CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

IDS/IPS

Intrusion Detection System

Ein **Intrusion Detection System**, abgekürzt IDS, ist in der Lage, auf Computer, Server oder Netzwerke gerichtete Angriffe zu **erkennen** und **darüber zu informieren**. Oft ergänzt das Intrusion Detection System die üblichen Funktionen einer Firewall.

Intrusion Prevention System

Ein **Intrusion Prevention System**, abgekürzt IPS, ist in der Lage, **Angriffe** auf Netzwerke oder Computersysteme zu **erkennen** und **automatische Abwehrmaßnahmen** zu ergreifen. Es sorgt gegenüber herkömmlichen Firewall-Systemen für einen zusätzlichen Schutz.

Funktionsweise IDS

- IDS überwachen den Netzwerkverkehr und analysieren ihn, um verdächtige Aktivitäten zu identifizieren. Sie verwenden dabei eine Kombination aus bekannten **Angriffssignaturen** und anormalen **Verhaltensmustern**

- **Signaturenbasiertes IDS erkennt** Angriffe **anhand bekannter Muster** oder Signaturen von Malware und anderen bösartigen Aktivitäten.

- **Anomaliebasiertes IDS** lernt das normale Verkehrsmuster und **erkennt** dann **Abweichungen**, die auf einen Angriff hindeuten könnten

Funktionsweise IDS

- Bei der Erkennung von verdächtigem Verhalten löst das IDS Alarme aus. Diese Alarme informieren die Netzwerkadministratoren oder ein zentrales Sicherheitsmanagementsystem

- IDS **protokollieren verdächtige Aktivitäten**, um sie für weitere Analysen und forensische Untersuchungen bereitzustellen

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm