

Verschlüsselung im Internet Mythen und Fakten

März 2020, Update November 2020, Update August/Okttober 2022

Peter Klatecki

Prokurist, CIO und Datenschutzkoordinator
der Jasper GmbH

p.klatecki@jasper-gmbh.de



1

Verschlüsselung bei der Datenübertragung im Internet

Wer sich nicht mit den verschiedenen Verschlüsselungsmethoden im Internet auseinandersetzt, und **wer hat schon Lust dazu**, über- oder unterschätzt das Potential der einzelnen Methoden.

Hier nun ein **kurzer Überblick über die Verfahren** und wozu sie dienen; und natürlich auch wozu nicht.

Zum Verständnis nötig ist eine oberflächliche Betrachtung der Datenübertragung in Rechnernetzen und speziell im Internet.

2

Warum das Ganze?

Jeder hat etwas zu verbergen!

Was heute harmlos ist, ist es morgen vielleicht nicht mehr...

„Nur weil Du selbst Deine Daten langweilig findest, ist das nicht für alle anderen genauso. Daten sind in den richtigen Händen viel wert und in den Falschen nichts (oder noch mehr). Geld ist für alle Menschen gleich viel wert, **Daten variieren in ihrem Wert**, je nachdem, ob derjenige, der über sie verfügt, in der Lage ist, sie zusammenzuführen, zu matchen, zu clustern oder zu vergleichen.“ (Lisa Figas, BoxCryptor)

Frage: „Gibst Du mir Dein eMail-Passwort?“

- Erhöhtes Interesse haben z.Bsp.:

1. **Staatliche Akteure**, die mit dem Argument der Verbrechensbekämpfung Überwachungssysteme aufbauen.
2. **Gewinnorientierte Unternehmen**, die aus den verfügbaren Daten Profile erstellen um z.Bsp. hoch-personalisierte Werbung auszuspielen.
3. **Kriminelle**, die sich durch betrügerische Handlungen Zugang zu Online-Identitäten und Zahlungsinformationen verschaffen, um sich persönlich zu bereichern.

3

Verschlüsselung bei der Datenübertragung im Internet

Auslöser für den Vortrag war die aktuelle Werbung von NordVPN



<https://nordvpn.com/de/country/germany/?vpn=brand&gclid=CjwKCAjw79iaBhAJEiwAPYwoCHbSpaTldwlicmM>

Deine IP: 212.110.196.227 • Internetanbieter: Plusnet • Dein Status: **Ungeschützt**

4

Agenda

Verschlüsselung bei der Datenübertragung im Internet Was sie kann und was nicht

1. Was ist Verschlüsselung?
2. Rechnernetze, Struktur, Protokoll TCP/IP
3. Nicht verschlüsselt
4. Maßnahme 0, Die Mutter aller Dinge
5. Maßnahme 1, WLAN verschlüsseln
6. Maßnahme 2, das HTTPS-Protokoll, SSL/TLS
7. Maßnahme 3, DNSSEC
8. Maßnahme 4, Der „richtige“ DNS-Server
9. Maßnahme 5, Das „Surf-VPN“
10. Maßnahme 5a, Das „Home-VPN“
11. Maßnahme 6, Das „Firmen-VPN“
12. Maßnahme 7, Cloud verschlüsseln
13. FIDO2 vs. Passwort
14. Krypto-Währungen (Exkurs)
15. Die dunkle Seite der Macht
16. Gefahren trotz Verschlüsselung
17. Krypto-Währungen (Exkurs)
18. Zusammenfassung

5

Verschlüsselung, historisch

- | | |
|------------------|---|
| ca. 1900 v. Chr. | Spezielle Hieroglyphen, Ägypten |
| 600-500 v. Chr. | Zeichenaustauschalgorithmus |
| 400 v. Chr. | Skytala |
| 170 v. Chr. | Plobyus Tafel (Buchstaben in Zahlen) |
| 50 - 60 v. Chr. | Alphabetische Substitution (Cäsar-Chiffre) |
| Ab 750 | Beginn der Kryptoanalyse (im Islam) |
| 1795 | Chiffrierzylinder (Jefferson) |
| 1918 | Enigma, Rotor-Schlüsselmaschine, WW2 |
| 1940 | Alan Turing knackt Enigma |
| 1976 | Diffie-Hellman-Schlüsselaustausch |
| 1977 | RSA (Rivest, Shamir, Adleman) |
| 1991 | PGP (Pretty Good Privacy v. Zimmermann) |
| ... | |



Skytala

**HAL**

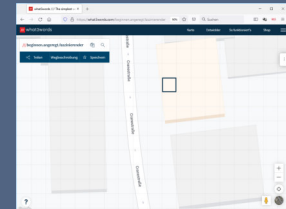
2001: Odyssee im Weltraum
von 1968, Cäsar-Chiffre

6

Verschlüsselung, Beispiel

Verabredung an einem bestimmten Ort,
die Adresse soll übermittelt werden.

- Schritt 1: **Angabe über What3Words**
 - Einteilung der Welt in Quadrate mit 3 m Kantenlänge
 - Adressierung über 3 Worte
 - Eingang Symphonium: **///beginnen.angeregt.faszinierender**
- Schritt 2: **Angabe dieser Adresse in Worten eines Buches**
 - Nummer der Seite – Nummer des Wortes
 - Harry Potter Band 3: **205-45 38-92 387-15** (das ist natürlich frei erfunden!)



7

Verschlüsselung, Arten

- **Symmetrisch**
 - Es gibt nur einen Schlüssel
 - Vorteil: Schnelle Verarbeitung, wenig Rechenleistung nötig
 - Nachteil: Schlüsselübergabe kann nicht gemeinsam mit Nachricht erfolgen
- **Asymmetrisch**
 - Ein öffentlicher Schlüssel (verschlüsseln)
 - Ein privater Schlüssel (entschlüsseln)
 - Vorteil: Der eigene Schlüssel (zum entschlüsseln) muss nicht übertragen werden
 - Nachteil: Höhere Rechenleistung nötig
- **Hybrid**
 - Nachricht wird symmetrisch verschlüsselt, der Schlüssel selbst asymmetrisch
 - Kombination der Vorteile von Symmetrisch/Asymmetrisch
 - Nachteil: relativ komplex (Fehlerwahrscheinlichkeit)

8

Verschlüsselung, Verfahren, Beispiele

- Symmetrisch
 - **AES** - Advanced Encryption Standard
 - **DES** - Data Encryption Standard, heute **Triple-DES** (3DES)
 - ...
- Asymmetrisch
 - **RSA** - Rivest–Shamir–Adleman
 - ...
- Hybrid
 - **TLS** – Transport Layer Security (vorher **SSL** - Secure Sockets Layer)
 - **PGP** – Pretty Good Privacy
 - ...
- Algorithmen in der Regel **quelloffen** ...

9

Verschlüsselung, knacken ?

Verschlüsselung knacken durch Superrechner

- Fugaku in Japan, **1,42 ExaFLOPS**, 158.976 Prozessoren (Arm)
= $1,42 \cdot 10^{18}$ Floating Point Operations per Second

Algorithmus	Dauer zum knacken (Brute-Force)
Rotations-Chiffre	Wenige Millisekunden
56 Bit DES	3 Minuten
128 Bit AES	24 Billionen Jahre
256 Bit AES	8 Nonillionen Jahre (10^{54} Jahre)

Einheiten der Gleitkommarechenleistung mit SI-Vorsätzen.	
kFLOPS	KiloFLOPS = 10^3 FLOPS
MFLOPS	MegaFLOPS = 10^6 FLOPS
GFLOPS	GigaFLOPS = 10^9 FLOPS
TFLOPS	TeraFLOPS = 10^{12} FLOPS
PFLOPS	PetaFLOPS = 10^{15} FLOPS
EFLOPS	ExaFLOPS = 10^{18} FLOPS
ZFLOPS	ZettaFLOPS = 10^{21} FLOPS
YFLOPS	YottaFLOPS = 10^{24} FLOPS

- mit **Know-How** (= passende Algorithmen) viel schneller möglich
- 1024 Bit oder sogar 2048 Bit heute in der Anwendung
- Universum, 13,8 Milliarden Jahre, $13,8 \cdot 10^9$

10

Verschlüsselung, knacken ?

Verschlüsselungsalgorithmus knacken durch **Quantencomputer**

- Aktuell noch kein kommerzieller Quantencomputer verfügbar
Mindestens noch 10 Jahre, eher 15 Jahre
- Algorithmus zum knacken aktueller Verschlüsselungsverfahren auf Quantencomputern **bereits seit 1992 verfügbar** (Peter Shor)
- Aktuell Entwicklung der **Post-Quanten-Kryptographie**
(Bsp. Vektor-Verfahren, Closest-Vector-Problem oder Shortest-Vector-Problem oder math. Funktionen n-ten Grades)
- Neue Verfahren („quantensicher“) sind im Auswahlverfahren und werden kommen

11

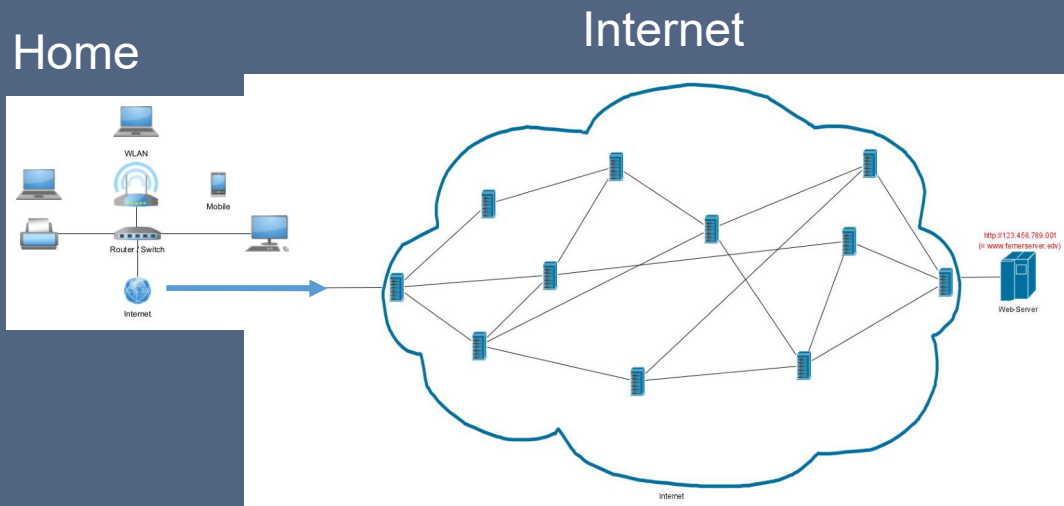
Verschlüsselung bei der Datenübertragung im Internet

Transport-Verschlüsselung vs. Ende-zu-Ende Verschlüsselung

- Transport (auch **Punkt-zu-Punkt**-Verschlüsselung genannt)
 - für den Übertragungsweg (**Data in Transport**)
 - Perfect Forward Secrecy
ein kryptographisches Verfahren, das bei jedem Verbindungsaufbau einen **neuen, zufälligen** Sitzungsschlüssel generiert
- Ende-zu-Ende (E2EE – End to End Encryption)
 - **Sender zu Empfänger**, diese haben ausschließlich Einsicht in die Nachricht
Beispiel: verschlüsselte Datei wird versandt, E-Mail
 - **Data in Rest**, gemeinsam auf Cloud-Daten zugreifen ...

12

Rechnernetze, Struktur



13

Rechnernetze, Protokoll

Ein **Protokoll** zeichnet auf, hält fest oder schreibt vor, zu welchem Zeitpunkt oder in welcher Reihenfolge welcher Vorgang durch wen oder durch was veranlasst wurde oder wird. (Wikipedia)

- Niederschrift
- Militärisches Protokoll
- Staats-Protokoll
- ...
- **Protokolle für digitale Kommunikation**, *Vorschriften zur Verständigung*
 - ARP, DHCP, DNS, FTP(S), SMTP, IMAP, HTTP(S), ... , IPX/SPX, Apple 2, NetBEUI, SMB ...
 - **TCP/IP** - OSPF

14

Rechnernetze

- heute ist im Internet **und** in den lokalen Rechnernetzen das **Protokoll TCP/IP** üblich
- Jeder Rechner **braucht/hat** eine **eindeutige Nummernkombination** (IP-Adresse, hier im Vortrag hauptsächlich IP/V4, IP/V6 Ergänzungen)
- Genutzte Namen (Domains) in die entsprechenden Nummern rückübersetzen durch den s.g. **DNS Dienst (Domain Name System)**
- Das **Internet** ist im Ursprung eine **militärische Erfindung** (ARPANET). Oberstes Ziel war, die Datenübertragung solange wie möglich aufrecht zu erhalten. Deswegen ist es im wahrsten Sinne des Wortes „ein Netz“.

15

Rechnernetze IP/V4 vs. IP/V6

- IP/V4
 - **2^{32}** Adressen, **4.294.967.296**
 - Seit 2011 keine weiteren (freien) Adressen mehr zu vergeben
 - Nach außen sichtbar ist die „externe“ IP-Adresse (Router, wg. **NAT**, 1994)
- IP/V5
 - experimentelles Protokoll für Echtzeitübertragung (nicht wirklich eingesetzt)
- IP/V6
 - **340 Sextillionen** IP-Adressen (**$3,4 \cdot 10^{38}$** , 128 Bit, $6,67 \cdot 10^{25}$ / m² Erdoberfläche)
 - Nach außen sichtbar ist die eigene (Rechner) IP-Adresse, weltweit (!), ggf. lebenslang, **kein NAT mehr nötig**
 - beinhaltet IPSec als Verschlüsselungsstandard (optional)
 - Heute häufig **Dual-Stack Implementierung**, intern (kann) V4 / extern V6

16

Rechnernetze IP/V4

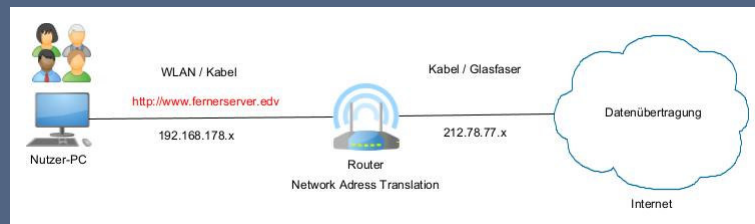
Private Nummernkreise

- Klasse A:
10.0.0.0 bis
10.255.255.254
- Klasse B:
172.16.0.0 bis
172.31.255.254
- Klasse C:
192.168.0.0 bis
192.168.255.254
↑
Subnetz

Network Address Translation ->

Öffentliche Adresse

(vom Provider, normalerweise regelm. erneuert/geändert)



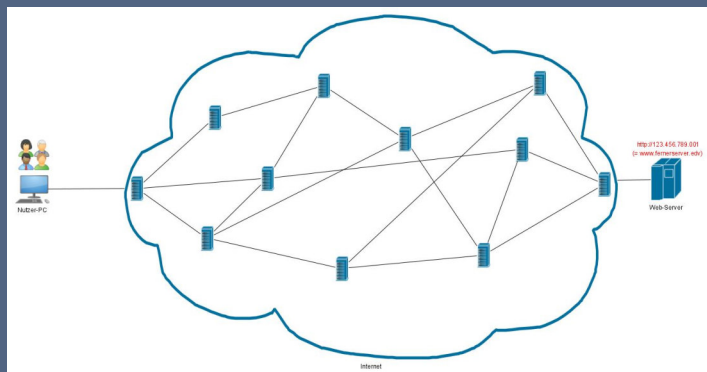
17

Rechnernetze IP/V4 und IP/V6

Es gibt (erst mal) **keine physikalische 1:1 Verbindung** zwischen zwei entfernten Teilnehmern, welche Daten tauschen (hier Nutzer-PC und Web-Server).

Aus technischen Gründen wird die zu übertragende Information **in kleine Pakete zerlegt** (segmentiert), diese Segmente werden nummeriert, einzeln verschickt und beim Empfänger in der richtigen Reihenfolge wieder zur ursprünglichen Nachricht zusammengesetzt.

Wichtig ist jedoch, dass sie in einem bestimmten, **definierten Zeitfenster (TTL)** am Ziel ankommen.

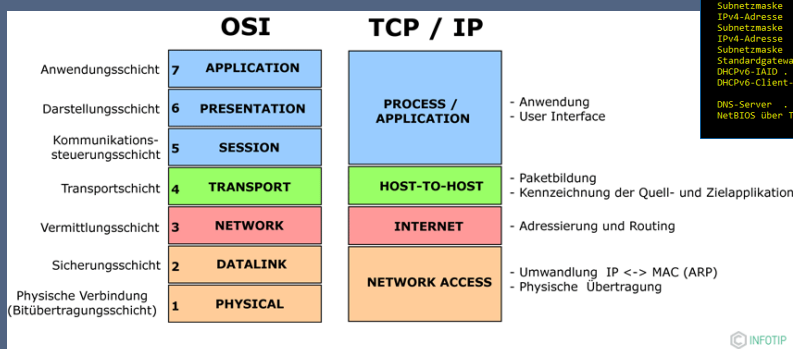


18

Rechnernetze IP/V4 und IP/V6

OSI Referenzmodell

- Standardisierungsorganisation ISO, Anfang der 80er Jahre (Open System Interconnect Reference Model)



```
Administrator: Eingabeaufforderung

Ethernet-Adapter Ethernet:

Verbindungsspezifisches DNS-Suffix:
Beschreibung: . . . . . : Realtek PCIe GbE family Controller
Physische Adresse . . . . . : 74-00-20-7F-B2-86
DHCP aktiviert: . . . . . : Nein
Autokonfiguration aktiviert: . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::5d8a:343d:89ac:db15%16(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.0.133(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
IPv4-Adresse . . . . . : 192.168.1.133(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
IPv4-Adresse . . . . . : 192.168.178.133(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.1.254
DHCPv6-IAID . . . . . : 91541547
DHCPv6-Client-DUID . . . . . : 00-01-00-01-19-E8-70-15-74-D0-28-7F-B2-86
DNS-Server . . . . . : 192.168.1.254
NetBIOS über TCP/IP . . . . . : Aktiviert
```

MAC-Adresse
Einmalig pro Netzwerkkarte!

INFOTIP

19

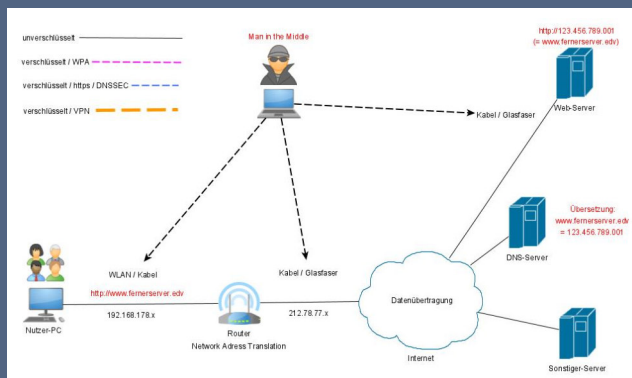
Nicht verschlüsselt

- Die **Kommunikation** zwischen zwei Internetteilnehmern **muss nicht verschlüsselt sein**. „Früher“ war sie das auch nie.

Hier eine typische Situation:

Der Nutzer PC befindet sich in einem Netz (heute mindestens mit seinem Heimrouter) mit den Adressen 192.168.x.x.

Der Router hat Richtung Internet eine Adresse aus dem Netz des Providers, hier 212.78.77.x, und ist damit offizieller Internetteilnehmer. Internetzugriff auf „fernserver.de“



20

Nicht verschlüsselt

Eine neugierige Person, „**Man in the Middle** / der Mann dazwischen / Angreifer“, könnte jetzt den Datenverkehr an verschiedenen Stellen abhören wollen.

Hierzu sind nur einige Stellen wirklich geeignet, da **nicht sicher ist** welchen Weg die vielen Datenpakete einer Nachricht/Anfrage jeweils durch das Internet nehmen.

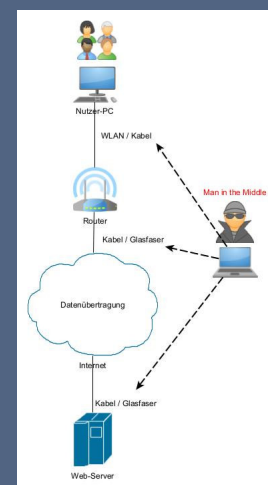
Es muss an Stellen gelauscht werden, an denen **alle Pakete sicher anzutreffen** sind.



21

Nicht verschlüsselt, ausspionieren

- Zugang zum **kabelgebundenen** Netzwerk im Haus
 - Zugangskontrolle
- Zugang zum **Funknetz/WLAN**
 - Funk durchdringt auch Wände
 - der Angreifer postiert sich einfach vor dem Haus
- Unmittelbar **nach dem Router**, Richtung Internet
 - in der Regel außer Haus, Richtung Anschlagkasten
- Kurz **vor dem Zielserver**
 - Hier treffen alle Datenpakete ein



22

Maßnahme 0, die Mutter aller Dinge!

Datensparsamkeit!

- Alles, was ich NICHT übertrage, kann auch nicht abgehört werden!
- Bsp.: „Kassengespräche bei ALDI“ (unverlangt erworbenes Wissen)



23

Maßnahme 1: WLAN verschlüsseln

- Schlagworte (Kürzel) hier sind **WEP, WPA, WPA2 und WPA3**. Allesamt Verschlüsselungsverfahren in Funknetzen.
 - WEP ist Jahrzehnte (Mehrzahl!) alt, gilt als „geknackt“
WPA ebenso
 - Aktuell häufig **WPA2**, gilt seit 2017 als „angeschlagen“
 - Nachfolger, **WPA3**, in aktueller Hardware und ggf. bei Updates

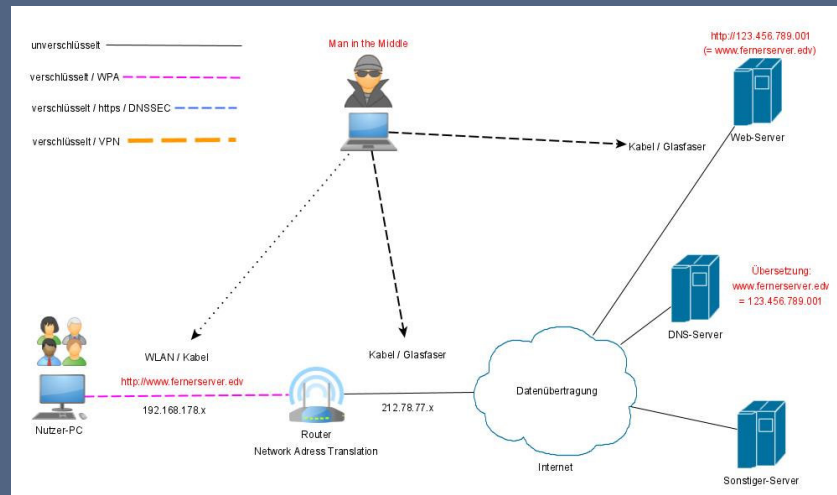
Mit der Verschlüsselung des WLAN-Verkehrs wird vor allem anderen unterbunden, dass sich **beliebige Rechner mit dem Netz verbinden können**. Wer nicht Teilnehmer des verschlüsselten Netzes ist kann dort auch nicht sinnvoll lauschen.

Die Datenübertragung **nach dem eigenen Netz (außerhalb) erfolgt aber immer noch im Klartext**. Die anderen o.g. Angriffspunkte stehen für den Angriff nach wie vor zur Verfügung.

24

Maßnahme 1: WLAN verschlüsseln

- Haus abgeschlossen (Zutritt)
- Funkstrecke verschlüsselt



Maßnahme 1: WLAN verschlüsseln

- **Datenverkehr** kann mit einer **beliebigen Maschine** empfangen werden, sinnvollen Inhalt kann man jedoch dort nicht entnehmen (weil verschlüsselt)
- Mit **ausreichend komplexem Schlüssel** ist ein „Man in the Middle“-Angriff direkt im WLAN **nahezu ausgeschlossen**
 - **min. 16 Stellen**, Buchstaben groß/klein, Zahlen, Sonderzeichen
- abgesehen von **Hintertüren** (absichtlich) oder **Fehlern** (unabsichtlich) in der **Firmware** der genutzten Hardware (WLAN-Router)
 - Es ist eine gute Idee die eingesetzte Hardware softwareseitig aktuell zu halten.

Maßnahme 1: WLAN verschlüsseln

„Störerhaftung“

- Unternehmer und Verbraucher, die ihr WLAN anderen zur Verfügung stellen, sollen nach dem Willen des Gesetzgebers **normalerweise nicht mehr** als sogenannte Störer für Urheberrechtsverstöße Dritter **haften** (seit 2017).
- WLAN-Betreiber können jedoch unter Umständen zu Inhaltssperren (s.g. Black-Listing) **verpflichtet** werden.
- Kommt es zu einer **Urheberrechtsverletzung** im heimischen WLAN, erhält im Falle einer **Abmahnung**, diese grundsätzlich **der Anschlussinhaber**, also in der Regel der WLAN-Betreiber, weil dieser den Internetzugang bereithält und von den Rechteinhabern regelmäßig über die **zentrale (äußere / NAT) IP-Adresse** ermittelt wird.

27

Maßnahme 2, das HTTPS-Protokoll, SSL/TLS

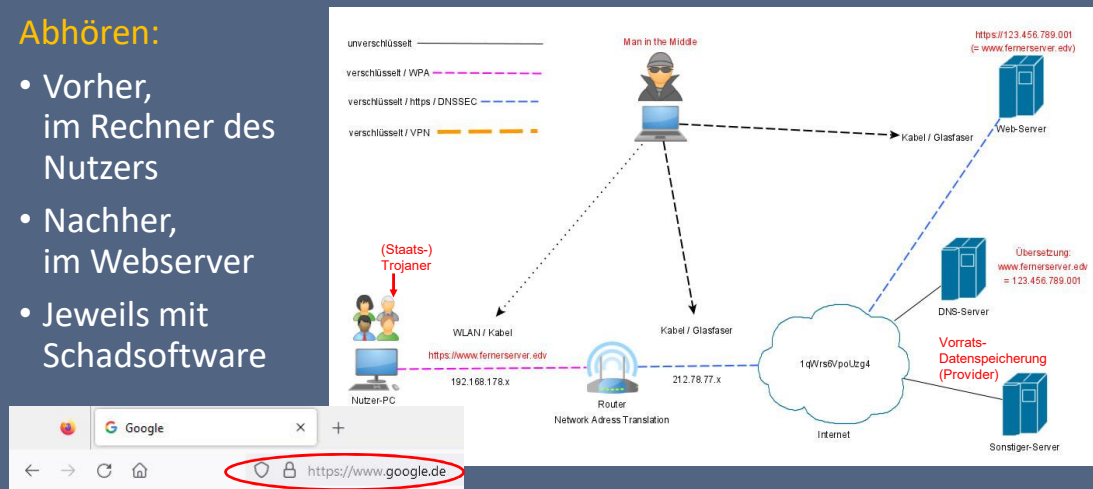
- **HTTPS** stellt eine Erweiterung des http Protokolls dar (Websurfing)
- S steht für Secure also „sicher“
Stichworte sind hier **SSL und TLS** (Verschlüsselungsprotokolle)
- Absicherung zwischen zwei Endstellen (ggf. erzwungen durch .htaccess)
- beinhaltet **Vertraulichkeit und Authentifizierung** (Zertifikate)
- **auch** bei der **E-Mail**-Kommunikation eingesetzt
- Der „**Man in the Middle / Angreifer**“ muss für das Mitlesen entweder den Schlüssel kennen (**unwahrscheinlich, da pro Sitzung automatisch erstellt**, Perfect Forward Secrecy), oder **errechnet** (dann war der Schlüssel zu schwach für die Leistung heutiger Rechner). Oder er muss **vor** der Verschlüsselung oder **nach** der Entschlüsselung ansetzen.

28

Maßnahme 2, das HTTPS-Protokoll, SSL/TLS

Abhören:

- Vorher, im Rechner des Nutzers
- Nachher, im Webserver
- Jeweils mit Schadsoftware

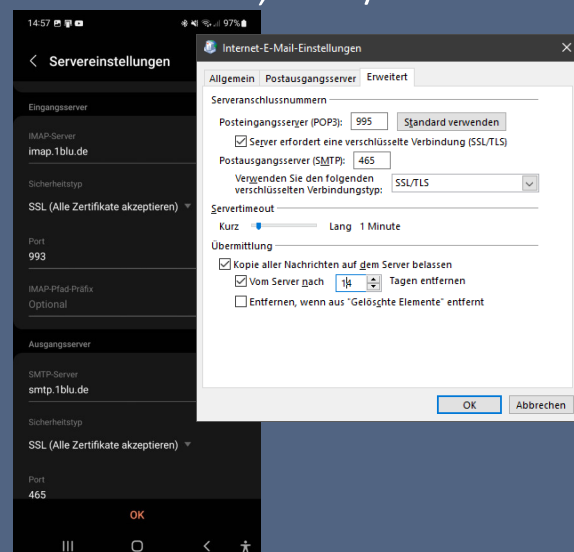


29

Maßnahme 2, das HTTPS-Protokoll, SSL/TLS

Verschlüsselung bei E-Mail

- es gibt kaum noch Mail-Server, die unverschlüsselte Kommunikation akzeptieren
- Richtige Kombination aus
 - Server(-Name)
 - TCP/IP Port
 - Verschlüsselungstyp



30

Maßnahme 3, DNSSEC

Wie funktioniert **DNS**?
(Domain Name System) Bsp.

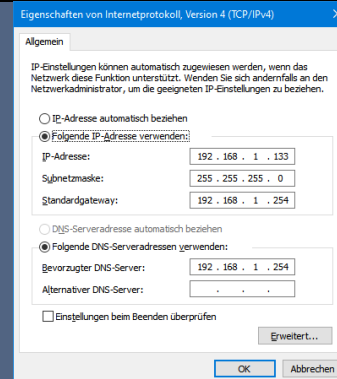
1. **Browseranfrage** **www.google.de**
2. Rechner fragt **lokalen Router**
(als zugeordneten DNS-Server)
3. Router fragt **Provider** DNS-Server
4. Als Antwort die **IP-Adresse**
5. Browser ruft
<https://142.250.184.195>
6. Seite wird angezeigt

```
C:\>ping www.google.de

Ping wird ausgeführt für www.google.de [142.250.184.195] mit 32 Bytes Daten:
Antwort von 142.250.184.195: Bytes=32 Zeit=21ms TTL=119
Antwort von 142.250.184.195: Bytes=32 Zeit=21ms TTL=119
Antwort von 142.250.184.195: Bytes=32 Zeit=21ms TTL=119
Antwort von 142.250.184.195: Bytes=32 Zeit=21ms TTL=119

Ping-Statistik für 142.250.184.195:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
            (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 21ms, Maximum = 21ms, Mittelwert = 21ms

C:\>
```



31

Maßnahme 3, DNSSEC

Abhören:

- Durch **Vorspiegelung** eines legitimen Ziels die Namensauflösung im befragten **DNS-Server** wird geändert und der Datenverkehr zum Angreifer umgeleitet, abgehört und weitergeleitet

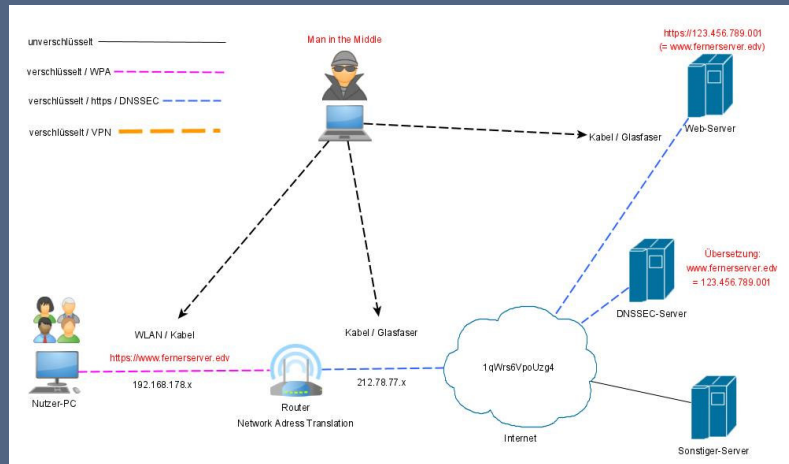
DNSSEC

- Stellt eine Sammlung von Maßnahmen dar, die es erlauben zu überprüfen ob die erhaltene DNS-Antwort tatsächlich von einem legitimen (DNS-) Server stammt

32

Maßnahme 3, DNSSEC

- Eine Änderung der Namenseinträge im DNS und eine **Umleitung** auf Server des Angreifers wird (soll) dadurch verhindert werden.



33

Maßnahme 4, Der „richtige“ DNS-Server

- Hauptkriterium zur Auswahl war bisher die Geschwindigkeit der Auflösung, oder **DNS vom Provider** wurde einfach akzeptiert
- MalWare wie Trojaner, Viren, Erpressersoftware und Andere gelangen aber meistens erst auf den Rechner, **nachdem der Nutzer** eine Funktion gestartet hat (natürlich unbewusst), welche den eigentlichen Bösewicht **von extern** nachlädt.
- zusätzliche Sicherheit zu durch einen DNS-Server, der „böswillige Ziele“ gar nicht erst auflöst

34

Maßnahme 4, Der „richtige“ DNS-Server

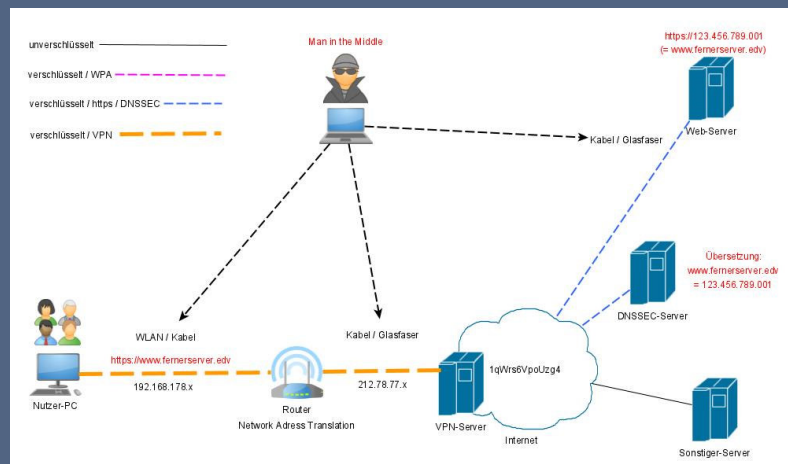
- QUAD9 (z.Bsp.)
betrieben von Non-Profit Organisation
(IBM, Packet Clearing House, Global Cyber Alliance und Weitere)
- **Kostenlos** nutzbar, auch mit DNSSEC
- **automatisches Blocken** von Domains, welche mit böswilligen Angriffen in Verbindung gebracht werden (werden nicht aufgelöst!)
- IPv4-Adresse 9.9.9.9 / IPv6-Adresse 2620:fe::fe
- Am besten im (Heim-)Internetrouter eintragen

35

Maßnahme 5, Das „Surf-VPN“

VPN

- Abkürzung für **Virtuelles Privates Netz**. Man kann es sich als **virtuelles Kabel** ohne Abgriffe oder Verzweigungen vorstellen, welches durch ein anderes, größeres Netz, nur für einen selbst, gelegt wird.



36

Maßnahme 5, Das „Surf-VPN“

Surf-VPN Vorteile

- „**Abhörsicher**“ in offenen/öffentlichen WLAN-Netzen
- **Ländergrenzen** überwinden
 - Videostreaming
 - Zensur
 - ...
- **Funktionen** und das Schutzniveau sind **abhängig von** Technik und Funktionsangebot des **Anbieters**



NordVPN, Vilnius, Litauen

37

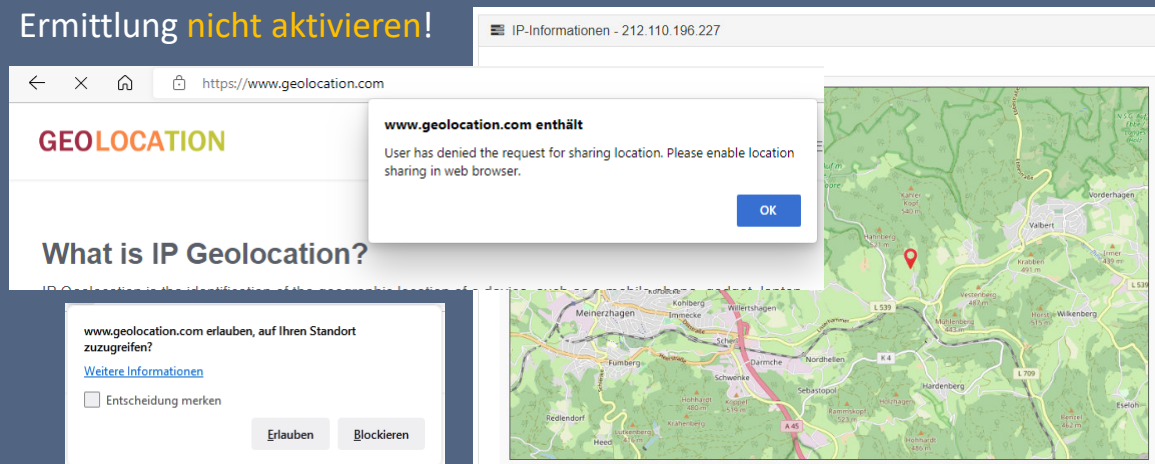
Maßnahme 5, Das „Surf-VPN“

„Du bist so interessant.“	Klar, ich bin ja sowieso einzigartig! Aber es schmeichelt mir trotzdem, wenn Du das sagst!
„Ich liebe Deinen Browserverlauf.“	Entweder Zugriff auf meinen Rechner, oder MalWare überträgt Dateien. -> Ich bin gehackt!
„Ich mag, dass Du nichts vor mir versteckst!“	???, Ich soll es also nur Euch (VPN-Anbieter) zeigen ... mmmhhhh
„ Ah, jetzt sehe ich Deine IP-Adresse. Du wohnst ja in einer tollen Gegend. “ Geolocation	Nicht wirklich schwer ..., manchmal aber doch, Fehlauswertungen möglich, eher wahrscheinlich https://www.iplocation.net/ / https://dnslytics.com/ / https://www.geolocation.com/de
„Du bist so besonders. Diese Werbung ist nur für Dich.“	Eigentlich finde ich das nicht schlecht, wenn ich keine Werbung erhalte, die mich NICHT interessiert.
„Ich habe so viel über Dich gelernt.“	Hättest doch bloß auf Facebook mein Follower werden müssen.
„Du bist so großzügig, mit Deinen persönlichen Daten.“	Was meinst Du? Die Postkarte im Supermarkt-Gewinnspiel?
„ Privatsphäre ein, Tracker und Viren aus. “	Wenn das nur so einfach wäre ...

38

Maßnahme 5, Das „Surf-VPN“, Geolocation

Ermittlung **nicht aktivieren!**



39

Maßnahme 5, Das „Surf-VPN“, Privatsphäre

- Surfen mit HTTPS-Protokoll **ist bereits verschlüsselt!**
- **Verschlüsselung muss** für den VPN Anbieter **aufgegeben werden**, sonst:
 - Kein Virensan
 - Kein Scan auf Tracker
 - Kein Scan auf sonstige MalWare (etwa RansomWare)
 - Keine Werbungsunterdrückung
 - ...
- Anbieter muss dann DNS und HTTPS Ziel sein, also:

Man in the Middle

40

Maßnahme 5, Das „Surf-VPN“

VPN-Probleme

- Vertrauen in den Anbieter
Auswertungen, Virensan, ...
- No-Logs Policy? (Abrechnung!)
- Datenlecks / DNS-Leaks
- IPV6 (evtl. kein NAT, IP-Leak)
- Split-Tunneling (mal VPN, mal nicht)
- Phishing / Social Engineering
- Anonymität
IPV6, **Browser-Fingerprinting**
<https://amiunique.org>
- Ggf. Streaming-Sperren (-> kein Netflix o.ä.)
- Bis zu 30 % Leistungsverlust (10 % ok)
- VPN endet am Server des Anbieters
- Für die meisten (Sicherheits-) Funktionen muss der VPN-Anbieter „Man-in-the-Middle“ sein (Bedrohungsschutz bei NordVPN)

41

Maßnahme 5a, Das „Home-VPN“

Volle VPN Funktion „nach Hause“

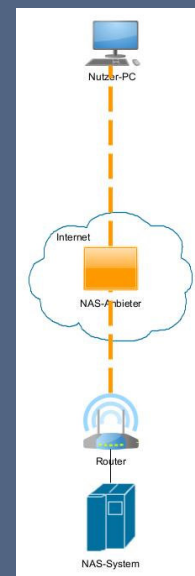
- Zugang **direkt im Router** einrichten
 - Nicht trivial!
 - Zugang **vom Internet aus** wird geschaffen, ohne ständige Nutzung

Empfehlung

- **NAS** (Network Attached Storage)
 - Zugang über **Anbieterfunktion (nur Verbindung)**
 - Einfach einzurichten
 - Datensicherheit durch VPN „von innen“
 - Datensicherheit durch Redundanz bei Festplatten
 - Zusätzliche Funktionen (Video- und Photo-Server, ...)



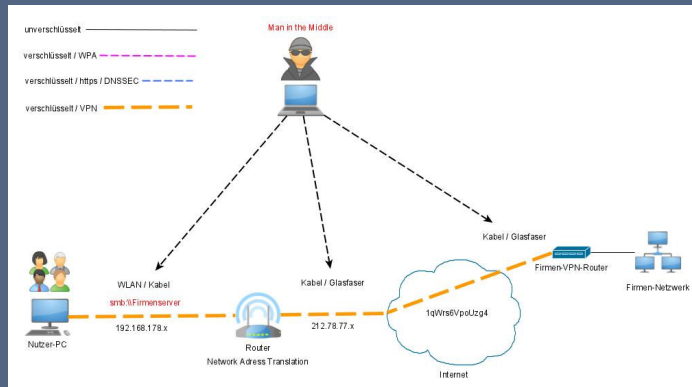
Synology DS220



42

Maßnahme 6, Das „Firmen-VPN“

- **sicherer Datenzugriff auf Firmenrechner** (Split VPN)
- der komplette Datenverkehr (zur Firma und zurück) wird verschlüsselt
- Diese VPN-Systeme dienen i.R. **nicht zur „normalen“ Internetkommunikation**



43

Maßnahme 7, Cloud verschlüsseln

Dateiablage in der Cloud für den Zugriff „von überall“

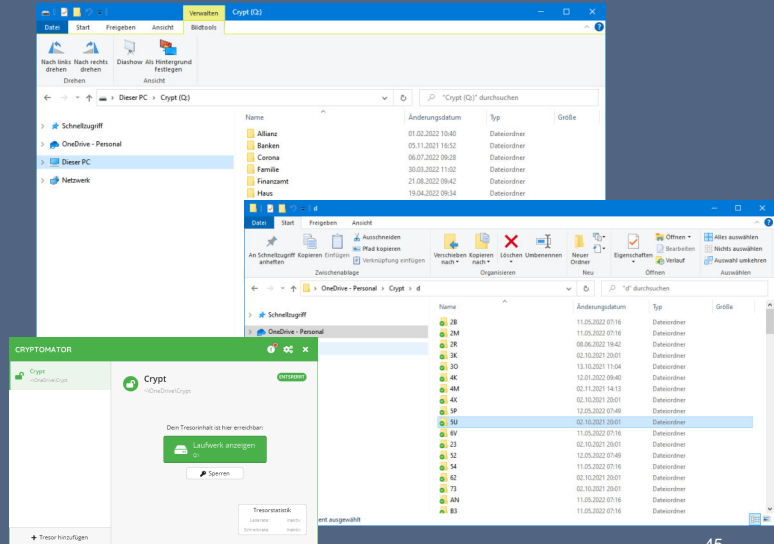
Kostenlos:

- OneDrive (Microsoft, 5GB enthalten in W10, W11, mit MS-Konto)
- Google Drive (Alphabet, 15GB, mit Google-Konto)
- HiDrive (IONOS, für Kunden)
- Amazon Drive (für Amazon Kunden, 5GB)
- DropBox (Dropbox Inc., 2GB)
- ...

44

Maßnahme 7, Cloud verschlüsseln, Data in Rest

- Cloud-Anbieter hat prinzipiell Zugriff
- „schützenswerte, private“ Daten verschlüsselt ablegen, Dateiverschlüsselung
- Beispiel: Cryptomator



45

FIDO2 vs. Passwort

• Fast Identity Online

- Asymmetrische Verschlüsselung
- Soll (Benutzername +) Passwort ablösen
- Zusätzliches Gerät erforderlich (Handy, Sicherheitsstick)
- Auch mit Biometrie (Fingerabdruck, Gesicht)
- (Nur) Online



• Passwort

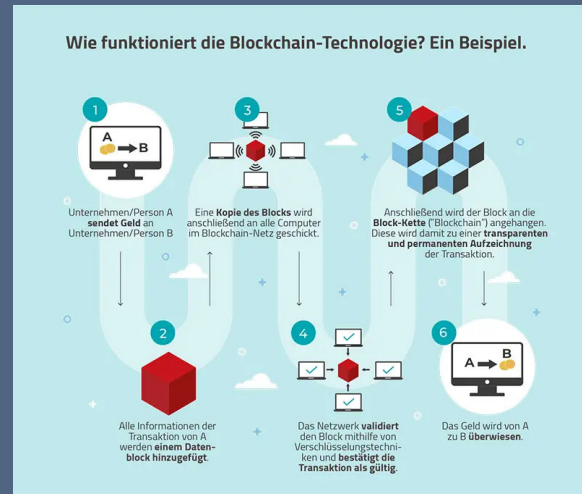
- Komplexes PW nötig
- Prinzipiell mit Brute-Force knackbar (heute)
- Kein zusätzliches Gerät erforderlich
- Jederzeit änderbar
- Auch für Offline-Login

46

Krypto-Währungen (Exkurs)

Bsp. BitCoin, Ethereum, ...

- Basis ist eine **verschlüsselte, verteilte Datenbank (Blockchain)**
- „Nodes“ übernehmen das „Mining“
- Blockchain u.a. auch für s.g. „Smart Contracts“
- Nachteile:
 - Energieverbrauch
 - 50% der Nodes (Rechenkraft) können ändern
 - „Bitcoin-Wale“
 - ...



47

Krypto-Währungen

- Über **9.500** verschiedene Kryptowährungen (gehandelt)
- <https://99bitcoins.com/deadcoins/> (**Friedhof** der Krypto-Währungen)
1706 tote Coins (Stand Juli 2022)
- Geld einnehmen mit Verschlüsselung ohne zu verschlüsseln
 - **OneCoin** (2014), praktisch wertloser Betrug (2016)
 - **Manipulierbare** Blockchain
 - Ruja Ignatova **verschwand(!)** mit ca. 4 Mrd. Dollar

48

Die dunkle Seite der Macht

- **Nicht staatlich:**

- Die organisierte Kriminalität kommuniziert **hoch-verschlüsselt**
- Die nichtorganisierte Kriminalität auch, je nach Intelligenzgrad
- RansomWare (Daten auf dem eigenen Computer werden verschlüsselt und Lösegeld erpresst)
- ...
- Und **wir alle in Zukunft auch**, mit den hier angeführten Methoden ... hoffentlich

- **Staatlich**

- Die CIA hört **angeblich** 100% des Internetverkehrs automatisiert ab (Schlüsselworte, trotz Verschlüsselung, also für alles **Man in the Middle?**) (bis Januar 2000 war Krypto-Export aus USA verboten)
- Unsere **19(!) Geheimdienste + BKA** haben den **Staats-Trojaner** („Pegasus“, lizenziert von NSO, Israel) über den Einsatz entscheiden **10 Ehrenamtliche (G10 Kommission), kein Richter!**
- ...

49

Die dunkle Seite der Macht, **historisch (Bsp.)**

Die Schweizer **Crypto AG** (1952) war ein international tätiges Unternehmen im Bereich der „Informationssicherheit“

- Herstellung von **Chiffriermaschinen**
- Verkauf der Maschinen an ca. **130 Regierungen** für die Staatskommunikation
- Seit 1970 im **Besitz des BND und der CIA** (50/50, heimlich gekauft, „Operation Rubikon, bis 1993“) aufgedeckt erst 2020 **Geheimdienstcoup des Jahrhunderts** (CIA)
- 2018 Verkauf an den schwedischen Unternehmer Andreas Linde, CyOne Security AG

50

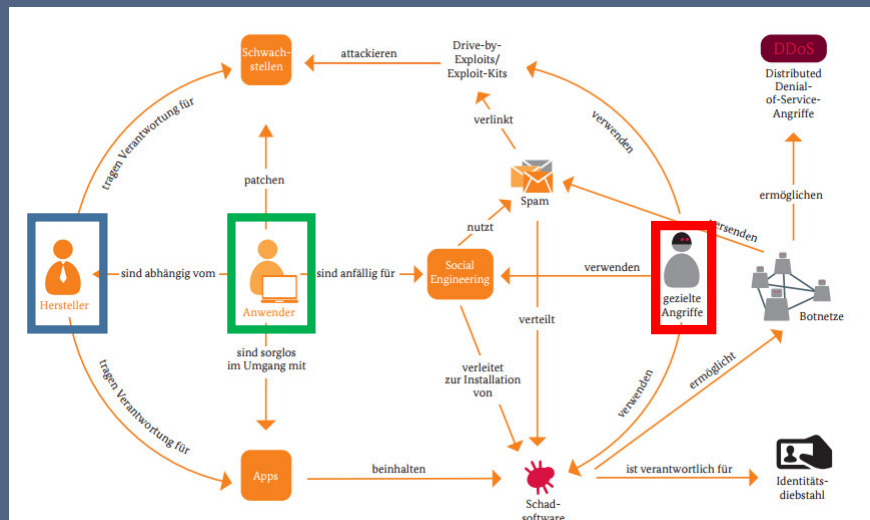
Gefahren **trotz** Verschlüsselung

Dies kann alles
auch
verschlüsselt
erfolgen!

Kopf
einschalten!



www.bleib-virenfrei.de



51

Zusammenfassung

Der Weg zur geschützten (**ziemlich** abhörsicheren, Transport) Internetnutzung ist eine Kombination der oben beschriebenen Maßnahmen.

- Nummer 1 bis 4 **müssen**, soweit verfügbar (DNSSEC), eingesetzt werden.

Maßnahme 1, **WLAN verschlüsseln**

obligatorisch!

Maßnahme 2, das **HTTPS-Protokoll**, SSL/TLS

(immer) verfügbar

Maßnahme 3, **DNSSEC**

im Router (Update)

Maßnahme 4, Der „richtige“ **DNS-Server**

manuell im Router

52

Zusammenfassung

- Maßnahme 5, **ein Surf-VPN**, bietet erstmal „nur“ Verschlüsselung zwischen zwei definierten Rechnern. Weitere Funktionen sind je nach Anbieter verfügbar, basieren aber nicht auf der VPN-Funktion.
- Beim Einsatz von kommerzieller VPN-Software **bringt der Nutzer dem Anbieter gehöriges Vertrauen entgegen**. Sämtlicher Datenverkehr läuft durch dessen Server, **ggf. entschlüsselt**.
- Für eine Vielzahl von angebotenen Funktionen **muss** der Anbieter „**Man in the Middle**“ sein.
- Maßnahme 5a, **Home-VPN per NAS**, ist (fast) völlig unproblematisch

53

Zusammenfassung

- Maßnahme 6, **Firmen VPN**
 - Home-Office
 - Standortkopplung
- Maßnahme 7, **Cloud verschlüsseln**
Sollte immer bei extern gespeicherten persönlichen Daten eingesetzt werden
- **Anfang und Ende** der Übertragungsstrecke sind **unverschlüsselt!**
(bei Transportverschlüsselung)

54

Zusammenfassung

- So wurde letztlich bekannt, dass der tschechische Anbieter **AVAST** Millionen mit dem **Verkauf von Kunden-Surf-Daten** an Marketingfirmen umgesetzt hat.
- Nun muss man wissen, dass **AVAST** einen **eigenen Virens scanner** im Angebot hat und vor einiger Zeit u.a. die Firmen **AVG** und **Piriform** zugekauft wurden.
- **AVG** hat eine **Internet-Suite** im Angebot welche aus Virens scanner, Webseitenschutz und **auch VPN Software** besteht, jetzt mit AVAST als Anbieter.
- Der Systemreiniger **CCleaner** stammt von **Piriform** und erhielt nach der Übernahme durch AVAST ein Modul, das den „Reinigungsbedarf“ des Rechners konstant überwacht. Dieses kann aber in den Optionen **deaktiviert** werden.

55

Zusammenfassung

- Mit den zur Verfügung stehenden Funktionen kann bereits ein **sehr guter Schutz** erreicht werden
- Am **anfälligsten** ist der Rechner „zwischen den Ohren“
- *„**Paradox ist**, wenn man den Facebook Post verschlüsselt überträgt“*
- *Die NSA sagt: „**Seit WhatsApp verschlüsselt**, hat der Versand von Nacktbildern um 30% zugenommen!“*

56

Zusammenfassung

(Krypto-)Tools für die tägliche Anwendung

- **Datei**
 - 7Zip, WinRar, ... , TrueCrypt, SecureStick, Folder Access
 - VeraCrypt, BitLocker (in Windows ab Pro Versionen)
- **Transfer**
 - OpenVPN, SoftEther VPN Client
- **Webseite** (eigene)
 - Let's Encrypt (Zertifikat, .htaccess), HTTPS-Checker
- **E-Mail**
 - PrettyGoodPrivacy (Einrichtung ist nicht trivial), Gpg4win
- **Cloud**
 - Cryptomator, BoxCryptor u.ä.
- **Telefon**
 - Simlar (Android, abhörsicher telefonieren)
- **Passworte**
 - KeePass XC
- **yEd**
 - wurde für die Netzwerk-Illustrationen verwendet (VISIO-Alternative)

57

Vielen Dank!

Ich wünsche erfolgreiches Anwenden!

Peter Klatecki

58