

# Network Security Fundamentals



# Andreas Grupp

Andreas.Grupp@fbu-rpt.de

# Carina Haag

haag.c@lanz.schule

# Tobias Heine

tobias.heine@springer-schule.de

# Uwe Thiessat

uwe.thiessat@gbs-sha.de

## Arten von Bedrohungen

Diebstahl von Informationen  
(Geschäftsgeheimnisse, Baupläne,  
Kreditkarteninformationen, ...)



Datenverlust oder Manipulation  
(Löschen, verschlüsseln oder abändern von  
Daten)



**HACKED**

Identitätsdiebstahl  
(Im Zeitalter von  
Social Media wenig  
Know-How notwendig)



Unterbrechung von Diensten  
(z. B. User kommen nicht mehr auf die  
Webseite eines Unternehmens)



## Typen von Schwachstellen

### ▪ Technologische Schwachstellen

- TCP/IP-Protokolle (HTTP, FTP, ICMP, SNMP, SMTP)
- Betriebssysteme (hier dokumentiert: <http://www.cert.org>)
- Netzwerk-Geräte (Router, Firewalls, Switches ...)

### ▪ Konfigurations-Schwachstellen

- Ungesicherte Benutzerkonten (PWs werden unsicher übertragen)
- Systemkonten mit einfach zu erratenden Passwörtern
- Unsichere bzw. unveränderte Standardeinstellungen
- Falsch konfigurierte Internetdienste (JavaScript, Terminal-Dienste, FTP- oder Webserver)
- Falsch konfigurierte Netzwerk-Geräte (ACLs, Routing-Protokolle, SNMP-Community-Strings)

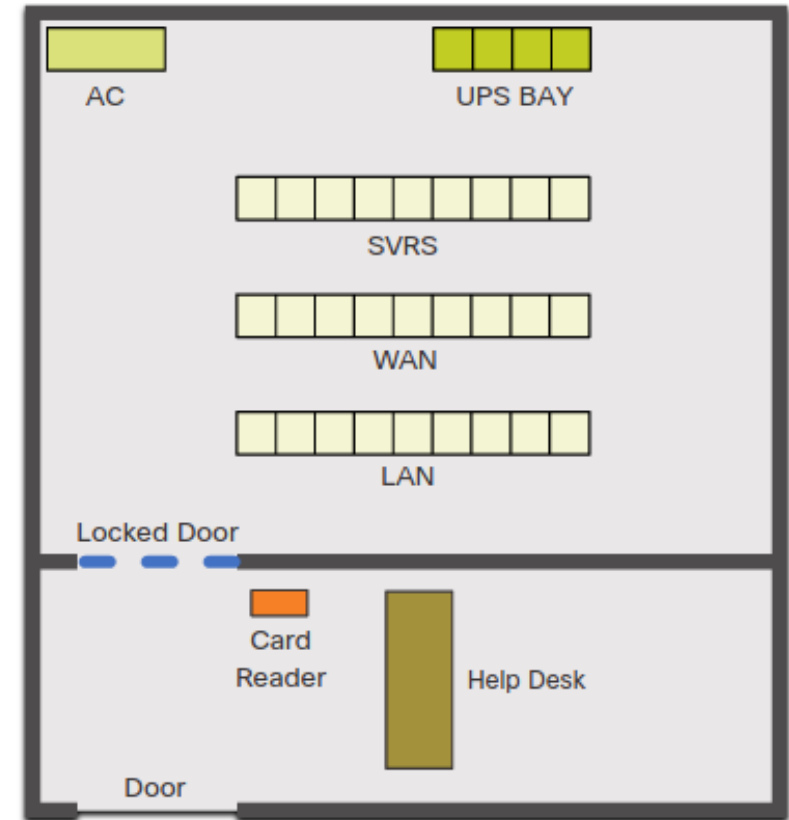
## Typen von Schwachstellen

### ▪ Policy-Schwachstellen (Richtlinien)

- Richtlinien liegen überhaupt nicht vor.
- Erschwerung der Umsetzung durch „Revier-Kämpfe“
- Unsichere Passwörter / Default-Passwörter
- Verschwendung von Ressourcen durch unzureichendes Monitoring und Auditing
- Unautorisierte Änderungen an der Topologie oder Installation nicht genehmigter Anwendungen schaffen Sicherheitslücken
- Nicht vorhandener/ nicht funktionierender Disaster-Recovery-Plan

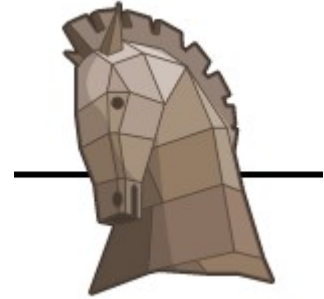
## Physikalische Sicherheit

- **Hardware Bedrohungen:**  
physischer Schaden an Geräten und Kabel
- **Umgebungs-Bedrohungen:**  
Temperatur, Feuchtigkeit
- **Elektrische Bedrohungen:**  
Spannungsspitzen und -abfälle, Leistungsverlust
- **Wartungsbedrohungen:**  
elektrostatische Entladung, Mangel an kritischen Ersatzteilen, schlechte Verkabelung, schlechte Kennzeichnung



## Was ist Malware?

- **Malware:** Malicious Software = Bösertige Software
- **Ziel:** Hosts/Netzwerk beschädigen oder stören, Daten beschädigen oder stehlen, Dienste beeinträchtigen, etc.



## Typen von Malware

- **Viren:** verbreiten sich selbstständig über andere Software (ausführbare Dateien).
- **Würmer:** ähnlich der Viren, benötigen aber keinen Wirt für die Reproduktion. Es werden Systemdienste genutzt.
- **Trojaner:** gibt sich als legitimes Programm aus und verleitet Anwender zur Installation. Sind vor allem für die Einrichtung von Backdoors bekannt, die einem Angreifer Zutritt verschaffen.

## Aufklärung (Reconnaissance Attacks)

Auch im lokalen Netz interessant.

- Angriffe auf ein bestimmtes Ziel erfolgen mehrschrittig. Am Anfang steht die Aufklärung: Geräte entdecken, Betriebssysteme erkennen, Dienste abfragen und dazugehörige Schwachstellen finden
  - **Internet Abfragen:** Welche IP-Adressräume gehören zu welchen Unternehmen (Tools: nslookup, whois).
  - **Ping Sweeps:** IP-Adressen identifizieren, die öffentlich erreichbar sind (Tools: ping, fping, gping, arping).
  - **Port Scans:** Identifizierung der Dienste die auf einem Server angeboten werden. (Tool: nmap)

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 3.5p1 (p)
53/tcp	open	domain	ISC Bind 9.2.1
111/tcp	open	rpcbind	2 (rpc #100000)
631/tcp	open	ipp	CUPS 1.1
953/tcp	open	rndc?	

## Aufklärung (Reconnaissance Attacks)

- Infos dazu gibt es im Netz ... z. B. unter <https://cve.mitre.org/>
- CVE: Common Vulnerabilities and Exposures  
Ziel: Einheitliche Namens-Konvention für Sicherheitslücken



### Search Results

There are **12** CVE entries that match your search.

Name
<a href="#">CVE-2020-5304</a> The dashboard in Whitebox of data. The attacker can
<a href="#">CVE-2017-8087</a> Information Leakage in
<a href="#">CVE-2015-7242</a> Cross-site scripting (XSS)
<a href="#">CVE-2014-9727</a> AVM Fritz!Box allows remote
<a href="#">CVE-2014-8886</a> AVM FRITZ!OS before 0.9.0 allows
<a href="#">CVE-2014-8872</a> Improper Verification of

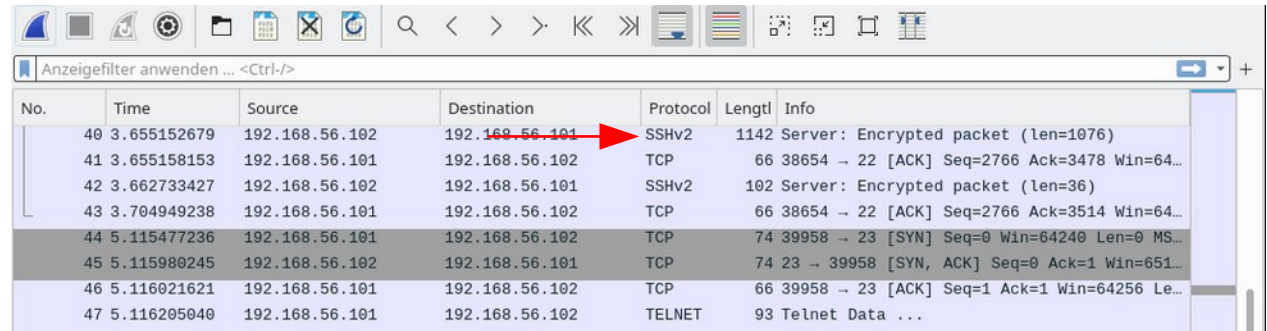
CVE-ID	
<b>CVE-2014-9727</b>	<a href="#">Learn more at National Vulnerability Database</a> • CVSS Severity Rating • Fix Information
Description	
AVM Fritz!Box allows remote attackers to execute arbitrary code	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help	
<ul style="list-style-type: none"><li>• EXPLOIT-DB:33136</li><li>• URL:<a href="http://www.exploit-db.com/exploits/33136">http://www.exploit-db.com/exploits/33136</a></li><li>• MISC:<a href="https://www.trustwave.com/Resources/Spider">https://www.trustwave.com/Resources/Spider</a></li><li>• OSVDB:103289</li></ul>	

Nicht aus dem  
offiziellen  
Kursmaterial



## Access Attacks

- **Ziel:** unautorisierter Zugriff auf Benutzerkonten, Datenbanken, etc.
- **Typen:**
  - **Passwort-Angriffe:** Brute-Force, Trojaner, Packetsniffer
  - Trust Exploitation
  - Port Redirection
  - Man-In-the-Middle



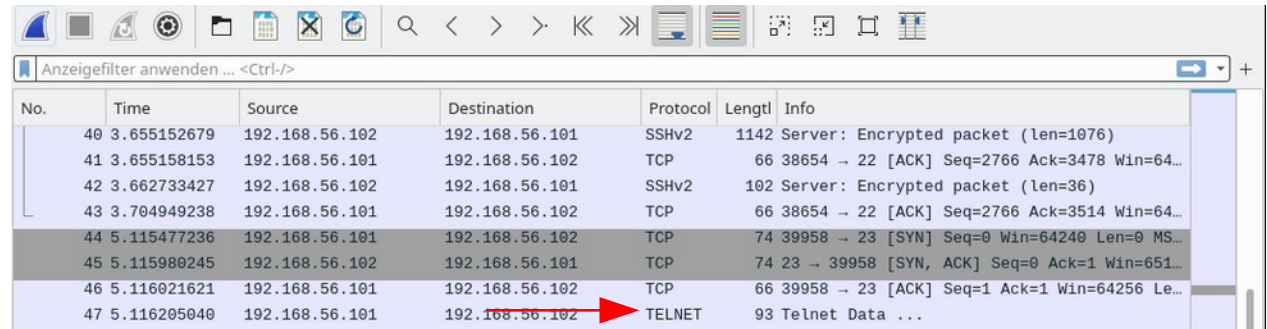
No.	Time	Source	Destination	Protocol	Length	Info
40	3.655152679	192.168.56.102	192.168.56.101	SSHv2	1142	Server: Encrypted packet (len=1076)
41	3.655158153	192.168.56.101	192.168.56.102	TCP	66	38654 → 22 [ACK] Seq=2766 Ack=3478 Win=64...
42	3.662733427	192.168.56.102	192.168.56.101	SSHv2	102	Server: Encrypted packet (len=36)
43	3.704949238	192.168.56.101	192.168.56.102	TCP	66	38654 → 22 [ACK] Seq=2766 Ack=3514 Win=64...
44	5.115477236	192.168.56.101	192.168.56.102	TCP	74	39958 → 23 [SYN] Seq=0 Win=64240 Len=0 MS...
45	5.115980245	192.168.56.102	192.168.56.101	TCP	74	23 → 39958 [SYN, ACK] Seq=0 Ack=1 Win=651...
46	5.116021621	192.168.56.101	192.168.56.102	TCP	66	39958 → 23 [ACK] Seq=1 Ack=1 Win=64256 Le...
47	5.116205040	192.168.56.101	192.168.56.102	TELNET	93	Telnet Data ...

```
.....,.....T.P.....k.c
..Ah.....^.\.....#4.....h....ecdsa-sha2-
nistp256...nistp256...A.k.M.dgo:...*y..JQ...f5.....;.....Q..g...Q..t.x...
%.p.Y#.....Q...c..l.x../Dx.....k..=.2..(a..c....ecdsa-sha2-nistp256...H...
.$&I.....Q.k.....e..%..e.)dl...oE.#/... ..D..Z...!r
....ilDE.....
.....
.e... ..Z.n..@:....Q..j.t.j].
7s.g3...QCp.....".....K..f.....LW...=.X.b...Q....*.M*...?:...
_D*'|.0....y..#{.?s|....6..Tf).A?.'......P:..2..D..
J!.....,e.....
.....e.....SH..m.yx...?...GE.....l.....E.0.=j.....r4...=.#...
2..C.D...Rs;.....U>:..w..H..SR3.r..C4.`...."....7....2.1..~...R...<Y...!..P.i??|
.....
```

SSH → verschlüsselt

## Access Attacks

- **Ziel:** unautorisierter Zugriff auf Benutzerkonten, Datenbanken, etc.
- **Typen:**
  - **Passwort-Angriffe:** Brute-Force, Trojaner, Packetsniffer
  - Trust Exploitation
  - Port Redirection
  - Man-In-the-Middle



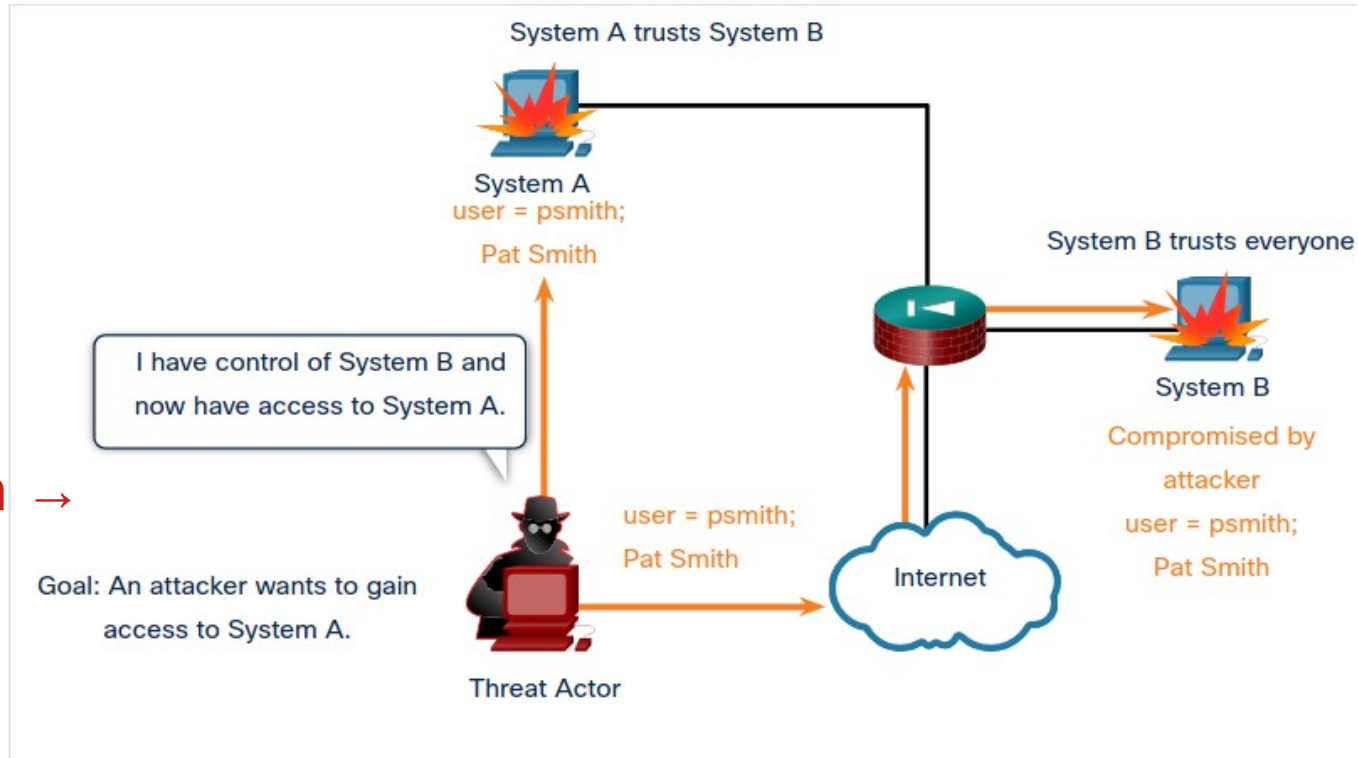
No.	Time	Source	Destination	Protocol	Length	Info
40	3.655152679	192.168.56.102	192.168.56.101	SSHv2	1142	Server: Encrypted packet (len=1076)
41	3.655158153	192.168.56.101	192.168.56.102	TCP	66	38654 → 22 [ACK] Seq=2766 Ack=3478 Win=64...
42	3.662733427	192.168.56.102	192.168.56.101	SSHv2	102	Server: Encrypted packet (len=36)
43	3.704949238	192.168.56.101	192.168.56.102	TCP	66	38654 → 22 [ACK] Seq=2766 Ack=3514 Win=64...
44	5.115477236	192.168.56.101	192.168.56.102	TCP	74	39958 → 23 [SYN] Seq=0 Win=64240 Len=0 MS...
45	5.115980245	192.168.56.102	192.168.56.101	TCP	74	23 → 39958 [SYN, ACK] Seq=0 Ack=1 Win=651...
46	5.116021621	192.168.56.101	192.168.56.102	TCP	66	39958 → 23 [ACK] Seq=1 Ack=1 Win=64256 Le...
47	5.116205040	192.168.56.101	192.168.56.102	TELNET	93	Telnet Data ...

```
ubuvvm login: vvaaddeerr
.
Password: starwars
.
Last login: Thu Sep 24 05:29:25 UTC 2020 from 192.168.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-ge
```

Telnet → verschlüsselt

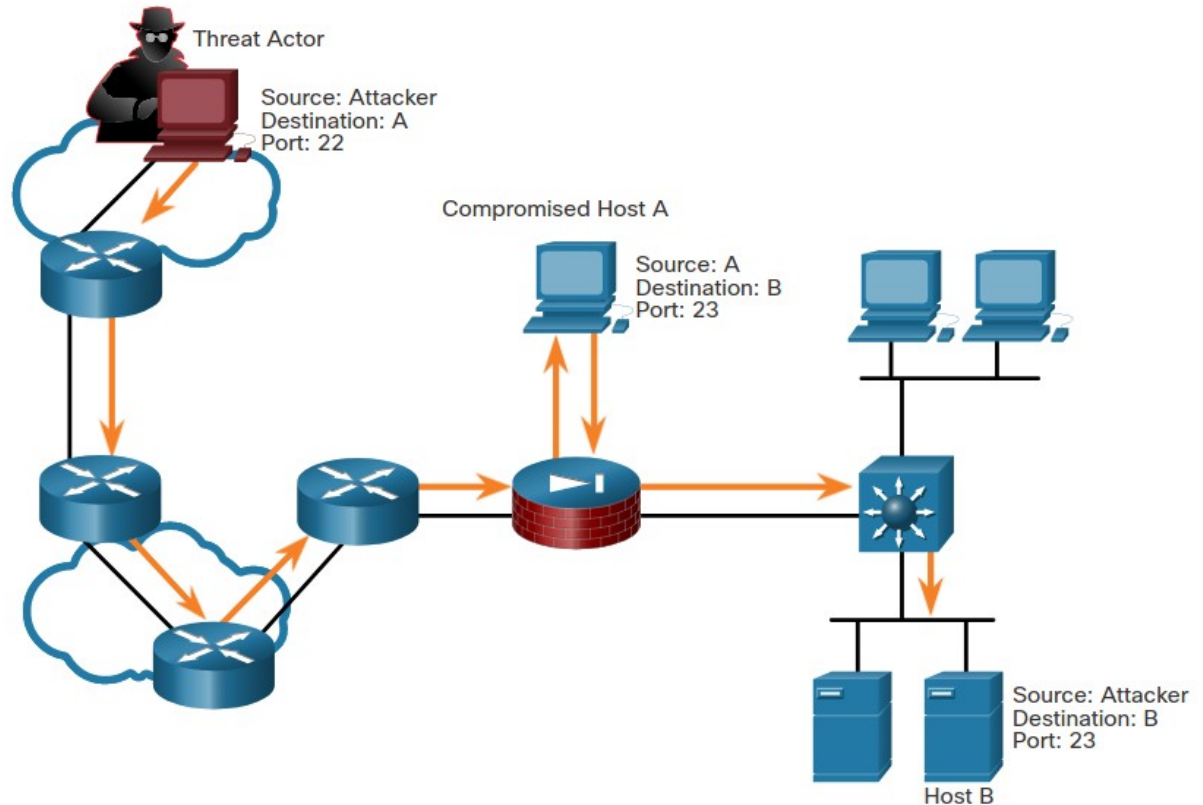
## Access Attacks

- **Ziel:** unautorisierter Zugriff auf Benutzerkonten, Datenbanken, etc.
- **Typen:**
  - Passwort-Angriffe: Brute-Force, Trojaner, Packetsniffer
  - **Trust Exploitation** →
  - Port Redirection
  - Man-In-the-Middle



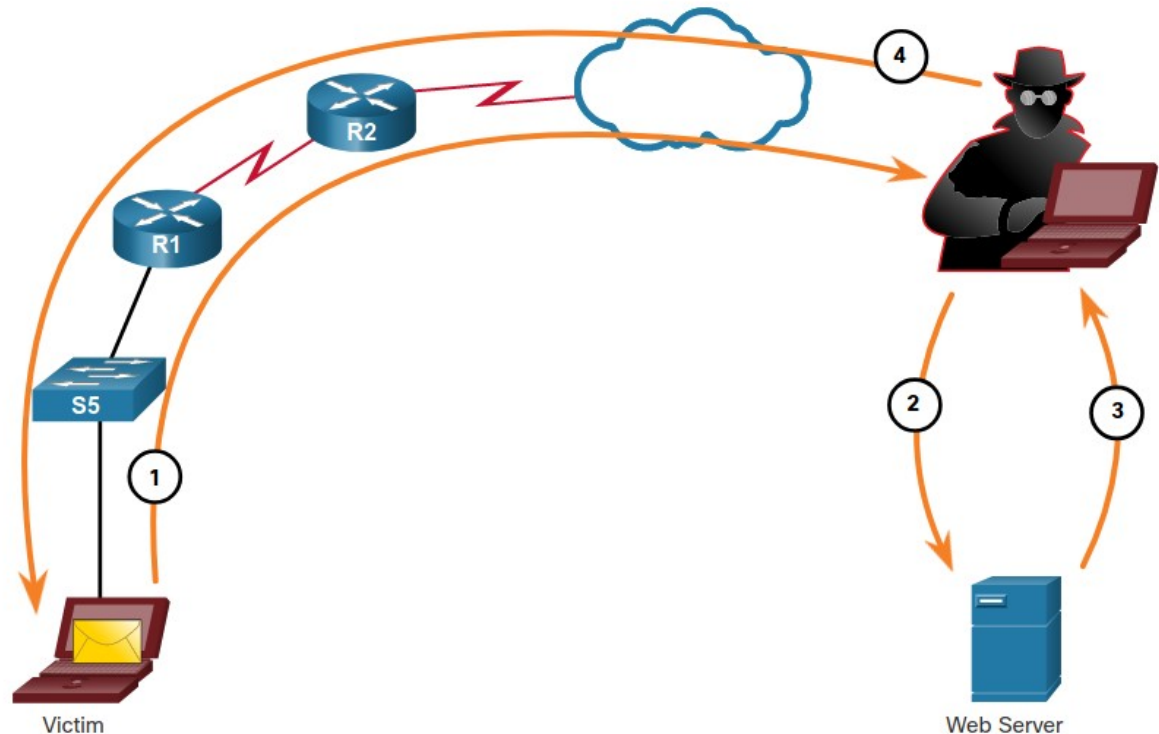
## Access Attacks

- **Ziel:** unautorisierter Zugriff auf Benutzerkonten, Datenbanken, etc.
- **Typen:**
  - Passwort-Angriffe: Brute-Force, Trojaner, Packetsniffer
  - Trust Exploitation
  - **Port Redirection** →
  - Man-In-the-Middle



## Access Attacks

- **Ziel:** unauthorisierter Zugriff auf Benutzerkonten, Datenbanken, etc.
- **Typen:**
  - Passwort-Angriffe: Brute-Force, Trojaner, Packetsniffer
  - Trust Exploitation
  - Port Redirection
  - **Man-In-the-Middle** →



- **Denial of Service:**

Legitimen Nutzern den Dienst (Service) verweigern (Deny)

Zwei Vorgehensweisen

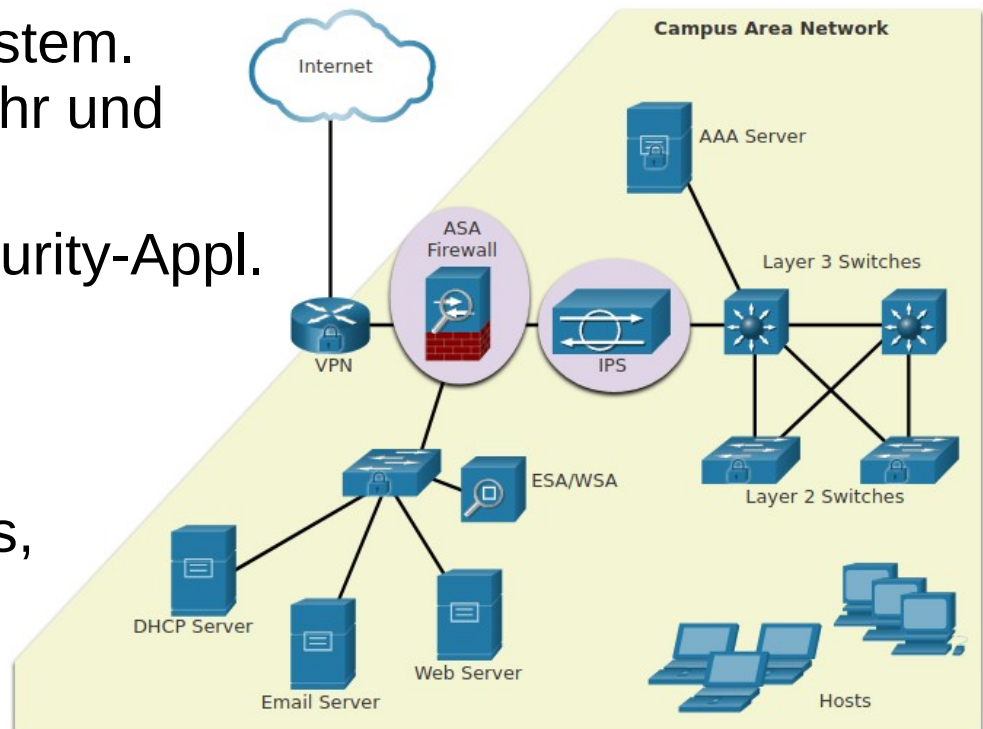
- **Schiere Datenmenge:** So viele Daten senden, dass entweder das Ziel selbst oder die Leitung zum Ziel überlastet wird.
- **Schadhafte Pakete:** Datenpakete so manipulieren, dass das Ziel mit deren Verarbeitung Probleme bekommt.

- **Distributed Denial of Service:**

- Angreifer weist viele Zombies eines Botnets an, DoS durchzuführen
- Anbieter haben mit dieser Angriffsart „Riesen“-Probleme.
- Durch die enorme Zunahme von IoT-Devices nur schwer eindämmbar. [Provider mit ins Boot holen]

## ▪ Defense-in-Depth-Ansatz (Mehrschichtige Verteidigung)

- **VPN** → Zugriff auf das Netz über verschlüsselte Tunnel
- **ASA Firewall** → Dedizierte Firewall. Nur Netzwerkverbindungen, die von innen initiiert wurden, sind zugelassen.
- **IPS** → Intrusion Prevention System. Überwacht den Netzwerkverkehr und greift bei Bedrohungen ein.
- **ESA/WSA** → Email-/Web-Security-Appl. filtert Spam-Mail und bekannte „Problem“-Webseiten
- **AAA-Server** → beinhaltet eine Datenbank von Nutzeraccounts, wer sich auf Netzwerkgeräte einwählen darf.





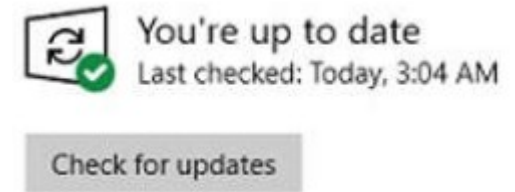
## Backups

Datenverlust kann mit Backups am besten begegnet werden. Konfigurationsdateien und IOS-Images gehören dazu.

- **Frequenz:** regelmäßige Durchführung von Voll-Backups in Kombination mit differentiellen und inkrementellen Backups
- **Speicher:** Backups sollten (auch) offsite gespeichert werden. Eine Rotation wie in der Security Policy vorgesehen muss eingehalten werden. (Pwned By The Owner: What Happens When You Steal A Hacker's Computer: <https://www.youtube.com/watch?v=Jwpg-AwJ0Jc>)
- **Sicherheit:** Backups müssen durch starke Passwörter geschützt werden.
- **Absicherung/Validierung:** Backups müssen validiert werden (Datenintegrität, Restore-Prozess)



Systeme müssen aktuell gehalten werden. Das „Stopfen“ der Sicherheitslücken gilt als eines der „wirksamsten“ Verteidigungsmittel.

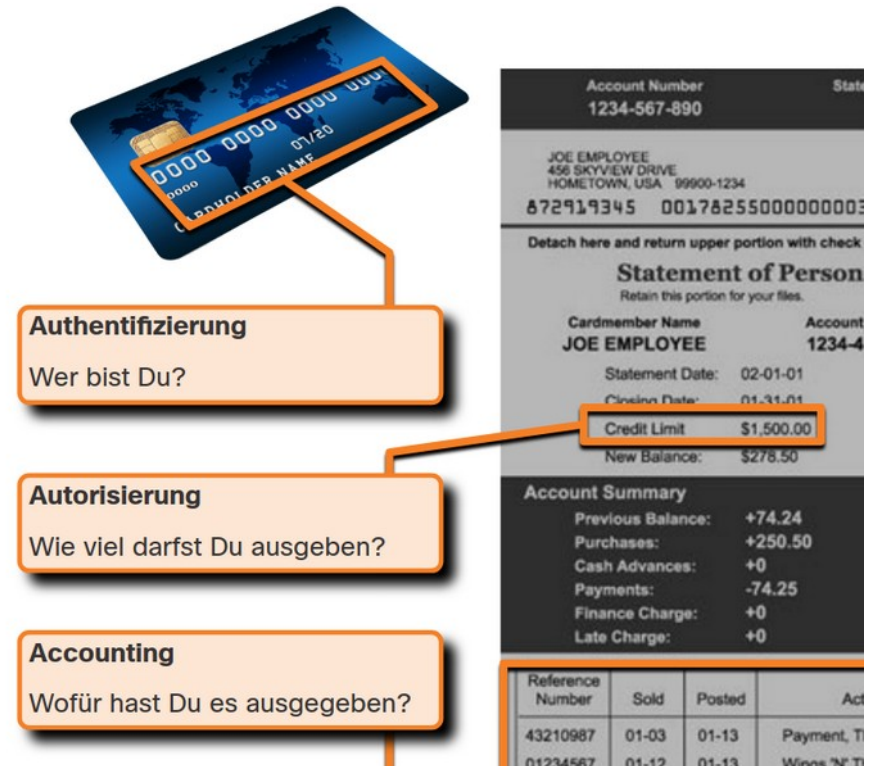


Drei Begriffe sollten unterschieden werden:

- Upgrade → nächste Version einer Software (Major-Release)
- Update → i.d.R. Änderungen im Funktionsumfang (Minor-Release)
- Patch → ausschließlich Fehlerbehebung (Patchlevel wird erhöht)

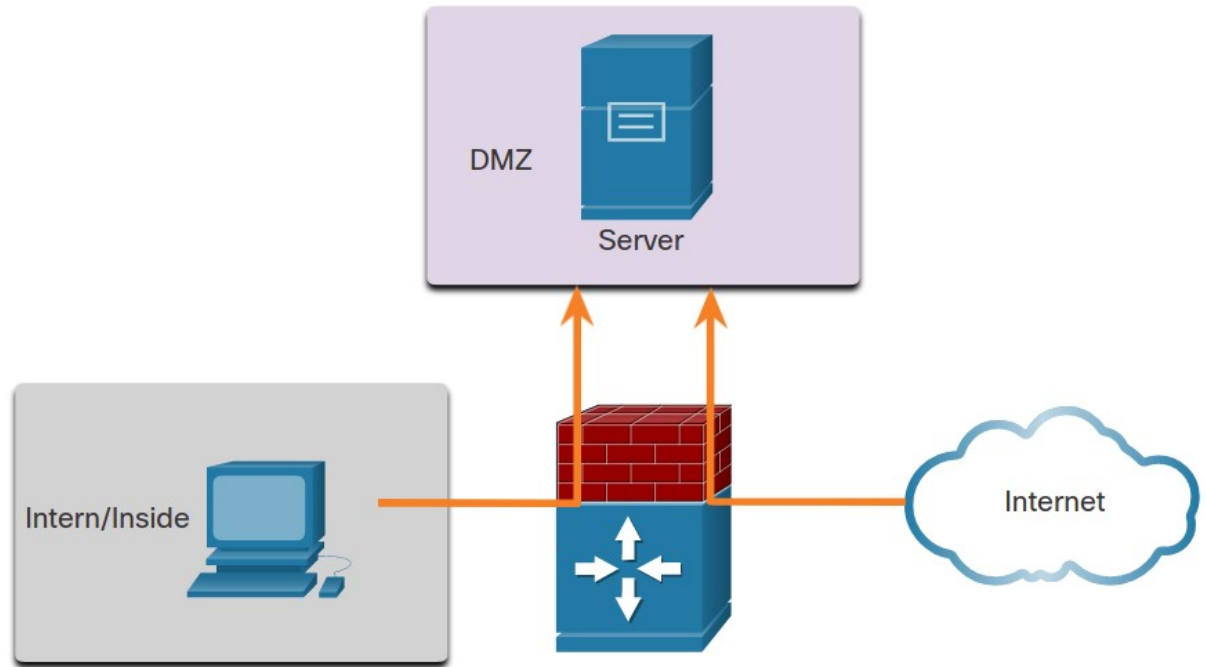
Achtung: Nicht nur Server- und Client-Betriebssysteme brauchen Aktualisierungen. Auch Switches und Router ... !

- Authentication, Authorization, Accounting (AAA oder Tripple-A)
  - **Authentication:**  
Wer ist berechtigt auf dem Gerät/Netzwerk zuzugreifen?
  - **Authorization:**  
Was dürfen die Benutzer auf dem Gerät/Netzwerk tun?
  - **Accounting:**  
Nachverfolgen, welche Aktionen auf dem Gerät/Netzwerk ausgeführt werden.



## Firewalls

- schützen Computer und Netzwerke, indem das Eindringen unerwünschten Datenverkehrs in Netzwerke abgeblockt wird.
- Sie sitzen zwischen zwei oder mehreren Netzwerken.
- Kontrollierter Zugriff von außen ist über eine DMZ möglich.



## Firewall-Arten

- **Paketfilterung:** verhindert oder gestattet den Zugriff auf Basis von IP- oder MAC-Adressen
- **Anwendungsfilterung:** verhindert oder gestattet den Zugriff auf Basis von Port-Nummern
- **URL-Filterung:** verhindert oder gestattet den Zugriff auf Websites auf Basis URLs oder Schlüsselwörtern
- **Stateful Packet Inspection (SPI):** eingehende Pakete müssen Antworten auf Anfragen interner Hosts sein. Unerwünschte Pakete werden blockiert, wenn sie nicht explizit zugelassen werden. Kann spezielle Angriffsformen wie Denial of Service (DoS) erkennen und herauszufiltern.

## Endpoint Security

- **Endgeräte:** Laptops, Desktops, Server, Smartphones und Tablets
- Deren Sicherheit gehört zu den **anspruchsvollsten Aufgaben** (Faktor Mensch als Ursache von Problemen)
- **Ansatzpunkt:**
  - Gut dokumentierte Sicherheitsregeln ...
  - ... die den Mitarbeitern bekannt sind.
  - Schulung von Mitarbeitern
  - Antivirus-Software
  - Aktivierte Firewall
  - Evtl. Host-Intrusion-Prevention-System



## Cisco AutoSecure

- Assistent zum Setzen von Basis-Sicherheits-Einstellungen
  - Banner
  - Absicherung des Privileged Exec Mode
  - Lokaler User
  - Block-Periode
  - SSH-Konfig
  - ...

```
Router# auto secure
      --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

## Passwörter


- Mindestens 10 Zeichen
- Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen (Vorsicht bei Leerzeichen).
- Pro Account-Typ → ein eigenes Passwort
- Kein sozialer Bezug (Partner, Verwandte, Haustiere, Infos aus dem Lebenslauf)
- Kein Wort aus einem Wörterbuch, Wortlisten
- Absichtlich falsch geschriebene Passwörter. Zum Beispiel Smith = Smyth = 5mYth oder Security = 5ecur1ty ... besser: Dialekt.
- Ändern Sie Kennwörter häufig.
- Schreiben Sie Kennwörter nicht (unverschlüsselt) auf und bewahren Sie sie nicht am Arbeitsplatz



## Passwörter

Nicht aus dem  
offiziellen  
Kursmaterial

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

 **HIVE SYSTEMS**

**-Data sourced from [HowSecureIsMyPassword.net](https://howsecureismypassword.net)**



## Passwörter

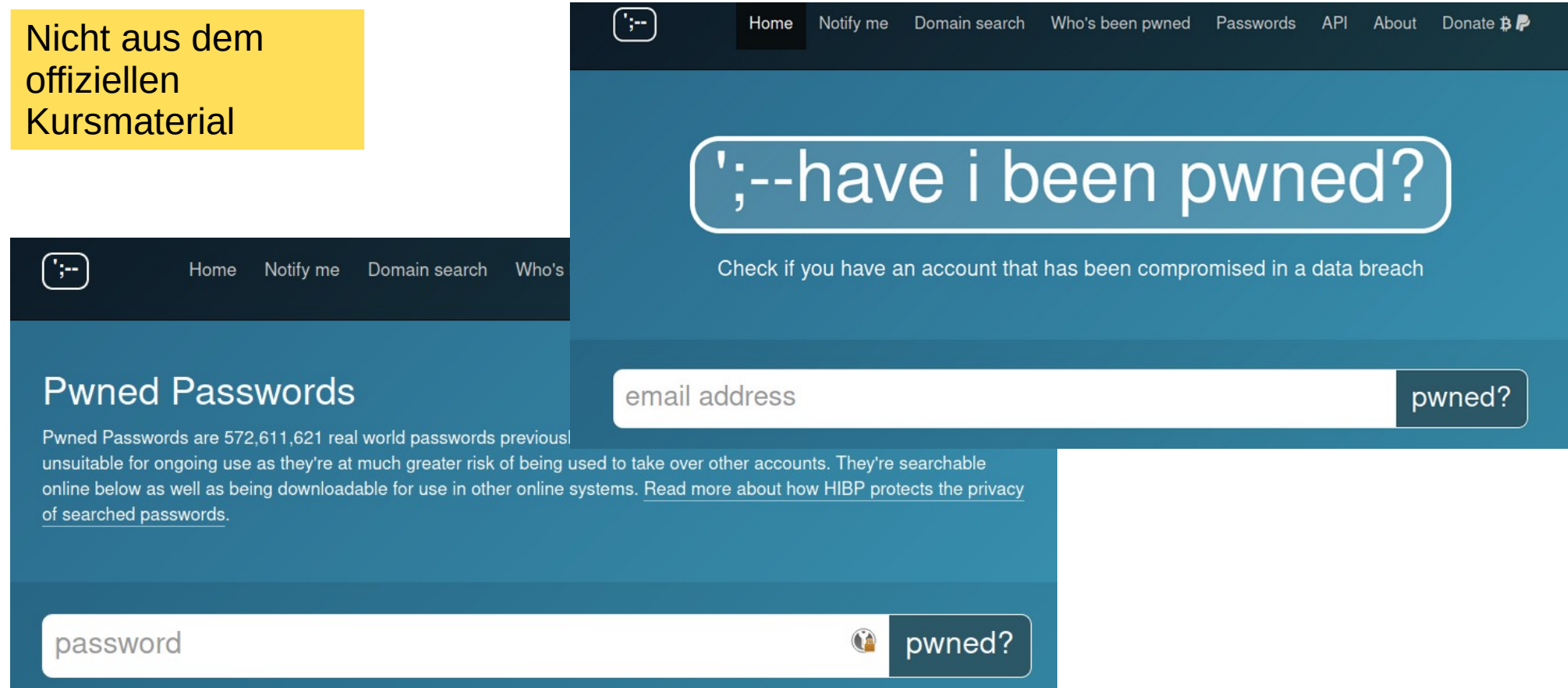
Nicht aus dem  
offiziellen  
Kursmaterial

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES		VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES	
1. USE ANTIVIRUS SOFTWARE				1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS				2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY				3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW				4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION				5. USE A PASSWORD MANAGER

## Passwörter

<https://haveibeenpwned.com/>

Nicht aus dem  
offiziellen  
Kursmaterial



The screenshot displays the Have I Been Pwned (HIBP) website. The top navigation bar includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading reads "';--have i been pwned?'". Below this, a subheading states: "Check if you have an account that has been compromised in a data breach". The page is divided into two main sections. The left section, titled "Pwned Passwords", contains text explaining that 572,611,621 real-world passwords have been previously compromised and are now unsuitable for use. It also mentions that these passwords are searchable online and provides a link to read more about how HIBP protects privacy. The right section features a search interface with a text input field labeled "email address" and a button labeled "pwned?". Below this, there is another search field labeled "password" with a button labeled "pwned?".

## Zusätzliche Passwortsicherheit

... auf einem Cisco-Router/-Switch

- Passwörter müssen verschlüsselt hinterlegt sein  
`service password-encryption`
- Passwortkomplexität festlegen  
`security passwords min-length 10`
- Brute-force-Angriffe verhindern  
`login block-for 120 attempts 3 within 60`
- Abmeldung nach längerer Inaktivität Accounts  
`exec-timeout 5 30`
- SSH statt Telnet nutzen

## SSH konfigurieren

- Hostname setzen (Defaultname wurde nicht akzeptiert)
- Domain setzen
- SSH-Schlüssel (> 1024 bit)
- Benutzer in der lokalen Datenbank anlegen  
Passwort wird mit dem Schlüsselwort „secret“ md5-verschlüsselt
- Authentifizierung gegenüber der lokalen Datenbank konfigurieren
- Eingehende Sitzung auf vty-Leitung für SSH aktivieren

## SSH konfigurieren

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
•Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

## Ungenutzte Services ausschalten

- Default-Dienste/-Ports anzeigen:  
Aktuell: `show ip ports all`  
Früher: `show control-plane host open-ports`
- Dann handeln und abschalten:

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot Local Address Foreign Address Service State
tcp *:23 *:0 Telnet LISTEN
tcp *:80 *:0 HTTP CORE LISTEN
udp *:67 *:0 DHCPD Receive LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

## Aktivitäten

- 16.1.4: Check Your Understanding - Security Threats and Vulnerabilities
- 16.2.5: Check Your Understanding - Network Attacks
- 16.2.6: Lab - Research Network Security Threats
- 16.3.8: Check Your Understanding - Network Attack Mitigation
- **16.4.6: Packet Tracer - Configure Secure Passwords and SSH**
- **16.4.7: Lab - Configure Network Devices with SSH**
- **16.5.1: Packet Tracer - Secure Network Devices**
- **16.5.2: Lab - Secure Network Devices**
- **16.5.4: Module Quiz - Network Security Fundamentals**

## Fragen ...

