

Intrusion Detection und Intrusion Prevention Systeme

Referent: Christian Götz

Dauer: 2 Tage

Intrusion Detection Systeme (IDS) sind ein wichtiger Baustein in einem Gesamt-Sicherheitskonzept. Ergänzend zu Firewalls, VPNs und Content-Security Systemen überwachen Intrusion Detection Systeme die Vorgänge im Netzwerk und alarmieren den Administrator, falls charakteristische Angriffsmuster erkennbar sind. Darüber hinaus bieten einige Hersteller so genannte Intrusion Prevention Systeme (IPS) an, die bei unerwünschten Vorgängen nicht nur alarmieren, sondern auch aktiv Gegenmaßnahmen ergreifen. Leider versteht fast jeder Hersteller etwas anderes unter dem Begriff IPS und dementsprechend sind die Produkte nicht immer miteinander vergleichbar.

Dieses Seminar veranschaulicht praxisnah die technischen Grundlagen, die Implementierung und den Betrieb von modernen Intrusion Detection und Intrusion Prevention Systemen. In der Einführung erfahren Sie den Aufbau und die Grundfunktionen heutiger IDS und IPS Systeme und wie diese sinnvoll eingesetzt werden können. Anschließend werden organisatorische Prozesse und Workflows zur Integration in bestehende Umgebungen besprochen und dabei Aspekte wie Verantwortlichkeiten, Positionierung und Dimensionierung behandelt. Abschließend werden auch Betriebsaspekte und mögliche Eskalationsprozeduren erläutert. Sie erhalten eine Produkt- und Marktübersicht sowie einen Kriterienkatalog samt Entscheidungshilfen.

Zielgruppe:

Administratoren, EDV-Leiter, Netzwerkverantwortliche und IT-Security Manager, die sich mit IT-sicherheitsrelevanten Themen beschäftigen.

Voraussetzung:

Kenntnisse in Netzwerkbetriebssystemen, grundlegende Netzwerkkennnisse in TCP/IP.

Termine:

nach Vereinbarung