UNIVERSITÄT LEIPZIG

IDS

Intrusion Detection Systems

Arne Brutschy

Problemseminar Mobilität und
Sicherheit im Internet
SS 2003

Prof. Dr. K. Irmscher
Institut für Informatik
Universität Leipzig

Einführung

Was ist ein Intrusion Detection System?

- Hard- oder Softwaresystem
- dient der Erkennung eines Angriffs oder Angriffversuchs
- Meldung des Angriffs
- evtl. auch Vereitelung des Angriffs

Arten von IDS (1)

Netzwerkbasierte Intrusion Detection Systeme (NIDS)

- Analysieren Verkehr auf dem Netzwerk
- Alle Pakete einer Verbindung werden gesammelt
- und werden auf Angriffsversuche hin untersucht

System Integrity Verifiers (SIV)

- Überwachen Integrität wichtiger Systemdateien
- Meistens mittels Bildung von Prüfsummen
- Arbeiten hostbasiert (HIDS)

Arten von IDS (2)

Log File Monitors (LFM)

- Überwachen Logdateien relevanter Systemdienste
- Arbeiten meistens hostbasiert

Deception Systeme

- Enthalten oder emulieren absichtlich Sicherheitslücken
- Werden stark überwacht
- Man versucht, Angreifer zu fangen
- oder zumindest ihre Techniken zu erlernen

In diesem Vortrag nur NIDS und verteilte HIDS.

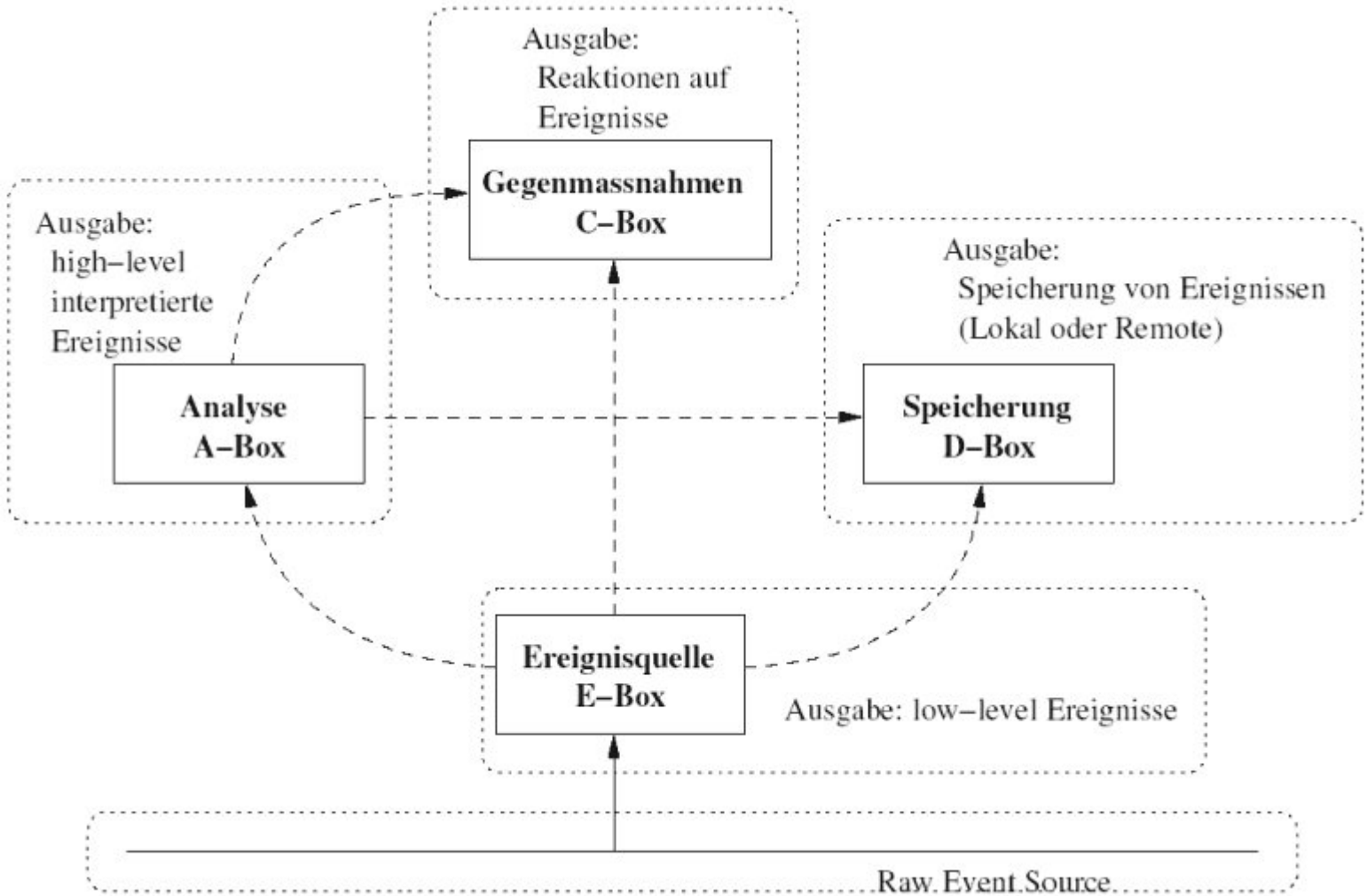
Aufgaben eines IDS

- Vermeidung von Problemen durch Abschreckung
- Erkennung von Problemen, die von anderen Sicherheitsmaßnahmen nicht erkannt wurden
- Erkennung von Vorzeichen eines Angriffs
- Dokumentation einer Bedrohung
- Aufdeckung von Sicherheitslücken

Architektur – NIDS

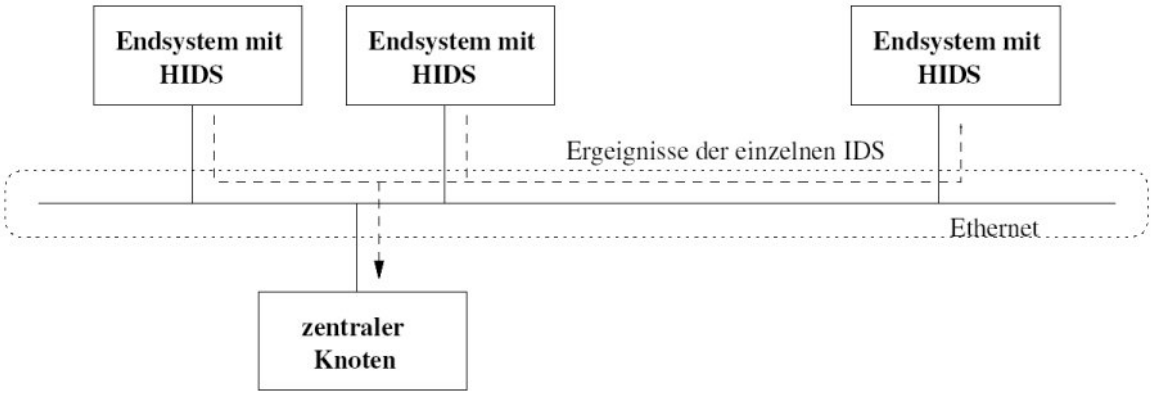
- Kommerzielle Systeme erlauben selten Einblick in die Architektur
- Deshalb Entwicklung des „Common Intrusion Detection Framework“
- Definiert Satz von allgemein üblichen Komponenten
  - Ereignisquelle
  - Analyseeinheit
  - Speicherung von Ereignissen
  - Reaktions- und Gegenmaßnameneinheit
- Diesem Rahmenwerk folgen die meisten der heutigen Implementierungen
- Beispiel: Snort

Architektur – CIDF



Architektur – verteilte HIDS

- Hostbasiertes IDS auf möglichst vielen Clients
- Zentraler Managementknoten
- Dieser korreliert alle auftretenen Ereignisse
- Vereinfacht Administration
- Kompensiert Hauptnachteil von HIDS



Architektur – hybride IDS

- Vereinigt HIDS und NIDS
- Kompensiert Hauptnachteile beider Systeme
- Hauptknoten korreliert auftretene Netzwerkereignisse mit denen auf den einzelnen Clients
- Hohe Leistungsanforderungen
- Sehr komplexe Systeme
- Noch nicht weit Verbreitet

Passive Analyse

IDS analysiert die durch passives Abhören des Netzwerksverkehrs erhaltenen Daten

- Signaturerkennung
  - Erkennt Muster bekannter Angriffe
  - Pattern Matching im Payload des Pakets
  - Andere Parameter wie z.B. typische Ports
- Statistische Analyse
  - Erkennt Anomalien im „normalen“ Netzwerkverkehr
- Andere, seltenere Methoden
  - Lernfähige Systeme
  - Semi-intelligente Systeme

Reaktionsarten

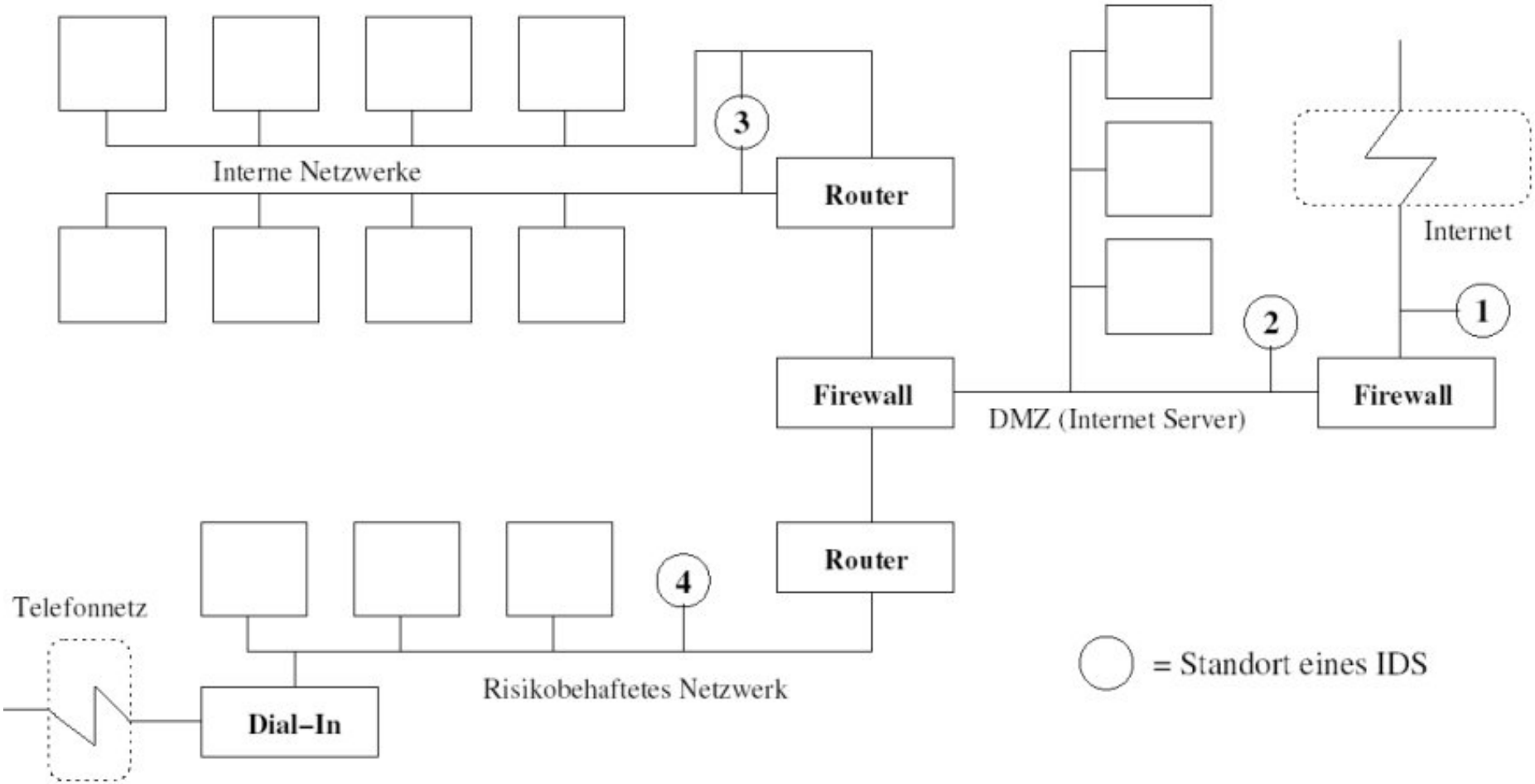
Passive Reaktionen

- Alarm und Benachrichtigung z.B. SNMP-Traps, Popup-Fenster, SMS etc.
- Logging

Aktive Reaktionen

- Beenden der Verbindung
- Aktivieren von Firewall-Regeln
- Aktionen gegen den Angreifer

Einsatz


Interne Netzwerke
3
Router
Internet
1
2
Firewall
DMZ (Internet Server)
Firewall
Router
4
Telefonnetz
Risikobehaftetes Netzwerk
Dial–In
= Standort eines IDS

Probleme

Unzureichende Informationen im Netzwerk

- Ein IDS kann nicht sicher vorhersagen, wie ein Endsystem ein empfangendes Paket verarbeitet
- Implementierungen der Protokollstacks sind inkonsistent
- Das System kann nicht auf einfache Weise wissen, welches OS ein Endsystem benutzt

Anfälligkeit für Denial of Service

- Da IDS passiv sind, lassen sie den Netzwerkverkehr im falle einer Überlastung unbeobachtet
- Ein Angreifer kann somit nach einem erfolgreichen DoS-Angriff das dahinterliegene Netzwerk angreifen

Angriffe (1)

Einfache Angriffe

- Änderung von Angriffskripten
- Paketfragmentierung
- Koordinierte, langsame Angriffe
- Langsame Scans

Denial of Service Angriffe

- Existieren manchmal aufgrund von Fehlern im IDS
- Meistens basieren sie auf Ressourcenmangel im IDS
- Beispiel: Fluten eines IDS mit sinnlosen Verbindungsrequests bis es keinen freien Hauptspeicher mehr hat

Missbrauch aktiver Reaktionen

- Aktive Reaktionen eines IDS können genutzt werden um Sicherheitslücken im System zu erzeugen
- Beispiel: Sperren von legitimen Verbindungen

Angriffe (2)

Insertion
- Einschleusen von Paketen in das IDS
- Angreifer sendet Pakete, die das IDS annimmt, das Endsystem aber verwirft

Evasion
- Pakete, die das IDS umgehen
- Angreifer sendet Pakete, die das IDS verwirft, das Endsystem aber annimmt

- Das IDS hat somit andere Daten als das Endsystem
- Damit umgehen der Signaturanalyse

Quellen

- Stuart Staniford-Chen, Dan Schnackenberg, Brian Tung, *Common Intrusion Detection Framework*, Oktober 1998.
  http://www.isi.edu/gost/cidf/papers/cidf-isw.txt

- Rebecca G. Bace, Peter Mell, *NIST Special Publication on Intrusion Detection Systems*, Februar 2001.
  http://www.snort.org/docs/nist-ids.pdf

- Robert Graham, *FAQ: Network Intrusion Detection Systems*, März 2000.
  http://www.robertgraham.com/pubs/network-intrusion-detection.html

- Thomas H. Ptacek, Timothy N. Newsham, *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection*, Januar 1998.
  http://www.insecure.org/stf/secnet_ids/secnet_ids.html

- Christopher Krügel, Thomas Toth, Engin Kirda, *Stateful Intrusion Detection for High-Speed Networks*, Mai 2002.
  http://www.infosys.tuwien.ac.at/Staff/chris/doc/2002_04.ps