**Datensicherheit: IDS und IPS**

1. Einführung in IDS und IPS

Definition IDS:

Intrusion Detection System überwacht Netzwerke und Systeme auf verdächtige Aktivitäten oder Sicherheitsrichtlinienverletzungen und meldet diese.

Definition IPS:

Intrusion Prevention System erweitert Funktionalität des IDS, indem es Angriffe erkennt und Maßnahmen zur Abwehr ergreift.

Ziel:

Schutz von Netzwerken/Systemen vor Angriffen

1. Unterschiede IDS und IPS

IDS

Passiv:

Erkennt Angriffe und informiert Admin’s, kein aktives eingreifen

Beispiele:

Snort (Network IDS), OSSEC (Host-based IDS)

IPS

Aktiv:

IDS + führt automatisch Gegenmaßnahmen durch z.B. blockieren von Datenverkehr

Beispiele:

Cisco IPS, Suricata (Auch als IDS einsetzbar)

1. Funktionsweisen von IDS

Erkennungsmodi

Signaturbasiert:

Erkennt bekannte Angriffe durch Vergleich mit Datenbank von Angriffssignaturen (Anhand deren Modus Operandi)

Anomaliebasiert:

Erkennt ungewöhnliche Verhaltensmuster,

die auf einen möglichen Angriff hindeuten können.

Komponenten

Sensoren:

Erfassen und analysieren Datenverkehr oder Systemaktivitäten

Management-Server:

Zentrale Einheit zur Analyse der gesammelten Daten und Generierung von Alarmen

1. Funktionsweisen von IPS

Erkennungsmodi

Wie bei IDS, zusätzlich mit Echtzeitverteidigung

Gegenmaßnahmen

Paketfilterung:

Blockiert verdächtigen Datenverkehr basierend auf vordefinierten Regeln

Verbindungstermination:

Schließt Verbindungen zu potentiellen Angreifern

Quarantäne:

Isoliert verdächtige Dateien oder Systeme zur weiteren Untersuchung

1. Einsatzmöglichkeiten

IDS

Frühzeitige Erkennung von Sicherheitsverletzungen

Hilft bei der Identifizierung von Schwachstellen und der Verbesserung der Sicherheitsrichtlinien

IPS

Echtzeitschutz, reduzierte Reaktionszeit, Auto-Abwehr ohne menschl. Eingreifen

1. Herausforderungen und Grenzen

IDS

Falsepositive, nur reaktiv

IPS

Performance, Falsepositive, Komplexe Config um effektiv zu sein

1. Praxisbeispiele

*~Wie immer ist es genauso sinnvoll wie Herr Hebig, gar nicht~*

1. Fazit

Herr Hebig ist immer noch genauso sinnlos wie ein Staubsauger in der Wüste und [das gleiche was schon vier mal in der PP wiederholt wurde].