

Einleitung

Der Einsatz von Intrusion Detection Systemen hat in den letzten zwei Jahren stark zugenommen. Die Installation von Firewalls alleine reicht heute definitiv nicht mehr aus, um Computersysteme und Netzwerke hinreichend zu schützen. Um einen Überblick über tatsächlich ablaufende Vorgänge zu bekommen und die Kontrolle bewahren zu können, sind Intrusion Detection Systeme eine zwingende Erweiterung der IT-Sicherheitsinfrastruktur.

Für einen Vergleich von Intrusion Detection Systemen, müssen zunächst die Vergleichskriterien und relevanten Parameter bestimmt werden. Die nachfolgenden Abschnitte sollen deshalb zunächst einen Überblick über Typen von Intrusion Detection Systemen und sich dahinter verbergende Technologien vermitteln, bevor die in der Praxis relevanten Auswahlkriterien diskutiert werden, die später den Erfolg einer Intrusion Detection Lösung maßgeblich beeinflussen.

1. Architektur eines Intrusion Detection Systems

1.1. Funktionskomponenten eines Intrusion Detection Systems

Prinzipiell besteht ein Intrusion Detection System (IDS) aus den folgenden drei Hauptkomponenten:

- Einer Komponente zur Datensammlung, welche relevante Informationen z.B. über den allgemeinen Systemzustand und die Betriebsmittelvergabe sammelt. In Abhängigkeit vom verwendeten Typ von Intrusion Detection System sammelt die Komponente Netzwerkdaten, Systemdaten wie z.B. Systemlogs oder Systemaufrufe. Wichtig ist, dass alle Daten durch diese Komponente erfasst und nachfolgenden Komponenten verlustfrei zur Verfügung gestellt werden können.
- Einer Komponente zur Datenanalyse, welche die gesammelten Daten im Hinblick auf mögliche Angriffe analysiert.
- Einer Komponente zur Ergebnisdarstellung, die das Analyseergebnis aufbereitet und Möglichkeiten bietet, beim Auftreten bestimmter Ereignisse weitere Aktionen zu initiieren, wie z.B. Ausgeben einer Alarmmeldung auf einer Konsole, Versenden einer Email an Administratoren oder Absetzen eines SNMP-Traps. Als Stichwort sei hier der Begriff „Intrusion Response“ genannt.

Ein System, das diese drei Komponenten kombiniert, wird auch als Sensor bezeichnet.

1.2. Verwaltungswerkzeuge

Neben Sensoren, den Modulen zur Erfassung und Analyse der Daten, muss das Intrusion Detection System Werkzeuge liefern, die eine Steuerung der Sensoren zulässt. Zu den Aufgaben dieser Werkzeuge gehört die Darstellung von Ereignismeldungen in Form einer Konsole, die Speicherung von Konfigurationsinformationen über die Sensoren und die dauerhafte Speicherung von Ereignismeldungen. Eine Komponente, die alle diese Aufgaben

vereint wird als Managementstation bezeichnet. Die Managementstation muss eine grafische Benutzeroberfläche oder ein „Command Line Interface“ zur Steuerung der Sensoren bereitstellen.

Eine Managementstation muss die Möglichkeit bieten, mehrere Sensoren zentral zu administrieren und Ereignismeldungen dieser Sensoren zu speichern.



cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de

2. Typen von Intrusion Detection Systemen

2.1. Unterscheidungskriterien

Der Begriff „Intrusion Detection System“ und der Funktionsumfang solcher Systeme unterlag in den vergangenen Jahren einem stetigen Wandel. Konnten erste Produkte lediglich einfache Vorgänge auf Systemen, wie z.B. Anmeldeversuche oder Zugriffe auf bestimmte Systemdateien überwachen und melden, haben sich der Funktionsumfang und die Einsatzgebiete für Intrusion Detection Systeme wesentlich erweitert.

Prinzipiell müssen vier Unterscheidungskriterien für Intrusion Detection Systeme in die Betrachtungen einbezogen werden:

- Intrusion Detection Systeme die Schwachstellen und Angriffsmöglichkeiten „präventiv“ auf Netzwerkebene erkennen.
- Intrusion Detection Systeme die Schwachstellen und Angriffsmöglichkeiten „präventiv“ auf Systemebene (Betriebssystemebene oder Applikationsebene) erkennen.
- Intrusion Detection Systeme die Angriffsversuche und Angriffe auf Netzwerkebene „in Echtzeit“ erkennen.
- Intrusion Detection Systeme die Angriffsversuche und Angriffe auf Systemebene (Betriebssystemebene oder Applikationsebene) „in Echtzeit“ erkennen.

2.2. Scanner

Obwohl es auf den ersten Blick etwas seltsam erscheinen mag, müssen auch „Netzwerkscanner“, „Systemscanner“ bzw. „OS-Scanner“ und „Applikationsscanner“ zur Familie der Intrusion Detection Systeme gerechnet werden. Betrachtet man als „Intrusion Detection System“ eine Gesamtlösung, sind Scanner eine unverzichtbare Erweiterung. Der effektivste Schutz vor Angriffen ist mit Sicherheit die Methode, Schwachstellen und Angriffsmöglichkeiten aufzuspüren und zu beheben, bevor es unbetenweise Dritte tun. Desweiteren können die Ergebnisse zur Ereignisskorrelation verwandt werden.

2.3. Networkbased Intrusion Detection Systems (NIDS)

Netzwerkbasierte Intrusion Detection Systeme erfassen den gesamten Datenverkehr in einem Netzwerksegment, analysieren die Daten und ermitteln anhand eines definierten Regelwerkes (z.B. anhand von Signaturen), ob es sich um einen Angriff (Intrusion) handelt.

Damit ein Intrusion Detection System den gesamten Datenverkehr mitlesen kann, muss es

sinnvoll in ein zu überwachendes Netzwerksegment integriert werden. Über ein so genanntes „Sniffer-Interface“ werden alle Daten, die über das Netzkabel transferiert werden mitgelesen und an ein Analysemodul transferiert.

Dieses „Sniffer-Interface“ muss direkt in das zu überwachende Netzwerksegment integriert werden und wird im „Promiscuous Mode“ betrieben. Um das IDS nicht selbst zum Ziel von Angriffen werden zu lassen, werden die Systeme in den „Stealth Mode“ versetzt, d.h. es wird kein Netzwerkprotokoll auf das Interface gebunden. Das System antwortet somit nicht mehr auf Anfragen und ist im Segment nicht mehr „sichtbar“. Über das Interface können aber weiter Daten gelesen („gesniff“) werden.

2.4. Network Nodebased Intrusion Detection Systems (NNIDS)

Im Gegensatz zu NIDS werden Network Nodebased Intrusion Detection Systems (NNIDS) direkt auf einem Zielsystem installiert. Moderne NNIDS analysieren den gesamten Datenverkehr von und zu einem Computersystem, analysieren Vorgänge auf Betriebssystemebene (z.B. Zugriffe auf Systemdateien, fehlgeschlagene Anmeldeversuche) und bieten rudimentäre Methoden zum Blocken von Netzwerkpaketen bei der Erkennung von Angriffen („Firewalling“).

Der große Vorteil von NNIDS liegt darin, dass typische Probleme wie sie in komplexen Netzwerkumgebungen auftreten umgangen werden können. Nachteilig an NNIDS ist, dass Produktivsysteme angefasst werden müssen und Rechenleistung, wenn auch nur minimal, zur Verfügung stellen müssen. Zudem arbeiten NNIDS nicht im „Stealth Mode“ und stellen somit zunächst selbst ein Ziel für Angriffe dar.

2.5. Hostbased Intrusion Detection Systems (HIDS)

Hostbased Intrusion Detection Systems (HIDS) verlieren zunehmend an Bedeutung – um nicht zu sagen, sie sind bereits bedeutungslos – und werden durch NNIDS oder „Intrusion Prevention Systeme“ zunehmend abgelöst. HIDS beziehen ihre Daten primär aus Logfiles. Die Netzwerkkommunikation eines Systems wird oftmals überhaupt nicht in die Analyse einbezogen, was z.B. dazu führt, dass selbst banale Portscans nicht erkannt werden können. Eine Unterart der HIDS sind die so genannten „System Integrity Verifiers“, die anhand von Prüfsummen bestimmen, ob Veränderungen am System vorgenommen wurden.

Der Nutzen einer solcher Intrusion Detection Lösung bleibt unter den heute bestehenden Bedrohungspotentialen sicherlich fraglich. Zudem werden Funktionen dieser Art heute auch von NNIDS und Intrusion Prevention Systemen als integraler Bestandteil angeboten.

2.6. Intrusion Prevention Systeme

Intrusion Detection Systeme bieten per se zunächst keinen Schutz. Angriffsversuche und Angriffe können zwar erkannt werden, um aber die Folgen eines solchen Angriffs abzuwenden, bieten rein auf die Erkennung ausgerichtete Systeme nur begrenzt Möglichkeiten Gegenmaßnahmen zu ergreifen. Diesen Mangel versuchen „Intrusion Prevention Systeme“ oder „Intrusion Protection Systeme“ zu beheben. Die Namen „Prevention System“ oder „Protection System“ sind Schöpfungen von Herstellern und stellen kein allgemeines Klassifizierungsmerkmal dar. Gemeinsam ist jedoch beiden Typen, dass sie neben der reinen Erkennung Angriffe bzw. die Folgen von Angriffen aktiv verhindern können.

Die Funktionsweise und die Systemebenen auf denen diese Intrusion Prevention Systeme funktionieren unterscheiden sich sehr stark von Produkt zu Produkt. Erste Versionen von Intrusion Prevention Systemen konnten nur ein oder mehrere Netzwerkkomponenten eines Rechnersystems überwachen und „unerlaubte“ Netzwerkverbindungen unterbrechen. Der große Vorteil z.B. gegenüber den klassischen „Personal-Firewalls“ lag aber bereits bei diesen Systemen darin, dass die Übertragung von Netzwerkpaketeten nicht aufgrund von Regeln erlaubt und unterbunden wurde, die definierten über welche Netzwerkprotokolle der Datentransport stattfinden sollte, sondern es wurde der Inhalt der Datenpakete analysiert und anhand eines im Intrusion Prevention Systeme kodierten Regelwerkes konnte festgestellt werden, ob es sich um unerlaubten Netzwerkverkehr handelt oder nicht. Da die reine Betrachtung des Netzwerkdatenverkehrs alleine aber nicht ausreicht, um heute einen umfassenden Schutz für Computersysteme zu bieten, mussten die Intrusion Prevention Systeme um die Fähigkeit erweitert werden, auch Prozesse und Applikationen auf dem zu schützenden System zu überwachen und zu steuern.



cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de

2.7. Inline Intrusion Detection Systeme

Inline Intrusion Detection Systeme werden als transparentes Gateway direkt in die Netzwerkverbindung eingeklinkt. Alle Daten werden dem IDS über ein Netzwerkkomponenteninterface zugeführt, untersucht und verlassen das System wieder über ein zweites Interface, sofern keine unerlaubten Netzwerkpakete entdeckt werden konnten. Das Inline Intrusion Detection System greift aktiv in den Netzwerkverkehr ein und erlaubt nur die Übertragung von legitimen Datenverkehr. Inline Intrusion Detection Systeme eignen sich somit dafür, kritische Netzwerksegmente aktiv zu schützen.

2.8. Application Intrusion Detection Systeme

Netzwerkbasierete Intrusion Detection Systeme können in der Regel nur sehr begrenzt überwachen, welche Ereignisse sich auf Applikationsebene abspielen. Um eine Erkennung auf Applikationsebene zu ermöglichen, wurden Application Intrusion Detection Systeme entwickelt, die Daten eines bestimmten Anwendungstyps bzw. eines Netzwerkprotokoll wie z.B. HTTP aus einem Datenstrom herausfiltern, die Datenpakete wieder zusammensetzen und nun nachfolgend versuchen, den Inhalt und die Bedeutung einer Anfrage an eine Applikation zu ermitteln. Das IDS versucht quasi die Anfrage zu verstehen und kann diese Anfrage in Echtzeit unterdrücken, sofern sich in der Anfrage Aufrufe mit schädlichem Inhalt befinden.

Diese Art der Erkennung von Schwachstellen ist noch sehr neu und funktioniert derzeit nur für wenige Anwendungen und Protokolle. Allerdings bietet dieser Ansatz den Vorteil, dass Überwachung auf Applikationsebene auch ohne aufwendige Integration von Security (Reverse-)Proxies möglich ist.

Autor: Christian Götz, Berater bei cirosec