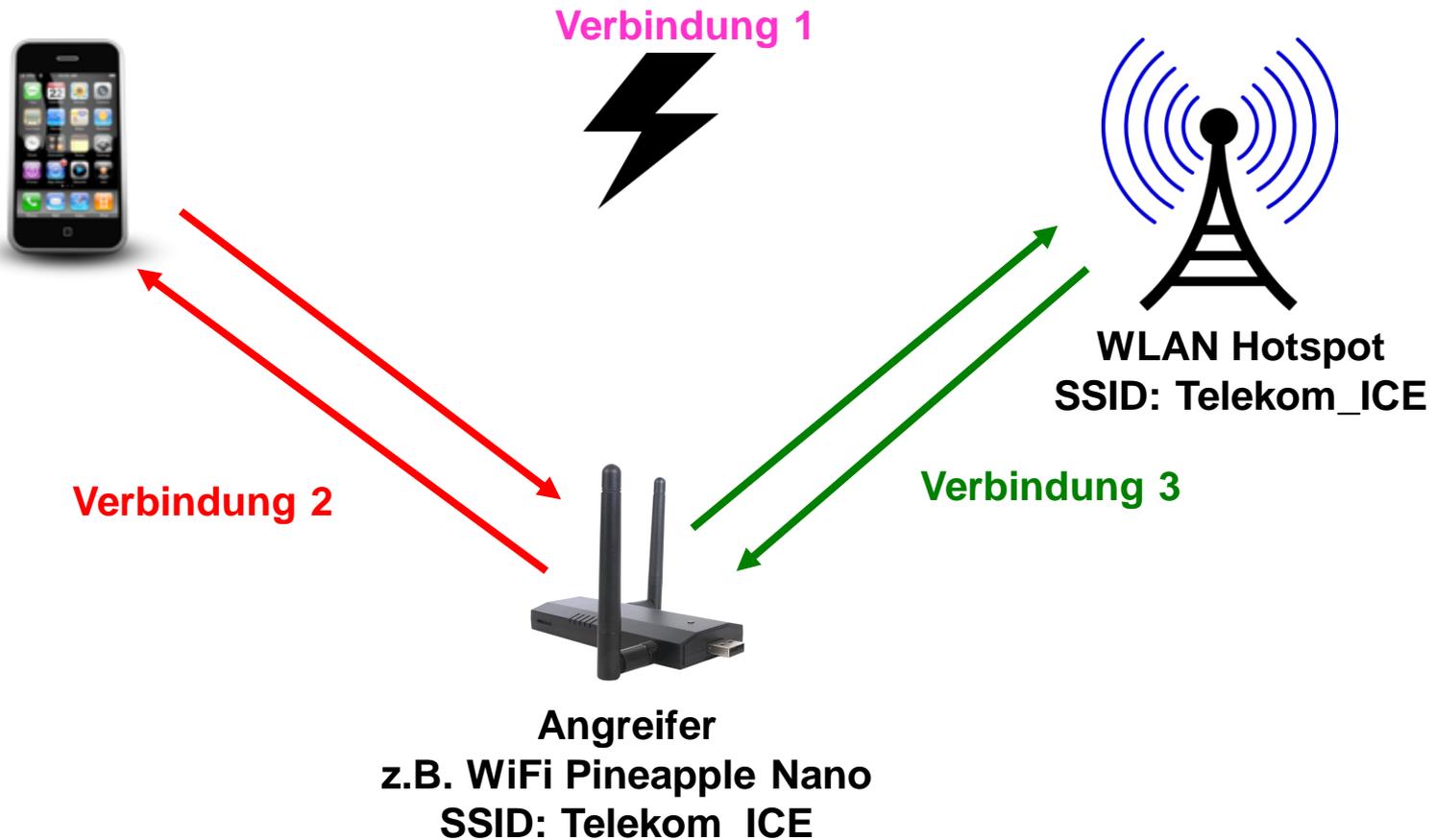
Standard: SSL / TLS Verschlüsselung bei Webseiten, die mit **https aufgerufen werden**

Beispiele: **https://cloud.bnmssp.de**

****https**://www.sparkasse-mainfranken.de**

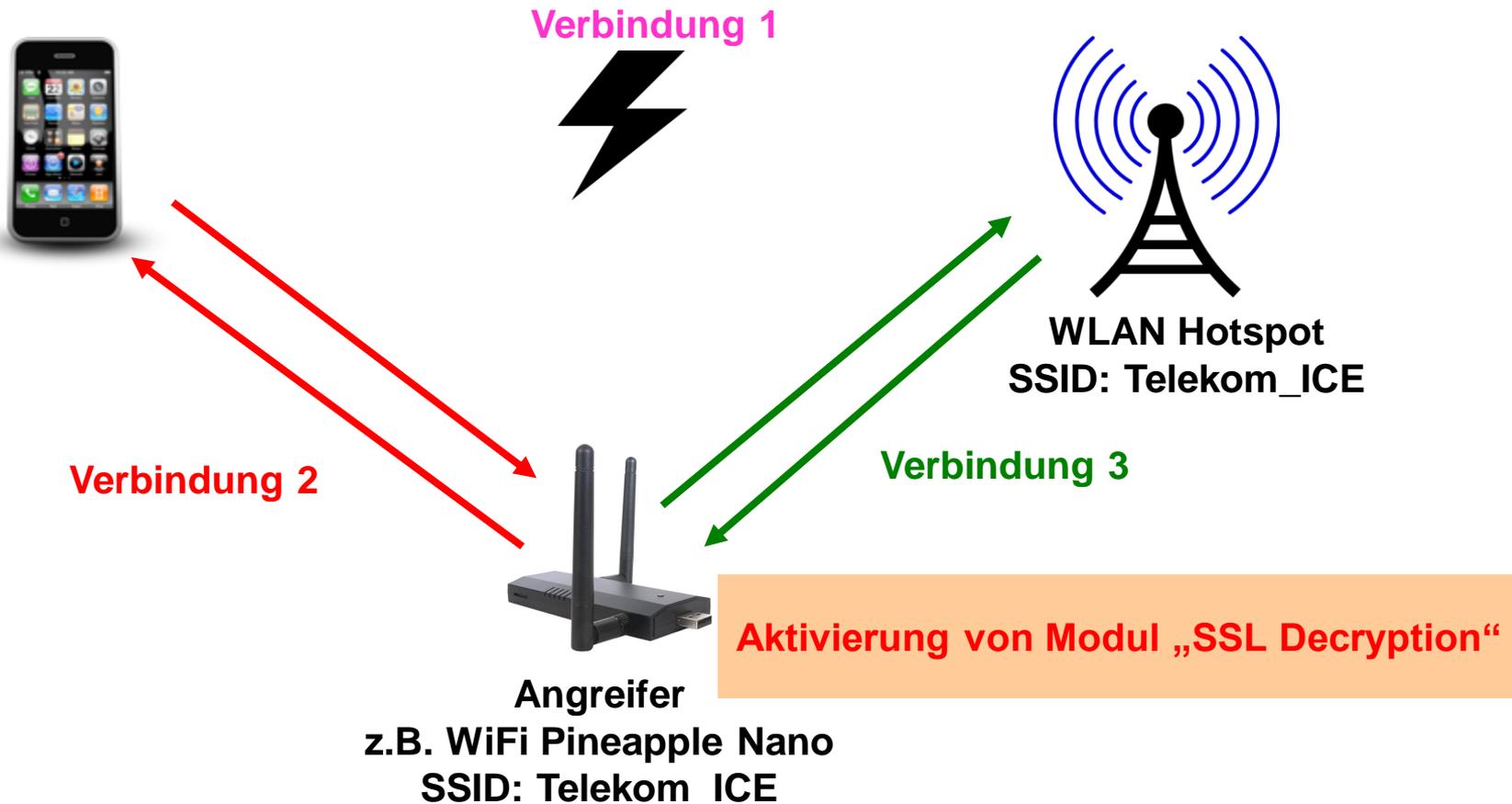
Angriffe auf SSL / TLS Verschlüsselung

Angriff: SSL / TLS Decryption während „Man in the middle Attacke“



Angriffe auf SSL / TLS Verschlüsselung

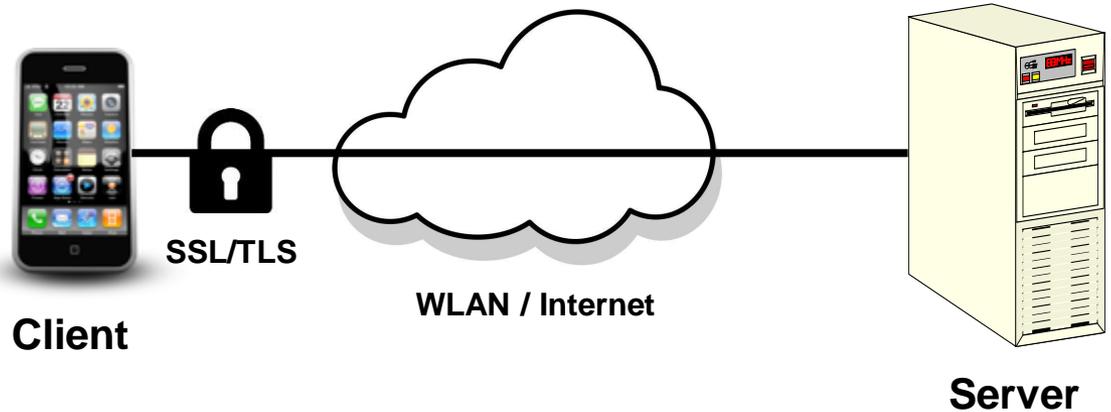
Angriff: SSL / TLS Decryption während „Man in the middle Attacke“



Angriffe auf SSL / TLS Verschlüsselung

Funktionsweise von SSL / TLS Decryption

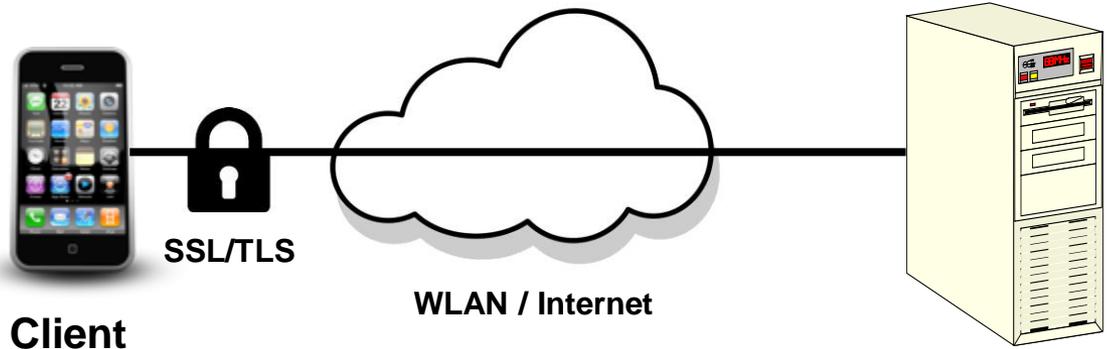
Sichere „Ende zu Ende
Verschlüsselung“ mit SSL / TLS



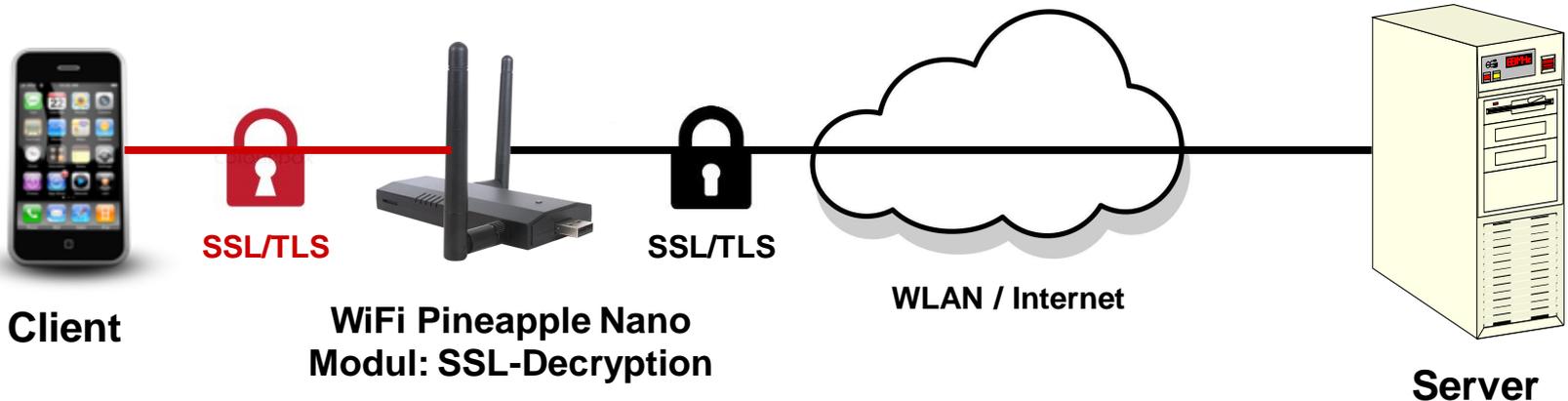
Angriffe auf SSL / TLS Verschlüsselung

Funktionsweise von SSL / TLS Decryption

Sichere „Ende zu Ende
Verschlüsselung“ mit SSL / TLS

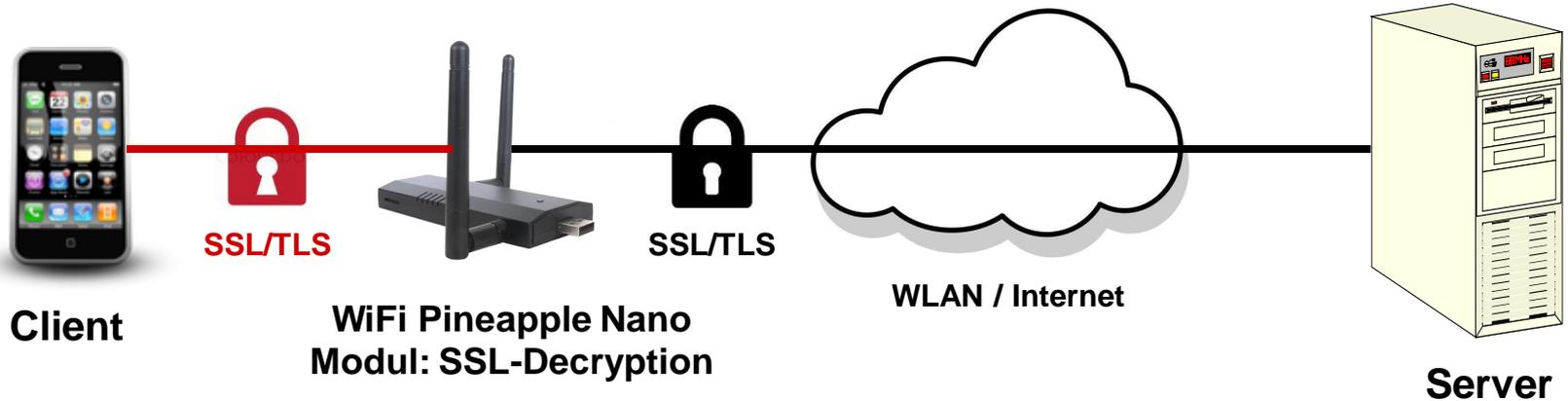


Keine „Ende zu Ende
Verschlüsselung“ mehr
2 Schlüssel auf dem Transportweg



Angriffe auf SSL / TLS Verschlüsselung

Funktionsweise von SSL / TLS Decryption



Warum funktioniert das?

- Der Server kann nicht erkennen, dass ein „falscher“ Client am Ende der Verbindung ist
Der Client weist sich gegenüber dem Server in der Regel nicht aus
- Der Client könnte erkennen, dass es sich bei der Gegenstelle nicht um den „richtigen“ Server handelt, doch tut er das in der Regel nicht oder nur unzureichend.
- Der Nutzer des Clients könnte erkennen, dass es der „falsche“ Server ist, aber das viel zu umständlich für die Praxis

Angriffe auf SSL / TLS Verschlüsselung

Wie findet der Client heraus, dass er wirklich mit dem richtigen Server per SSL / TLS kommuniziert ?

Über Zertifikate

- Noch bevor Nutzdaten über die SSL-Verbindung geschickt werden, sendet der Server sein Zertifikat mit seinem öffentlichen Schlüssel an den Client
- Webbrowser führt intern eine Liste von vertrauenswürdigen Zertifizierungsstellen
- Ist das Zertifikat mit dem sich der Server ausweist, von einer dieser Zertifizierungsstellen unterschrieben (beglaubigt), dann stellt der Browser ohne weitere Nachfragen und Hinweise die SSL / TLS Verbindung zum Server her
- Ist Zertifikat von einer nicht beannten Zertifizierungsstelle ausgestellt, abgelaufen oder passt nicht zur aufgerufenen Domainnamen gibt es eine Hinweismeldung

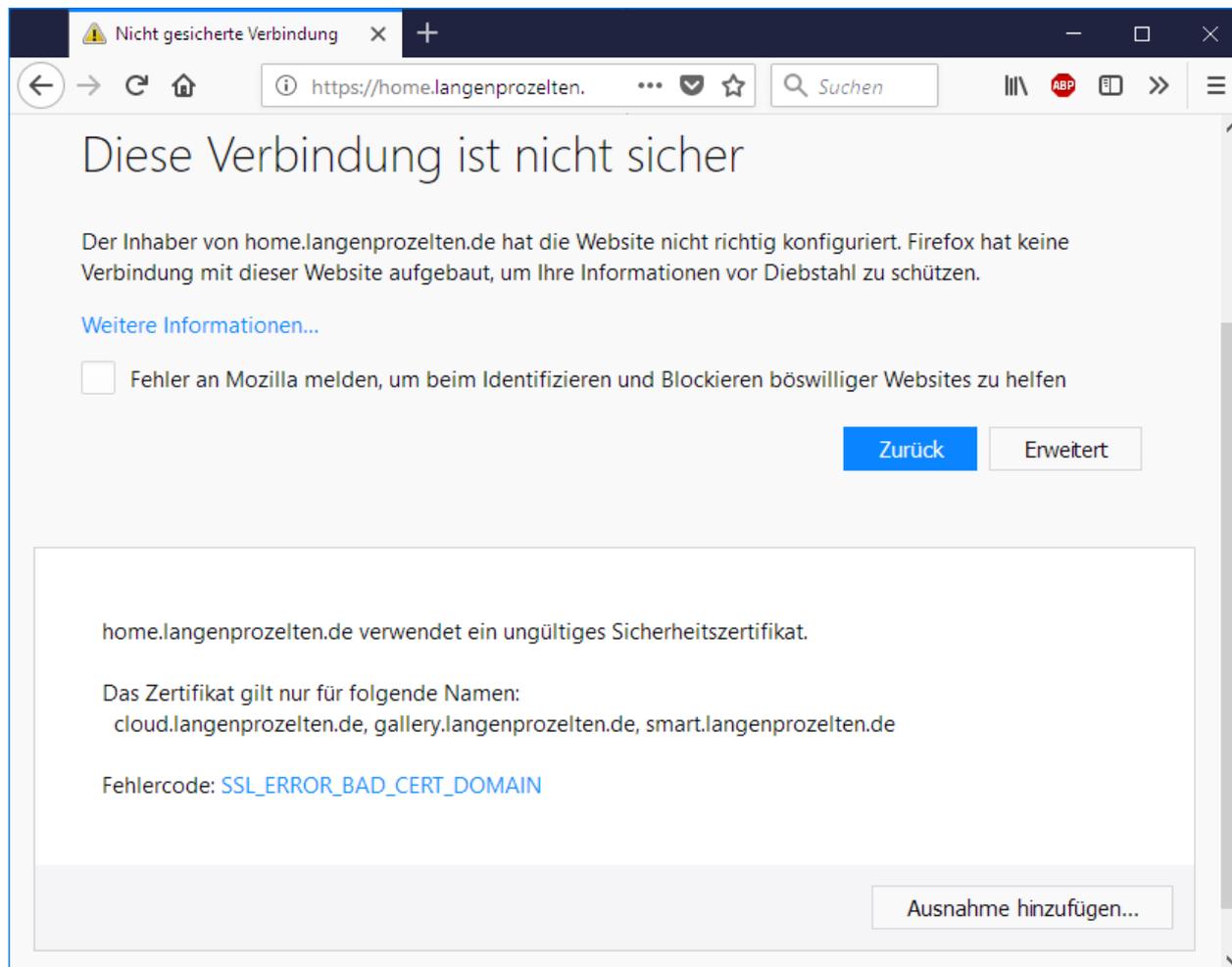
Problem

Angriffe auf SSL / TLS Verschlüsselung

Hinweismeldungen bei fehlerhaften Zertifikaten

Fehlergrund:

**Zertifikat passt nicht
zum Domainnamen**



The screenshot shows a Firefox browser window with a security warning. The address bar shows the URL `https://home.langenprozelten.de`. The main content area displays the message "Diese Verbindung ist nicht sicher" (This connection is not secure). Below this, it states: "Der Inhaber von home.langenprozelten.de hat die Website nicht richtig konfiguriert. Firefox hat keine Verbindung mit dieser Website aufgebaut, um Ihre Informationen vor Diebstahl zu schützen." (The owner of home.langenprozelten.de has not configured the website correctly. Firefox has not established a connection with this website to protect your information from theft.) There is a link for "Weitere Informationen..." (More information...). A checkbox is present with the text "Fehler an Mozilla melden, um beim Identifizieren und Blockieren böswilliger Websites zu helfen" (Report error to Mozilla to help identify and block malicious websites). At the bottom right of the warning area are two buttons: "Zurück" (Back) and "Erweitert" (Advanced). A detailed error message box at the bottom contains the text: "home.langenprozelten.de verwendet ein ungültiges Sicherheitszertifikat." (home.langenprozelten.de uses an invalid security certificate.), "Das Zertifikat gilt nur für folgende Namen:" (The certificate is valid only for the following names:), "cloud.langenprozelten.de, gallery.langenprozelten.de, smart.langenprozelten.de" (cloud.langenprozelten.de, gallery.langenprozelten.de, smart.langenprozelten.de), and "Fehlercode: `SSL_ERROR_BAD_CERT_DOMAIN`" (Error code: `SSL_ERROR_BAD_CERT_DOMAIN`). At the bottom right of this box is a button labeled "Ausnahme hinzufügen..." (Add exception...).

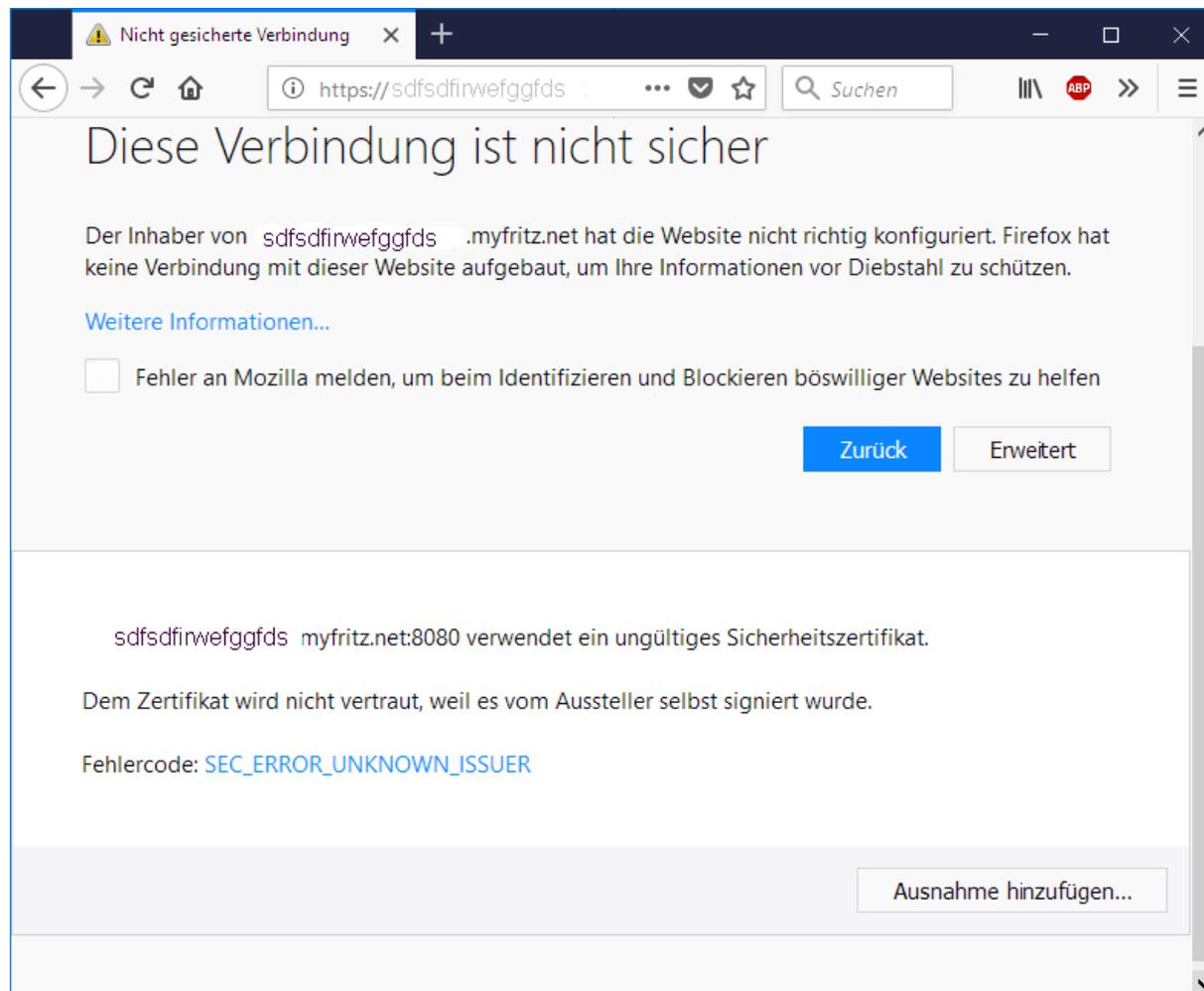
Angriffe auf SSL / TLS Verschlüsselung

Hinweismeldungen bei fehlerhaften Zertifikaten

Fehlergrund:

Zertifikat ist nicht von einer im Browser hinterlegten Zertifizierungsstelle unterschrieben

Es wurde selbst erstellt.



The screenshot shows a Firefox browser window with a security warning. The address bar displays a placeholder URL: `https://sdfsdfirwefggfds`. The main content area contains the following text:

Diese Verbindung ist nicht sicher

Der Inhaber von `sdfsdfirwefggfds`.myfritz.net hat die Website nicht richtig konfiguriert. Firefox hat keine Verbindung mit dieser Website aufgebaut, um Ihre Informationen vor Diebstahl zu schützen.

[Weitere Informationen...](#)

Fehler an Mozilla melden, um beim Identifizieren und Blockieren böswilliger Websites zu helfen

[Zurück](#) [Erweitert](#)

`sdfsdfirwefggfds` myfritz.net:8080 verwendet ein ungültiges Sicherheitszertifikat.

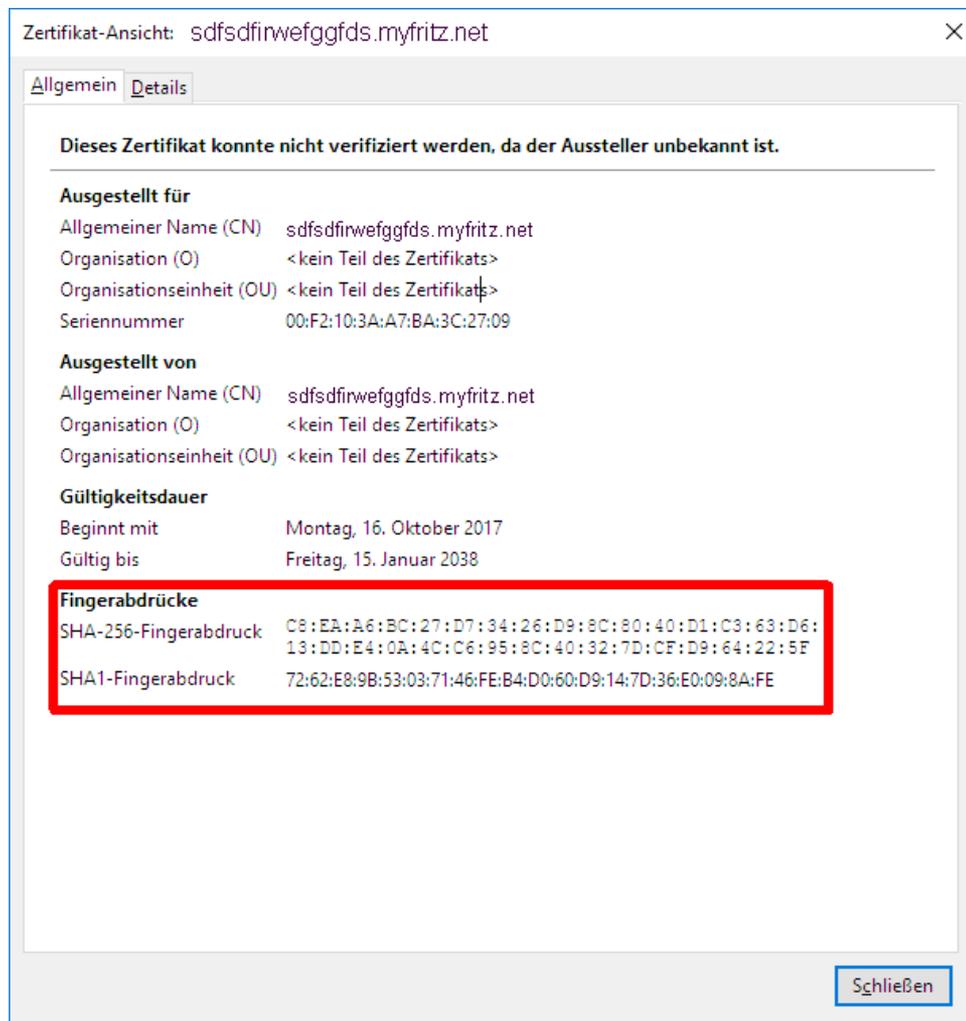
Dem Zertifikat wird nicht vertraut, weil es vom Aussteller selbst signiert wurde.

Fehlercode: [SEC_ERROR_UNKNOWN_ISSUER](#)

[Ausnahme hinzufügen...](#)

Verhalten bei Zertifikatsfehlermeldungen

- Am besten nicht weitersurfen auf der betroffenen Webseite in einem Hotspot-Netz
- Wenn man weiß, dass es eine eigene Seite ist, die man mit einem selbst signiertem Zertifikat versehen hat, prüfen, ob er Fingerabdruck dieses Zertifikats stimmt



Zertifikat-Ansicht: sdfsdfirweggfds.myfritz.net

Allgemein Details

Dieses Zertifikat konnte nicht verifiziert werden, da der Aussteller unbekannt ist.

Ausgestellt für

Allgemeiner Name (CN)	sdfsdfirweggfds.myfritz.net
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	00:F2:10:3A:A7:BA:3C:27:09

Ausgestellt von

Allgemeiner Name (CN)	sdfsdfirweggfds.myfritz.net
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>

Gültigkeitsdauer

Beginnt mit	Montag, 16. Oktober 2017
Gültig bis	Freitag, 15. Januar 2038

Fingerabdrücke

SHA-256-Fingerabdruck	08:EA:A6:BC:27:D7:34:26:D9:8C:80:40:D1:C3:63:D6:13:DD:E4:0A:4C:C6:95:8C:40:32:7D:CF:D9:64:22:5F
SHA1-Fingerabdruck	72:62:E8:9B:53:03:71:46:FE:B4:D0:60:D9:14:7D:36:E0:09:8A:FE

Schließen

Angriffe auf SSL / TLS Verschlüsselung

Kann ich einem Zertifikat vertrauen, dass vom Browser nicht beanstandet wurde ?

Antwort: JAIN

- Es gibt Zertifizierungsstellen, die sehr einfach ohne große Prüfung Zertifikate ausstellen
- Es gibt Zertifizierungsstellen, die gehackt wurden
- Schreibweise von Domain unbedingt anschauen
z.B. <https://www.sparkasse-mainfranken.de>

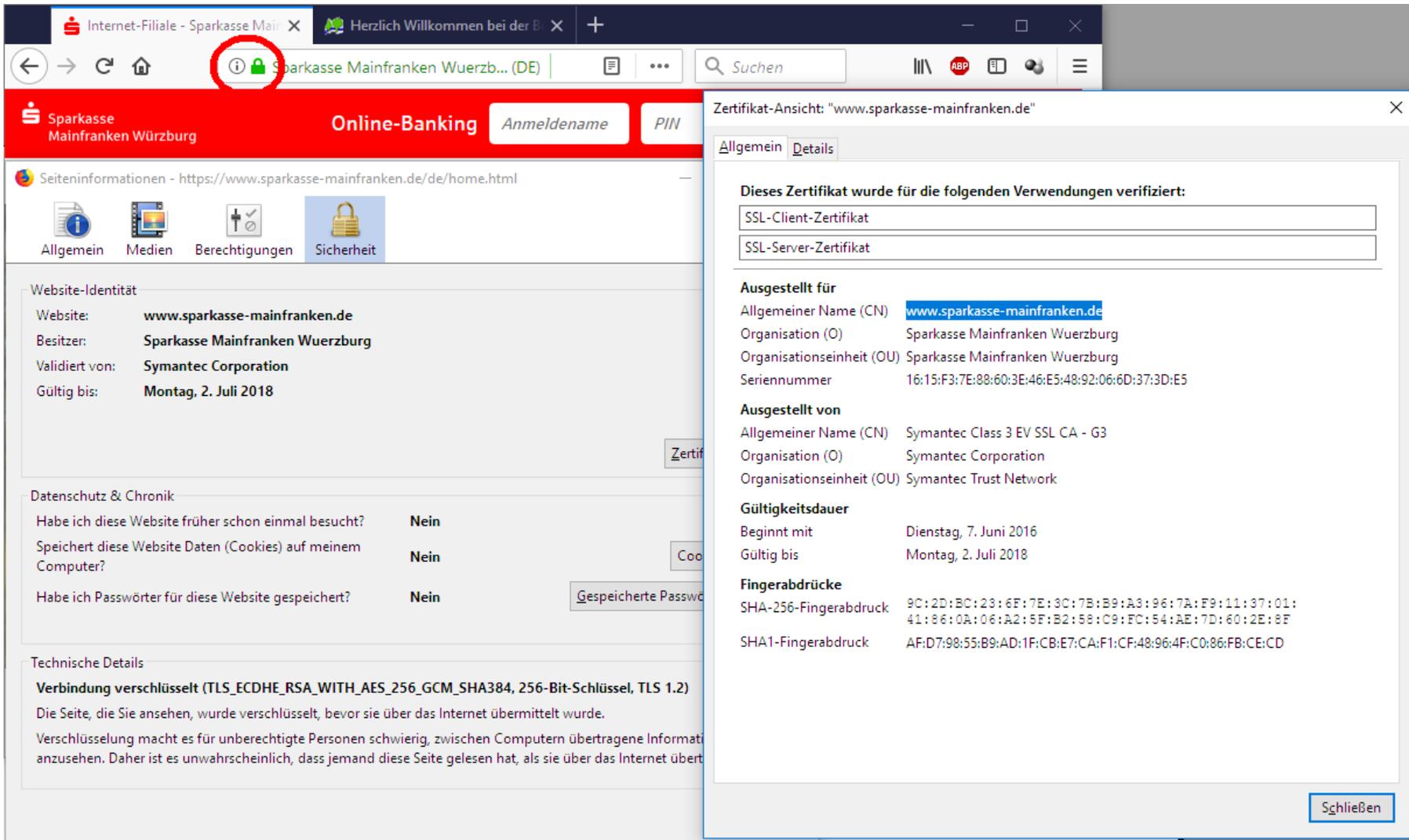
Angriffe auf SSL / TLS Verschlüsselung

Kann ich einem Zertifikat vertrauen, dass vom Browser nicht beanstandet wurde ?

Antwort: JAIN

- Es gibt Zertifizierungsstellen, die sehr einfach ohne große Prüfung Zertifikate ausstellen
- Es gibt Zertifizierungsstellen, die gehackt wurden
- Schreibweise von Domain unbedingt anschauen
z.B. <https://www.sparkasse-mainfranken.de>

Beispiel für ein EV-Zertifikat



The screenshot shows a web browser window with a security warning icon circled in red. The address bar shows the URL `https://www.sparkasse-mainfranken.de`. The page content includes a red header for "Sparkasse Mainfranken Würzburg" and a "Seiteninformationen" section with icons for "Allgemein", "Medien", "Berechtigungen", and "Sicherheit".

The "Seiteninformationen" section displays the following details:

- Website-Identität:
 - Website: `www.sparkasse-mainfranken.de`
 - Besitzer: **Sparkasse Mainfranken Wuerzburg**
 - Validiert von: **Symantec Corporation**
 - Gültig bis: **Montag, 2. Juli 2018**
- Datenschutz & Chronik:
 - Habe ich diese Website früher schon einmal besucht? **Nein**
 - Speichert diese Website Daten (Cookies) auf meinem Computer? **Nein**
 - Habe ich Passwörter für diese Website gespeichert? **Nein**
- Technische Details:
 - Verbindung verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-Bit-Schlüssel, TLS 1.2)**
 - Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.
 - Verschlüsselung macht es für unberechtigte Personen schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Internet übertr...

The "Zertifikat-Ansicht" window shows the following details:

Zertifikat-Ansicht: "www.sparkasse-mainfranken.de"

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- SSL-Client-Zertifikat
- SSL-Server-Zertifikat

Ausgestellt für

- Allgemeiner Name (CN) `www.sparkasse-mainfranken.de`
- Organisation (O) `Sparkasse Mainfranken Wuerzburg`
- Organisationseinheit (OU) `Sparkasse Mainfranken Wuerzburg`
- Seriennummer `16:15:F3:7E:88:60:3E:46:E5:48:92:06:6D:37:3D:E5`

Ausgestellt von

- Allgemeiner Name (CN) `Symantec Class 3 EV SSL CA - G3`
- Organisation (O) `Symantec Corporation`
- Organisationseinheit (OU) `Symantec Trust Network`

Gültigkeitsdauer

- Beginnt mit `Dienstag, 7. Juni 2016`
- Gültig bis `Montag, 2. Juli 2018`

Fingerabdrücke

- SHA-256-Fingerabdruck `9C:2D:BC:23:6F:7E:3C:7B:B9:A3:96:7A:F9:11:37:01:41:86:0A:06:A2:5F:B2:58:C9:FC:54:AE:7D:60:2E:8F`
- SHA1-Fingerabdruck `AF:D7:98:55:B9:AD:1F:CB:E7:CA:F1:CF:48:96:4F:C0:86:FB:CE:CD`

Buttons: **Zertifikat-Ansicht**, **Schließen**

Angriffe auf SSL / TLS Verschlüsselung

Kann ich einem Zertifikat vertrauen, dass vom Browser nicht beanstandet wurde ?

Verhaltensregel

- Betreiber von Webseiten, die sensible Daten vom Nutzer abverlangen, verwenden in der Regel EV-SSL Zertifikate (grüne Zertifikate)
- Greift man von einem Hotspot-Netz aus auf solch einen Service zu (z.B. Bank, Onlineshop) und es wird kein grünes Zertifikat angezeigt, dann Sitzung noch vor Eingabe von Zugangsdaten beenden !!!

Angriffe auf SSL / TLS Verschlüsselung

Kann ich einem Zertifikat vertrauen, dass vom Browser nicht beanstandet wurde ?

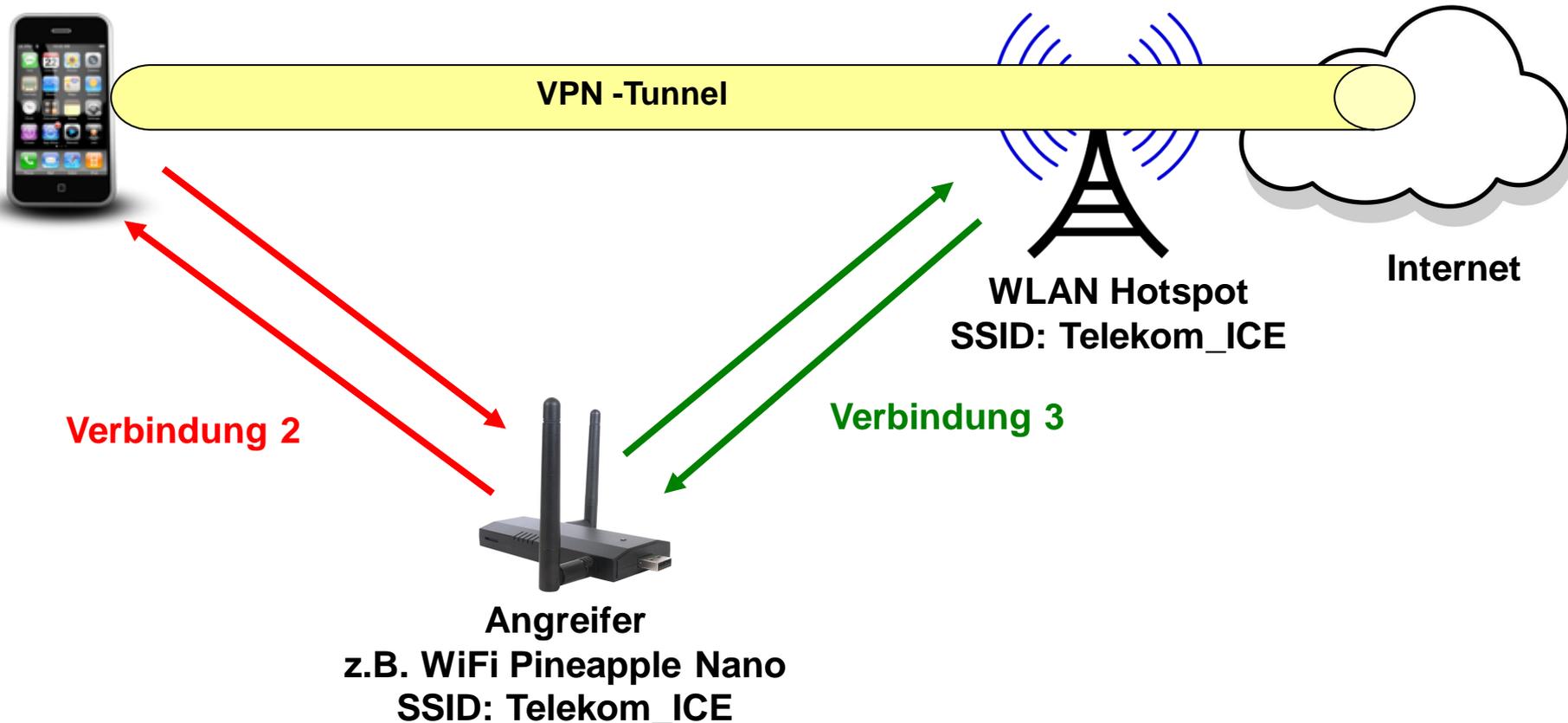
Auch EV-Zertifikate könnten gefälscht sein

Wer ganz sicher gehen möchte der...

- Nutzt gar kein Hotspot-Netz für sensible Dienste
- Statt dessen Mobilfunkdatenverbindung verwenden
- Oder jedes mal den Fingerabdruck vom Zertifikat mit dem Original-Fingerabdruck vergleichen
 - > In der Praxis viel zu aufwendig

Bester Schutz gegen Man in the Middle Attake

VPN-Tunnel vom Endgerät zu einer sichereren Stelle im Internet



VPN-Tunnel sorgt dafür, dass alle Daten Ende zu Ende Verschlüsselt übertragen werden

Bester Schutz gegen Man in the Middle Attake

VPN-Tunnel vom Endgerät zu einer sichereren Stelle im Internet

Wichtig dabei ist:

- Sicheres VPN-Protokoll wählen (z.B. IPsec)
- Sichere Verschlüsselungsalgorithmen verwenden (z.B. AES 256)
- Vertrauenswürdigen Tunnelendpunkt wählen
- Sicherstellen, dass VPN-Funktion am mobilen Endgerät eingeschaltet ist, bevor man einen Hotspot verwendet

Bester Schutz gegen Man in the Middle Attake

VPN-Tunnel vom Endgerät zu einer sichereren Stelle im Internet

Realisierungsmöglichkeiten

- VPN-Dienst (App) verwenden (Problem: Vertrauenswürdig???)
- Als Tunnelendpunkt den eigenen Internetfestnetzanschluss verwenden

Bester Schutz gegen Man in the Middle Attake

VPN-Tunnel vom Endgerät zu einer sichereren Stelle im Internet

Eigene Fritz!Box als Tunnelendpunkt verwenden



Vorraussetzung damit das funktioniert

- Internetanschluss **muss** eine **öffentliche IPv4** Adresse haben z.B. 188.33.54.123 (Adresse kann dabei fest oder dynamisch sein)
- **Möglichst hohe Upstreambandbreite** am Internetanschluss

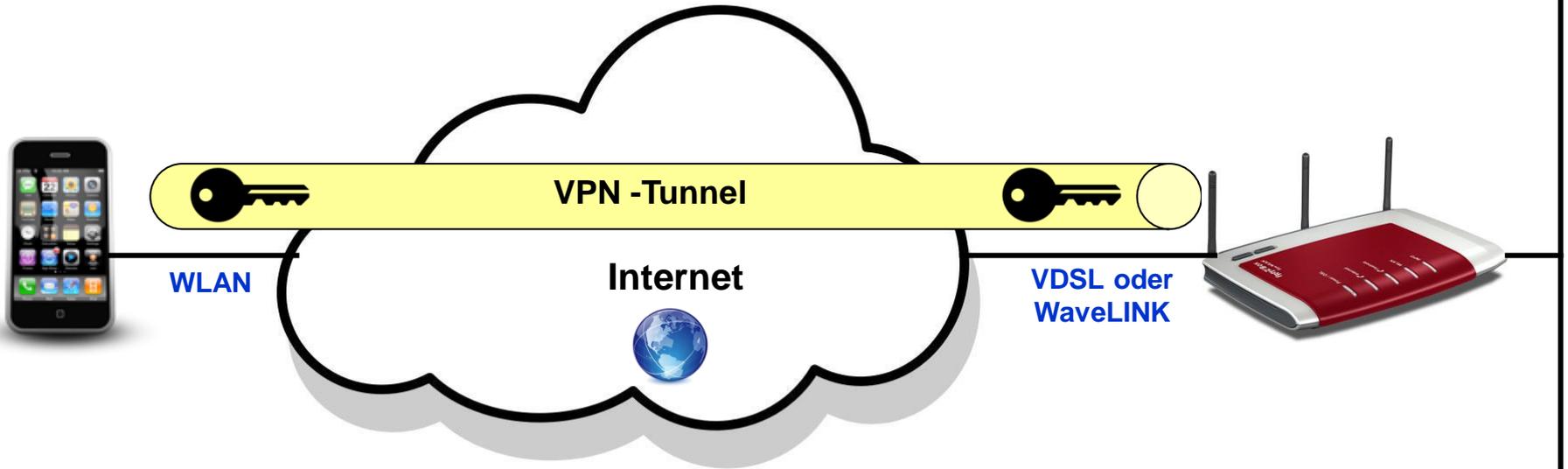
Anschluss	Downstream	Upstream (typisch)
ADSL 16000	16 Mbit/s	2 Mbit/s
VDSL 50000	50 Mbit/s	10 Mbit/s
VDSL 100000	100 Mbit/s	20 oder 40 Mbit/s
Breitbandkabel	500 Mbit/s	50 Mbit/s
WaveLINK 3.0	10 Mbit/s	10 Mbit/s

Erforderliche Hard- und Software

VPN-Konzentrator	Endgerät	VPN-Client (Beispiel)
Fritz!Box  z.B. 7270, 7490, 7590	Windows Notebook oder Tablet	Shrew Soft VPN Client
	Linux Notebook	Shrew Soft VPN Client
	Apple iPhone / iPad	Bereits im Betriebssystem integriert
	Android Smartphone / Tablet	Bereits im Betriebssystem integriert
	Apple Mac	Bereits im Betriebssystem integriert

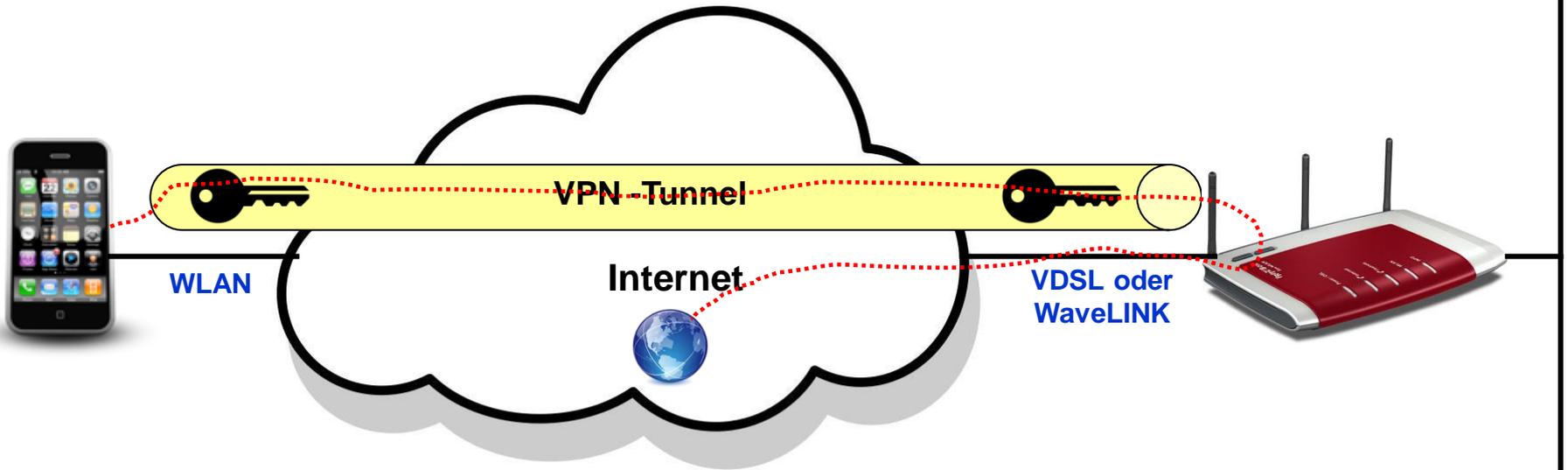
**Windows hat leider von Hause aus keinen standardkonformen IPSec-Client on Board
-> Client von Fremdhersteller notwendig (da gibt es zahlreiche, meist kostenpflichtig)**

Das VPN-Prinzip



Heimnetz

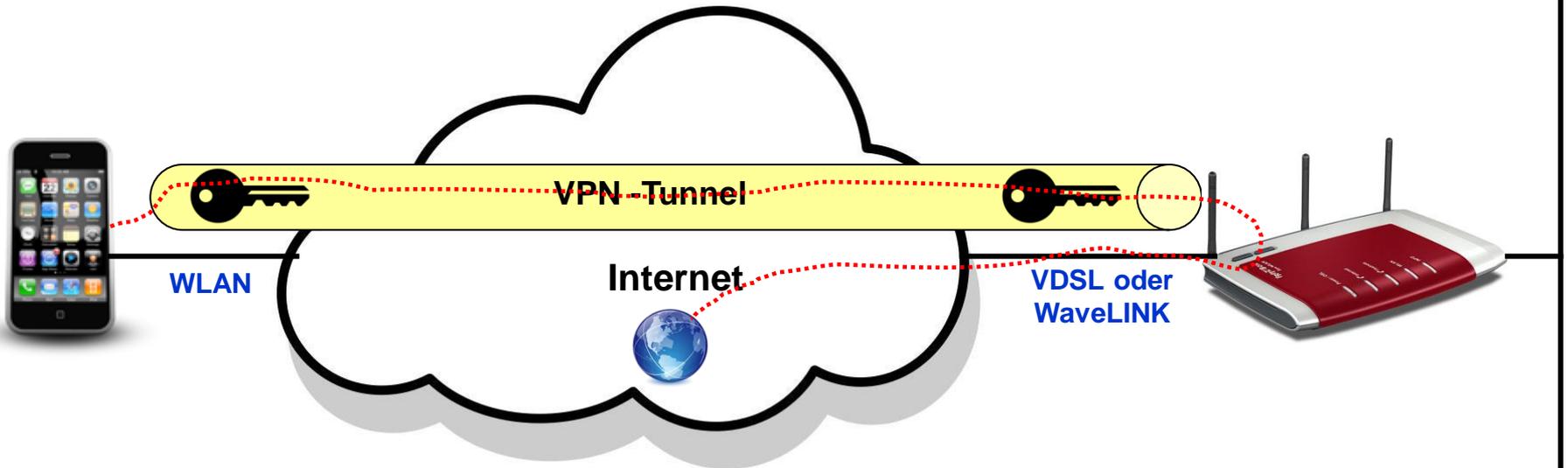
Das VPN-Prinzip



Heimnetz

VPN-Tunnel sorgt dafür, dass alle Pakete Ende zu Ende Verschlüsselt übertragen werden

Das VPN-Prinzip



Heimnetz

Ergebnis für die Internetverbindung:

- Das Smartphone (Client) tauscht Daten übers WLAN und Internet nur verschlüsselt aus
- Client-Daten laufen immer über den Umweg Fritz!Box (VPN-Konzentrator)
- Client-Daten erhalten als Absender-IP-Adresse immer die der Fritz!Box

Konfiguration der Fritz!Box als VPN-Konzentrator

1. DnyDNS-Dienst konfigurieren

- a. Bei fester IP-Adresse nicht erforderlich
- b. Bei DSL oder Breitband-Kabel funktioniert DynDNS-Dienst von AVM (MyFritz!)
- c. Bei WaveLINK 3.0 braucht man einen echten DynDNS-Dienst, z.B. vom Bürgernetz
(-> Mail an admin@bnmsp.de mit Bitte um Einrichtung von DynDNS)

Konfiguration der Fritz!Box als VPN-Konzentrator

1. DnyDNS-Dienst konfigurieren

- a. Bei fester IP-Adresse nicht erforderlich
- b. Bei DSL oder Breitband-Kabel funktioniert DynDNS-Dienst von AVM (MyFritz!)
- c. Bei WaveLINK 3.0 braucht man einen echten DynDNS-Dienst, z.B. vom Bürgernetz
(-> Mail an admin@bnmsp.de mit Bitte um Einrichtung von DynDNS)

2. VPN-Benutzer anlegen

Konfiguration der Fritz!Box als VPN-Konzentrator

- 1. DnyDNS-Dienst konfigurieren**
 - a. Bei fester IP-Adresse nicht erforderlich
 - b. Bei DSL oder Breitband-Kabel funktioniert DynDNS-Dienst von AVM (MyFritz!)
 - c. Bei WaveLINK 3.0 braucht man einen echten DynDNS-Dienst, z.B. vom Bürgernetz
(-> Mail an admin@bnmsp.de mit Bitte um Einrichtung von DynDNS)
- 2. VPN-Benutzer anlegen**
- 3. Erzeugte VPN-Zugangsdaten wegsichern (hier geht nur Screenshot)**

Konfiguration der Fritz!Box als VPN-Konzentrator

1. DnyDNS-Dienst konfigurieren

- a. Bei fester IP-Adresse nicht erforderlich
- b. Bei DSL oder Breitband-Kabel funktioniert DynDNS-Dienst von AVM (MyFritz!)
- c. Bei WaveLINK 3.0 braucht man einen echten DynDNS-Dienst, z.B. vom Bürgernetz (-> Mail an admin@bnmsp.de mit Bitte um Einrichtung von DynDNS)

2. VPN-Benutzer anlegen

3. Erzeugte VPN-Zugangsdaten wegsichern (hier geht nur Screenshot)

Erzeugte VPN-Zugangsdaten (Beispiel):

```
Typ:                IPSec Xauth PSK                :   Protokoll und erweiterte Authentifikation über Pre-shared-key (PSK)

Server-Adresse:     zfds884jfuz884434.myfritz.net   :   DNS-Name oder IP-Adresse Fritz!Box
                                                            = 91.214.10.99
                                                            = mm.dyn.bnmsp.de

Account:             max                          :   Username für XAuth

Kennwort:            Kennwort des Fritz!Box-Users max :   Passwort für XAuth

IPSec Identifier:    max                          :   IPSec-User/Gruppe

IPSec Pre-shared-Key: xgsdZG73ndog876fd           :   eigentlicher Schlüssel
```

Konfiguration der Fritz!Box als VPN-Konzentrator

1. DnyDNS-Dienst konfigurieren

- a. Bei fester IP-Adresse nicht erforderlich
- b. Bei DSL oder Breitband-Kabel funktioniert DynDNS-Dienst von AVM (MyFritz!)
- c. Bei WaveLINK 3.0 braucht man einen echten DynDNS-Dienst, z.B. vom Bürgernetz (-> Mail an admin@bnmsp.de mit Bitte um Einrichtung von DynDNS)

2. VPN-Benutzer anlegen

3. Erzeugte VPN-Zugangsdaten wegsichern (hier geht nur Screenshot)

Erzeugte VPN-Zugangsdaten (Beispiel):

```
Typ:                IPSec Xauth PSK                :   Protokoll und erweiterte Authentifikation über Pre-shared-key (PSK)

Server-Adresse:     zfds884jfuz884434.myfritz.net    :   DNS-Name oder IP-Adresse Fritz!Box
                                                            = 91.214.10.99
                                                            = mm.dyn.bnmsp.de

Account:            max                            :   Username für XAuth

Kennwort:           Kennwort des Fritz!Box-Users max :   Passwort für XAuth

IPSec Identifier:   max                            :   IPSec-User/Gruppe

IPSec Pre-shared-Key: xgsdZG73ndog876fd           :   eigentlicher Schlüssel
```

Schritt-für-Schritt-Anleitung vom Hersteller AVM:
<https://avm.de/service/vpn/uebersicht/>

Konfiguration von IPSec Windows Client Shrew Soft VPN Client

- 1. Client aus Internet herunterladen**
- 2. Client Installieren**
- 3. Client konfigurieren**
- 4. Testen**
- 5. Optionale Funktionserweiterungen konfigurieren**

Schritt-für-Schritt-Anleitung von AVM:

<https://avm.de/service/vpn/tipps-tricks/vpn-verbinding-zur-fritzbox-mit-shrew-soft-vpn-client-einrichten/>

Fragen ?

**Vielen Dank für Eure
Aufmerksamkeit**