Begrüßung & zur Sicherheitslage

Sicherheitstage SS 2006

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

14.06.2006

Programm - Änderung

Mittwoch 14.6.

09:15-11:00 Begrüßung & zur Sicherheitslage
11:15-12:15 Firewall-Schutz für Institute
12:15-12:30 Abwehr von SSH-Bruteforce-Angriffen I

Donnerstag 15.6.

09:00-09:30 Abwehr von SSH-Bruteforce-Angriffen II
09:30-10:45 Netfilter / IP-Tables
11:15-12:45 Sicherheit unter Linux
14:00-17:00 Workshop zu Linux

Freitag 16.6.

09:15-10:15 Digitale Zertifikate von der UH-CA
10:15-10:45 Sophos
11:15-12:00 Puremessage, Sophos unter Linux
12:00-12:45 Abschlussdiskussion & Fragen

Vorfälle/Statistik

Bedrohungslage:

- Angriffe
- Kommerzialisierung
- BOT-Netze
- Rootkits

mobile Rechner:

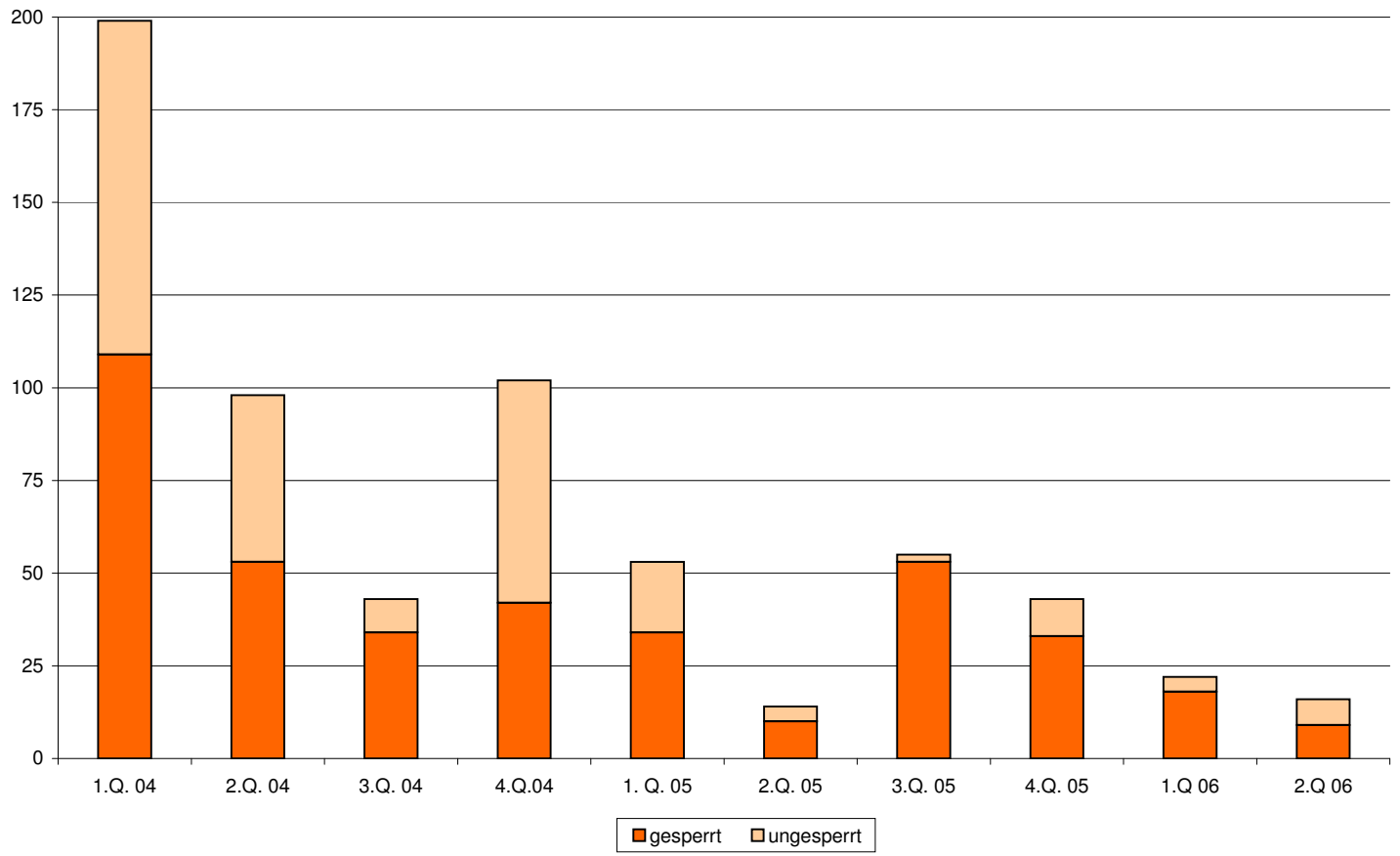
- allgemein
- UH-WLan

Dienste des RRZN

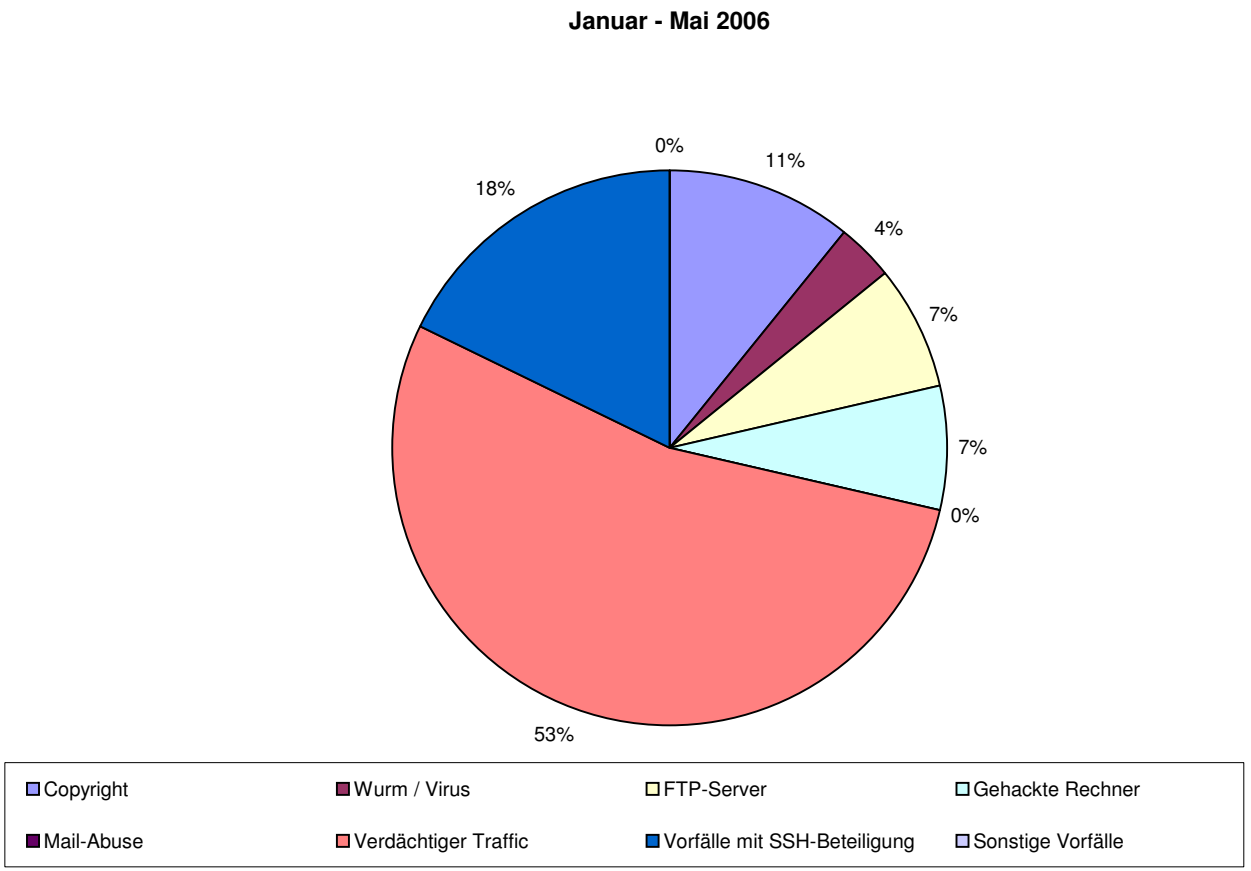
Organisatorisches

R|R|Z|N

Anzahl und Sperrungen



Vorfallsarten



Typische Probleme

- erratene Passwörter (Bruteforce)
  $\longrightarrow$ Zugriff reicht, lokale Exploits meist einfach
- gleiche Passwörter auf mehreren Systemen
  $\longrightarrow$ „Durchwandern“, größerer Schaden

- viele Dienste auf einem Server (Mail, Web, Fileserver)
  $\longrightarrow$ leichtes Eindringen, großer Schaden
- keine oder nur lokale Logs
  $\longrightarrow$ leicht fälschbar, unklarer Infektionszeitpunkt
- unklare Zuständigkeit / Konfiguration / Diensteangebot
  $\longrightarrow$ keine Updates / Passwortänderung / Neuinstallation ...

und natürlich Windows-Clients, Viren/Trojaner, Javascript, ...

Bedrohungslage: Angriffe

Schadsoftware

- Viren, Würmer ⟵ übermorgen bei Sophos
- social Engineering: Trojaner, Phishing
- BOT-Netze, Root-Kits ⟵ gleich

Bruteforce-Angriffe

- Portscan ⟵ morgen bei IP-Tables
- SSH-Loginversuche ⟵ heute bei SSH-Bruteforce
- Denial-of-Service, Spam-Mails

Netzangriffe

- Sniffing
- Spoofing (ARP, IP, DNS)
- Man-in-the-Middle

Bedrohungslage: Kommerzialisierung

Erpressung

- Verschlüsselung von Daten, Entschlüsselung gegen Geld:
  Troj/Zippo-A; PGPCoder: Forderung 200 Euro

```
Some files are coded.
To buy decoder mail: n781567@yahoo.com
with subject: PGPcoder 000000000032
```

- Androhung von dDoS $\longrightarrow$ Schutzgeld

„Dienstleistung“

- Spam-Versand
- Computersabotage bei Konkurrenten (z.B. DoS)
- Änderungen beim Google-Ranking
- allgemeiner: Bot-Vermietung

Phishing

BOT-Netze

- Rechner wird nach Infektion zu ferngesteuertem „Bothost“
- Infektionsweg wie üblich, bleibt aber unbemerkt
- Bothost wartet auf Kommandos
  - häufig per IRC, teilweise P2P-Protokolle,
    Bothost meldet sich bei IRC an (Firewall evt. unwirksam)
  - meist verschlüsselt
  - IRC-Server/Master heißen „C&C-Host“ (Command&Control)
- Botnet: Sammlung von Bothosts (bis zu 1.5 Millionen)
- Einsatzzweck:
  - Selbstzweck: Weiterverbreitung, Code-Update, ...
  - Spam-Versand, distributed Denial-of-Service (dDoS), ...
- Bots dienen zunehmend kommerziellem Interesse

R|R|Z|N

allgemeine Eigenschaften

verstecken vor den normalen Tools & Benutzern

- Dateien
- Prozesse / Daemons
- Netzwerkverbindungen

und damit

- sich selbst
- ihre Schadfunktionalität

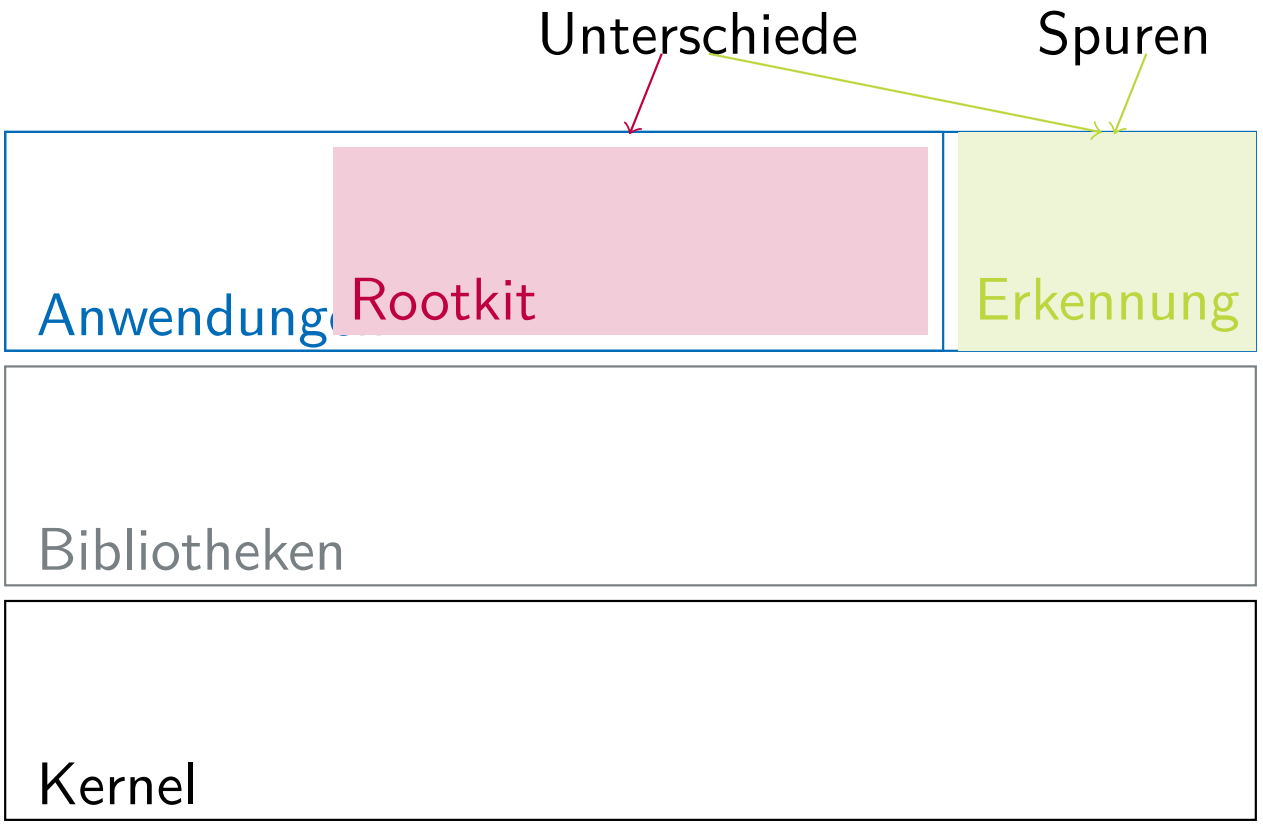
$\longrightarrow$ ähnlich Stealth-Viren, nur umfassender

- erste Rootkits waren für Unix
- inzwischen Mehrzahl für Windows

R|R|Z|N

erste Rootkits

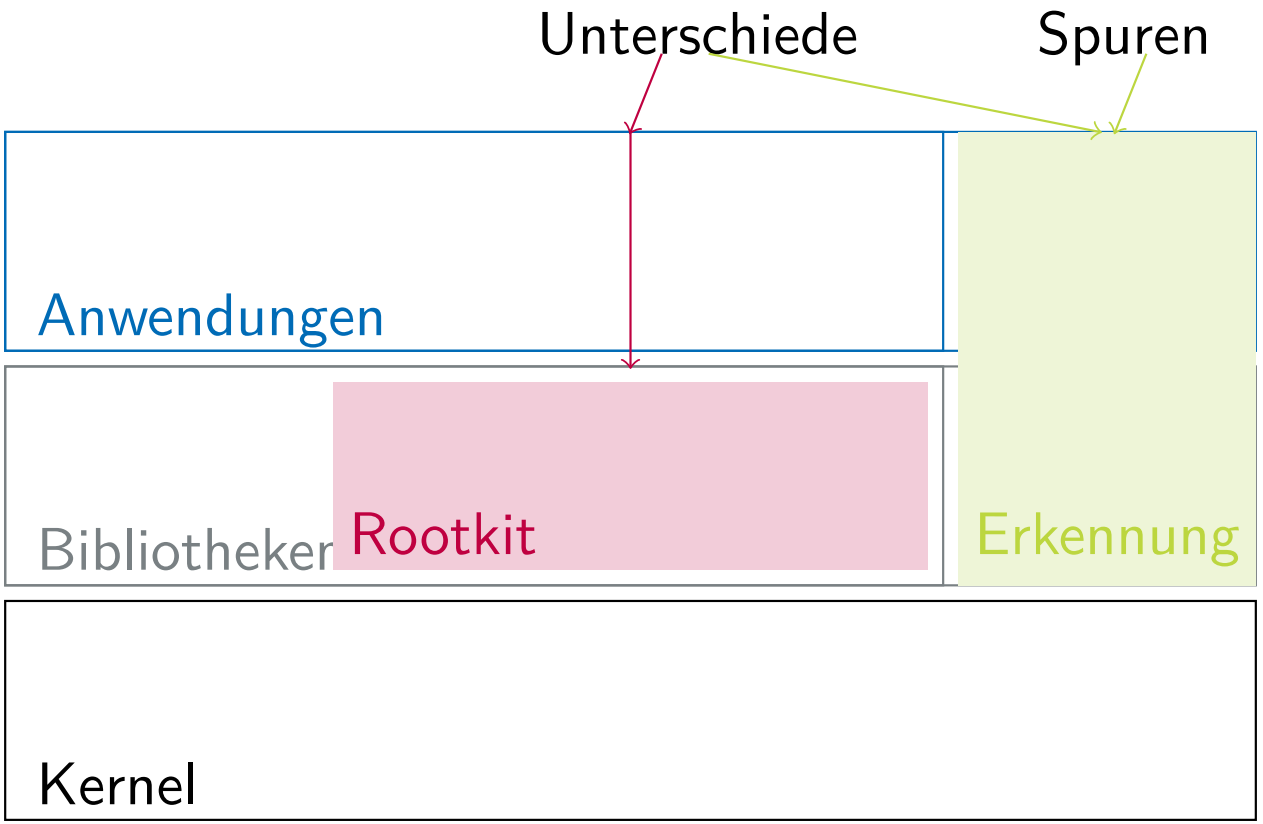
- Anwendungen / Utilities werden ersetzt (z.B. `ls`)
- Erkennung durch Nutzung anderer Utilities (z.B. perl-Skript)



R|R|Z|N

ältere Rootkits

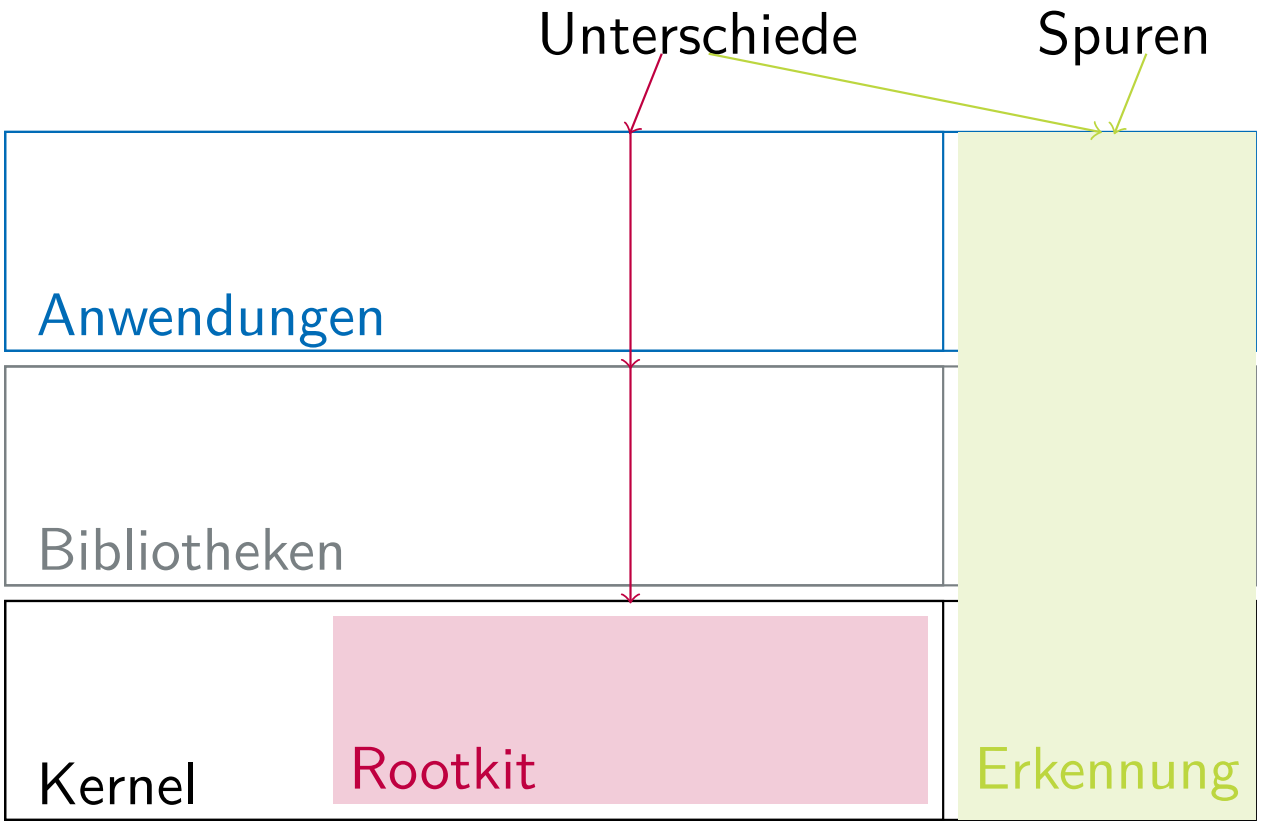
- Bibliotheken werden ersetzt (z.B. File-Funktionen)
- Erkennung durch Umgehung von Bibl. (z.B. statisch gelinkt)



R|R|Z|N

aktuelle Rootkits

- Kernel wird verändert (z.B. Filesystem-API)
- Erkennung durch Kernel-Umgehung (Hardwarezugriff)



Rootkiterkennung

- Finden von Rootkit-Spuren aus sauberem System (Boot-CD), z.T. im laufenden System („SicherheitsLücken des Rootkit“)
- Vergleich Hardwaredirektzugriff mit Zugriff über OS
- Soll-Ist-Vergleich mit Prüfsummen
- Analyse des Netzwerkverkehrs

Tools

- Virenscanner (z.B. unter Win-PE, Knoppix)
- *Windows:* RootkitRevealer (Sysinternals, free), BlackLight (F-Secure, beta), Strider-Ghostbuster (Microsoft, Prototyp)
  Unix: `chkrootkit`, Rootkit Hunter; Tools-CD INSERT
- `tripwire` (Prüfsummen), `cfengine`; Backup-Compare-Lauf
- IDS / IPS, Log-Auswertung

Schutz vor Rootkits

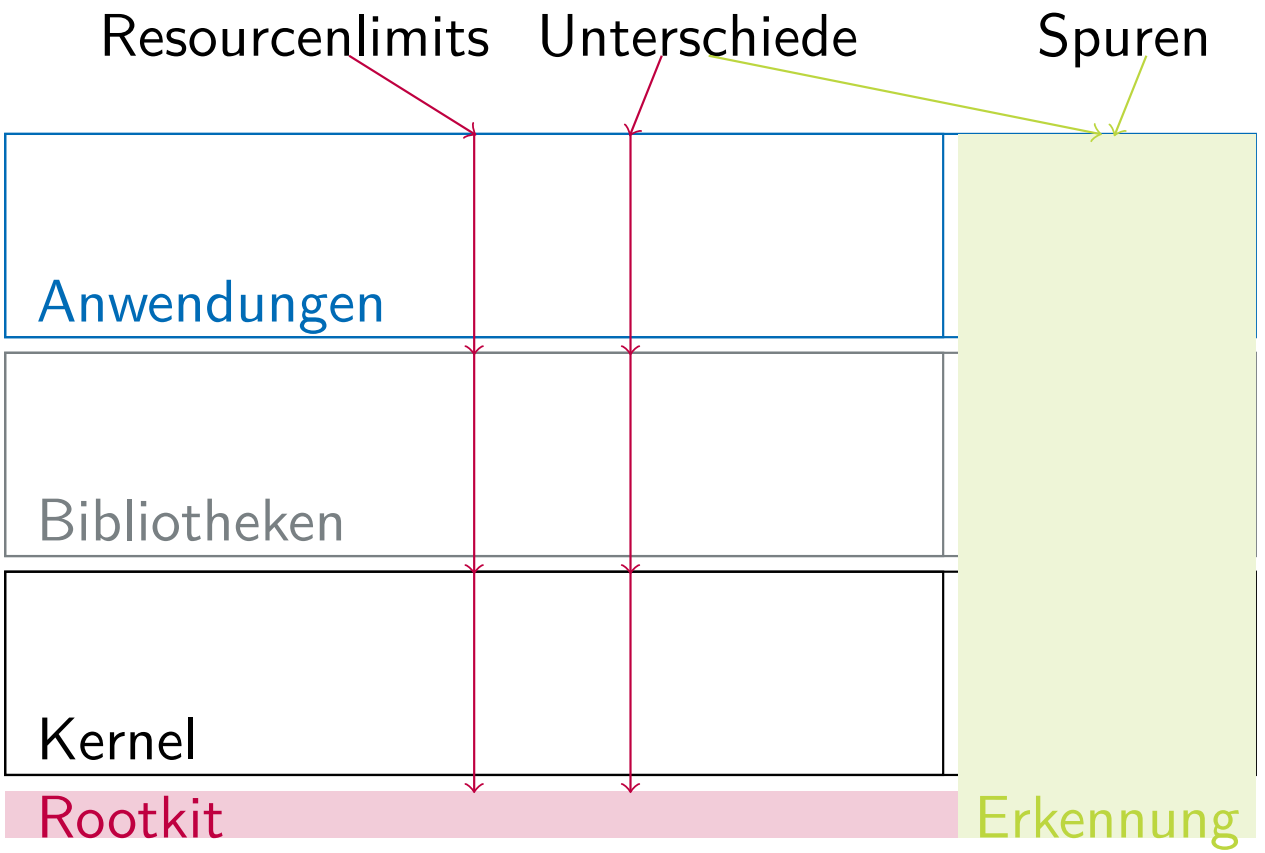
Infektionswege wie bei Spyware, Trojanern, Viren, ...

- regelmäßiges Update von System und Applikationen
- Virenschutz
- Firewall
- vorsichtiger Nutzer: Javascript, Mailanhänge, „Tools“
- OS-Design (z.B. SE-Linux):
  - unpriviligierte Kernelmodule / Treiber
  - kein Recht auf Kerneleingriff für root
  - frühzeitige, unwiederkehrbare Rechteaufgabe
  - Code-Signing

R|R|Z|N

zukünftige Rootkits

- System läuft in virtueller Maschine
- Erkennung von außerhalb; Resourcen/Verhalten



Rootkits auf Basis virtueller Maschinen (VMBR)

Stand

- bei heutigen Rechnern & Netzen unauffällig
- Proof-of-Concept existiert:
  `http://www.eecs.umich.edu/Rio/papers/king06.pdf`
- evt. Ausschalten nur simuliert (Standby)

Erkennung

- Boot von sauberem Medium (CD) nach Netztrennung
- Netzwerkverkehr
- Laufzeitreduzierung
- Resourcenlimits (z.B. Swapping bei RAM-Ausnutzung)

gute „Rootkits“

unter Verwendung von Rootkit-Technologie:

- Verbergen von Log-Dateien, Überwachungsdiensten
- Unumgehbarkeit durch tiefe Implementation, z.B.
  - Personal-Firewall
  - Virenscanner
- Dienste statt `chroot`-Jail in virtueller Maschine

Prinzip: tiefer ansetzen als eindringende Schadsoftware

besser: mobile Geräte

d.h. Notebook / Tablet-PC, PDA / Organizer, Mobiltelefon;
auch: Speichermedien, WLan / Irda / Bluetooth

Gefährdungen für mobile Geräte

- Notebook außerhalb des UH-Netzes
- veraltete Virenscanner- / Systemsoftware
- Diebstahl von Geheimnissen (Dateien, Passwörter)
- Verlust von Daten (fehlendes Backup)
- Ungeplante Netzverbindungen

Gefährdungen für Institute

- Umgehung von Firewalls
- Einschleppen von Schadsoftware
- unauthorisierte Nutzer / Geräte im Lan
  - Gerät: Ethernet-Dose, Brücke über WLan/Irda/Bluetooth
  - Nutzer: Admin-Zugang auf eigenem Notebook
- Diebstahl von Geheimnissen (z.B. Passwörter)

  z.B. auch Mail-Passwörter über POP3

R|R|Z|N

Maßnahmen

Übliches

mG,I: Sicherheitssoftware: Virenschutz, Personal-Firewall

mG,I: regelmäßige Updates

Besonderes

mG,I: Verwendung verschlüsselter Protokolle
I: wegen Mithörender am Lan, mG: wegen Verbindung über Internet

I: Autostart-Funktion deaktivieren

mG: Dateiverschlüsselung, keine Passwortspeicherung

mG: Gerätekennzeichnung, Kensington-Lock, Bios-Pw

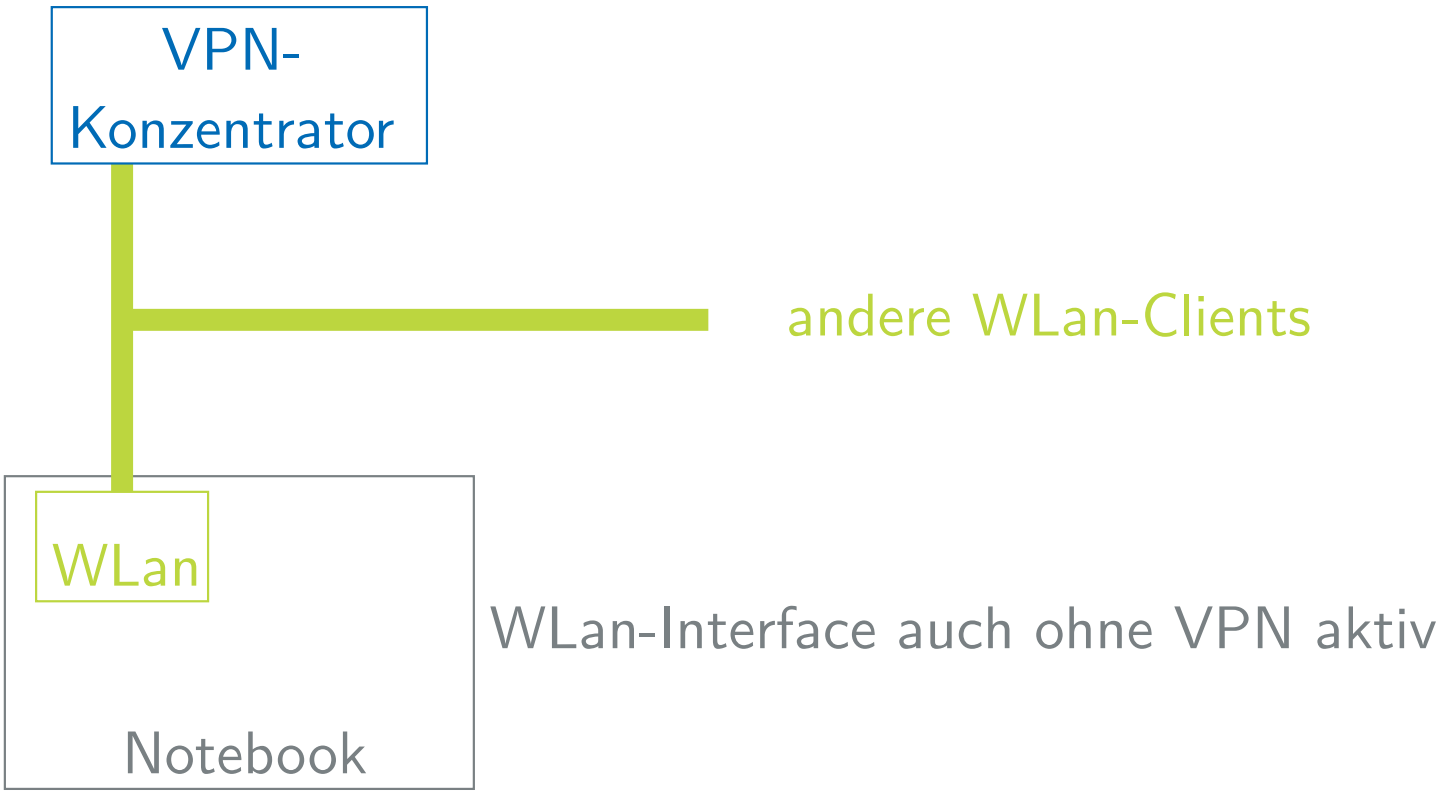
I: nur wenig Vertrauensvorschuss für Lan bzw. bestimmte IP

mG: Schnittstellendeaktivierung

R|R|Z|N

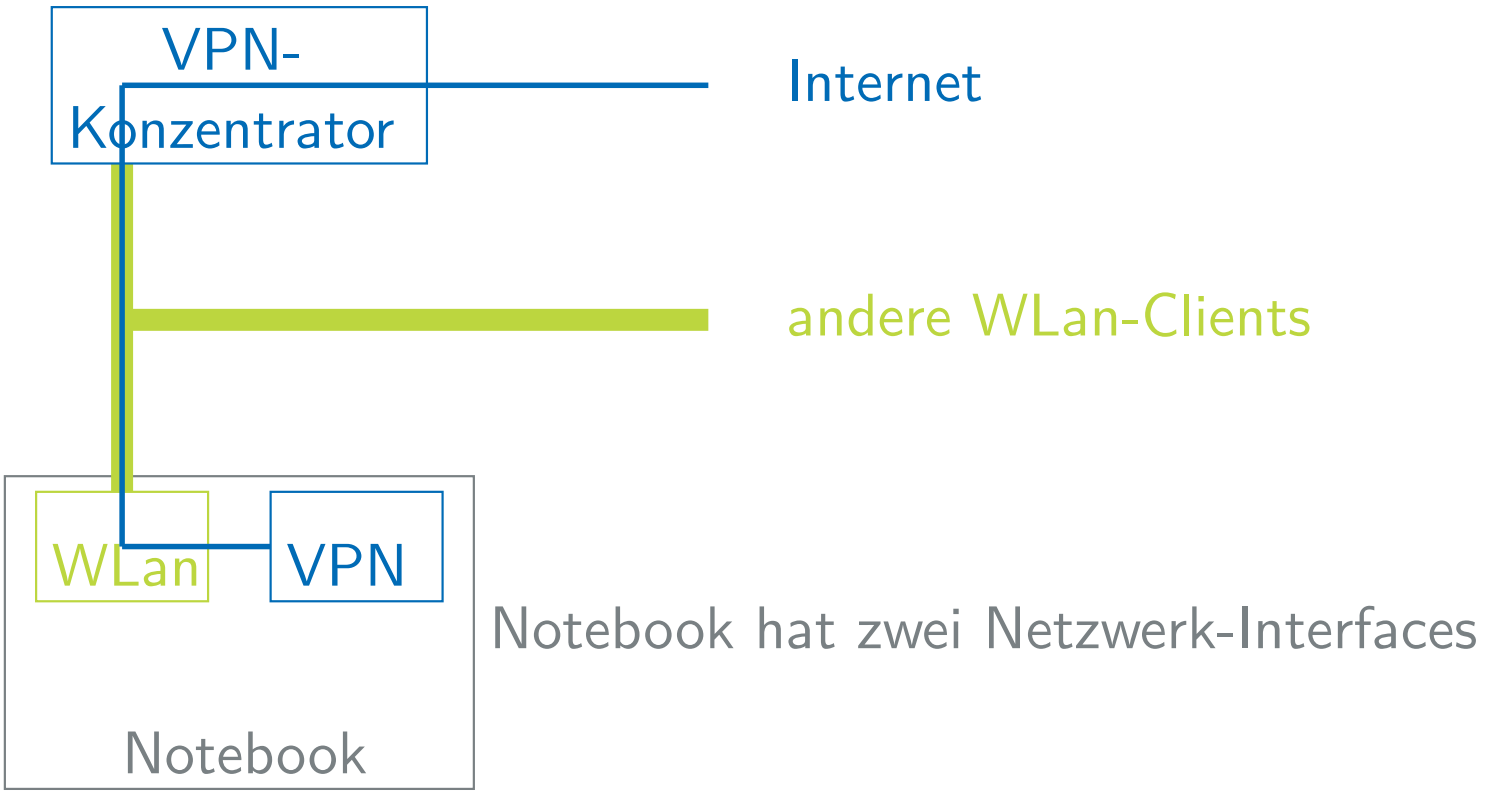
Netzwerkverbindungen

- unverschlüsselte Verbindung im lokalen WLan



Netzwerkverbindungen

- unverschlüsselte Verbindung im lokalen WLan
- verschlüsselter Tunnel mit VPN ins Internet



Bedrohungen

- lokales WLan `192.168.*` meist automatisch aktiv
- Schadsoftware anderer Clients kann angreifen,
  ggf. ohne Firewall-Schutz
- Clients können auch UH-Fremde ohne VPN-Zulassung sein
- Cisco-Client deaktiviert direkten WLan-Zugriff erst mit VPN

Schutz

- Deaktivierung WLan, fallweise Aktivierung
- Übliches: Updates, Virenscanner, Personal-Firewall, ...
- neue RRZN-Firewall-Policy:
  keine UH-fremden Zugriffe ins VPN

Angebot

- WSUS: Windows Update
- Sophos: Virenscanner
- Netzschutz: Firewall
- Mail: Puremessage, Serverbetrieb
- Archiv und Backup
- Webhosting (statische Inhalte)
- . . . mehr im Dienstleistungskatalog
  `http://www.rrzn.uni-hannover.de/rrzn_dlk.html`

Diensteauslagerung ans RRZN

Vorteil

- Dienstetrennung
- „größere“ Lösung, Kompetenzbündelung
- Kosteneinsparung
- Zeitersparnis

Nachteil

- Ferne, Reaktionszeit
- Beantragung, Umstellung
- evt. weniger Flexibilität wegen Standardisierung

R|R|Z|N

Security-E-Mail-Adressen

`security@rrzn.uni-hannover.de`

- Versand erfolgt signiert mit DFN-Zertifikat
  aber ggf. Warnung bei fehlendem CA-Zertifikat
- verschlüsselter Empfang möglich

`sec-`*`INST`*`@ou.uni-hannover.de`

- löst alte `security@`*`INST`*`.uni-hannover.de` ab
- B-Rundschreiben 42/2005 (inzwischen abgelaufen)
- unbedingt aktuell halten:
  - erstmalige Einrichtung bitte zurückmelden ($\frac{1}{4}$ steht aus)
  - Weiterleitungsziel(e) aktualisieren; ggf. löschen oder neu