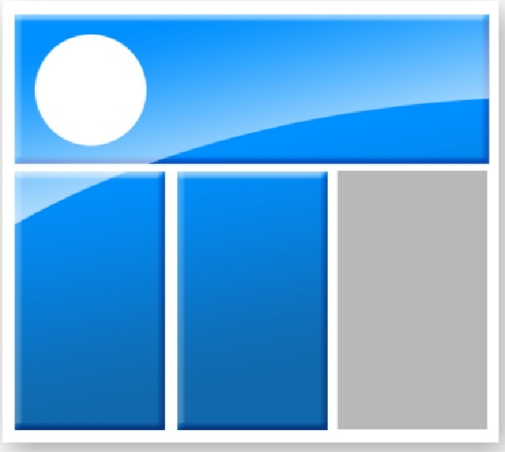
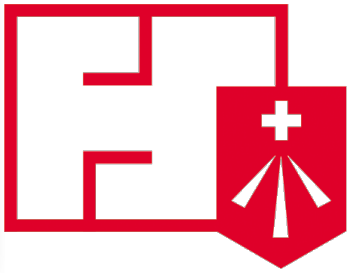
Grundlagen: Sicherheit in lokalen Netzen

5. Stralsunder IT-Sicherheitskonferenz





fachhochschule
stralsund

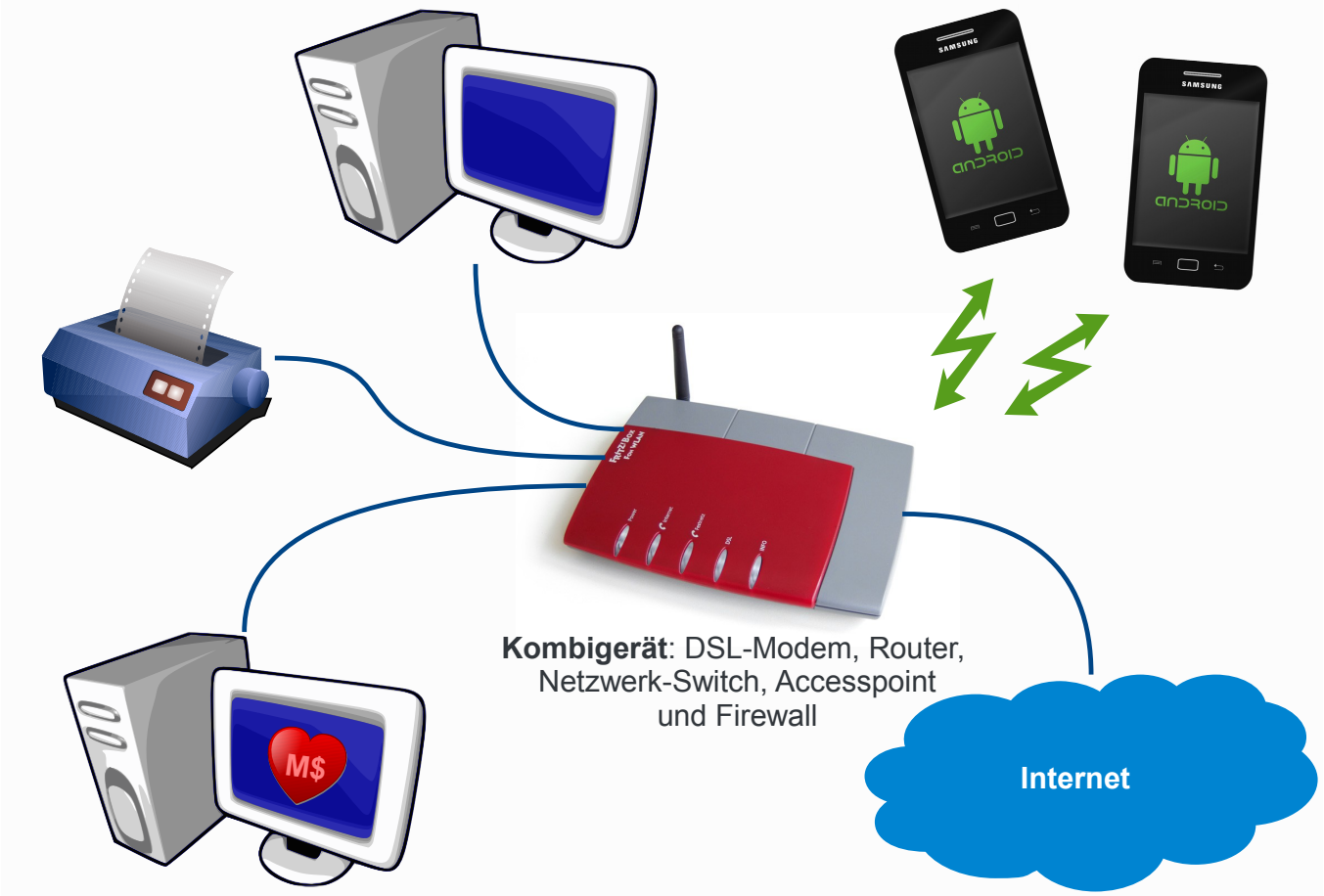
Prof. Dr.-Ing. Andreas Noack

<andreas.noack@fh-stralsund.de>

Worum geht es in den nächsten 20 Minuten?

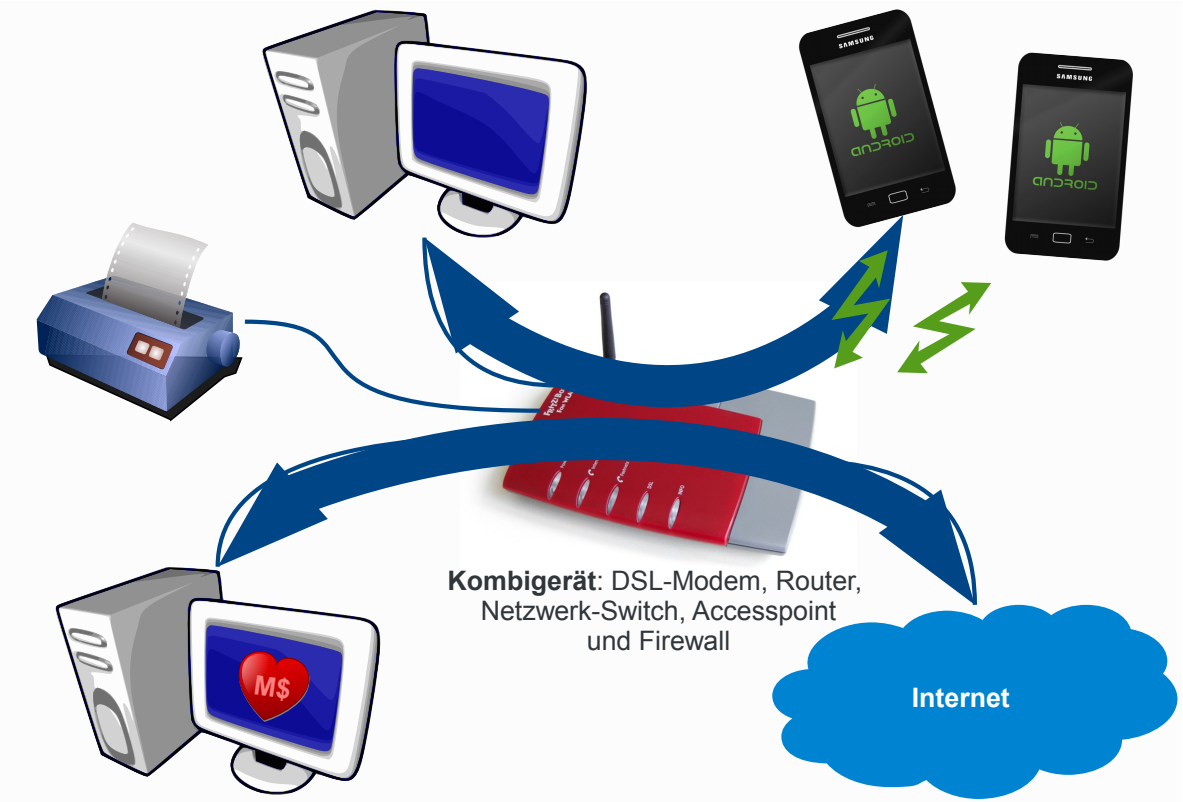
(1) Ein paar Grundlagen zu lokalen Netzen
(2) Hackerangriffe ☺
(3) Gegenmaßnahmen

Was ist ein Local Area Network (LAN)?



Viele haben ein **lokales Netzwerk** (LAN) zuhause,
...doch ist es auch sicher?

Kommunikation im (W)LAN



Die **Kommunikation** zwischen zwei Netzwerkteilnehmern:

- direkt
- Switch/Accesspoint sendet Daten **nur** an die Beteiligten

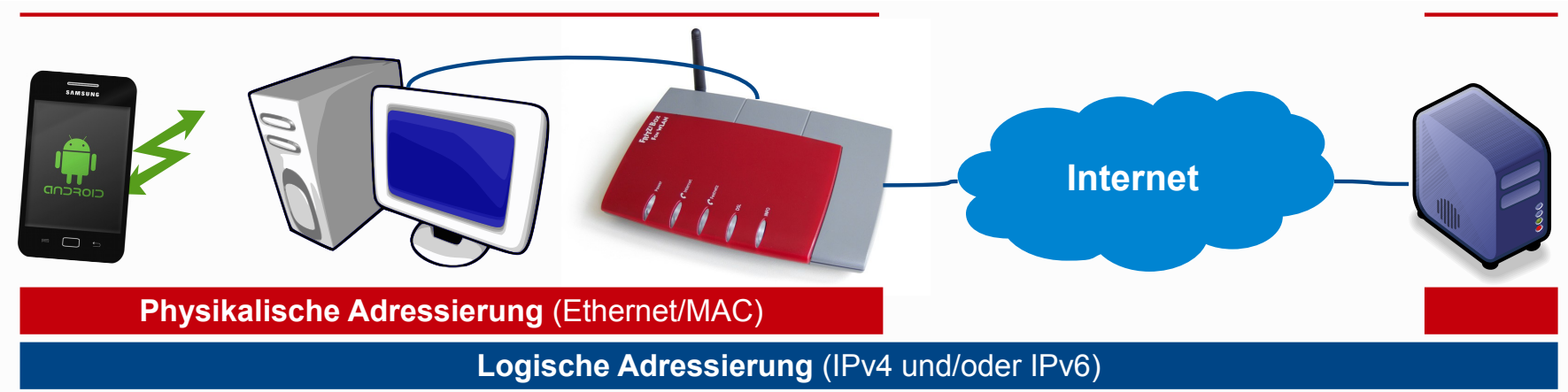
Was bedeutet das?
Fremde Kommunikation abhören oder verändern ist (*...ohne weiteres* ☺) nicht möglich!

Der Vollständigkeit halber...

Multi- und Broadcasts: Es gibt Kommunikation, die an mehrere/alle Teilnehmer gerichtet ist. Diese wird natürlich von allen empfangen...

WLAN-Funkwellen werden von **allen** Teilnehmern in Reichweite empfangen. Jeder sieht, *wer* kommuniziert, aber meistens nicht *was* (verschlüsselt).

Mehrere Adressen für jedes Gerät



Physikalische Adressierung

Jedes Endgerät hat eine physikalische (MAC-)Adresse, die für die Kommunikation innerhalb eines Subnetzes benötigt wird.

- MAC Adresse des Ethernet-Protokolls (LAN), z.B. `00:11:22:33:44:55`

Logische Adressierung

Zusätzlich hat jedes Endgerät eine logische Adresse (z.B. IPv4 oder IPv6), die sowohl innerhalb als auch außerhalb eines Subnetzes für die Adressierung verwendet wird.

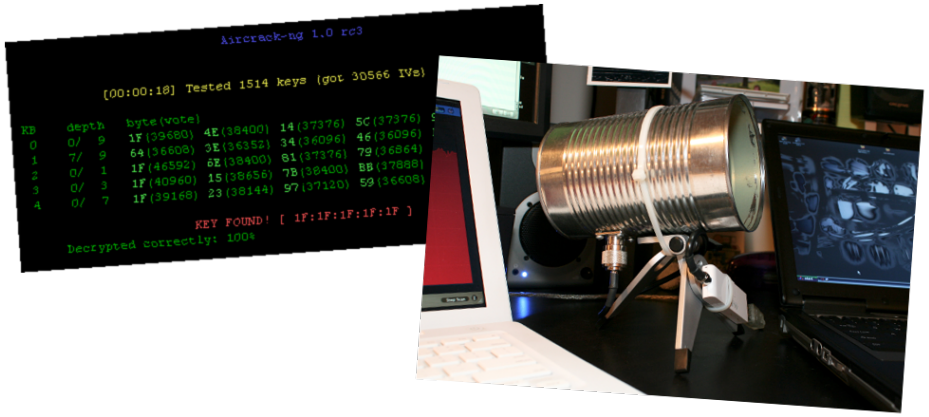
- IPv4 Global eindeutig, z.B. `194.94.72.152` oder nur lokal: `192.168.0.1`
- IPv6 Global eindeutig, z.B. `2a00:1328:e000:452::26` oder nur lokal: `fe80::1234:56ff:fe78:9abc`

Wie bekommt der Angreifer Zugang zu dem LAN?

Angriff über WLAN

Wenn der Angreifer keinen physikalischen Zugang hat, bietet sich ein Angriff über WLAN an:

- **Schwaches Sicherheitssystem** (*unverschlüsselt oder WEP*)
- **Schwaches Passwort** (*z.B. bekanntes Wort oder nur 8 Zeichen?*)
- **Aktives WPS** (*Wi-Fi Protected Setup*) ohne Gegenmaßnahmen



Aircrack-ng [Air16] und
Cantenna (*Selbstbau Richtfunkantenne*)

USB Rubber Ducky Deluxe [Hak16]

Social Engineering

Zugang mit Charme oder Dreistigkeit erschleichen, z.B.

- *"Der neue Admin aus der IT"*
- *Ein auf dem Parkplatz "verlorener" USB-Stick mit Trojaner*

Der Überblick im LAN

Der Überblick im LAN

- *Welche Endgeräte sind im Netzwerk erreichbar? (**Wer?**)*
- *Welche Dienste bieten die Endgeräte an? (**Was?**)*
- *Welche Dienstversionen und Betriebssysteme sind im Einsatz (**Details?**)*
  → Schwachstellen ☠☠☠

Mit Netzwerkscannern wie `fing` [OVE16], Portscannern wie `nmap` [Lyo16] und Pentesting-Tools wie `metasploit` [Rap16] lassen sich diese Informationen bequem erheben!
Gegenmaßnahme: Ein Intrusion Detection System (IDS) kann Scans erkennen.

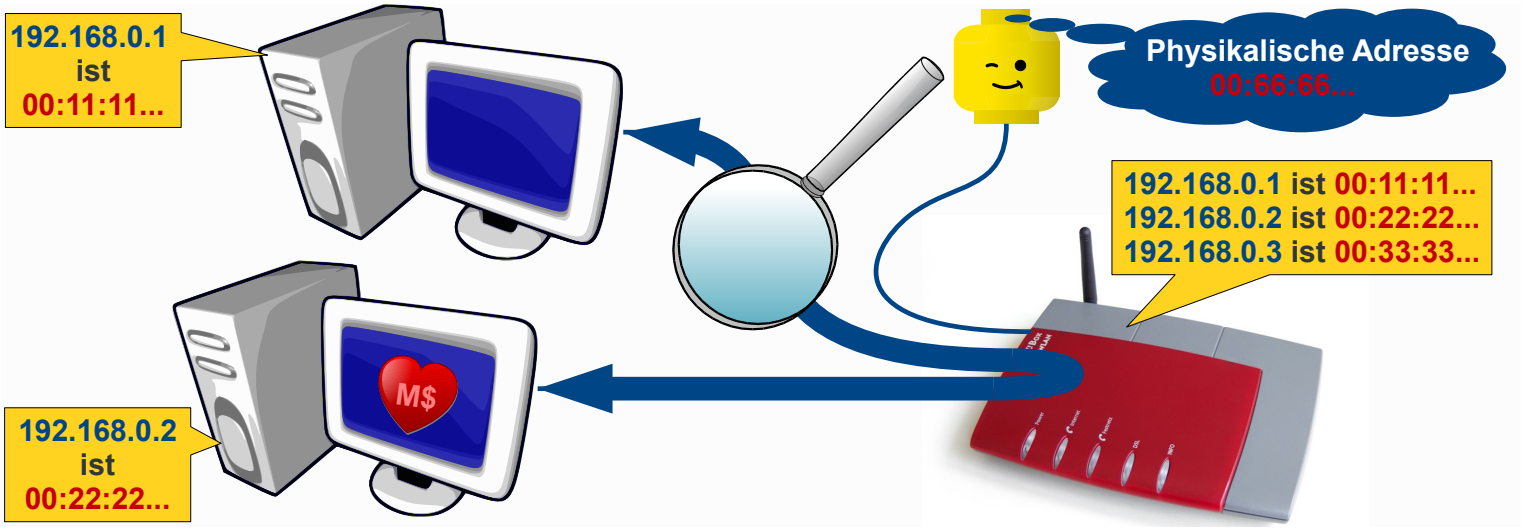
Ein kleines Beispiel!

...wie sieht so ein Portscan in der Praxis aus?

```
# nmap -sS -O 192.168.1.1
Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-24 13:06 CEST
Nmap scan report for WIN-O7P24T4G0SC.lan (192.168.1.1)
Host is up (0.00022s latency).
Not shown: 993 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
10243/tcp open unknown
MAC Address: 00:0C:31:A6:F5:13 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
Network Distance: 1 hop
```

Portscan mit nmap [Lyo16]

Kommunikation abhören und verändern

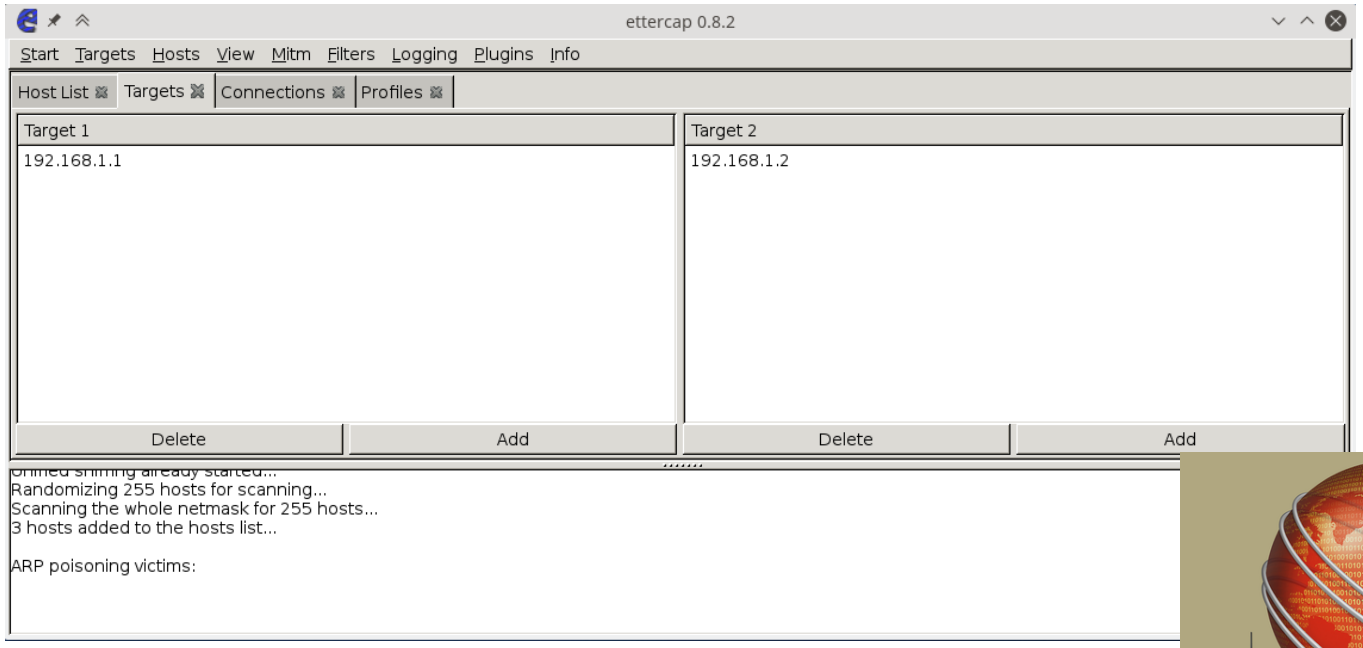


Eine Möglichkeit, Kommunikation abzuhören ist ARP-Spoofing (nur IPv4)

Wenn zwei Geräte kommunizieren, nutzen sie die **physikalischen Adressen** (MAC). Vorab bekannt sind aber nur die **logischen Adressen** (IP).
⇒ **ARP-Tabelle**: *Jeder merkt sich für eine gewisse Zeit, welche physikalische Adresse zu welcher logischen passt.*

Der Angriff. Der Hacker fälscht ARP-Nachrichten. Jeder glaubt, dass sein Kommunikationspartner eine neue physikalische Adresse nutzt, die des Hackers.
→ *Die Kommunikation wird zum Hacker geleitet, dieser hört sie ab oder verändert sie, und leitet sie später an das eigentliche Ziel weiter.*

Kommunikation abhören und verändern II

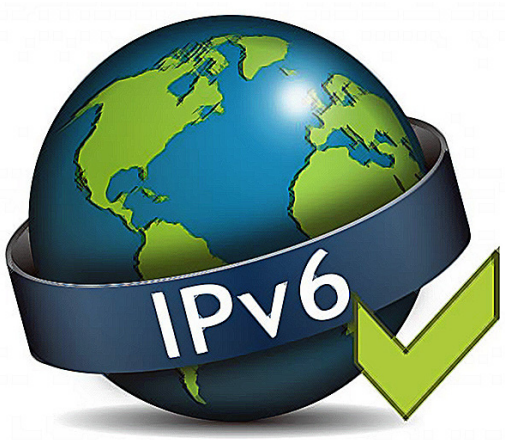


Ein Tool für ARP-Poisoning: Ettercap [OV16]

Ettercap unterstützt

- Aktive (Verändern) und passive Angriffe (Abhören)
- ermöglicht ARP-Spoofing, DNS-Spoofing uvm.
- Plugins zur Behandlung von VPN, Dateitransferprotokollen, uvm.

Kommunikation abhören und verändern III



Wird mit dem neuen IP-Protokoll (IPv6) alles besser?

Leider nein, leider gar nicht...IPv6 setzt anstatt ARP das Neighbor Discovery Protocol (NDP) ein. NDP ist noch viel mächtiger als ARP und genauso ungeschützt! [Mar16]

⇒ **Ähnliche (und noch ein paar mehr...) Angriffe funktionieren gegen IPv6!**

Gibt es Gegenmaßnahmen?

- Professionelle Netzwerkswitches ermöglichen die Überwachung der Zuordnung von logischen und physikalischen Adressen.
- Intrusion Detection Systeme wie `arpwatch` [Lab09] können ARP-Spoofing ebenfalls feststellen.

Passwörter knacken: Bruteforce und Wörterbuchangriffe

Haben Sie schwache Passwörter im Einsatz?

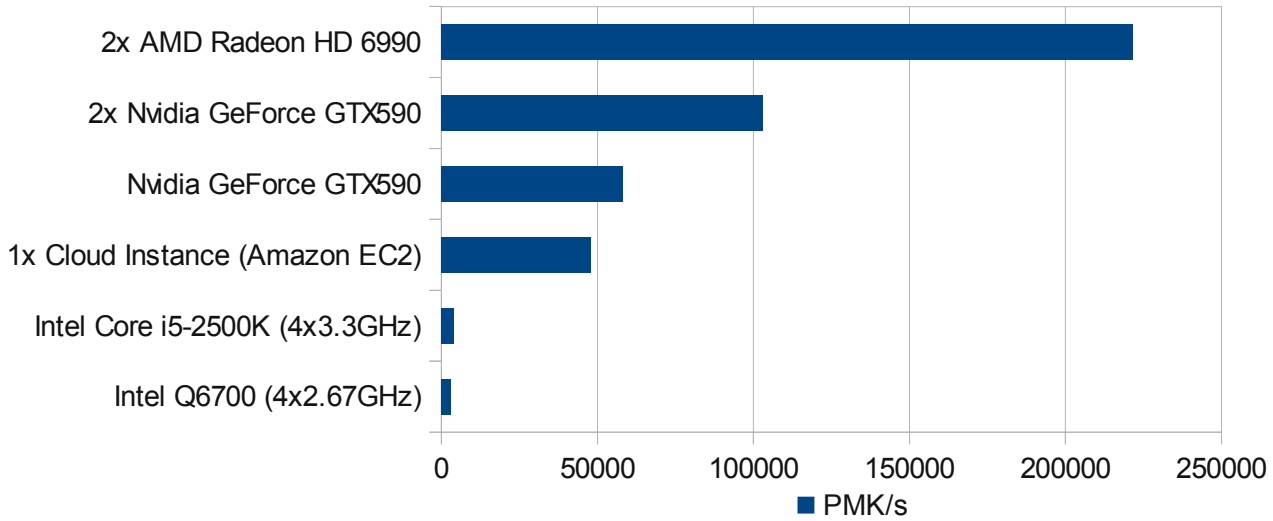
Viele Unternehmen und auch Privatpersonen verwenden **schwache** Passwörter, z.B.

- **Kurzes** Passwort (6-7), wenige mögliche **Zeichen** (z.B. nur Ziffern)
- Passwort basiert auf **Wort** ($\in$ Wörterbuch) oder **Schema** (z.B. `Andreas82`)

Der Hacker hat grundsätzlich zwei Möglichkeiten:

- **Bruteforce**. *Alles durchprobieren!*
- **Wörterbuchangriff**. *Die häufigsten (z.B. deutschen) Wörter ausprobieren.*

Mit **GPU**- und **Cloud-Computing** geht das Knacken dabei noch schneller...



WPA-Crack: Pairwise Master Keys (PMK) pro Sekunde [Ku11]

Die Identität des Computers stehlen

Einige Dienste verwenden (*immer noch...*) Adressen zur Identifizierung der Endgeräte:

- **Logische IP-Adressen**, denn unser DHCP-Server kümmert sich ja darum, dass jeder die richtige IP-Adresse bekommt...
  Beispiele: Spezielle Firewallkonfiguration, NFS, Host-based SSH, ...
- **Physikalische MAC-Adressen**, denn diese sind ja nicht fälschbar (Mythos™), oder...?
  Beispiele: MAC-Filter im Accesspoint, spezielle Firewallkonfiguration, ...

```
# ifconfig eth0
eth0  Protokoll:Ethernet Hardware Adresse 54:01:be:72:f5:91
      inet Adresse:192.168.0.1 Bcast:192.168.0.255 Maske:255.255.255.0
      ...
```

Linux Konsole: Adressen von Netzwerkkarte (eth0) anzeigen

```
# ifconfig eth0 192.168.13.37 hw ether 00:11:22:33:44:55
# ifconfig eth0
eth0  Protokoll:Ethernet Hardware Adresse 00:11:22:33:44:55
      inet Adresse:192.168.13.37 Bcast:192.168.0.255 Maske:255.255.255.0
      ...
```

IP und MAC-Adresse auf beliebige Werte ändern aka. Hacker-Magic ☺

Gegenmaßnahme? Setzen Sie bei Sicherheitskonzepten nicht auf Adressen! ☠☠☠

Dienste blockieren: Denial of Service (DoS)

Denial of Service (DoS) bedeutet, dass ein Dienst von seinem regulären Betrieb abgehalten wird. Mehrere Möglichkeiten, z.B.

- **Auslasten der Netzwerkverbindung**
  Dies ist eher unüblich in LANs, da oftmals keine großen Bandbreitenunterschiede bestehen.

  Beispiele: *Floodping, UDP-Flooding, ...*
- **Auslasten der Resourcen**
  Hier geht es um die Resourcen auf dem Zielsystem oder im Netzwerk, z.B. CPU, RAM, Festspeicher oder die Anzahl freier IP-Adressen.

  Beispiele: *SYN-Flooding, SSL/TLS DoS, DHCP-Flooding, ...*
- **Ausnutzen eines Konzept- oder Implementierungsfehlers**
  In komplexer Software gibt es oft den ein oder anderen Fehler... Noch schlimmer ist es, wenn es Konzeptfehler sind, die sich oftmals nicht einmal beheben lassen.

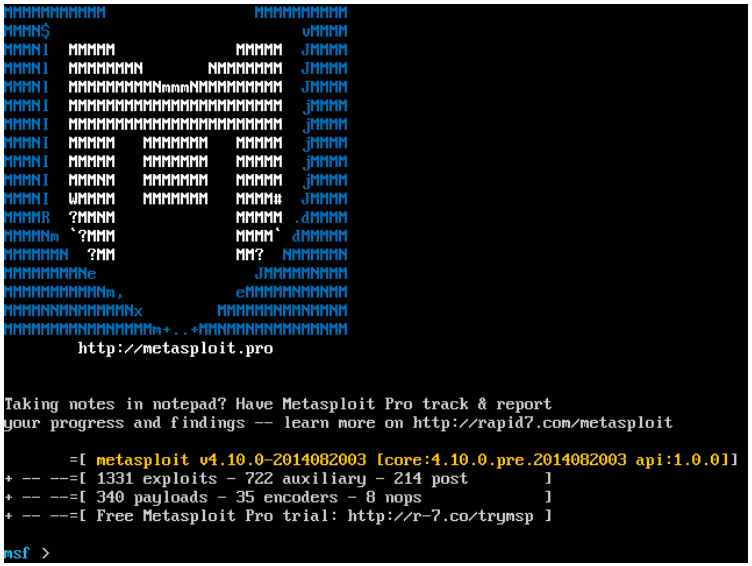
  Beispiele: *DoS mit ARP-Poisoning, IPv6-Floodrouter, Netbios-Nuke (Win95), ...*

Distributed Denial of Service (DDoS) und Gegenmaßnahmen

Greifen mehrere Endgeräte (z.B. gesteuert von einem Angreifer) ein Ziel an, so nennt man das DDoS. In lokalen Netzen tritt soetwas sehr selten auf.

Gegenmaßnahme: *Halten Sie Ihre Software aktuell! Einige Angriffe werden zudem auch von Intrusion Detection Systemen (IDS) erkannt.*

Fremde Systeme kompromittieren



Penetration Testing Tool: `metasploit` [Rap16]

Schwachstellen ausnutzen...

Wenn ein Programm auf einem System über eine **Schwachstelle** (*z.B. möglicher Pufferüberlauf*) verfügt, kann das System in manchen Fällen **vollständig** kompromittiert werden.

1. Hacker nutzt Schwachstelle (*z.B. Pufferüberlauf*) mit **Exploit** aus.
2. Der Exploit transportiert Schadcode (*z.B.* **Shellcode**)
3. Shellcode kompromittiert das System (*z.B. erzeugt Remotesteuerung*)

Klingt kompliziert, ist das schwer?

Das Finden **neuer** Schwachstellen, das Schreiben von Exploits und Shellcode benötigt viel Fachwissen und Erfahrung...

Das Ausnutzen **bekannter** Lücken ist mit Tools wie `metasploit` [Rap16] oder (noch einfacher) dessen grafischer Oberfläche `armitage` [LLC16] **für fast jeden möglich**. **Beste Gegenmaßnahme**: *Spielen Sie Sicherheitsupdates zeitnah ein!*

Alles auf einen Blick!

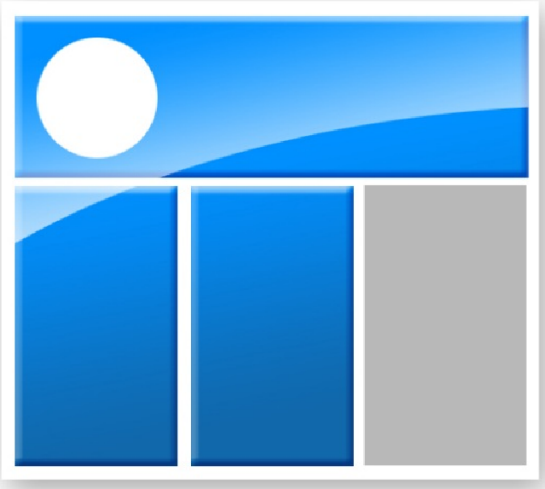
	Was war das Problem?	Gegenmaßnahme!
Zugang zum Netz	WLAN, Social Engineering	Gute Passwörter, kein WPS, Awareness gegen SE
Überblick im Netz	Portscanning und Security Scans	IDS
Kommunikation abhören/verändern	ARP-Spoofing, uvm.	Kommunikation Ende-zu-Ende verschlüsseln, IDS
Passwörter knacken	Schlechte Passwörter vs. schnelle Systeme	Gute Passwörter, z.B. Merksatz-Prinzip™
Adressen klauen	IP und MAC-Adressen lassen sich fälschen	Identifizierung nicht auf Basis von Adressen!
DoS	Überlast für Netz, Resourcen + Fehler	Updates installieren, IDS
Systeme kompromittieren	Schwachstellen in der Software	Updates installieren!

Zusammenfassung

Bild: *https://flickr.com, Mr. Robot (TV series)*

Lessons learned

1. Es gibt eine ganze Menge **Sicherheitsprobleme** in lokalen Netzen! Das war nur eine kleine Auswahl...
2. **Was kann ich dagegen tun?** Gute Passwörter verwenden und brav Updates installieren!
3. *Seid vorsichtig und habt Spaß!*



Vielen Dank für Ihre Aufmerksamkeit!

Literatur I

[Air16] Aircrack-ng Team.
Aircrack-ng Webpage, 2016.
https://aircrack-ng.org/.

[Hak16] HakShop.
USB Rubber Ducky Deluxe – HakShop, 2016.
http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe?variant=353378649.

[Ku11] Andrew Ku.
Praxis WLAN-Sicherheit: WPA mit CPUs, GPUs und Cloud geknackt, 2011.
http://www.tomshardware.de/WLAN-Einbruch-Hacken-Brute-Force,testberichte-240879.html.

Literatur II

[Lab09] Lawrence Berkeley National Laboratory.
Arpwatch - the ethernet monitor program; for keeping track of ethernet/ip address pairings.
http://ee.lbl.gov/, 2009.

[LLC16] Strategic Cyber LLC.
Armitage - Cyber Attack Management for Metasploit.
http://www.fastandeasyhacking.com, 2016.

[Lyo16] Gordon Lyon.
Nmap - Free Security Scanner For Network Exploration & Security Audits., 2016.
http://nmap.org.

Literatur III

[Mar16] Marc "van Hauser" Heuse.
THC-IPV6 - attacking the IPV6 protocol suite, 2016.
https://www.thc.org/thc-ipv6/.

[OV16] Alberto Ornaghi and Marco Valleri.
Ettercap Home Page.
https://ettercap.github.io/ettercap/, 2016.

[OVE16] OVERLOOKSOFT.
Fing Website, 2016.
https://www.fingbox.com/features.

[Rap16] Rapid7.
Penetration Testing Software — Metasploit.
https://metasploit.com, 2016.