Intrusion Detection (IDS)

Alarmanlage im Netzwerk

Dipl.-Inf. Marco Thorbrügge

DFN-Workshop „RZ-bezogene Netzdienste“

21. bis 22.03.2002 in Kassel

DFN CERT

IDS: Einsatzzweck

(Sammlung und) Auswertung von Informationen (Daten) zum Zwecke der Erkennung von

- Missbrauch (Angriffe, Portscans, Würmer, ...)
- Anomalien im Betrieb (vorherige Erhebung des Normalzustandes notwendig)

DFN CERT

Unterscheidung: Arten von IDS

IDS unterteilen sich grob in 3 Kategorien:

- NIDS (Network based IDS):
  - erhebt Kommunikationsdaten eines kompletten (Sub)Netzwerks (Bsp.: *snort*)
- HIDS (Host based IDS):
  - nur für einen einzelnen Host zuständig (Bsp.: *tripwire*)
- Application based IDS:
  - „eingebaut“ in Anwendungen (Bsp.: verschiedene Serveranwendungen wie *Apache*, *wu-ftpd*)

DFN CERT

IDS: Was wird untersucht?

- IDS sammelt Pakete, die zu einer Verbindung gehören
- Gesamte Verbindung wird betrachtet (Pakete werden zusammengesetzt)
- Nicht nur der Header-, sondern auch der Datenteil wird untersucht
- Auch einzelne Pakete können zugeordnet werden (Bsp: Portscans)

DFN CERT

IDS: Momentaufnahme

- IDS wird heutzutage meist als Einbruchsalarmanlage genutzt
- Reaktive Ansätze fragwürdig, eher sogar gefährlich (Gegenscans, Abbrechen der Verbindung, etc.)
- Korrelation zwischen mehreren IDS nur sehr eingeschränkt möglich
- Frühwarnung nicht gegeben
- IDS derzeit sehr ressourcenintensiv

DFN CERT

IDS: Zukünftige Entwicklungen

- Entwicklung vom IDS hin zum (DFN-weiten) Frühwarnsystem
- Einsatz von IDS als Mittel zur Beweissicherung (Forensik)
- Einsatz von IDS in Höchstgeschwindigkeitsnetzen
- Einsatz verteilter IDS-Sensoren

DFN CERT

Notwendige Unterstützung für Anwender

Sehr großer Forschungsbedarf:

- Lastverteilung bei IDS in Hochgeschwindigkeitsnetzen
- Einsatz von IDS in VPN-Umgebungen (IPSec)
- Korrelation von IDS-Daten mit anderen Informationen (Netflow)
- Sichere Kommunikation zwischen verteilten IDS
- Zentrale Administration verteilter IDS (Policy-Verteilung)
- IDS als Verifikationswerkzeug für Firewalls

➢ Durchführung IDS-Forschungsprojekt:

Sammlung von Know-How, von dem DFN-Anwender profitieren

DFN CERT