IDS/IPS

Inhaltsverzeichnis

IDS erkennt verdächtigen Netzwerk- oder Systemverkehr, IPS kann ihn zusätzlich blockieren. Beide ergänzen Firewalls durch inhaltliche bzw. verhaltensbasierte Analyse.

1 Funktionsweise

Sensoren prüfen Pakete oder Host-Ereignisse anhand von Signaturen und Anomalien. Ein IDS alarmiert; ein IPS greift aktiv in den Traffic-Pfad ein.

- **Network IDS/IPS:** Verkehr im Netzspiegel oder Inline
- **Host IDS:** lokale Integrität und Verhalten
- **Signatures & Anomalies:** bekannte und ungewöhnliche Muster

2 Typische Einsatzbereiche

- Perimeter und Segmentgrenzen
- Schutz kritischer Serverstrecken
- Erkennung von Exploits und Scan-Aktivitäten

3 Wichtige Hinweise

- Inline-IPS kann bei False Positives Dienste stören.
- Signatur-Updates und Baselines pflegen.
- Alerts brauchen klare Zuständigkeiten.

4 Fazit

IDS/IPS erhöhen Sichtbarkeit und Abwehrtiefe – am wirksamsten als abgestimmte Schicht neben Firewall, Hardening und Monitoring.