Was ist ein Intrusion-Detection-System (IDS)?

IONOS Redaktion
10.10.2023
6 mins

Inhaltsverzeichnis

Moderne Intrusion-Detection-Systeme sind eine lohnende Ergänzung zur herkömmlichen Firewall. Sie analysieren und überwachen Systeme und ganze Netzwerke in Echtzeit, entdecken potenzielle Gefahrenherde und informieren dann umgehend den Administrator oder die Administratorin. Die eigentliche Abwehr eines Angriffs erfolgt dann im Anschluss über eine zusätzliche Software.

Was steckt hinter einem IDS (Intrusion-Detection-System)?

So fortschrittlich moderne Sicherheitssysteme für Rechner und Netzwerke auch sind – auch Cyber-Angriffe werden immer geschickter und durchdachter. Daher ist es empfehlenswert, sensible Infrastrukturen mit unterschiedlichen Mechanismen zu schützen. Ein Intrusion-Detection-System (IDS) stellt dabei eine erstklassige Ergänzung zur Firewall dar: Ein solches Angriffserkennungssystem **entdeckt Angriffe und potenzielle Gefahren frühzeitig** und informiert Administratoren und Administratorinnen umgehend. Diese können dann die notwendigen Schritte einleiten, um die Attacke abzuwehren. Das Intrusion-Detection-System kann Angriffe auch entdecken, wenn diese bereits die Firewall durchbrochen haben.

Anders als zum Beispiel ein Intrusion-Prevention-System wehrt ein IDS keine Attacken selbst ab. Stattdessen analysiert das Intrusion-Detection-System sämtliche Aktivitäten in einem Netzwerk und **gleicht sie mit speziellen Mustern ab**. Kommt es zu ungewöhnlichen Aktionen, alarmiert das System den Nutzer oder

die Nutzerin und liefert genaue Informationen über die Herkunft und die Art des Angriffs.

> **Tipp**
>
> Nähere Informationen über die Unterschiede zwischen Intrusion-Detection- und Intrusion-Prevention-System erhalten Sie in unserem separaten Artikel zu diesem Thema.

Welche Arten von Intrusion-Detection-Systemen gibt es?

Man unterscheidet zwischen drei Arten von Intrusion-Detection-Systemen. Diese können hostbasiert (HIDS) oder netzwerkbasiert (NIDS) sein oder alternativ einen hybriden Ansatz verfolgen, der die Grundsätze von HIDS und NIDS verbindet.

HIDS: Hostbasierte Intrusion-Detection-Systeme

Das hostbasierte Intrusion-Detection-System ist die älteste Form des Sicherheitssystems. Hier wird das IDS direkt auf dem entsprechenden System installiert. Es analysiert Daten unmittelbar **auf der Log- und Kernel-Ebene** und überprüft auch andere Systemdateien. Um dem Einsatz eigenständiger Workstations gerecht zu werden, greift das hostbasierte Intrusion-Detection-System auf sogenannte **Monitoring-Agenten** zurück, die den Datenverkehr vorfiltern und die so gewonnenen Erkenntnisse an den zentralen Server weiterleiten. Dieser Ansatz ist zwar sehr genau und umfassend, kann aber unter anderem durch DoS- und DDoS-Attacken überwunden werden. Zudem ist dieses Intrusion-Detection-System vom jeweiligen Betriebssystem abhängig.

NIDS: Netzwerkbasierte Intrusion-Detection-Systeme

Ein netzwerkbasiertes Intrusion-Detection-System scannt Datenpakete, die **innerhalb eines Netzwerks** hin- und hergeschickt werden. Ungewöhnliche oder abweichende Muster

werden so schnell erkannt und gemeldet. Problematisch kann in diesem Zusammenhang die schiere Menge der versendeten Daten werden. Übersteigt diese die Kapazitäten des Intrusion-Detection-Systems, kann keine lückenlose Überwachung mehr stattfinden.

Hybrides Intrusion-Detection-System

Viele Anbieter setzen mittlerweile auf hybride Intrusion-Detection-Systeme, die beide zuvor genannten **Ansätze verbinden**. Ein solches System setzt sich zusammen aus hostbasierten Sensoren, netzwerkbasierten Sensoren und einer **Managementebene**, auf der die Ergebnisse zusammenlaufen und tiefergehend analysiert werden. Auch die Steuerung wird von dieser Ebene aus durchgeführt.

Einsatzzweck und Vorteile eines IDS

Ein Intrusion-Detection-System sollte **niemals als Ersatz für eine Firewall gesehen oder genutzt werden**. Stattdessen stellt es eine erstklassige Ergänzung dar, die im Zusammenspiel mit der Firewall Gefahren deutlich besser identifiziert. Da das Intrusion-Detection-System selbst die höchste Schicht des OSI-Modells analysieren kann, werden so häufig neue und bisher unbekannte Gefahrenherde gefunden. Das gilt selbst, wenn die Firewall bereits überwunden wurde.

Wie funktioniert ein Intrusion-Detection-System?

Die am häufigsten genutzte Art der Intrusion-Detection-Systeme ist das hybride Modell, welches sowohl am Host als auch im Netzwerk ansetzt. Die gesammelten Informationen werden im zentralen Managementsystem ausgewertet, wobei drei verschiedene Komponenten zum Einsatz kommen.

Datenmonitor

Der Datenmonitor **sammelt mithilfe von Sensoren alle relevanten Daten** und filtert diese nach Relevanz. Hierbei handelt es sich einerseits um Informationen auf der Seite des Hosts wie Log-Dateien und Systeminformationen. Andererseits werden auch Datenpakete, die über das Netzwerk versendet werden, berücksichtigt. Das IDS erfasst und sortiert unter anderem **Quell- und Zieladressen** sowie andere wichtige Eigenschaften. Die wichtigste Voraussetzung ist dabei, dass die gesammelten Daten entweder aus einer verlässlichen Quelle oder vom Intrusion-Detection-System selbst stammen. Nur so kann gewährleistet werden, dass Daten nicht im Vorfeld manipuliert worden sind.

Analyzer

Die zweite Komponente des Intrusion-Detection-Systems ist der Analyzer. Dieser **wertet alle erhaltenen und vorgefilterten Daten aus** und nutzt dafür verschiedene Muster. Die Überprüfung erfolgt in Echtzeit, wodurch insbesondere CPU und Arbeitsspeicher unter Umständen vor große Herausforderungen gestellt werden können. Nur wenn die entsprechenden Kapazitäten ausreichen, kann die Analyse schnell und ordentlich durchgeführt werden. Dem Analyzer stehen dafür zwei unterschiedliche Methoden zur Verfügung:

- **Misuse Detection**: Bei der Misuse Detection (dt. „Missbrauchserkennung“) untersucht der Analyzer die erhaltenen Daten nach bereits bekannten Angriffsmustern. Diese werden in einer separaten Datenbank hinterlegt und ständig aktualisiert. Erfolgt der Angriff mit einer bereits erfassten Signatur, kann er auf diese Weise frühzeitig entdeckt werden. Angriffe, die dem System zu diesem Zeitpunkt noch

nicht bekannt sind, werden hingegen auf diese Weise nicht erkannt.

- **Anomaly Detection**: Grundlage für die Anomaly Detection (dt. „Anomalie-Erkennung“) ist die Betrachtung des gesamten Systems. Sobald einzelne oder mehrere Arbeitsschritte von der Norm abweichen, wird diese Anomalie gemeldet, zum Beispiel wenn die CPU-Auslastung über einen bestimmten festgelegten Wert hinausgeht oder Zugriffe auf eine Seite ungewöhnlich zunehmen. Auch die zeitliche Abfolge unterschiedlicher Ereignisse kann vom Intrusion-Detection-System überprüft werden, um unbekannte Angriffsmuster zu erkennen. Unter Umständen werden allerdings auch harmlose Anomalien gemeldet.

ⓘ Hinweis

Zu den typischen Auffälligkeiten, die ein gutes IDS erkennt, zählen ein erhöhter Traffic und vermehrte Zugriffe auf Login- und Authentifizierungsmechanismen. Das macht die Sicherheitstechnik zu einer erstklassigen Lösung gegen Brute-Force-Attacken. Um die Trefferquote zu erhöhen, verwenden viele moderne Intrusion-Detection-Systeme KI für die Anomaly Detection.

Alarmierung

Die dritte und letzte Komponente des Intrusion-Detection-Systems ist die eigentliche Alarmierung. Wurden ein Angriff oder zumindest Auffälligkeiten entdeckt, informiert das System den Administrator oder die Administratorin. Diese Benachrichtigung kann **per E-Mail, über einen lokalen Alarm oder per Meldung auf das Smartphone oder Tablet** erfolgen.

Welche Nachteile hat ein Intrusion-Detection-System?

Auch wenn das Intrusion-Detection-System eine gute Ergänzung für die Sicherheitsarchitektur ist, ist auch diese Methode nicht fehlerfrei. Einige mögliche Nachteile haben wir weiter oben schon kurz angerissen. So sind hostbasierte IDS anfällig für DDoS-Angriffe und netzwerkbasierte Intrusion-Detection-Systeme können bei größeren Netzwerkstrukturen an ihre Grenzen geraten und dadurch Datenpakete übersehen. Gleichzeitig liefert die Anomaly Detection – je nach Konfiguration – häufig falsche Alarmmeldungen. Zudem eignen sich sämtliche IDS **lediglich zur Gefahrenerkennung**. Für die Abwehr eines Angriffs muss zusätzliche Software genutzt werden.

Intrusion-Detection-System: Das Beispiel Snort

Eines der bekanntesten und beliebtesten Intrusion-Detection-Systeme ist Snort. Das Sicherheitstool, das bereits 1998 von Martin Roesch entwickelt wurde, ist nicht nur plattformübergreifend und Open-Source, sondern stellt Nutzerinnen und Nutzern auch **umfangreiche Präventionsmaßnahmen als Intrusion Prevention System** zur Verfügung. Das Programm gibt es kostenlos und in einer kostenpflichtigen Version, für die zum Beispiel Aktualisierungen schneller bereitgestellt werden.