7.2 Schwachstellen, Angriffe, Verteidigung

Generelle Problematik der Kommunikation im Netz:

- Absender hat keine Kontrolle über die abgesendete Nachricht
- Eintreffender Nachrichtenverkehr ist schwer zu kontrollieren

Maxime: Wenn du ganz sicher gehen willst,
geh *nicht* ans Netz!

Terminologie:

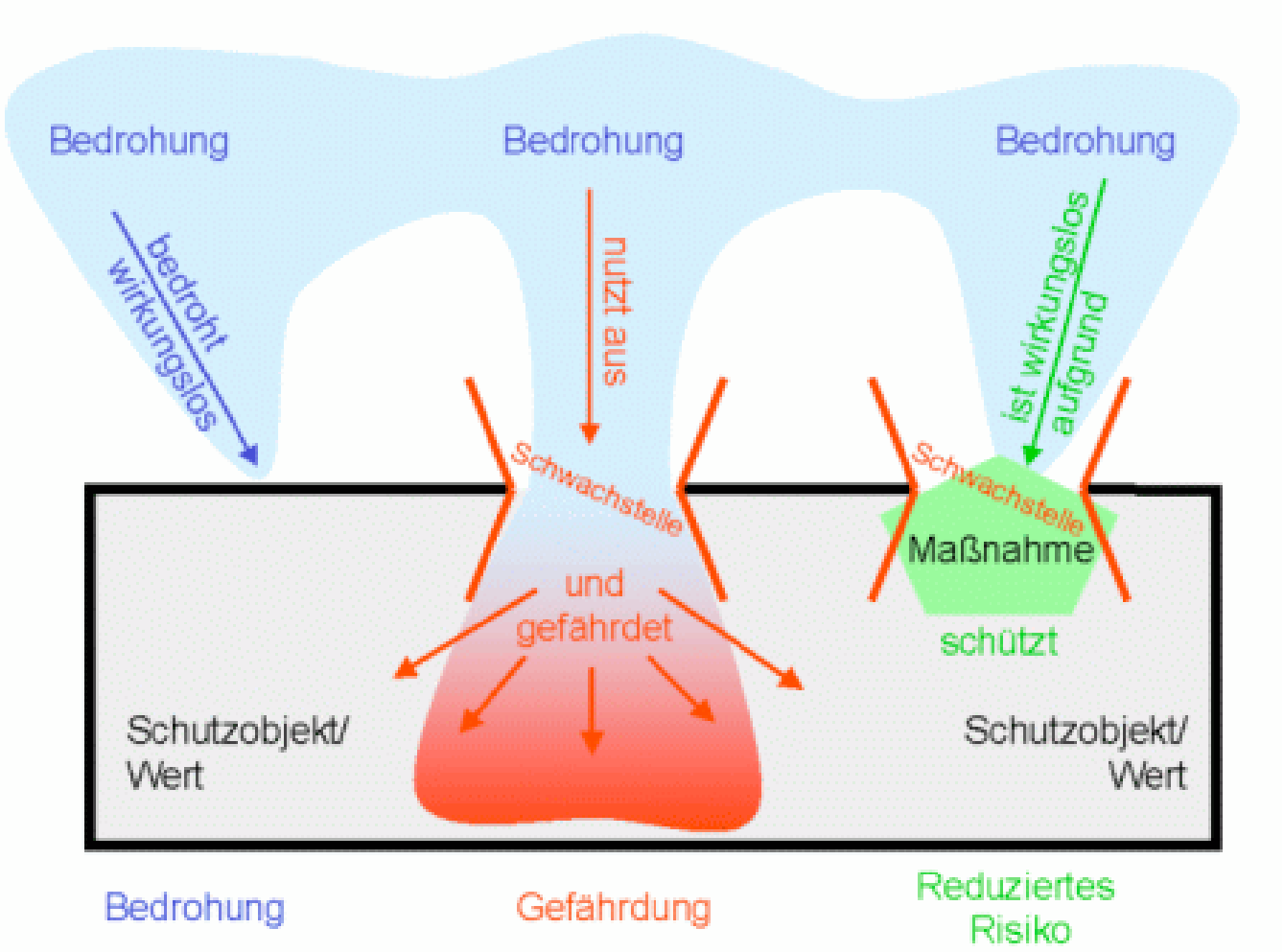
Angriff, Bedrohung *(attack, threat)*

liegt vor, wenn ein **Angreifer** versucht, ein Sicherheitsziel zu verletzen - z.B. den Inhalt einer vertraulichen Nachricht zu lesen. Gelingt ihm dies,

so liegt eine **Schwachstelle, Sicherheitslücke** *(vulnerability)* vor - z.B. die Nachricht konnte zwischen Sender und Empfänger abgehört werden und war nicht (oder nicht gut) verschlüsselt.

Schwachstellen sind *Nachlässigkeiten* der Benutzer oder *Softwarequalitätsmängel* (Entwurf und/oder Implementierung).

Sicherheitsmechanismen (z.B. Verschlüsselung) sind dann entweder konzeptionell unzureichend oder werden nicht richtig eingesetzt.



Terminologie des BSI - www.bsi.de/fachthem/sinet/gefahr/index.htm

„Bedrohung + Schwachstelle = Gefährdung"

Jargon: "Angriffe durch **Hacker**"

Der *CCC*: "Wir sind Hacker, keine **Cracker**!"

Anspruch: "Wir entdecken Schwachstellen, nutzen sie aber nicht kriminell aus."

Im Englischen zur Verdeutlichung auch *ethical hacking.*

Die Übergänge zwischen "Hacker" und "Cracker" sind fließend.

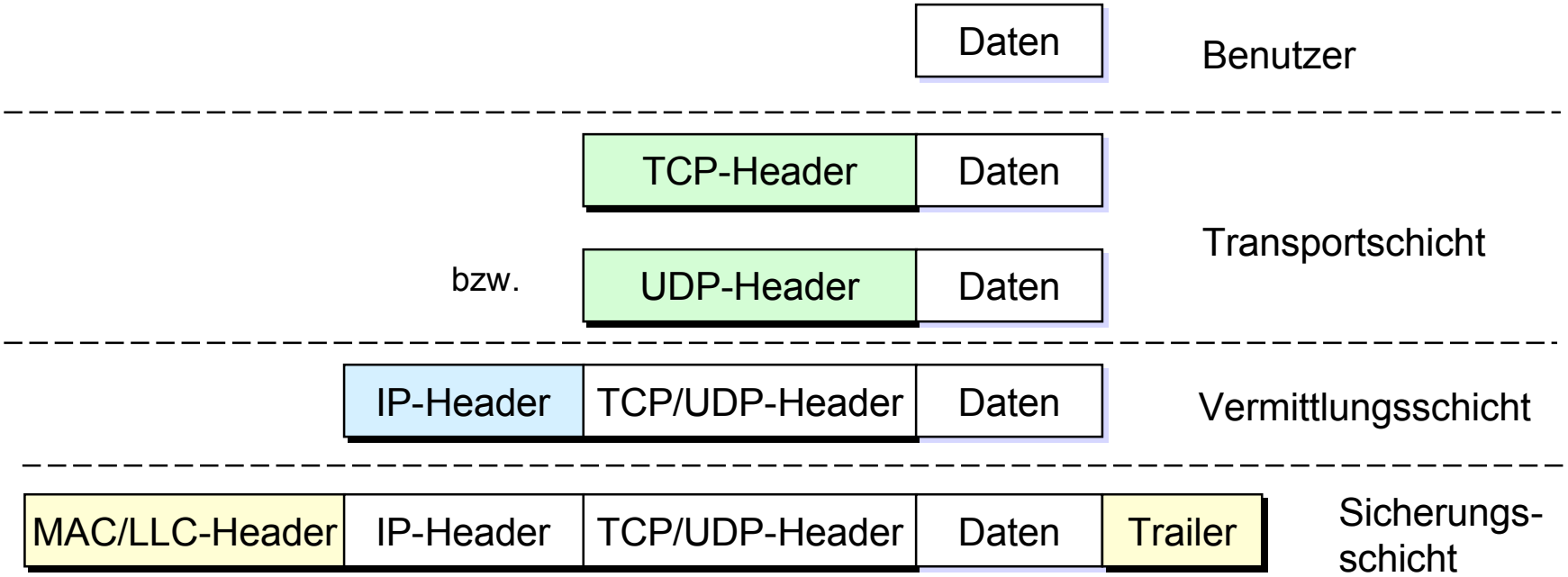
Empfehlenswert: "Hacker" bei Wikipedia.

Angreifer benötigt

- *Kenntnisse* von
  - Betriebssystemen
  - Netzinfrastruktur
  - Quellcode von System- und Anwendungssoftware
- *Rechte*, typischerweise Systemzugang als
  - Normalbenutzer
  - Systemverwalter
  - Systementwickler
- evtl. *physischen Zugang*
  - zum Übertragungsmedium
  - zum Rechner, Router, ...

Zur Erinnerung: Protokolle und Dienste im Internet

- IP leitet Datenpakete durch das Netzwerk zur Empfängerstation
- TCP/UDP fügen Prozessadressierung (Ports) zu IP hinzu
- TCP garantiert darüber hinaus einen zuverlässigen Byte-Strom
- Protokolldateneinheiten (PDUs) werden gekapselt



(Quelle: H. Ritter, Telematik, WS 05/06)

Klient	Dienst	Port	Prot.	Socket	Login	Programm
daytime	daytime	13	tcp/udp	stream	root	daytimed
ftp	ftp	21	tcp	stream	root	ftpd
ssh	ssh	22	tcp	stream	root	sshd
telnet	telnet	23	tcp	stream	root	telnetd
mailtool	smtp	25	tcp	stream	root	sendmail
tftp	tftp	69	udp	dgram	root	tftpd
browser	http	80	tcp	stream	root	httpd
rlogin	login	513	tcp	stream	root	rlogind
rsh	rsh	514	tcp	stream	root	rshd
rcp						
.....						

(meist in /usr/sbin)

Typische Mechanismen für die Netzsicherheit:

Kryptographie: Verschlüsseln, Signieren, MACs

Firewalls: partielle Abschottung von Endsystemen oder Teilnetzen vom Internet

Intrusion Detection: Einbruchserkennung (wenn schon nicht -verhinderung)

Sicherheit der Endsysteme nicht vergessen:

- ☛ Sicherheitsmechanismen der Endsysteme richtig einsetzen
  - z.B. codebasierter Java-Zugriffsschutz
- ☛ Software-Qualitätsmängel im Endsystem können Schwachstellen bedeuten (z.B. Pufferüberlauf, 5.4.1←)

Zur Erinnerung:

Das Internet ist extrem gut abgesichert gegen technische Fehler - nicht aber gegen unerwünschte Manipulationen durch entschlossene und kompetente Angreifer !