Datensicherheit IV

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Bedrohungen

Die Bedrohungen für Netzwerke und Server sind sehr vielfältig. Alleine durch die enorme Anzahl der Software, die im täglichen Einsatz ist, kann sich jeder einzelne Fehler im Code auch auf andere Bereiche auswirken. Die folgende

- **Buffer Over ow mit Code Injektion**
  Ein Buffer Over ow stellt das Einschleusen von Assembler Code in eine laufende Software dar. Anfällig für solche Attacken ist jeglicher Code, der keine Überprüfung von Pufferbereichen vornimmt[3] (z.B. C Funktionen wie `strcat()`, `strcpy()`, `sprintf()`, `vsprintf()`, `Ucopy()`, `gets()` **oder** `scanf()`**).**

- **Denial of Service (DoS)**
  Durch Senden von ungültigen oder sehr vielen Daten wird ein bestimmter Dienst zum Absturz gebracht und steht dann nicht mehr zur Verfügung.

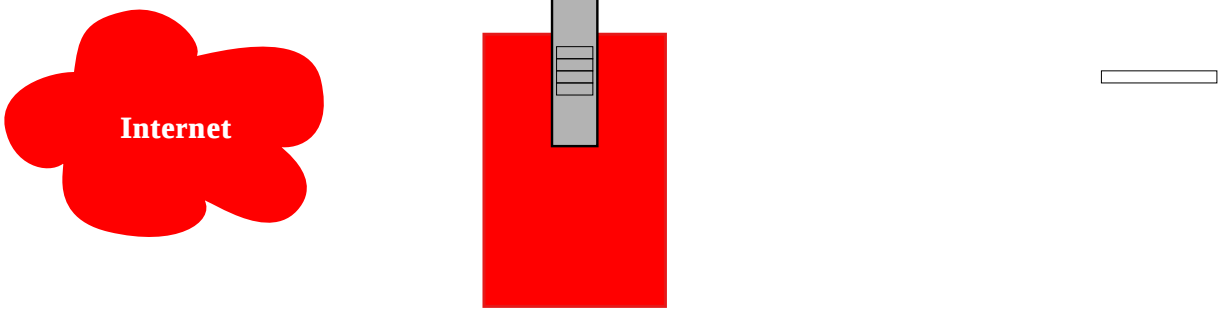
- **Mißkon gurationen**
  Darunter fällt ein sehr großer Bereich,

Kapitel 2

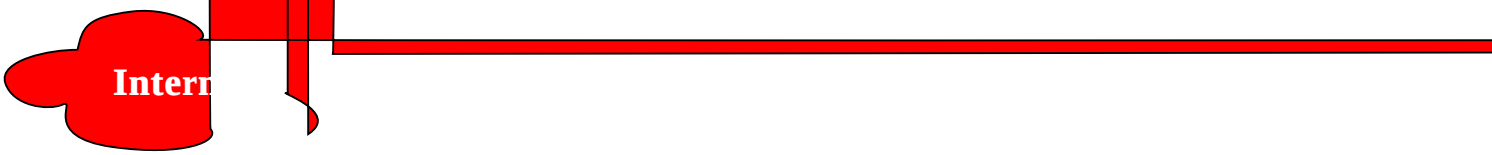
Sicherheitsmaßnahmen

"

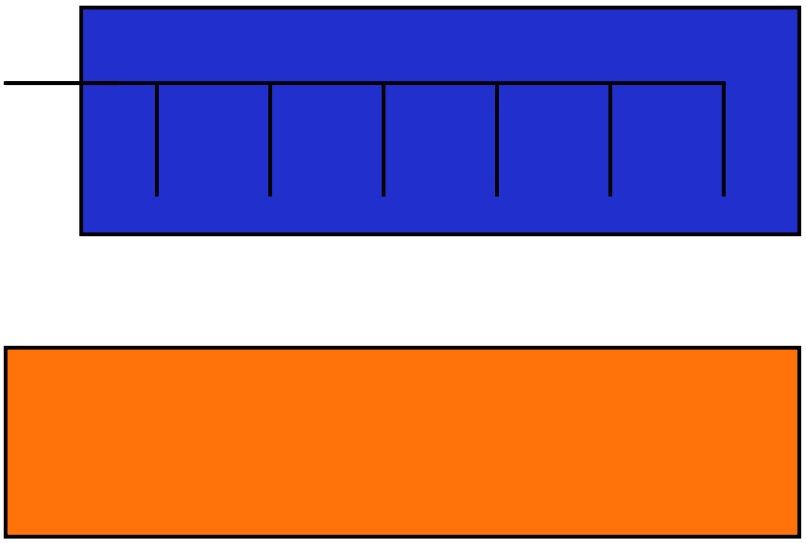
Einsatz von Prox Servern



2.2.2 Scree bnet Architektur



2.2.3 Mehrere interne Netzwerke



2.3.2 Deaktivieren aller unnötigen Services

- **Säubern der Init-Skripts**
  $\longrightarrow$ die Maschine muß nach dem Booten richtig eingestellt sein
- **Säubern der `inetd` Services**
  $\longrightarrow$ Empfehlung: Einsatz von `xinetd`
- **unn¨**

2.3.4 Rekon gurieren der Maschine für Production Environment

- **Kon gurieren des Kernels**
  - **keine Verwendung von Kernel Modulen**
    $\longrightarrow$ es existieren trojanische

2.4.3 FTP Server

- **Betrieb des Servers in einer `chroot` Umgebung (möglicherweise per FTP User)**
- **kein Betrieb eines anonymen FTP Servers**

2.4.4 Mail Transport Agents (MTAs)

- **Korrektes Einbinden des Servers in den**

Kapitel 3

Angriffe auf Netzwerke und Server

A n

3.1.1 Ethereal - Packet Analyzer

- **Abfangen und Darstellen von Paketen auf jedem Interface**
- **Darstellen von Paketen aus Dumps von anderen Tools**
  tcpdump, NAI Sniffer / Sniffer Pro, NetXray, LANalyzer, Shomiti, AIX iptrace, RAD-COM WAN / LAN Analyzer, Lucent / Ascend Produkte, HP-UX nettl, Toshiba ISDN Router, ISDN4BSD i4btrace, Microsoft Network Monitor, Sun snoop
- **Abspeichern von Dumps in verschiedenen Formaten**
  libpcap (tcpdump), Sun snoop, Microsoft Network Monitor, NAI Sniffer
- **Filterkriterien & Suchfunktionen**
- **Protokolldekoder für eine Vin von Protokollen[1]**
- **TCP Stream Verfolgung**
- **TCP Analyse**
  - **–in (Zeit-Sequenznummer Graph)**
  - **–in chsatz Graph**
  - **–inT Graph**

Ethereal besitzt auch ein Tool namens tetnereal

- **Port Scannen (auch mit gefälschten Source-Adressen,**

  - **Pakete mit Längen $>$ 65534 (Linux und BSD)**
  - **beliebige Pakete mit veränderten Parametern und Codes**
    - **Parameter Problem**
    - **Destination Unreachable**
    - **Time Exceeded, etc.**

- **Senden unter Verwendung von Source Routing Optionen**

3.1.5 nmap - Network Mapper

-

3.1.6 Sonstige Tools

- ping
- traceroute
- tracepath
  Auf der lokalen Maschine
  - ip **oder** ifconfig
- tr
-

Kapitel 4

Intrusion Detection Systeme

- **Grundfunktionen** `alert / log / pass`
- **unterstützt derzeit TCP, UDP & ICMP**
  In Zukunft geplant: ARP, IGRP, GRE, OSPF, RIP, IPX
- **Snort kann die folgenden Paketinformationen testen**
  - `TTL` **- Wert des IP Pakets**
  - `I`

- **ICMP Host**

- **Kombinieren von mehreren Log les**

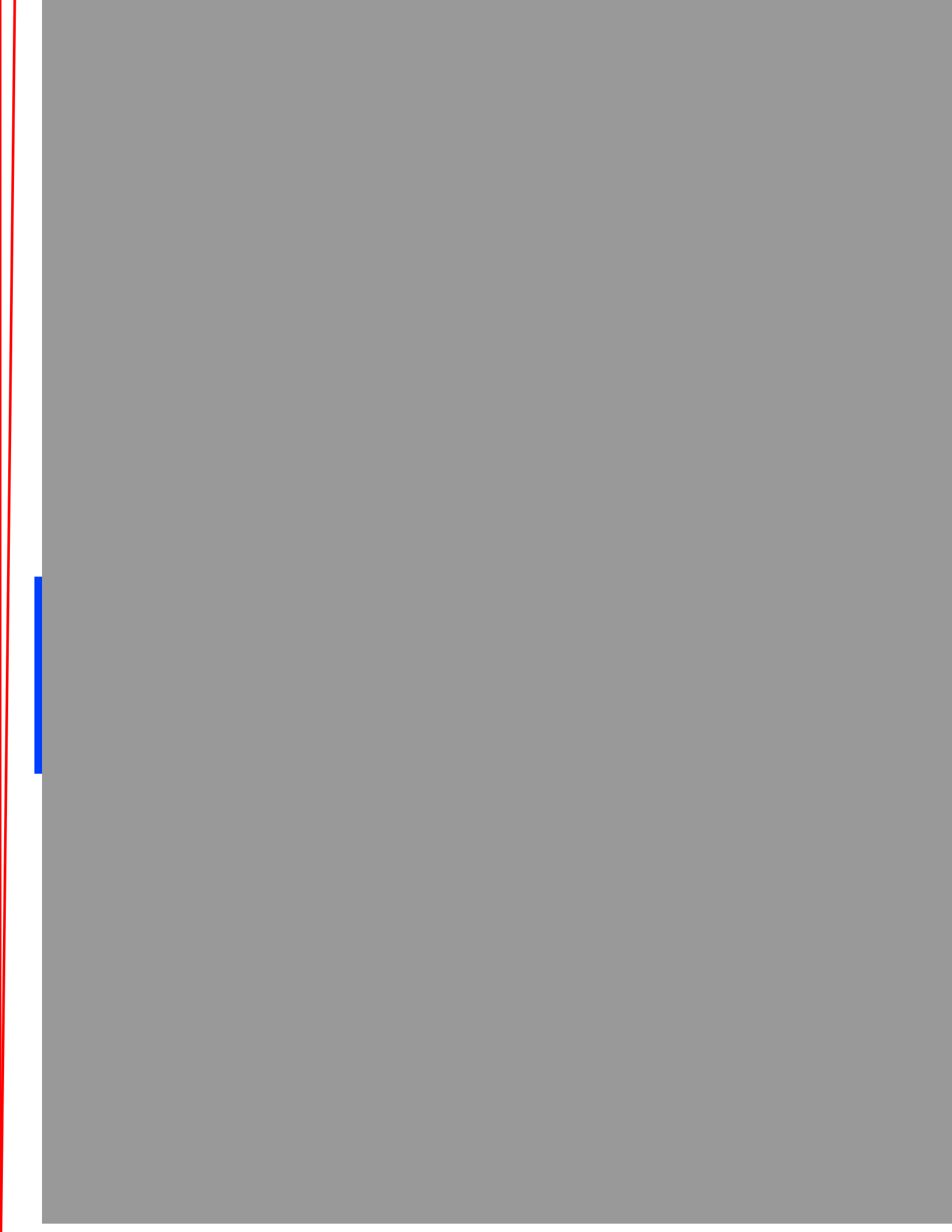
- **Performanceveränderungen**
  $\longrightarrow$ **CPU Last, E/A, Plattenplatz**
- **Zustandsänderungen („Phasenübergänge“) von Systemen**
- **Interaktionen - Logias**
  - **zu ungewöhnlichen Zeiten**
  - **von bestimmten Benutzern**
  - **von**

n n n n

- **Wie**

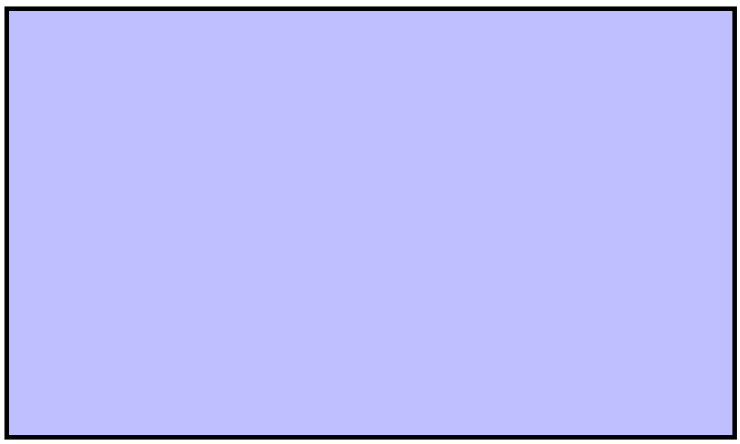
- **Welche Applikationen sollen überwacht werden?**
- **Welche Teile**

- **Planung des Logdatentransports**
  ⟶ zentrales Log Repository
  ⟶



M n c n

- **Einsetzen vkn HUBs in Segmente**
  - –



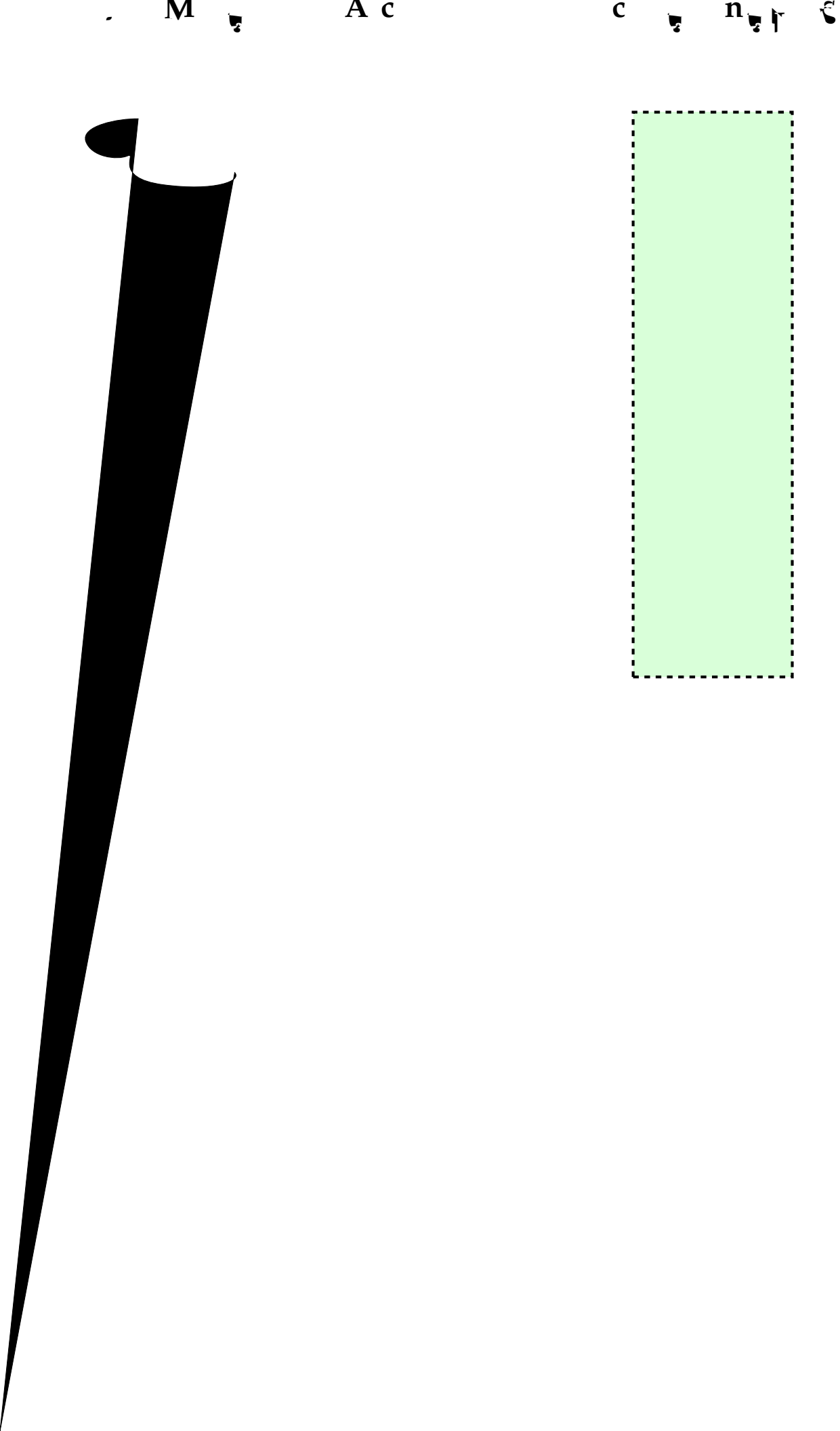
Sichtbare IDS Sensoren sind angreifbar:

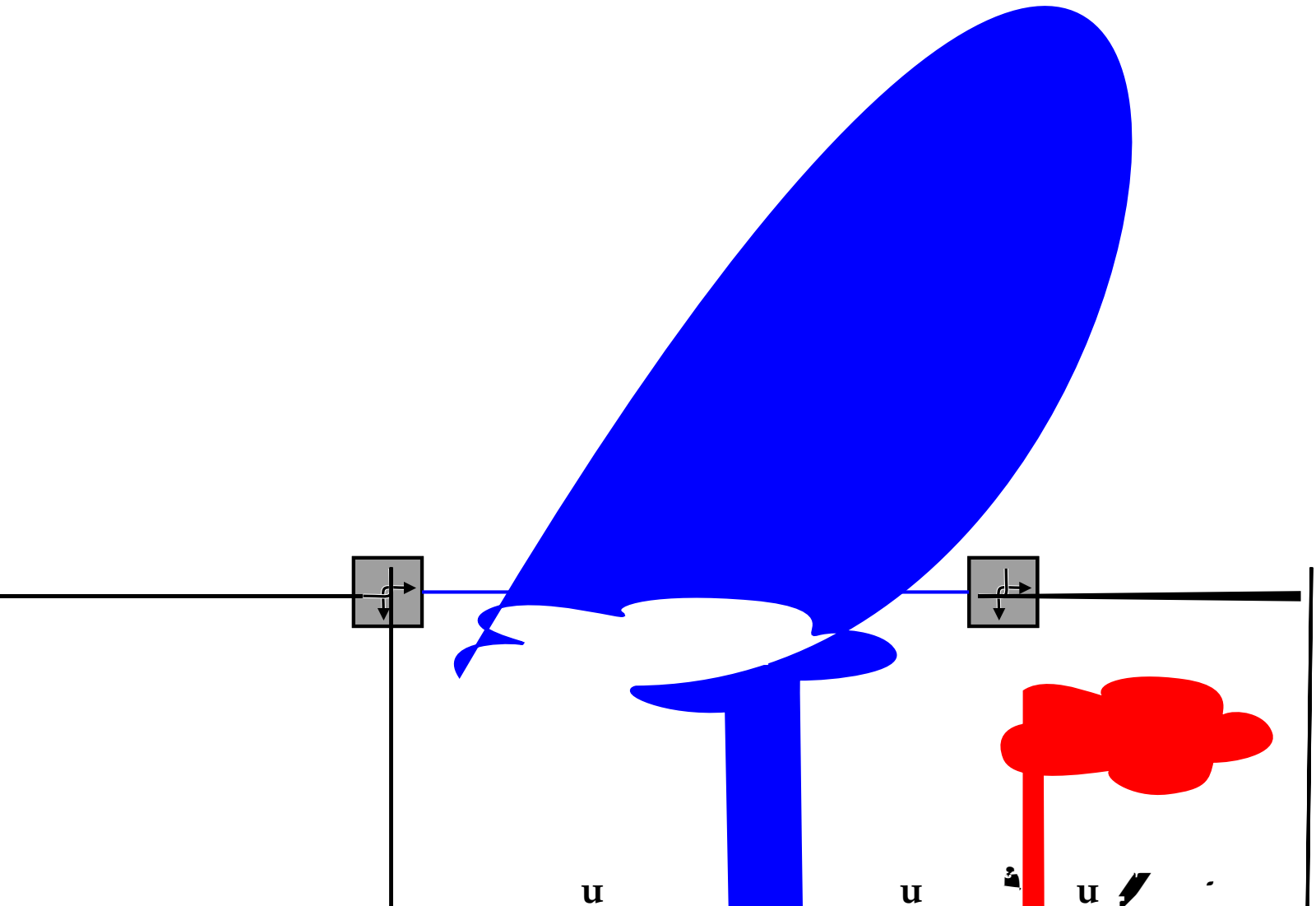
- **Sensor mit Paket ut blenden**
  - **IP Pakete mit gefälschten Quelladressen**
  - **fragmentierte Pakete**
  - **Versuch den Sensor durch Überlastung auszuschalten**

denz

n n nc

- **Abstimmen der Signaturen**
  $\longrightarrow$ **je weniger Checks, desto schneller der Sensor**
  $\longrightarrow$ **NIDS Regeln unbedingt auf Einsatzort abstimmen**
- **Verteilung der Sensoren auf das Netzwerk**
- **Verteilung der Aufgaben auf mehrere Sensoren**
  $\longrightarrow$ **Aufteilung von Pr**




u
u
u


NIDS
NIDS

5.13.1 Rechtsfragen beim Überwachen von Netzwerken

Darf man überhaupt ef zient Auswerten?

- **Begriff „Sniffen“**
  umfaßt das Aufzeichnen und Auswerten von Netzwerkverkehr
- **Sniffen Rechtzei.1**

-

5.13.2 Grundsätzliche Quellen für rechtliche Aspekte

- **EU Datenschutzrichtlinie**[1]
- **DSG 2000**[2]
  - **Recht auf Geheimhaltung (DSG 2000, Verfassungsbestimmung)**
  - **Informationsrecht (**

5.13.3 Auswerten der IDS Daten

- **IDS generieren sehr viele Daten**
- **datenbankgestützte Auswertung für ernsthafte Analyse erforderlich**
  - **Einsatz von Data Mining Methoden**
  - **Erkennen von Mustern und Anomalien**
  - **Suche**

5.13.5 Der Einsatz von Data Mining Verfahren

- **Data Mining ist kein Real Time Verfahren**
  $\longrightarrow$ **Daten stehen nicht**

5.13.6 Beispiel für kontinuierliches Monitoring

- **Überwachung mehrerer Maschinen durch Samhain Sensoren**
  → **Meldung aller Ereignisse an Yule Prozeß am Logserver**
- **DMZ und LAN wird durch Snort Server beobachtet**
  → **je eine Netzwerkkarte pro Snort Sensor Prozeß**
  → **lokale Packet Capture Logs**
  → **Ereignisse gehen an Logserver**
- **periodisches Wandeln von System- und Maillogs in SQL**
  → **Perl Skripte konvertieren (a52 24.9l9aillogs)Tjsyslodg64 0 Td82Td (ur)Tj&2 24.0 028mhain**

5.13.7 Möglichkeiten zur selbstständigen Anomaliebeschreibung

- **De nition eines Feature Sets für Gruppen von Systemen**
  Sammlung von Daten
  - **im Normalzustand**
  - **mit simulierten Attacken**

  Beispiele für kategorisierte Paketdumps in den Daten zum Knowledge Discovery in Databases (KDD) Cup 1999[4]
- **Verarbeitung**