Attacken auf Computersysteme

Patrick Kosiol

Vortrag im Rahmen der Veranstaltung
Sicherheit in Rechnernetzen II

HOCHSCHULE harz
Hochschule für angewandte Wissenschaften (FH)

28.01.04

Gliederung

- Motivationen der Angreifer
- Prinzipielle Abläufe der Angriffe
- Angriffstechniken
- Fazit

Motivation der Angreifer

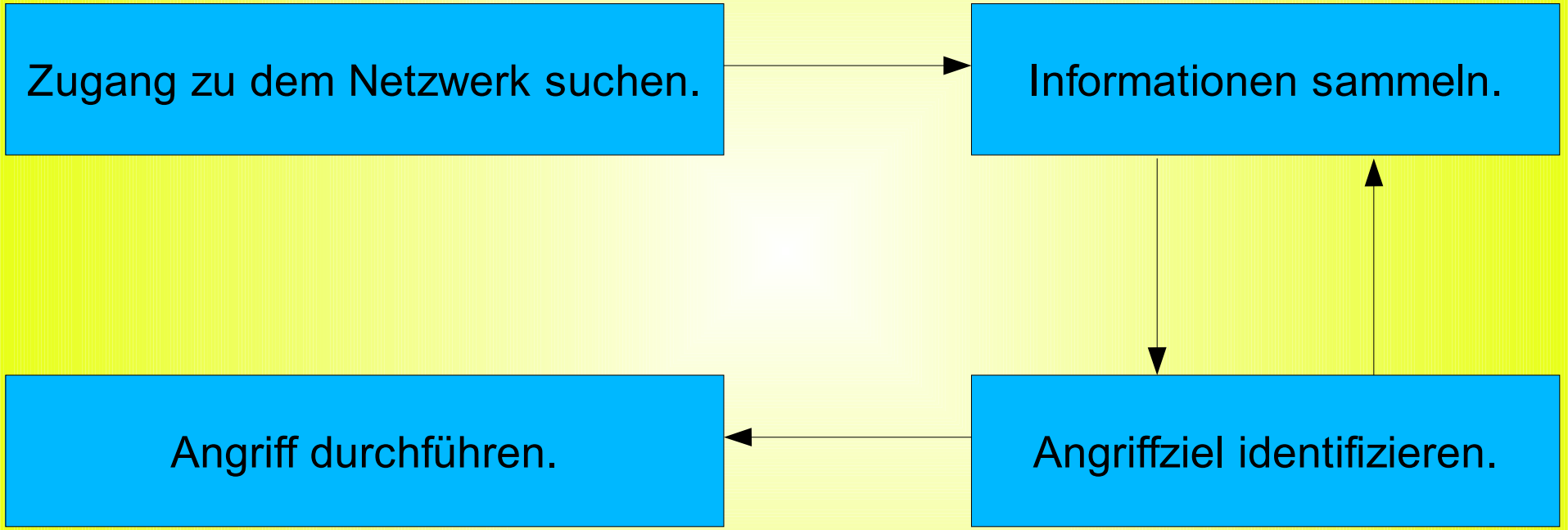
Zwei grundsätzliche Kategorien:

- Freizeit – Hacker
- Profitorientierte Hacker

Offerieren ihre verschiedenen Ziele.

Lösungsmöglichkeiten können entwickelt werden.

Prinzipielle Abläufe der Angriffe



Abläufe müssen effektiv gestört werden!

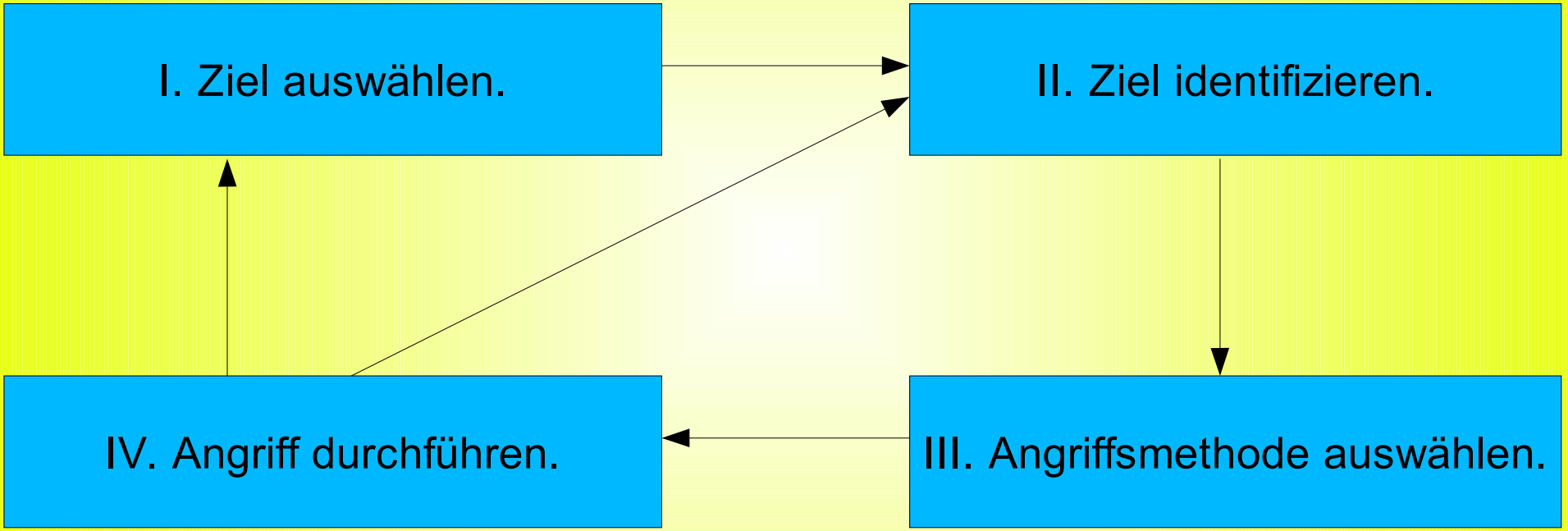
Wege der Hacker

- Über einen Rechner in dem anzugreifenden Netzwerk
- Per Remote Control (z.B.: DialUp o.ä.)
- Via Internet
- Durch direktes Verbinden zum Netzwerk (z.B.: WLAN)

→ Grenzen von Netzwerken → müssen geschützt werden!

→ Firewallsysteme

Angriffszenario



Je mehr Informationen der Hacker erlangt, desto mehr kann er seine Angriffe ausdehnen!

Zuhören und Mitschneiden von Daten

- Passwörter sniffen
- Analysieren des Netzwerkverkehrs
- Scannen von Netzwerkadressen und deren Ports
- IP Half–Scan Attack
- IP / ARP Spoofing
- ...

Denial of Service

- Distributed DoS
- Ping of Death
- SYN / LAND Attack
- Ping (ICMP) Flood & Smurf Attack
- UDP Bomb / UDP Flood
- ...

Fazit

- Geringe Auswahl an Angriffen.
- Beliebt → Viel genutzt.
- Firewallsysteme können die Gefahr reduzieren.
- Admin muss aktuelle Informationen haben.
- Gut konfigurierte Firewalls.
- Gleichgewicht zwischen Sicherheit und Dienste-anforderung finden.

Vielen Dank für Ihre Aufmerksamkeit!

Patrick Kosiol