

## Logdaten-Analyse-System

Eine technische Lösung für das Erkennen von Angriffen

**Johannes Mrosek**  
**mrosek [at] internet-sicherheit [dot] de**

Institut für Internet-Sicherheit  
<https://www.internet-sicherheit.de>  
Fachhochschule Gelsenkirchen



# Agenda

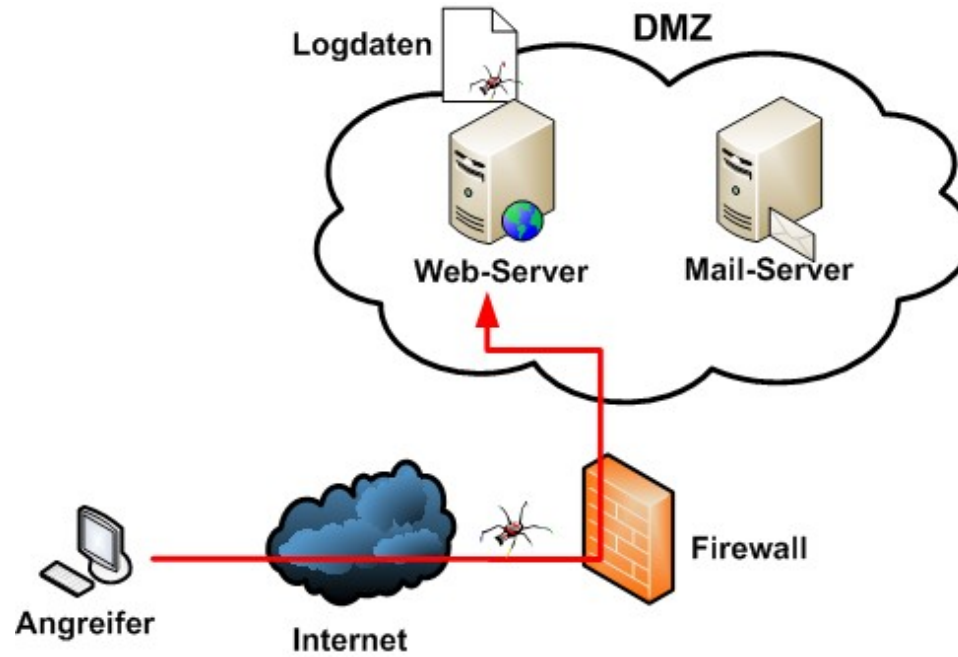
- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

# Logdaten-Analyse-System

## → Konzept (1/3)

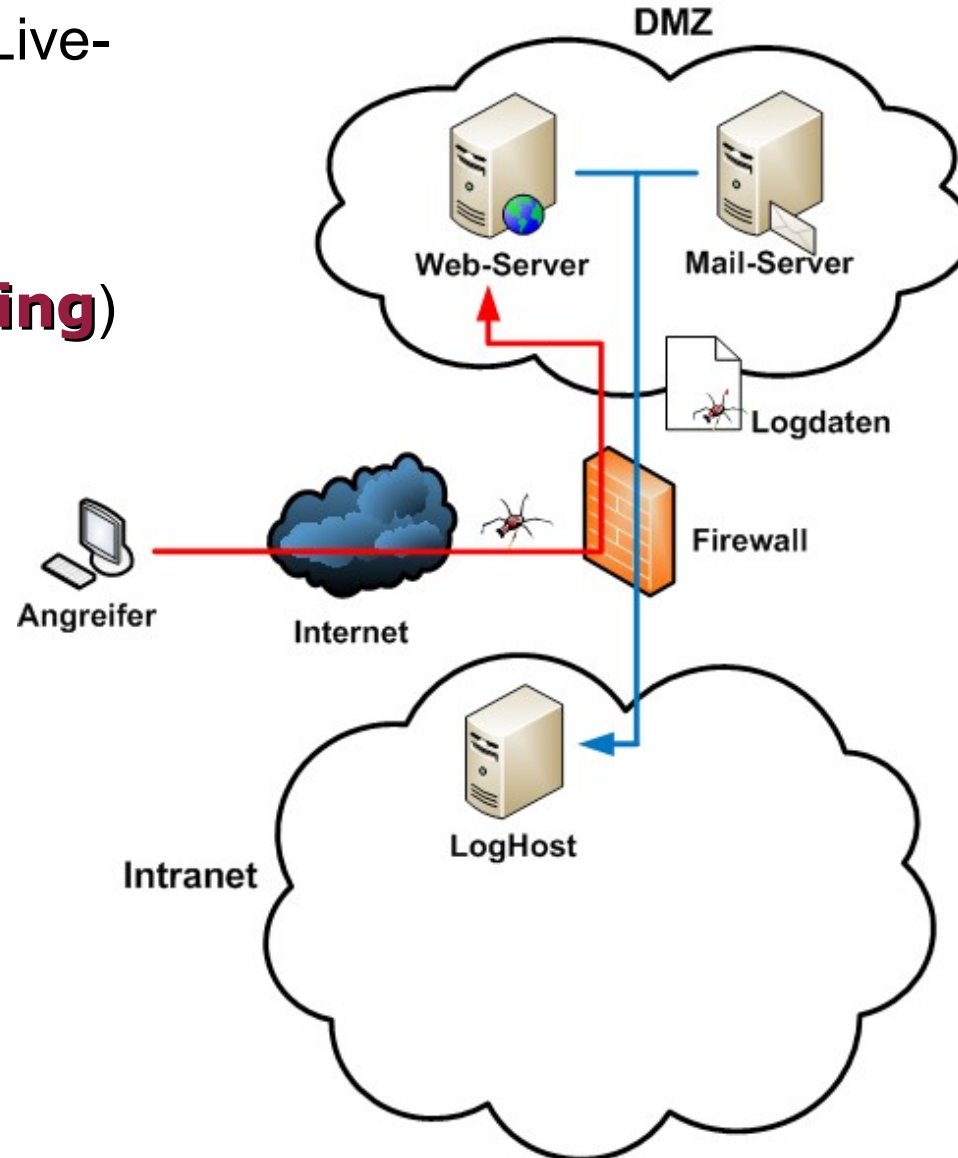
- In Logdaten wird gesamte Kommunikation eines Dienstes aufgezeichnet
- Kommunikation mit potentiellen Angreifern wird also auch erfasst
- Angriffe hinterlassen signifikante Muster in den Protokollen



# Logdaten-Analyse-System

## → Konzept (2/3)

- Logdaten werden als Live-Datenstrom an einem zentralen Log-Host zusammengeführt (**Centralized Logging**)
- Erhöhung der Übersichtlichkeit
- Korrelation der Daten
- Leichtere Weiterverarbeitung

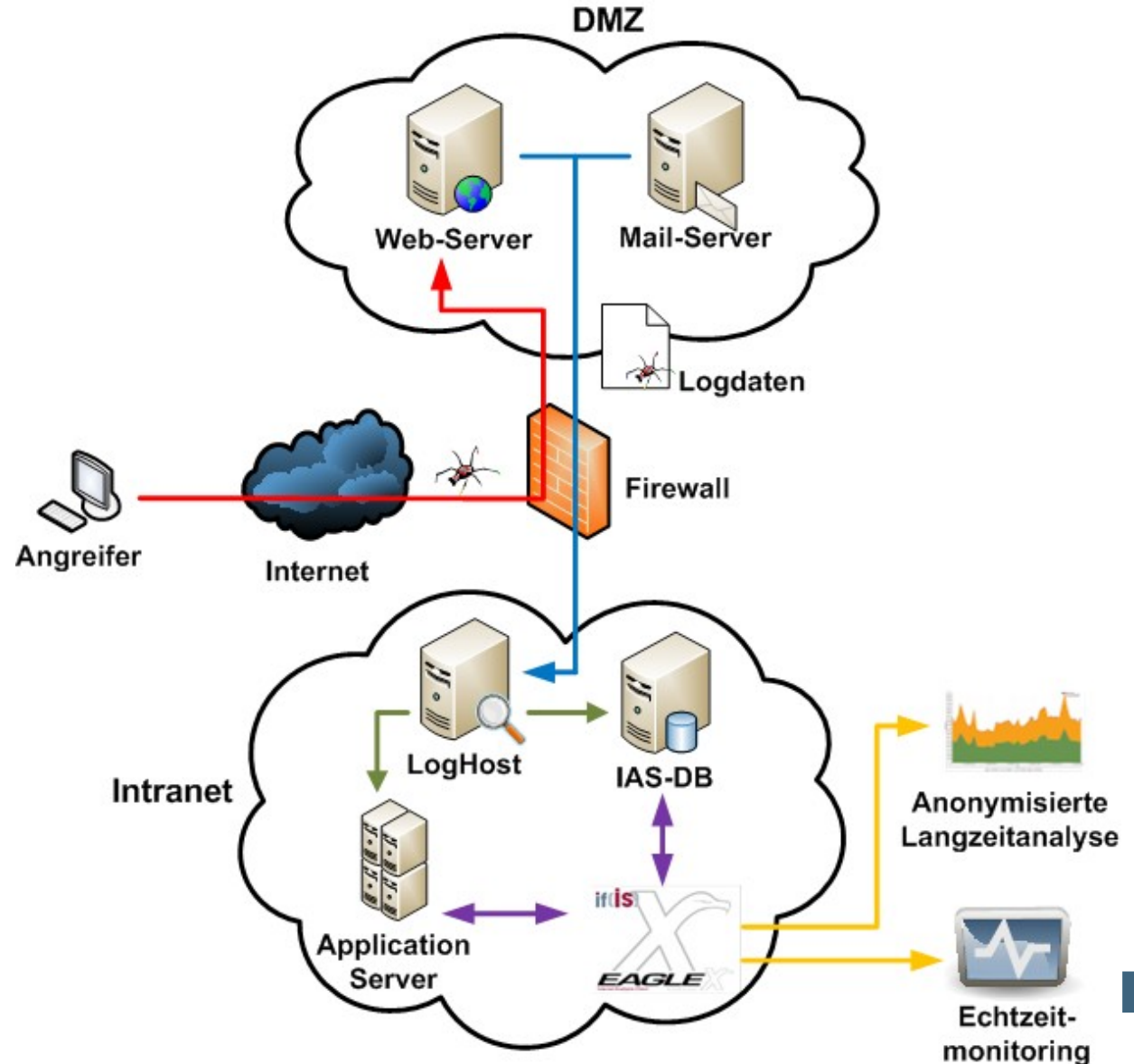


# Logdaten-Analyse-System

## → Konzept (3/3)

- Livedatenstrom wird auf Angriffe hin untersucht (**Intrusion Detection**)

- Anonymisierte Langzeitanalyse
- Echtzeitanalyse mit Alarmierung

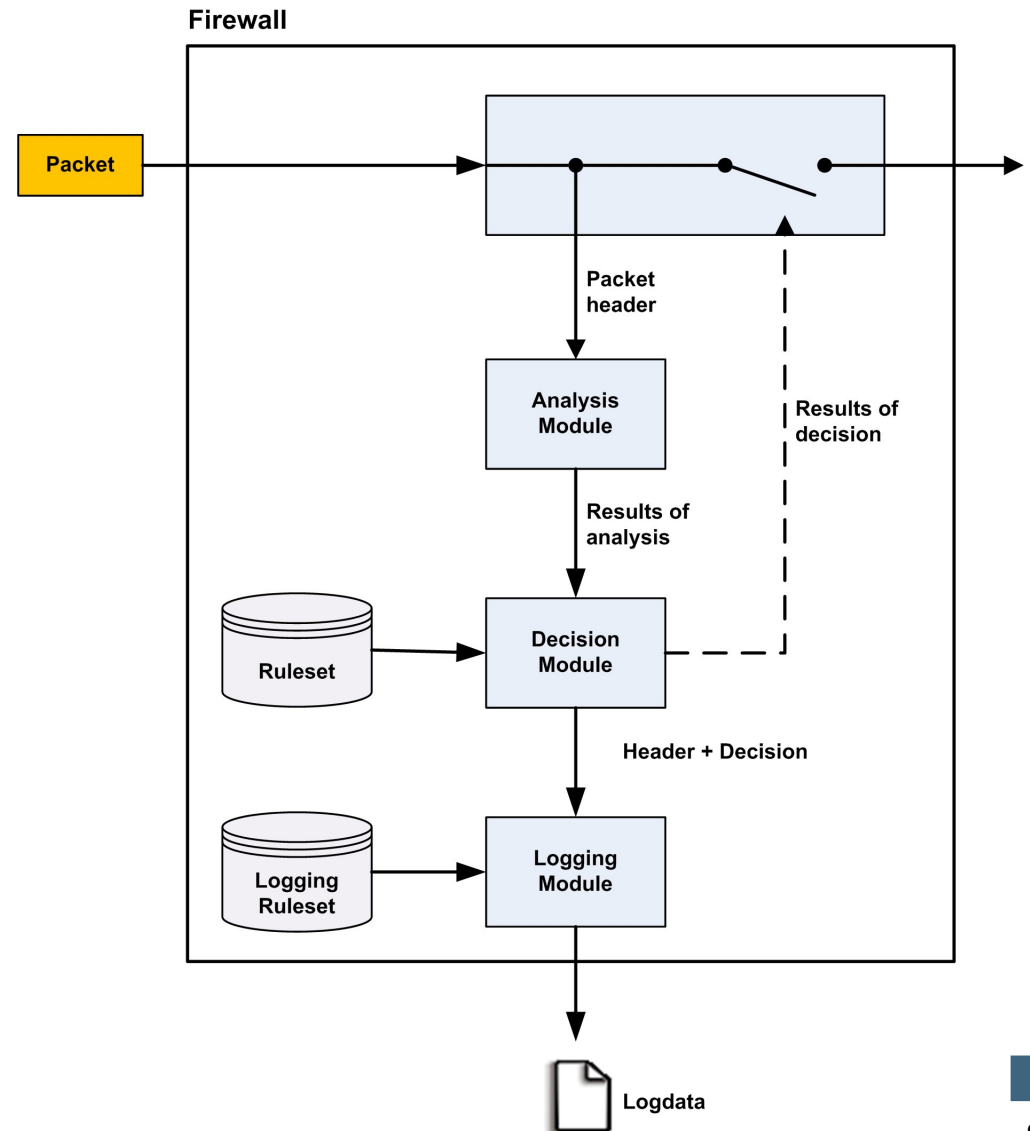


- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

- richtige Menge an Logdaten ist wichtiger Eingabeparameter des Systems
- je mehr Logdaten, desto mehr Informationen und desto genauere Aussagen sind möglich
  - wird zu wenig geloggt, funktioniert das System nicht
  - wird alles geloggt, funktioniert das System aber auch nicht
    - wichtige Informationen „gehen im Rauschen unter“
    - Performance
- Ob ein Logdatum sicherheitsrelevante Informationen erhält, lässt sich meist nur im Kontext zu anderen Logdaten erkennen
  - ein fehlgeschlagener Anmeldeversuch ist wahrscheinlich ein Versehen
  - tritt dieser aber mit 999 weiteren fehlgeschlagenen Versuchen auf, ist er Teil eines Einbruchversuchs
- Sicherheitsrelevante Informationen in Logdaten < **5%**, meist **implizit**

### ■ Beispiel Firewall

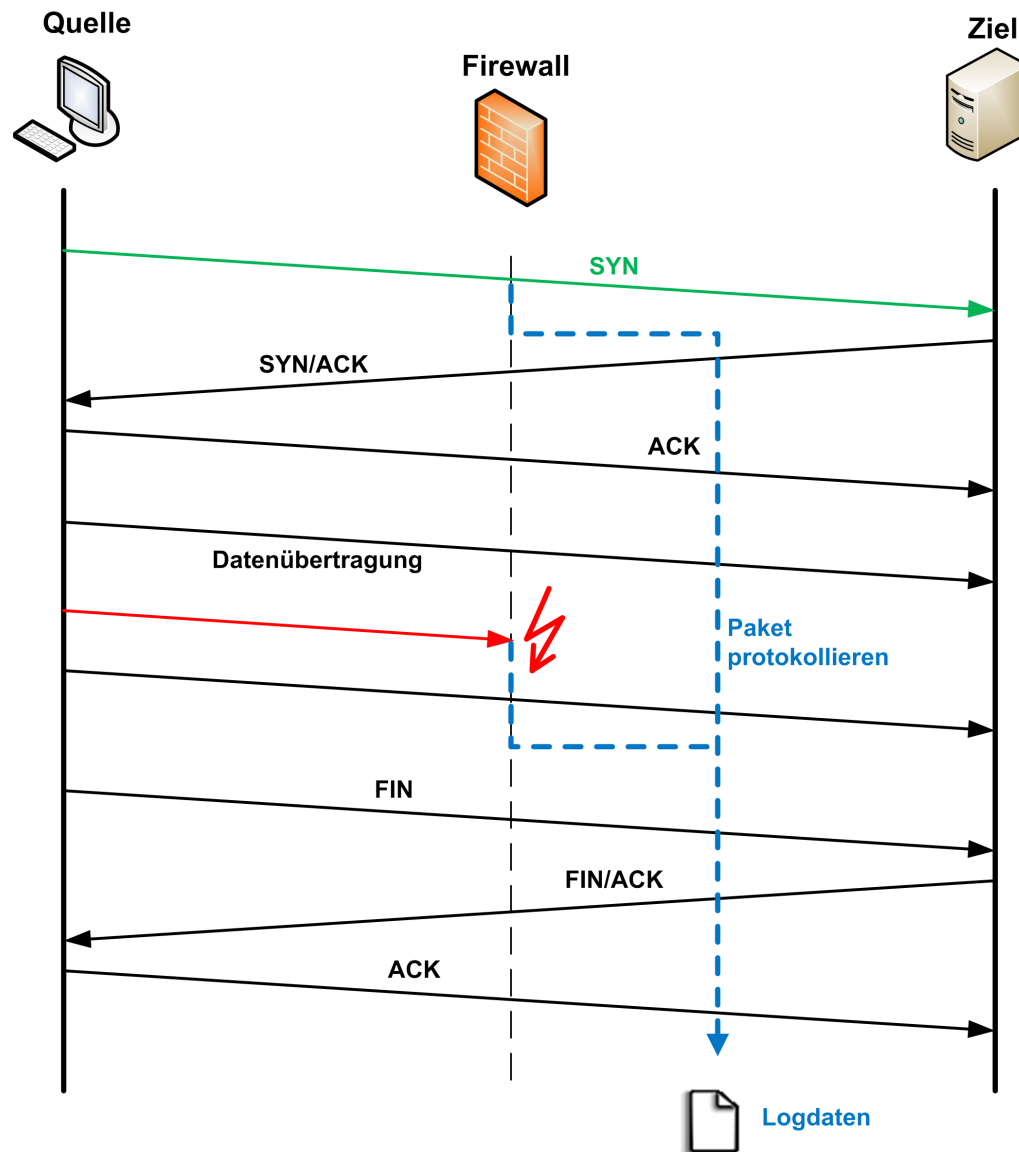
- Paket Header werden geloggt
- aber nicht jeder Header
  - Vermeidung extrem hohen Overheads
  - Definition von Logregeln in der Firewall
  - Korrektes Verhalten des Analyse-Systems hängt von diesen Regeln ab



# Logdaten-Analyse-System

## → Log Reduction (3/3)

- Firewall loggt
  - immer das erste Paket des Verbindungsaufbaus, also **ein Logdatum pro TCP-Verbindung**
  - alle Pakete, die von der Firewall zurückgewiesen oder verworfen werden
- Reduzierung aller Paket Header auf eine kleine Teilmenge, die geloggt wird
- die meisten Angriffe, die sich über Firewall-Logdaten erkennen lassen, lassen sich auch allein über diese Teilmenge erkennen



# Agenda

- Konzept
- Log Reduction
- **Echtzeitanalyse**
- Anonymisierte Langzeitanalyse
- Datenschutz
- Entwicklung

### ■ Vorgehen

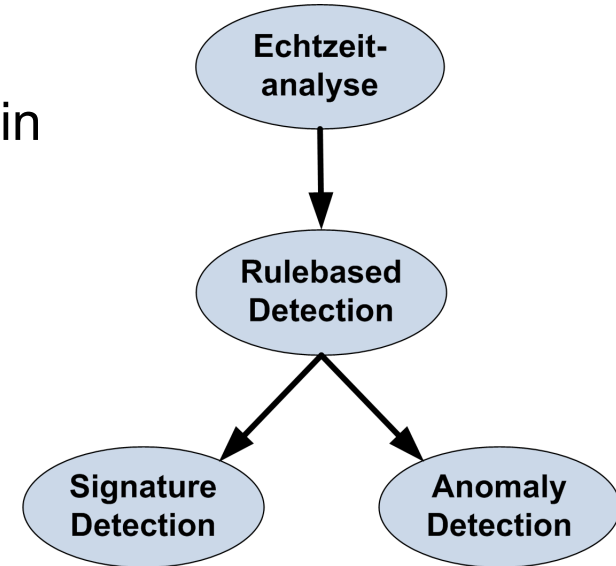
- Regelbasierte Überprüfung des Logdatenstroms in nahezu Echtzeit auf Angriffssignaturen in einer **lokalen Sicht**
- Einsatz geeigneter Algorithmen und Analysetechniken

- **Signature Detection**

- Präzise Erkennung bekannter Muster
  - z.B. SYN/FIN-Scan

- **Anomaly Detection**

- Erkennung von Anomalien im Kommunikationsverhalten über Schwellenwertanalyse auf Schicht 4
- Auflösung über eine Heuristik
- Dynamische Schwellenwertanpassung über das Verhalten der letzten halben Stunde



### ■ Ziele

- Auslösen eines Alarms bei Detektion eines Angriffs
- zeitnahe Reaktion auf einen Angriff
- Ergreifen von Schutzmaßnahmen gegen konkrete Bedrohung
  - Dienste anhalten, Ports schließen, User-Accounts sperren, Systeme abschalten, ...
- **Schadensminimierung**
- Grundlage zur **Forensik** und **juristischen Verfolgung** von Angreifern

- Alarme stehen im Bezug zu den originalen Logdaten und stellen diese im Schadszenario bereit
  - enthalten sensible, personenbezogene Informationen
    - IP-Adressen
    - E-Mail-Adressen
    - Benutzernamen
  - Informationen über die Alarme stehen ausschließlich dem Betreiber des Logdaten-Analyse-Systems zu Verfügung

# Logdaten-Analyse-System

## → Echtzeitanalyse (4/5)

- Beispiel - DDoS-Angriff aus dem Peacomm-Botnet
  - EagleX-Plugin Log-Viewer

The screenshot displays the LAS Log-Viewer application window. At the top, there are control buttons for 'Start', 'Stop', and status indicators for 'Offline' (selected) and 'Online'. A checkbox for 'Zyklisches Löschen' is also present. The main interface is divided into two main sections: 'Angriffsübersicht' (Attack Overview) and 'Angriffsdetails' (Attack Details).

**Angriffsübersicht:** This section shows a tree view of attacks. The root node is 'Distributed DoS Attack on 194.94.127.5'. It contains several sub-attacks, each with a list of specific attack types and their source IP addresses. For example, one sub-attack is 'Multiple DoS Attack by 122.164.177.195 on 194.94.127.5', which includes 'SYN Flood by 122.164.177.195 on 194.94.127.5 on Port [25428]' and 'ICMP Ping Flood by 122.164.177.195 on 194.94.127.5 [Echo Request]'. Other sub-attacks are listed for source IPs 58.187.139.175, 123.19.62.1, 203.87.207.14, and 41.232.162.50.

**Angriffsdetails:** This section provides specific information about the selected attack. The description is 'Distributed DoS Attack'. The status is 'Aktiv' (Active) and the success is 'Unbekannt' (Unknown). The start time is '04.07. 12:34:16' and the end time is '04.07. 12:38:45'. The total number of logs is 8433, and the current number of logs is also 8433. The absolute frequency is 1880 logs per minute, and the last frequency is also 1880 logs per minute.

**Angreifer (Attackers):** A list of source IP addresses is shown in a scrollable box:

- 41.232.162.50
- 41.251.49.12
- 58.186.214.135
- 58.186.222.186
- 58.187.77.165
- 58.187.139.175
- 58.187.184.201
- 58.187.235.185
- 59.149.198.210
- 79.183.124.50
- 81.36.70.107

**Ziele (Targets):** A list of target IP addresses is shown in a scrollable box:

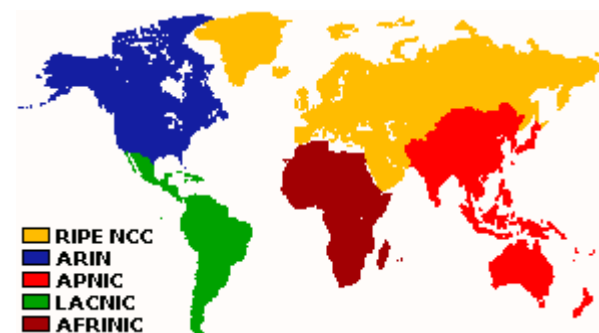
- 194.94.127.5

# Logdaten-Analyse-System

## → Echtzeitanalyse (5/5)

### ■ Beispiel - DDoS-Angriff aus dem Peacomm-Botnet

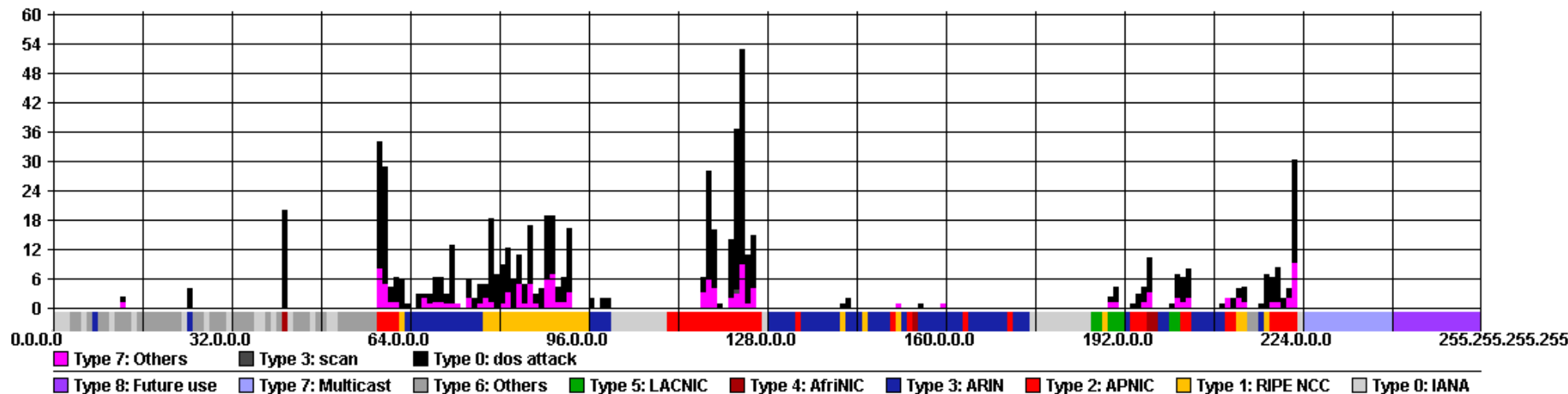
#### ■ IP-Map-Viewer



Quelle: Wikipedia

# ip addr

Datasource: VSYB - View: LAS Distributed



- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

### ■ Vorgehen

- Anwendung des Prinzips der **Deskriptoren** auf geloggte Ereignisse
  - Definition von Ereignissen in Logdaten (Deskriptoren)
  - Zählen dieser Ereignisse (Deskriptoren)
  - Graphische Darstellung der zeitlichen Häufigkeitsverläufe
  - ...
- **Anonymisierung** der Logdaten
- Wiederverwendung aller IAS-Tools möglich
  - Report-System
  - Neuronale Netze
- Aktuell gut 650.000 Deskriptoren für Firewall-Logdaten

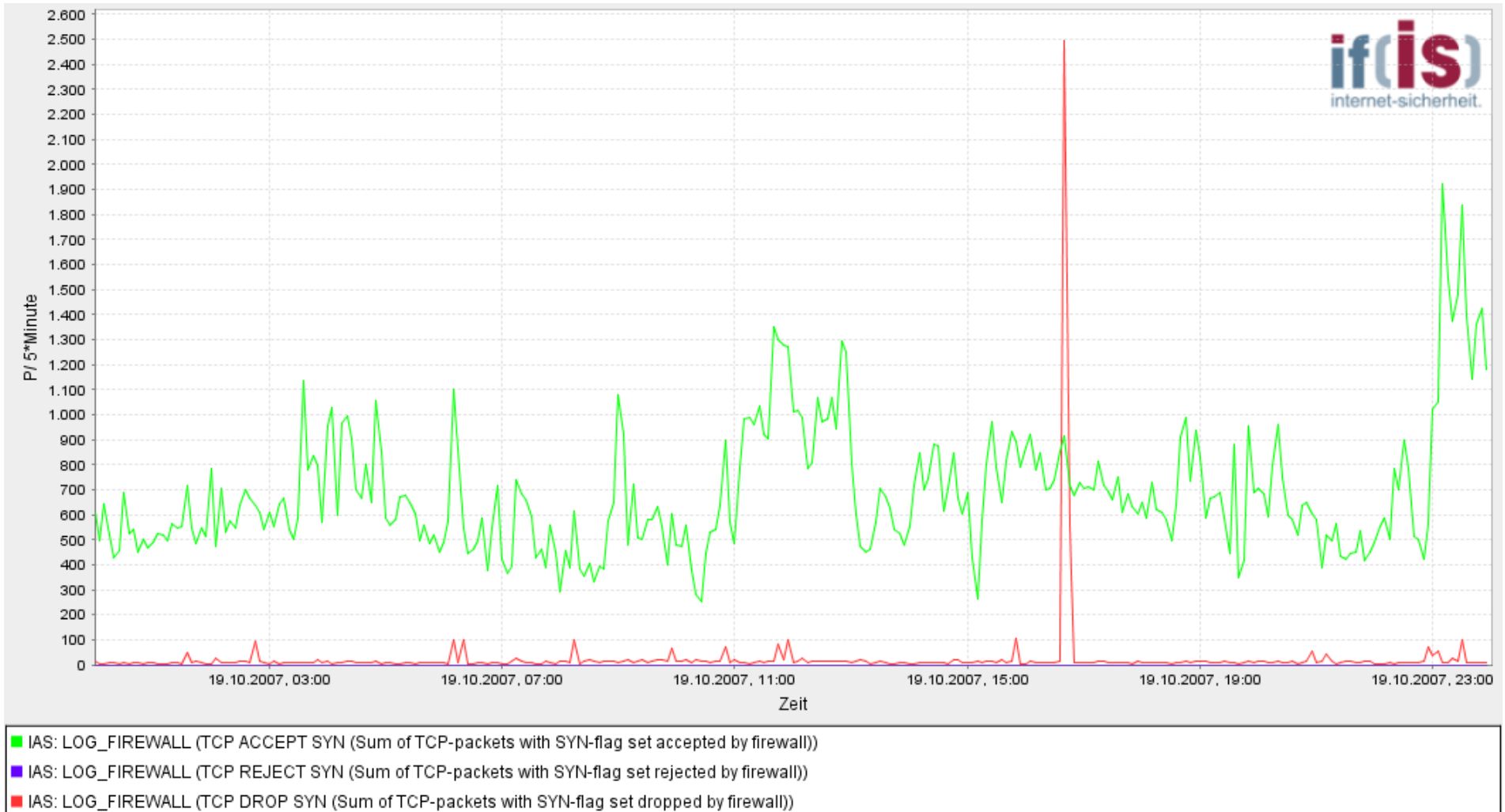
### ■ Ziele

- Ergänzung des Datenbestandes des **IAS**
- Schaffung eines **Referenzsystems** zum IAS
- Zusammenfügen der statistischen (anonymisierten) Logdaten mehrerer Netzwerke zu einer **globalen Sicht**
- Statistische Auswertung der Logdaten
  - Beschreibung von Mustern, Profilen, Technologietrends
  - Überblick über den aktuellen Zustand des Internets
  - Erkennung von Angriffssituationen und Anomalien
  - Prognosen von Mustern und Angriffen

# Logdaten-Analyse-System

## → Anonymisierte Langzeitanalyse (3/3)

### ■ Beispiel - TCP ACCEPT, DENY, REJECT



# Agenda

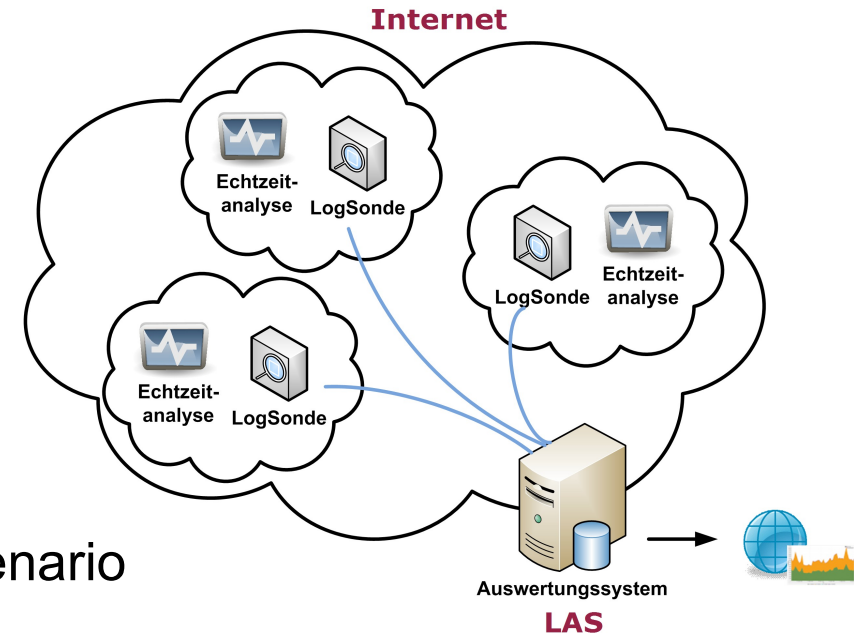
- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

### ■ Langzeitanalyse

- Prinzip der Deskriptoren
- Anonymisierung per Konzept
- Vom Datenschutz her unbedenklich

### ■ Echtzeitanalyse

- Darstellung der Logdaten im Schadszenario
  - nur Logdaten, die Angriffe identifizieren, werden dargestellt
  - alle anderen Logdaten werden verworfen
- keine automatische Speicherung der Logdaten
- Logdaten werden nach 24 Stunden aus der GUI des Logdaten-Analyse-Systems entfernt
- wichtige Logdaten können manuell gesichert werden



# Agenda

- **Konzept**
- **Log Reduction**
- **Echtzeitanalyse**
- **Anonymisierte Langzeitanalyse**
- **Datenschutz**
- **Entwicklung**

- Integration weiterer Logdatentypen
  - neue Deskriptoren
  - neue Echtzeitanalysemodule
- Integration von Metadeskriptoren
  - z.B. für erkannte Angriffe / Angriffstypen
- Anbindung ans Alarmierungsmodul
- Optimierung der
  - Erkennungstechniken / -algorithmen
  - Heuristik
- Pseudonymisierung der angezeigten Logdaten in Abhängigkeit von Benutzerrechten

## **Logdaten-Analyse-System**

Eine technische Lösung für das Erkennen von Angriffen

**Vielen Dank für Ihre Aufmerksamkeit**

**Fragen ?**

**Johannes Mrosek**  
**mrosek [at] internet-sicherheit [dot] de**

Institut für Internet-Sicherheit  
<https://www.internet-sicherheit.de>  
Fachhochschule Gelsenkirchen

