Intrusion Detection System

aus Wikipedia, der freien Enzyklopädie

Ein **Intrusion Detection System** (englisch *intrusion* ‚Eindringen', **IDS**) bzw. **Angrifferkennungssystem** ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen.

Inhaltsverzeichnis

- 1 Architekturen
  - 1.1 Host-basierte IDS
  - 1.2 Netzwerk-basierte IDS
  - 1.3 Hybride IDS
- 2 Funktionsweise
- 3 Nachteile
- 4 Honeypot
- 5 IDS-Software
- 6 Einzelnachweise
- 7 Weblinks

Architekturen

Man unterscheidet drei Arten von IDS:

- Host-basierte IDS.
- Netzwerk-basierte IDS.
- Hybride IDS.

Host-basierte IDS

Sie stellen die älteste Art von Angrifferkennungssystemen dar. Sie wurden ursprünglich vom Militär entwickelt und sollten die Sicherheit von Großrechnern garantieren. Ein HIDS muss auf jedem zu überwachenden System installiert werden. Der Begriff „Host" darf allerdings nicht missverstanden werden. In diesem Kontext ist als Host jedes System gemeint, auf welchem ein IDS installiert ist, und nicht lediglich der Begriff „Host" als Synonym für einen Großrechner.

Ein HIDS muss das Betriebssystem unterstützen. Es erhält seine Informationen aus Log-Dateien, Kernel-Daten und anderen Systemdaten wie etwa der Registrierungsdatenbank. Es schlägt Alarm, sobald es in den überwachten Daten einen vermeintlichen Angriff erkennt. Eine Unterart der HIDS sind sogenannte „System Integrity Verifiers", die mit Hilfe von Prüfsummen bestimmen, ob Veränderungen am System vorgenommen wurden.

Vorteile:

- Sehr spezifische Aussagen über den Angriff.
- Kann ein System umfassend überwachen.

Nachteile:

- Kann durch einen DoS-Angriff ausgehebelt werden.
- Wenn das System außer Gefecht gesetzt wurde, ist auch das IDS lahmgelegt.

Netzwerk-basierte IDS

NIDS versuchen, alle Pakete im Netzwerk aufzuzeichnen, zu analysieren und verdächtige Aktivitäten zu melden. Diese Systeme versuchen außerdem, aus dem Netzwerkverkehr Angriffsmuster zu erkennen. Da in der heutigen Zeit überwiegend das Internetprotokoll eingesetzt wird, muss auch ein Angriff über dieses Protokoll erfolgen. Mit nur einem Sensor kann ein ganzes Netzsegment überwacht werden. Jedoch kann die Datenmenge eines modernen 1-GBit-LANs die Bandbreite des Sensors übersteigen. Dann müssen Pakete verworfen werden, was keine lückenlose Überwachung mehr garantiert.

Vorteile:

- Ein Sensor kann ein ganzes Netz überwachen.
- Durch Ausschalten eines Zielsystems ist die Funktion des Sensors nicht gefährdet.

Nachteile:

- Keine lückenlose Überwachung bei Überlastung der Bandbreite des IDS.
- Keine lückenlose Überwachung in geswitchten Netzwerken (nur durch Mirror-Port auf einem Switch).

Hybride IDS

Hybride IDS verbinden beide Prinzipien, um eine höhere Abdeckung bei der Erkennung von aufgetretenen Angriffen gewährleisten zu können. Man spricht in diesem Zusammenhang von netz- und hostbasierten Sensortypen, die an ein zentrales Managementsystem angeschlossen sind. Viele heute eingesetzte IDS verfügen über eine solche, hybride Funktionsweise.

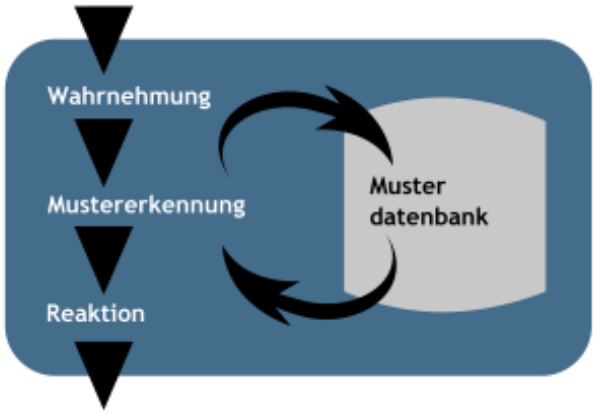
Ein hybrides IDS besteht zumeist aus folgenden Komponenten:

- Management.
- Hostbasierte Sensoren (HIDS).
- Netzbasierte Sensoren (NIDS).

Funktionsweise

Grundsätzlich gibt es zwei Verfahren zur Einbruchserkennung: den Vergleich mit bekannten Angriffssignaturen und die so genannte statistische Analyse. Die meisten IDS arbeiten mit Filtern und Signaturen, die spezifische Angriffsmuster beschreiben. Der Nachteil dieses Vorgehens ist, dass nur bereits bekannte Angriffe erkannt werden können.

Der komplette Prozess unterteilt sich dabei in drei Schritte. Die Wahrnehmung eines IDS wird durch Sensoren ermöglicht, die Logdaten (HIDS) oder Daten des Netzwerkverkehrs (NIDS) sammeln. Während der Mustererkennung überprüft und verarbeitet das Intrusion Detection System die gesammelten Daten und vergleicht sie mit Signaturen aus der Musterdatenbank. Treffen Ereignisse auf eines der Muster zu, so wird ein „Intrusion Alert“ (Einbruchs-Alarm) ausgelöst. Dieser kann vielfältiger Natur sein. Es kann sich dabei lediglich um eine E-Mail oder SMS handeln, die dem Administrator zugestellt wird oder, je nach Funktionsumfang, eine Sperrung oder Isolierung des vermeintlichen Eindringlings erfolgen.



Andere IDS verwenden heuristische Methoden, um auch bisher unbekannte Angriffe zu erkennen. Ziel ist, nicht nur bereits bekannte Angriffe, sondern auch ähnliche Angriffe oder ein Abweichen von einem Normalzustand zu erkennen.

In der Praxis haben signaturbasierte Systeme mit Abstand die größte Verbreitung. Ein Grund dafür ist, dass ihr Verhalten leichter voraussehbar ist. Ein Hauptproblem beim praktischen Einsatz von IDS ist, dass sie entweder viele falsche Warnungen (falsch positiv) generieren oder einige Angriffe nicht entdecken (Falsch negativ).

Anstatt nur einen Alarm auszulösen, wie ein IDS, ist ein **Intrusion Prevention System** (kurz **IPS**) in der Lage, Datenpakete zu verwerfen, die Verbindung zu unterbrechen oder die übertragenen Daten zu ändern. Oft wird hierbei eine Anbindung an ein Firewallsystem genutzt, durch das dann bestimmte durch das IPS definierte Regeln angewandt werden.

IPS/IDS neuerer Bauart arbeiten oft mit einer Kombination aus *Stateful inspection*, *Pattern Matching* und Anomalieerkennung. Damit lassen sich Abweichungen von der im RFC-Standard (Request for Comment) festgelegten Protokollspezifikation erkennen und verhindern.

Darüber hinaus werden auch in anderen Bereichen Bestrebungen nach derartigen Systemen deutlich, wie beispielsweise der Schutz von Telefonanlagen durch intelligente, signaturbasierte Intrusion Detection.

Nachteile

- Da ein Intrusion-Detection-System in der Regel eine aktive Komponente ist, besteht die Möglichkeit, dass es als Angriffsziel genutzt wird. Intrusion-Detection-Systeme, die sich in-line – d. h. ohne gebundenen IP-Stack und IP-Adressen – in ein Netzwerk einbinden lassen, sind von dieser Gefahr nur begrenzt betroffen.
- Im Gegensatz zu Intrusion-Prevention-Systemen werden Angriffe nur erkannt, aber nicht verhindert.

Honeypot

→ Hauptartikel: Honeypot

Ein Honeypot ist ein Computer im Netzwerk, der Hacker verleiten soll, genau diesen anzugreifen. Auf diesem Computer befinden sich weder wichtige Daten noch Dienste, die regulär genutzt werden. Er dient lediglich dazu, die Angriffe auf einen isolierten Teil des Netzwerkes zu lenken, indem bewusst Sicherheitslöcher geöffnet bleiben. Werden Aktivitäten auf diesem Computer wahrgenommen, handelt es sich höchstwahrscheinlich um einen Angriff. Außerdem kann mit Hilfe eines Honeypots mehr über die Vorgehensweise des Angreifers erfahren werden. Aus den beobachteten Angriffen können dann Verteidigungsstrategien für das übrige Netzwerk abgeleitet werden. Der Honeypot ist damit ein weiterer Bestandteil des IDS. Das Konzept des Honeypots hat allerdings einen Nachteil: Ein Honeypot kann als Eintrittspunkt dienen, um weitere Angriffe auf das Netzwerk durchzuführen.

IDS-Software

Auf dem freien Markt gibt es eine ganze Reihe von kommerziellen Angrifferkennungssystemen. Aber auch freie Software ist dort zu finden:

- Snort[1] ist ein freies Netzwerk-IDS für Unix/Linux-, Mac-OS-X- und Windows-Systeme.[2] **Snort** kann mittels diverser Module zur Auswertung der Daten (bspw. ACID) oder Module zur Intrusion Prevention (bspw. SnortSAM) aufgewertet werden.
- Samhain[3] ist ein Host-basierendes System, das auf vielen Plattformen läuft. Viele Linux-Distributionen enthalten bereits vorgefertigte Pakete dieser Software. Durch kryptographische Signaturen können Verfälschungen an Konfigurations-Dateien und der Kommunikation über Netzwerk aufgedeckt werden.
- Prelude[4] als hybrides IDS, welches diverse andere Programmpakete (Snort, Samhain u. a.) integriert, steht ebenso für die Plattformen Linux, BSD, Solaris und Mac OS X zur Verfügung (auch für unterschiedliche Architekturen wie x86, PowerPC, SPARC usw.).
- Eine andere Entwicklung ist das Projekt *Hogwash*. Dieses IDS arbeitet auf Layer 2 und bindet sich somit mit keiner IP-Adresse an angeschlossene Netzwerke. Es wird dadurch schwerer angreifbar und ermöglicht es, ohne aufwendige Konfiguration der beidseitig angeschlossenen Systeme eingesetzt zu werden.
- Xray IDS ist ein kostenpflichtiges Host-IDS. Es ist das erste System, welches speziell für Windows entwickelt wurde.[5]
- Botshield ist eine schnell einsetzbare Host-IDS/IPS Software für Windows Server. Das System schützt wichtige Ports und Dienste wie z. B. RDP (Remote Desktop), HTTP (Web Server) und Datenbanken. Täglich mehrfach aktualisierte Blacklists verhindern zudem Angriffe durch bekannte Bot-Netzwerke und Hacker.[6]

Einzelnachweise

1. http://www.snort.org/
2. http://www.winsnort.com/
3. Intrusion Detection mit Samhain (http://www.admin-magazin.de/Das-Heft/2010/01/Intrusion-Detection-mit-Samhain)
4. IDS mit Prelude (http://www.admin-magazin.de/Das-Heft/2011/01/Plattformunabhaengiges-korreliertes-und-erweiterbares-IDS-mit-Prelude)
5. http://www.xray-ids.com/
6. http://www.botshield.de/

Weblinks

- BSI: Intrusion-Detection-Systeme (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/InternetundlokaleNetze/IntrusionDetectionSystemeIDS/intrusiondetectionsystemeids_node.html)