

---

# Virenschutz in der Praxis

- Wie gelangt ein Virus über den Browser auf den Client-Desktop?
- Analyse der technischen Abläufe
- Technische und organisatorische Schutzmaßnahmen



---

## Virenschutz in der Praxis

Wie gelangt ein Virus über den Browser auf den Client-Desktop?

Karl-Peter Hertleif  
infodas GmbH.  
Rhonestrassen 2, 50765 Köln  
E-Mail: [kp.hertleif@infodas.de](mailto:kp.hertleif@infodas.de)

---

# Gliederung

1. Virenarten
2. Einfache Infektion
3. Schutzmaßnahmen vor einer einfachen Infektion
4. Komplexes Firmennetz
5. Infektionswege
6. Technische Analyse
7. Technische Schutzmaßnahmen
8. Organisatorische Schutzmaßnahmen

---

# Virenarten

- **Virus** : Programm-Modifikation, die sich eigenständig auf legalen Pfaden im Rechner ausbreitet
  - Link-Virus (File-Virus): Virus-Code ist in das ausführbare Programm (Image-File auf der Platte) eingebunden
  - Boot-Virus (RAM-Virus): Virus-Code liegt im Hauptspeicher (in einem Systembereich)
  - Makro-Virus: Virus-Code ist in Makros in Dokumenten eingebettet

---

# Virenarten

- **Trojanisches Pferd:** versteckte Funktion, die die Ausführung unerlaubter Operationen ohne Wissen des Benutzers veranlasst
- **Logik-Bombe:** Programmfunktion, die bei Eintreten einer bestimmten Bedingung eine unerlaubte Operation auslöst

---

# Virenarten

- **Wurm:** Programm, das sich eigenständig durch Vervielfältigung im Rechner / in einem Netz ausbreitet
  - lokal von geringer Bedeutung
  - in Netzen Weiterverbreitung in mehreren Schritten:
    - Suchen angreifbarer Rechner
    - Kopieren eines Pilotprogramms auf den Zielrechner
    - Ausführung des Pilotprogramms auf dem Zielrechner
    - Erzeugung und Start einer neuen Kopie des Wurms ...

---

# Eigenschaften von Viren

- Spezielle Gefahren:
  - bei entsprechender Kenntnis einfach zu schreiben
  - aus Experimenten als extrem wirkungsvoll erkannt
- Ablauf einer Infektion:
  - Start eines kranken Programms
  - Infektion weiterer Programme
  - Ausbreitung der Krankheit
  - Infektion sensitiver Systemteile
  - Seuche: vollständige Infektion
  - Ausbruch der Krankheit:
    - Erkennen des Triggers
    - Auslösen fremder / gefährlicher Operationen
    - Zerstörung des Systems

---

# Programm-Schema eines (File-)Virus

```
program VIRUS ::=
  (MARKE:
    (V1: ! Infektionsteil - Verbreitung des Virus
      <suche anderes Programm P>;
      if <P enthält MARKE> then
        goto V1;
      P := VIRUS + P; ! kopiere VIRUS in Programm P
    )
    (V2: ! Wirkungsteil - logisch von V1 unabhängig
      if <beliebige Bedingung> then
        ! z.B. Freitag, der 13.
        <richte beliebigen Schaden an>;
        ! z.B. lösche Platte
      )
    )
  )
```

---

# Der Schadens-Mechanismus

- Typische auslösende Bedingungen:
  - Ablauf eines Zeitintervalls seit der Infektion
  - Überschreiten eines Grenz-Datums
  - Infektion bestimmter/globaler Systemteile
- Denkbare Schäden:
  - automatischer Eintrag von Benutzerberechtigungen
  - unendliche Schleife: „denial of service“
  - Zerstören von Daten:
    - hart
    - durch Einbringen von Inkonsistenzen
  - Datendiebstahl durch Kopieren

---

# Der Schadens-Mechanismus

- Spezielle Charakteristika von Viren-Schäden
  - Weite Verbreitung des Virus, ehe ein erkennbarer Schaden auftritt
  - Schaden an anderer Stelle als der Erst-Infektion
  - Gleichzeitige Schädigung vieler verschiedener Stellen
  - Auch Schäden an sensitiven Systemteilen

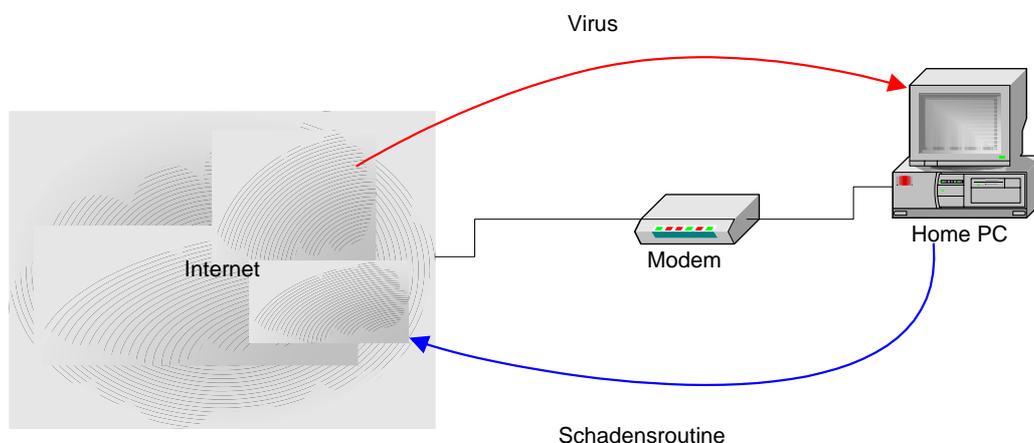
---

# Verbreitungsmechanismen

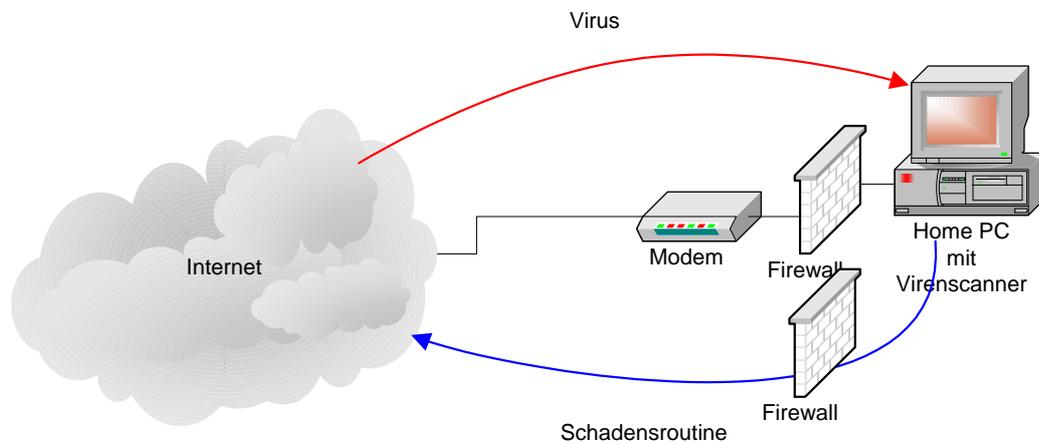
- Viren müssen ausgeführt werden, um aktiv werden zu können:
  - Kopieren von Programmen und Daten ist ungefährlich, solange diese nicht als Programm ausgeführt werden
  - Viren entstehen nicht - sie müssen ins System aufgenommen worden sein!
  - Gefahr durch in Daten eingebettete Programme (Makro-Viren, Java-Applets)

---

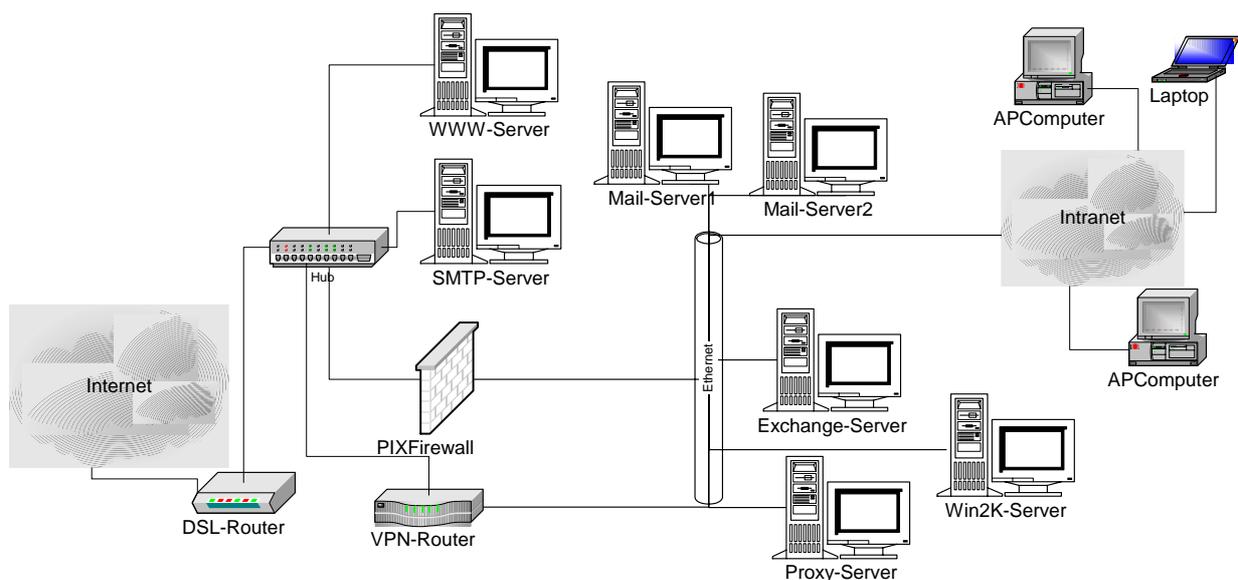
## Einfache Infektion



# Schutz bei einer Einfachen Infektion



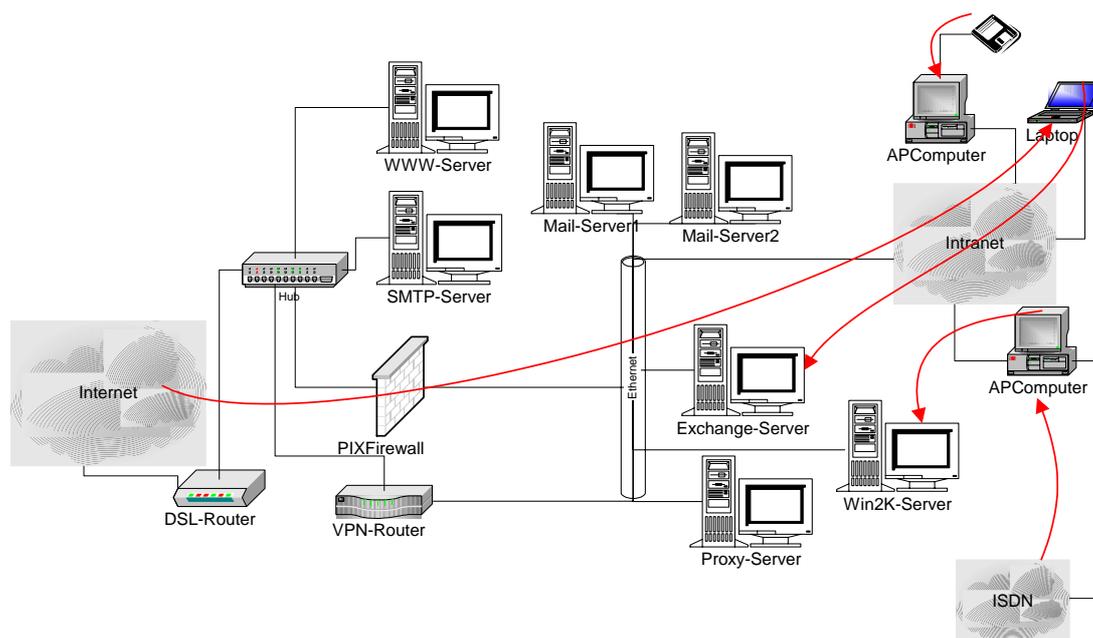
# Komplexes Firmennetz



# Komplexes Firmennetz

- Verkehr von internen Arbeitsplätzen zum Internet ist immer erlaubt
- Damit ist Datenverkehr auch wieder ins Intranet erlaubt (NAT)
- Externer DNS zum internen DNS-Server (UDP )
- Datenverkehr vom externen Mailserver zu den internen Mailservern
- Virens Scanner für den SMTP-Verkehr
- POP3 zu externen POP3-Servern

# Infektionswege



---

# Technische Analyse

- Wie kann der Virus in das Netzwerk kommen?
- Welche zusätzlichen Wege ins Netzwerk wurden aktiviert?
- Warum war das nötig?
- Welche Verbreitungswege hat der Virus genommen?
- Welche Schadensroutinen hat der Virus mitgebracht?
- Was muss für die Zukunft beachtet werden?

---

# Erkennung von Virus-Code

- Vollständige Überprüfung von Programmen ist nicht durchführbar
- Automatische Erkennung von Viren ist prinzipiell unmöglich
- Schutzprogramme zur Erkennung / Vernichtung von Viren:
  - können von entsprechend geschriebenen Viren ausgetrickst werden
  - wirken jeweils nur gegen bestimmte Klassen von Viren
  - allgemeine Suchprogramme
    - finden wahrscheinlich nicht alle Viren
    - können aber zu falschen Alarmen führen

---

# Erkennung von Programm-Infektionen

- Jede Infektion erfordert Schreibzugriff auf die zu infizierenden Image-Files bzw. Dokument-Vorlagen
- Infektionen vergrößern in der Regel die infizierten Image-Files
  - Aber: „längentreue“ Viren
- Überprüfung von Größe des Image-Files und „Last-Modified“-Datum und Vergleich mit einer Referenz-Version
  - Kann bei PCs über Schreibzugriff auf zentrale Datenstrukturen des Dateisystems gefälscht werden

---

# Erkennung von Programm-Infektionen

- Binärvergleich mit einer Referenz-Version
- Checksummen-Vergleich:
  - Erstellen einer Checksummen-Liste einer Referenz-Version
    - Liste muß gegen Manipulation geschützt sein
  - Vergleich der aktuellen Checksummen mit dieser Liste
- Referenz-Version muß korrekt sein:
  - „sauber“ vom Distribution Medium (read-only!) generieren
  - Distribution Medium (read-only / CD-ROM) direkt verwenden

---

# Erkennung von Programm-Infektionen

- Automatische Alarme bei Programm-Änderung
  - dürfen nicht umgehbar/manipulierbar sein
  - müssen korrekt eingesetzt werden
    - ⇒ Verwaltungsaufwand
  - äußerst wirkungsvolles Erkennungsverfahren - wenn nicht zu viele Fehlalarme durch schlecht geschriebene Software ausgelöst werden

---

## Schutz gegen Verbreitung

- Kein Einsatz von Programmen unbekannter / zweifelhafter Herkunft
  - zweifelhaft ist jede Software, die über undefinierte Kanäle (getauschte Disketten, öffentliche Mailboxes, E-Mail Anhänge) kopiert wurde
  - Was ist jedoch mit KERMIT und sonstiger Freeware?
- Gründliche Inspektion aller Programme vor ihrem Einsatz
  - Wer macht / kann / darf das ???
- Auch keine Fremd-Software bei Benutzern zulassen (???)
  - Aber jedes Dokument, das als Anhang an eine E-Mail empfangen wurde, ist in diesem Sinne ein Programm!
- Keine Programm-Entwicklung der Benutzer zulassen (???)
  - Hilft, gibt aber alles keine Garantie gegen Infektionen

---

# Beseitigung von Infektionen

- Arbeiten sind von einem „sauberen“ System her auszuführen:
  - vom Distribution Medium aus neu generieren - ohne den geringsten Rückgriff auf Software des infizierten Systems
  - alle Daten und Programme des infizierten Systems (einschließlich der Systemprogramme) sind als Daten zu behandeln
  - keine Ausführung von Programmen des infizierten Systems!!!
  - wenn möglich, von einem unprivilegierten Account aus arbeiten

---

# Beseitigung von Infektionen

- Randbedingungen bei der Arbeit in Multi-User-Systemen:
  - für jeden infizierten Account sind die Arbeiten separat durchzuführen
  - Arbeiten sind grundsätzlich von einem unprivilegierten Account aus auszuführen
  - Vergleiche über System-Utilities durchführen, die von diesem Account aus nicht verändert werden können
  - keine der potentiell infizierten Programme dürfen ausgeführt werden

---

# Beseitigung von Infektionen

- Offene Fragen:
  - Ist es sicher, daß das System wirklich nicht infiziert wurde?
  - Was ist die Referenz-Version für ein System, das permanent gewartet wird?

---

# Technische Schutzmaßnahmen

- Die zusätzlichen Wege ins Firmennetz wieder schließen!
- Alle Systeme mit geeigneter Software wieder virenfrei machen!
- Dazu sind alle Systeme vom Netz zu nehmen und einzeln zu überprüfen, angefangen bei den Servern!
- Das bestehende Schutzkonzept ist neu zu definieren, damit in Zukunft hier nichts mehr passieren kann!

---

# Technische Schutzmaßnahmen

- Mitarbeiter informieren, damit sie sensibel auf die zu ergreifenden Maßnahmen reagieren.
- Mit den Analyseergebnissen ein neues Schutzkonzept aufstellen.
- Zeitrahmen für die Umsetzung des neuen Schutzkonzeptes aufstellen.
- Beschaffungsmaßnahmen umgehend beantragen und einleiten.

---

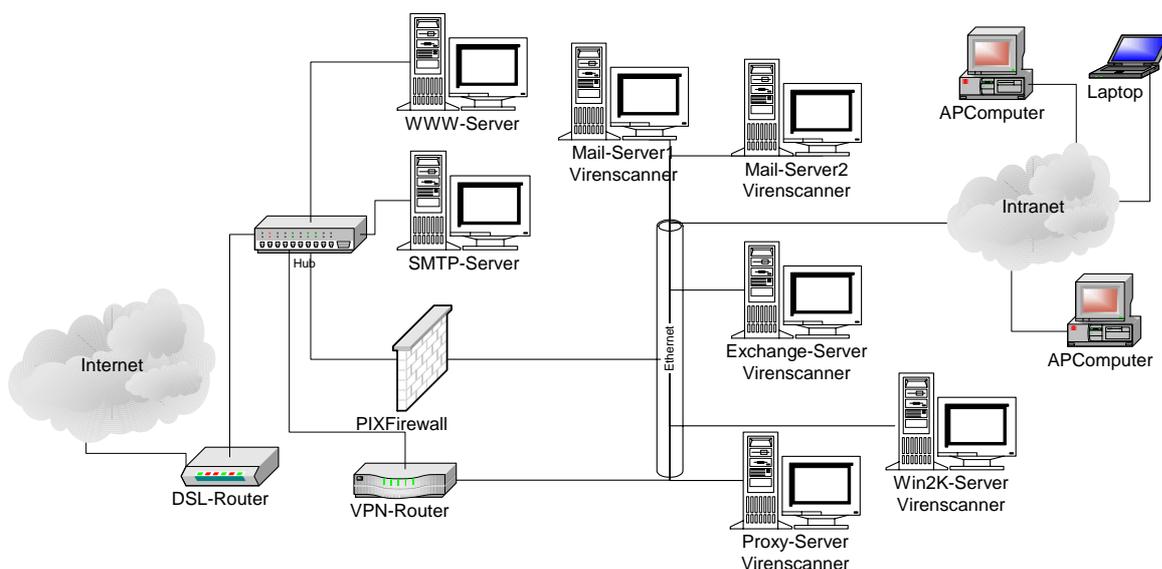
# Technische Schutzmaßnahmen

- Installation zusätzlicher AntiVirensoftware
- Es dürfen nur bestimmte Server ins Internet.
- AP-Computer benutzen immer einen Proxy-Server mit zusätzlichem Virens scanner für HTTP- und FTP-Verkehr.
- Kein interner AP-Computer kann direkt ins Internet.  
(Einstellungen auf der Firewall)
- SMTP-Verkehr wird auf einem Server gescannt bevor die Mail zugestellt wird.
- POP3 zu externen Servern geht nur über einen eigenen Proxy-Server mit eigenem Virens scanner.

# Technische Schutzmaßnahmen

- Alle AP-Computer/Laptops bekommen einen Virens scanner, der immer automatisch upgedatet wird.
- Verschiedene OS der Serversysteme installieren.
- Monokulturen vermeiden.

# Technische Schutzmaßnahmen



---

# Verhinderung von Infektionen

- Korrekter Schutz der System-Dateien (incl. - Programme und -Bibliotheken)
  - Unprivilegierte Benutzer können nicht das System infizieren
  - Infektion bleibt auf Benutzer beschränkt, solange der Systemverwalter keine infizierten Programme ausführt
- Keine Vergabe von Privilegien an Benutzer, die Viren haben könnten / entwickeln könnten
  - Keine Aneignung erhöhter Rechte durch Viren
  - Keine Infektion des Systems durch Viren bei Benutzern

---

# Verhinderung von Infektionen

- Betrieb eines Online Virenwächters
- Striktes Konfigurations-Management
- Keine Ausführung zweifelhafter Software auf vernetzten Systemen / unter System-Rechten
  - Software eigener, nicht vertrauenswürdiger Benutzer
  - Fremd-Software fragwürdigen Ursprungs
- Überprüfung unbekannter Software auf Quarantäne-Rechnern
- Keine automatische Ausführung von Programmen, die Anhänge an E-Mails lesen

---

# Verhinderung von Infektionen

- Keine allgemeine Zugreifbarkeit zweifelhafter Software
  - keine Zugriffsrechte über Benutzergruppen hinweg
  - Analyse neuer Software in einer abgeschotteten Umgebung
- Keine privilegierte Installation zweifelhafter Software
  - „Timeo Danaos et dona ferentes...“
- Systemprogramme eventuell auch gegen Lesezugriff sperren
  - Bei Großrechnern übliche Kontrollen bieten erheblichen Schutz

---

# Organisatorische Maßnahmen

- Virenschutzbeauftragter
- Keine Sonderlocken für die Bequemlichkeit
- VA über den Virenschutz
- Ständige Überprüfung der Maßnahmen
  - Aktualität des Virenscanners
  - Ist der Monitor noch aktiv
  - Gibt es vielleicht einen neuen Virus, was meldet der Virenschanner
  - etc...
- etc...

---

# Schlußbemerkungen

- Ständige Überprüfung eventueller Bedrohungs-Szenarien.
- Ständige Anpassung der bestehenden Schutzmaßnahmen
- Das bedeutet, man darf sich nicht auf seinen Lorbeeren ausruhen.
- Es gibt immer neue Viren und damit auch neue Herausforderungen.

---

Fragen?

