Intrusion Detection Systeme

Überblick

Bei den Vorteilen und der Bequemlichkeit, die Internet, Intranet oder Extranet mit sich bringen, wird leider oft übersehen, welche Gefahren von dieser neuen Art der Kommunikation ausgehen. Immer häufiger erfolgen Angriffe auf die IT-Infrastruktur von Unternehmen, um Daten zu stehlen bzw. zu verändern oder um die Kontrolle von Diensten oder Rechnern zu stören bzw. zu übernehmen. Diese Angriffe können sowohl aus dem Internet als auch aus dem internen Netzwerk erfolgen.
Ein Intrusion Detection System (IDS) soll Angriffe in Echtzeit erkennen und Alarmmeldungen absetzen sowie alle Ereignisse protokollieren. Ein IDS funktioniert also ähnlich einer Alarmanlage. Werden Abweichungen von einem definierten Normalzustand erkannt, wird das Ereignis dokumentiert und in Abhängigkeit von der Konfiguration z.B. ein bestimmter Alarm ausgelöst.

Leistungsmerkmale

Das Ziel von Intrusion Detection ist es, Angriffe zu erkennen, diese den für die Systemsicherheit zuständigen Personen zu melden und evtl. geeignete Gegenmaßnahmen einzuleiten. Je nach Einsatzgebiet unterscheidet man zwischen Netzwerk- und Host-basierten Intrusion Detection Systemen.

Ein IDS besteht aus den folgenden Hauptkomponenten:

- Komponente zur Datensammlung und Datenanalyse
  (Welche Informationen weichen von einem definierten Normalzustand ab ?)
- Komponente zur Ergebnisdarstellung und Administration
  (Analyseergebnisse werden benutzergerecht aufbereitet und dienen dem Sicherheitsbeauftragten als Entscheidungshilfe für das weitere Vorgehen)

Vorteile

Intrusion Detection Systeme erhöhen die Sicherheit im Netzwerk eines Unternehmens.
Im wesentlichen bieten diese Systeme folgende Vorteile:

- Automatisches Erkennen von internen und externen Angriffen auf Rechnersysteme und Firmennetze
- In Abhängigkeit von der Security-Policy können bei den Angriffen diverse Aktionen ausgelöst werden, z.B. ein Alarm oder die Änderung von Firewall-Regeln
- Automatische Benachrichtigung der zuständigen Personen im Fall eines Angriffs
- Automatische Bearbeitung von Datenströmen

Ergebnisse/Dokumentationen

Je nachdem, wie unser Einsatz im Bereich Intrusion Detection System genau definiert ist, können folgende Leistungen und Dokumentationen erbracht bzw. erstellt werden:

- Herstellerunabhängige Beratung zu Intrusion Detection Systemen
- Erstellen eines Grob- und/oder Feinkonzeptes mit detaillierter Dokumentation
- Anbieter- und Produktauswahl
- Testbetrieb und Implementierung

Dauer

Wir erbringen Beratungsdienstleistungen sowohl auf Festpreis- als auch auf Stunden-Basis. Aufgrund unserer Flexibilität können wir jedes Engagement so gestalten, dass Ihren finanziellen und technischen Anforderungen genau entsprochen wird.