Intrusion-Detection und Prevention

Erfahrungsbericht aus Münster

vorgestellt von

Cornelia Ossendorf

24.10.06

Marketingbeschreibung für Intrusion Prevention Systeme

„ Intrusion-Prevention-Technologie ist der logische Nachfolger und die Ergänzung zu herkömmlichen Firewalls für Hosts und Netzwerke und wurde entwickelt um Schutz zu bieten, den einfache Firewalls nicht mehr gewährleisten können“

Auszug aus einem Whitepaper von McAfee zum Thema Host und Network Intrusion Prevention

Definitionen

- IDS
  Systeme für die Überwachung von Computern und Datennetzen mit dem Ziel Angriffe und Missbrauch zu erkennen und zu analysieren.

- IPS
  Geht über die Definition IDS hinaus.
  Das System ist fähig, Angriffe in Echtzeit zu erkennen und abzuwehren.

Bestandteile IDS/IPS

- Netzwerkbasierende Systeme, **Netzsensoren**
- Rechnerbasierende Systeme, **Hostsensoren**
- Managementstationen
  - *Datenbankkomponenten*
  - *Auswertungsstationen*

.

Netzsensoren

- Typische Vertreter sind:
  - McAfee Intrushield 4000
  - 3Com TippingPoint 2400
  - Sonicwall Pro 5060
  - Top Layer Attack Mitigator IPS 5500
- im Netzwerk in Münster im Einsatz:

Ziele in Münster

- Entlastung der Netzabteilung
  - Mandatenfähigkeit
- Netzzonen gegeneinander schützen
  - Universität
  - RAS-Bereich
  - Radiologie
  - UKM, UKM-ZMK

Was ist IDS/IPS nicht ?

- 100 % Schutz
- Einmalige Installation ohne Pflege sondern ein sich entwicklender Prozess
- Keine One-WoMan-Show, es verlangt koordiniertes Arbeiten verschiedener Institute