Begrüßung & zur Sicherheitslage

Sicherheitstage WS 2006/2007

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

20.11.2006

Programm - Änderung

Montag 20.11.

09:15-10:00 IT-Sicherheit an der LUH
10:00-10:45 Zur Sicherheitslage
11:15-11:45 Windows-Imaging
11:45-12:45 Firewall-Schutz für Institute

Dienstag 21.11.

09:15-10:45 Windows-Richtlinien
11:15-12:45 Drucken im Netz

Mittwoch 22.11.

09:15-10:15 Digitale Zertifikate
10:15-10:45 Sophos & WSUS
11:15-12:00 Windows-Installation, Fernwartung
12:00-12:45 Abschlussdiskussion & Fragen

Donnerstag 7.12.

14:00-17:00 Workshop (separate Anmeldung)

Vorfälle/Statistik

Bedrohungslage:

- Angriffe
- Social Engineering
- Rootkits

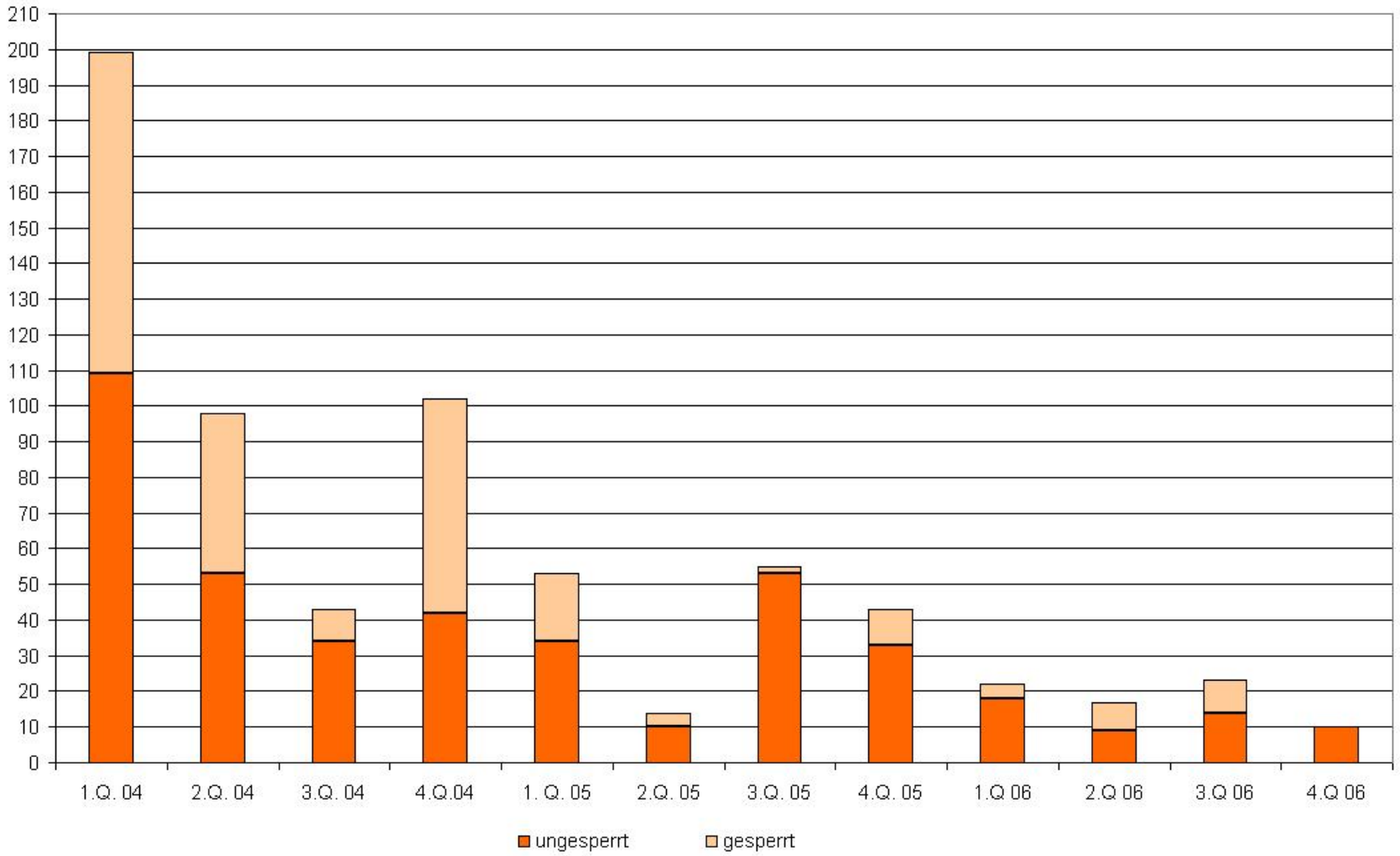
UH-WLan & VPN

Dienste des RRZN

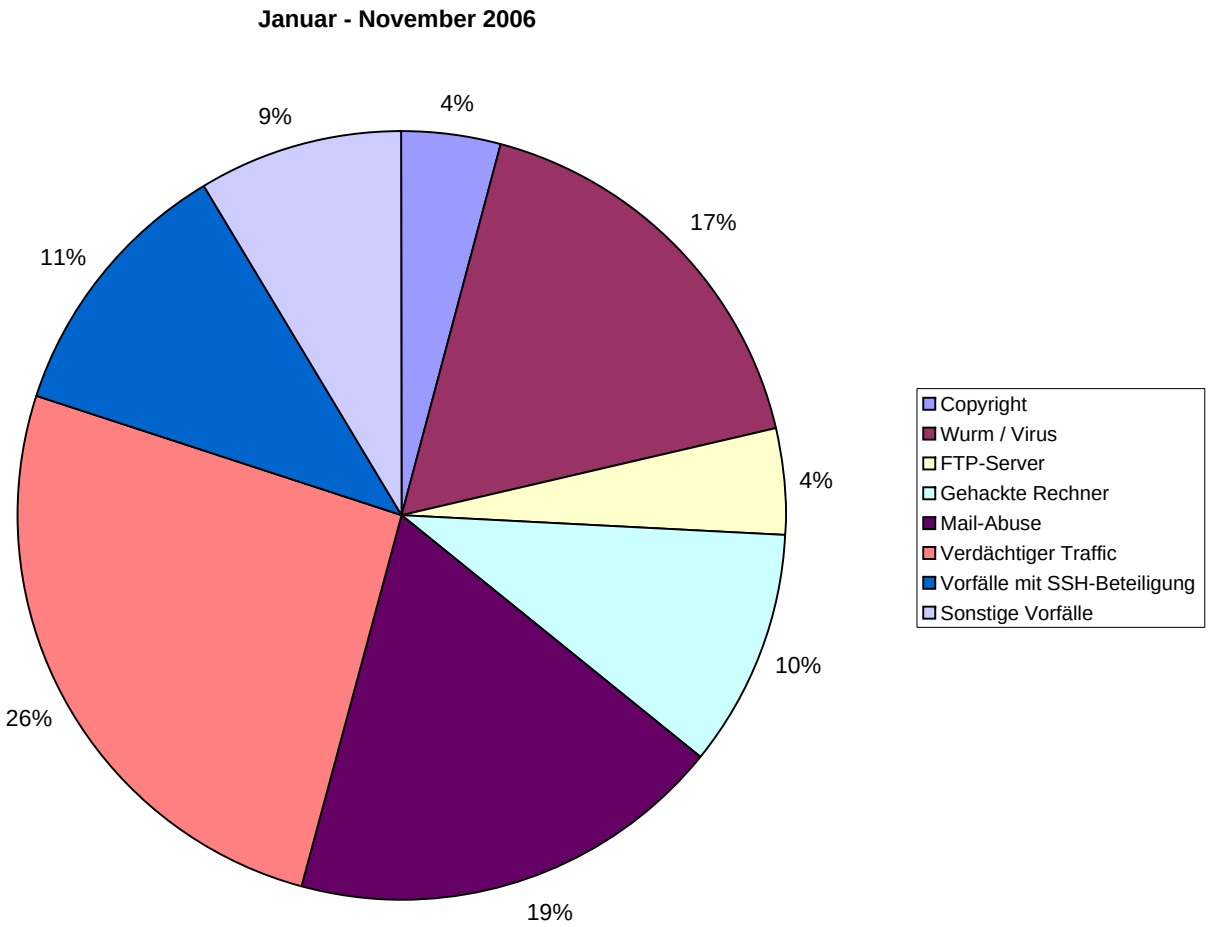
Organisatorisches

R|R|Z|N

Anzahl und Sperrungen

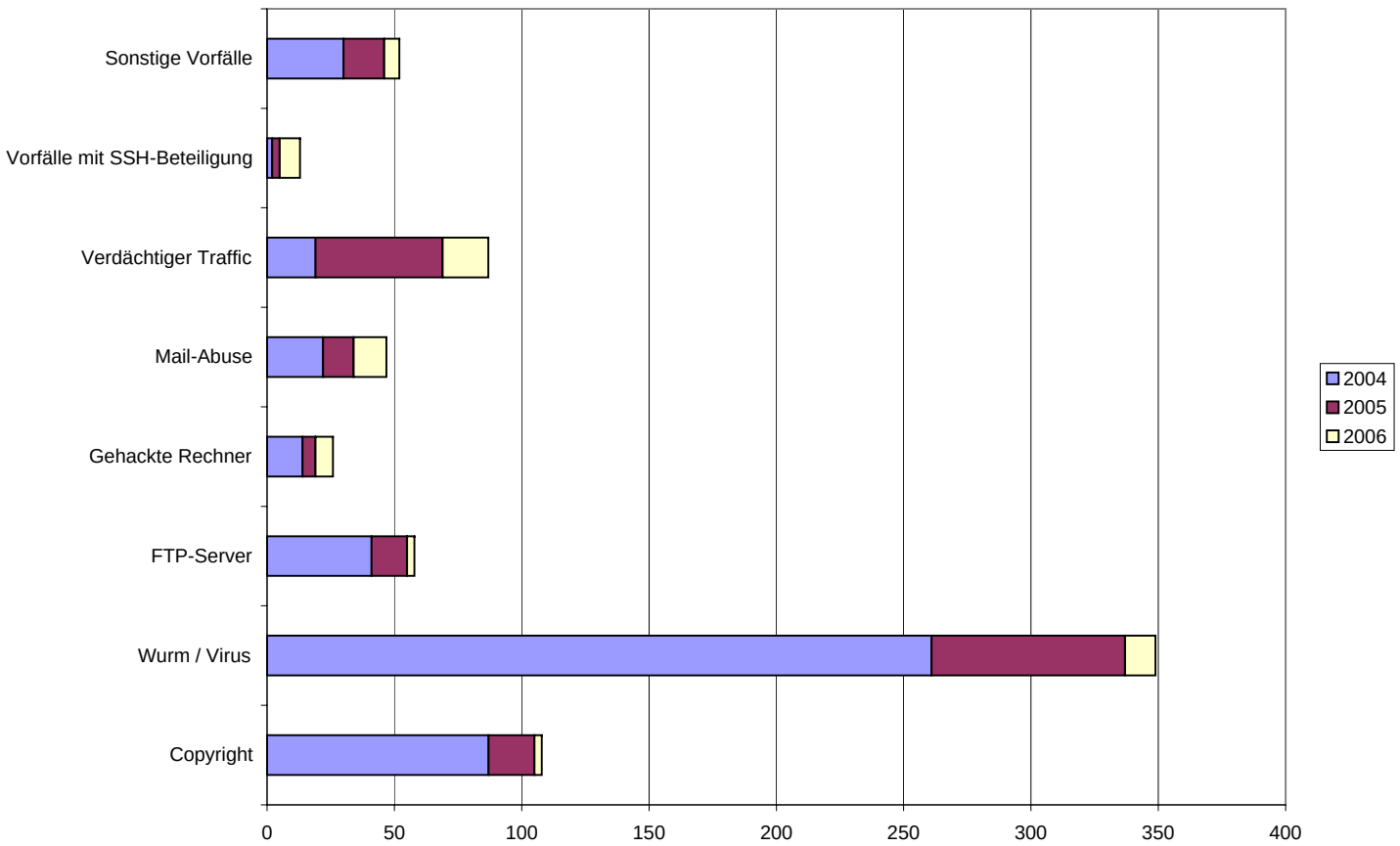


Vorfallsarten



R|R|Z|N

Vorfallsarten – Änderung



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 Sophos
- social Engineering ⟵ gleich; morgen Richtlinien
- BOT-Netze, Root-Kits ⟵ gleich

Bruteforce-Angriffe

- Portscan ⟵ heute Netzschutz
- SSH-Loginversuche
- Denial-of-Service, Spam-Mails

Netzangriffe

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

R|R|Z|N

Beispiel: Locken auf Webseite

> Eine nicht naeher beschriebene Schwachstelle im Microsoft Agent bei der Verarbeitung von .ACF Dateien (Microsoft Agent Character Datei) ermoeglicht einem entfernten Angreifer die Ausfuehrung beliebigen Programmcodes. ACF-Dateien koennen z.B. zur Gestaltung einer Webseite als interactive, animierte Objekte eingebunden werden. *Der Angreifer muss zur Durchfuehrung seines Angriffs sein moegliches Opfer daher auf eine manipulierte Webseite locken.*Die erfolgreiche Ausnutzung der Schwachstelle ermoeglicht einem entfernten Angreifer die Ausfuehrung von Programmcode von entfernten Standorten aus. Ist der Benutzer am Opfer-System mit administrativen Rechten angemeldet, so ist eine vollstaendige Kompromittierung des Opfer-Systems moeglich.
>
> (Auszug Warnmeldung CB-K06/1156)

- Angriff beginnt meist mit Spam oder gezielter Mail.
- Bei gezieltem Angriff vorher Analyse des Opfersystems und Auswahl geeigneter Schwachstellen.

Bedrohungslage: Social Engineering

R|R|Z|N

Unwissenheit

- unsichere Einstellungen im Browser / Mailprogramm
- Word-, Power-Point-Dateien etc. per Mail / Web

Neugier

- USB-Sticks, CD-ROMs
- Öffnen von Mails / gefährlichen Dateiformaten

Gutgläubigkeit

- Trojaner & Spyware: „Utilities“ aus dem Netz
- Anfragen per Mail

. . . auf dem Vormarsch, häufig mit ▸ BOT -Installation

R|R|Z|N

allgemeine Eigenschaften

verstecken vor den normalen Tools & Benutzern

- Dateien
- Prozesse / Daemons
- Netzwerkverbindungen

und damit

- sich selbst
- ihre Schadfunktionalität

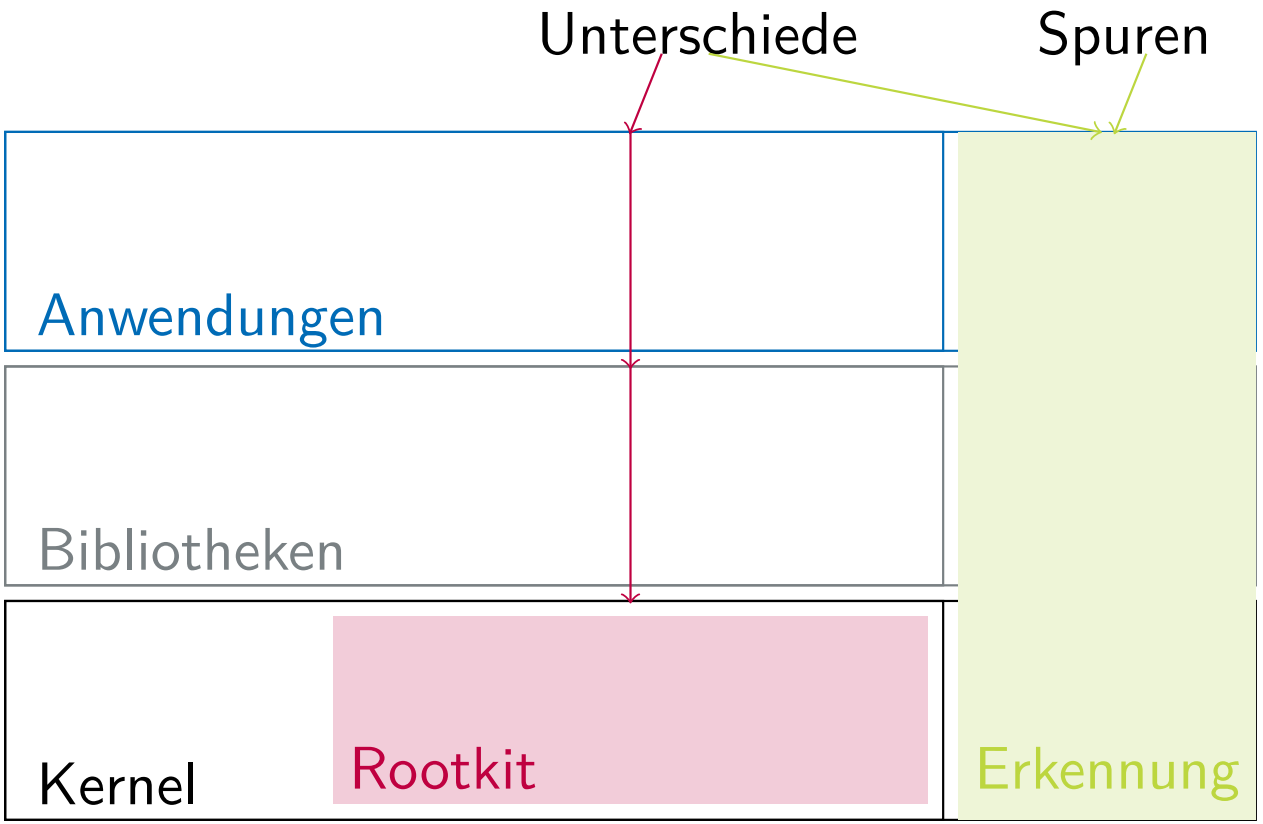
$\longrightarrow$ ähnlich Stealth-Viren, nur umfassender

- erste Rootkits waren für Unix
- inzwischen Mehrzahl für Windows

R|R|Z|N

aktuelle Rootkits

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



R|R|Z|N

Rootkitdemo

HackerDefender

- Open-Source-Rootkit inkl. Backdoor
- 296 kB inkl. Doku; Source (Assembler,C,Delphi) ca. 94 kB
- Konfiguration über Ini-Datei, ein-/ausschaltbar, als Dienst
- versteckt Dateien, Registrykeys, Prozesse, Dienste, Ports, die mit speziellem String beginnen (z.B. `hxdef...`)
- Backdoor:
  - benötigt keine extra Ports: auf allen Ports wird nach einem speziellen Schlüsselwort gesucht
    $\longrightarrow$ durch Portscan nicht auffindbar
- Redirector:
  - bzgl. Opfer-Ports wie Backdoor
  - Windows-Client auf Hackerseite lenkt Netzwerkverkehr um

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

R|R|Z|N

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

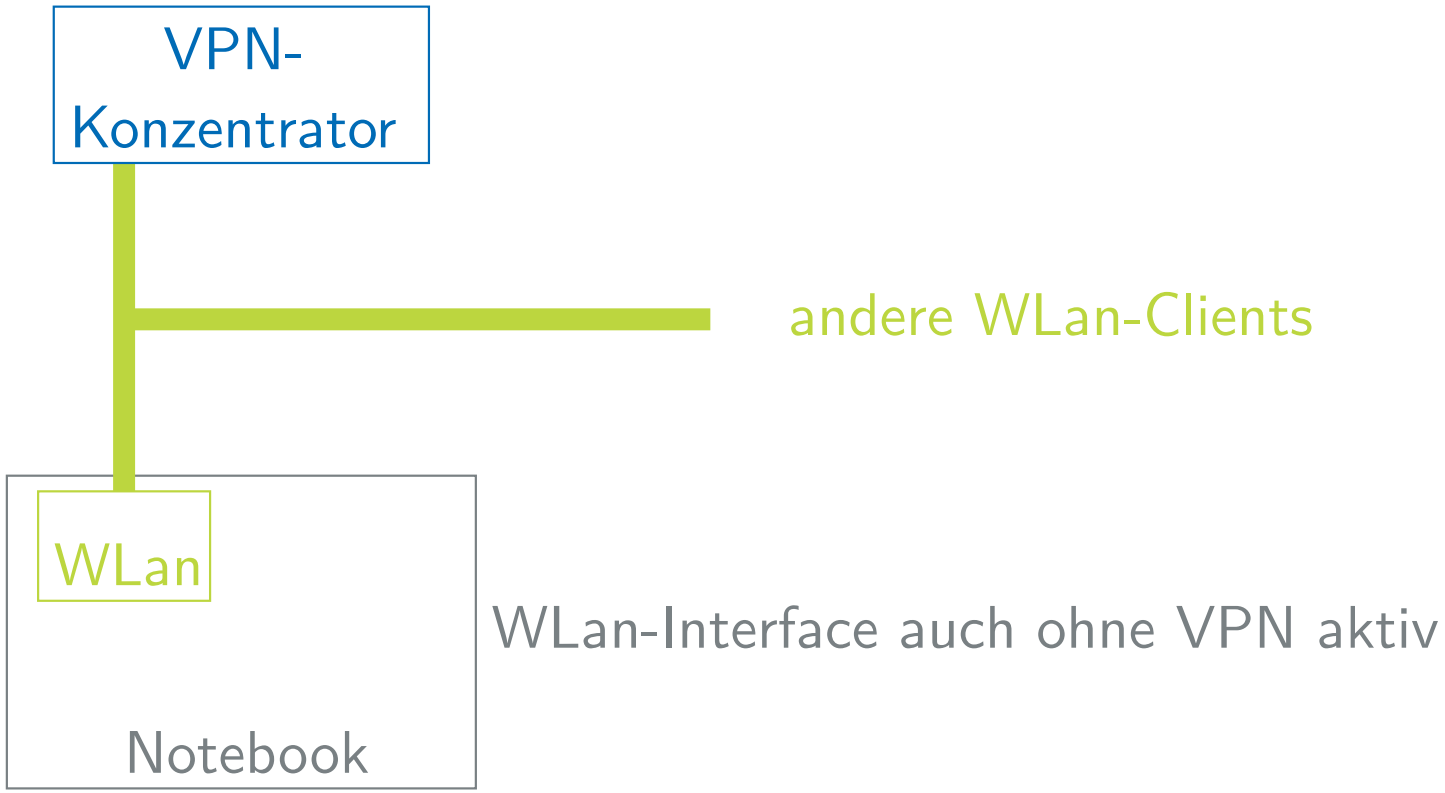
Literatur

W. Dolle: Neue Methoden zur Erkennung von Windows Rootkits

R|R|Z|N

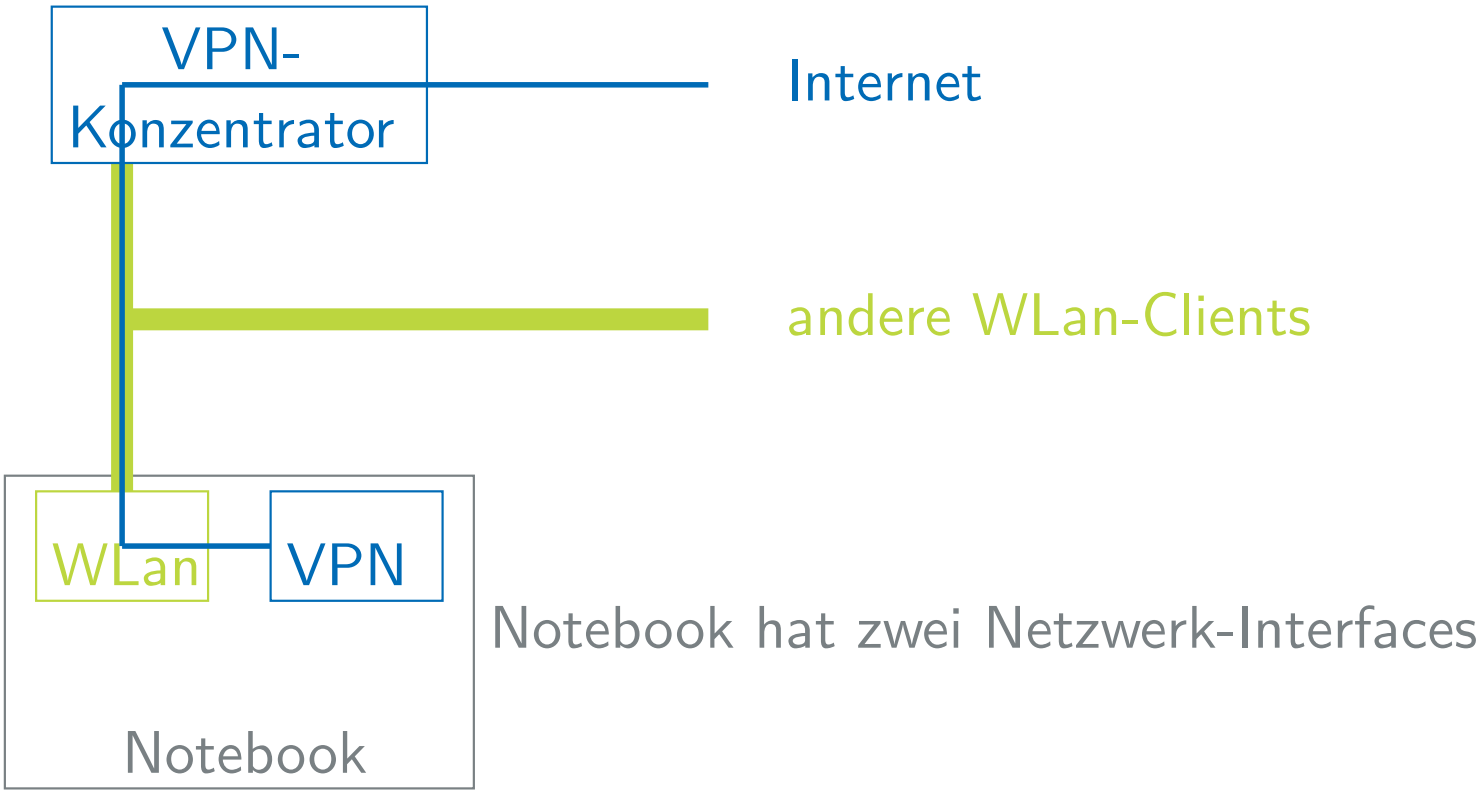
bisher

- unverschlüsselte Verbindung im lokalen WLan



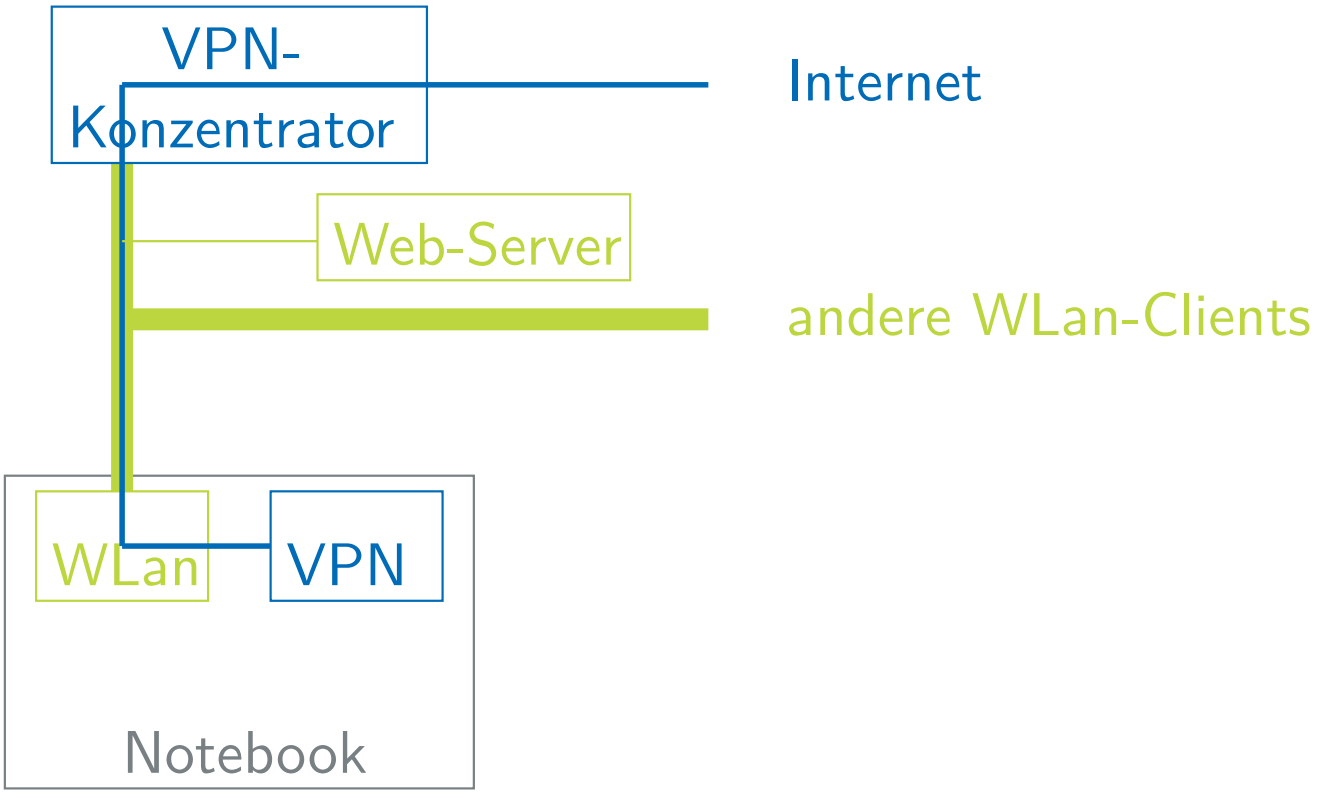
bisher

- unverschlüsselte Verbindung im lokalen WLan
- verschlüsselter Tunnel mit VPN ins Internet
- VPN mit Pre-Shared-Key lässt Man-In-The-Middle-Attack zu.



jetzt

- Mit neuem Client (zertifikatsbasiert) kein MITM möglich.
- Client-Download & Hilfe im unverschlüsselten Netz
  per DNS-Umleitung auf Web-Server (evt. Browserneustart)



R|R|Z|N

Angebot

- WSUS: Windows Update
- Sophos: Virenscanner
- Netzschutz: Firewall
- Mail: Puremessage, Serverbetrieb
- Archiv und Backup ⟵ Umstieg Unitree auf SamFS
- Webhosting (statische Inhalte) ⟵ vgl. ORG.BEN 40
- . . . 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 ⟵ wird dran gearbeitet
- 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
- Vorfälle melden: Bedrohungen kennen, aus Fehlern lernen

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

- hat alte `security@`*`INST`*`.uni-hannover.de` abgelöst
- B-Rundschreiben 42/2005 (inzwischen abgelaufen)
- unbedingt Weiterleitungsziel aktuell halten / regelmäßig lesen

R|R|Z|N

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

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