Intrusion Detection Systeme

IDS

Definition (BSI)

- Aktive Überwachung von Systemen und Netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch. Aus allen im Überwachungsbereich stattfindenen Ereignissen sollen diejenigen gefunden werden, die auf Angriffe, Missbrauch und Sicherheitsverletzungen hindeuten (?) um diese anschliessend vertieft zu untersuchen. Die Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.

Alternative Definition

- Beobachten der Vorgänge in einem Netzwerk oder auf den Servern - Workstations - anhand von verschiedenen Mustern
- Vergleich der aktuellen Vorgänge mit den Mustern und Entscheiden wie auf die aktuellen Vorgänge regiert wird

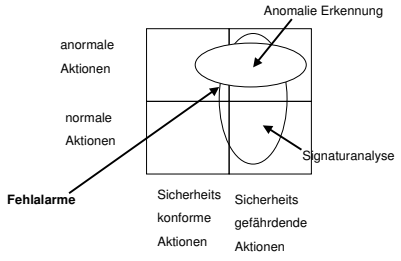
Hauptkomponenten

- Datensammlung
  - Ermittlung von Informationen quantitativer und qualitativer Art.
  - Quantitativ - z.B. Anzahl der Pakete die an einem Port x im Zeitraum y ankamen.
  - Qualitativ. - z.B. Benutzer x hat eine Email versendet Benutzer y hat Datei z geöffnet

Hauptkomponenten

- Datenanalyse
  - Analyse der gesammelten Daten anhand bestimmter Muster bzw. Regeln hinsichtlich möglicher Angriffe
- Ergebnisdarstellung
  - Aufbereitung der ermittelten Daten um dem Admin eine Übersicht zu ermöglichen
  - Versendung einer Mail, SMS oder vergl. An definierte Adressen

Erkennung von Angriffen



Anormalieerkennung

- Erfassen von Daten in einem Netzwerk über einen bestimmten Zeitraum hinweg
- Aus diesen Informationen werden Daten über einen Normalzustand des Netzes entwickelt (Auslastung, Dienste, Protokolle, Nutzer etc.) Entwicklung von Schwellenwerten
- Werden in einer 3. Phase Schwellenwerte überschritten, wird ein Alarm ausgelöst und entsprechende Gegenmassnahmen eingeleitet

Anormally Detection

- Unbekannter hat sich Zugang zum Passwort und ID eines Nutzers verschafft. IDS bemerkt die Anmeldung und reagiert nicht. Erst, als der Nutzer über bestimmte Systemkommandos oder Programme die dieser Nutzer normalerweise nicht nutzt, andere Server scannt, wird ein Alarm ausgelöst

Misuse Detection

- Es werden Muster definiert, die als Angriff gewertet werden. Diese Muster nennt man auch Signaturen. Dies kann z.B. die Suche nach bestimmten Strings sein
- Suche nach “/etc/passwd”

Protokollanalyse

- Es wird nach Abweichungen von „standard“ Verhalten gesucht. Viele Ereignisse weichen von standard Verfahren ab, deshalb kann so mit guter Performance eine effektive Angriffserkennung durchgeführt werden.

Problemfälle

- Nicht von der Statistik abweichende Angriffe werden möglicherweise nicht erkannt
  - false negatives
- Geändertes Nutzerverhalten führt zu vielen (!) Fehlalarmen
  - false positives

Intrusion Prevention

- Monitor Application Behavior
  - was führt ein Programm normalerweise aus ?
  - Auf welche Ressourcen wird zurückgegriffen ?
- Wenn einer der Punkte nicht stimmt, handelt es sich um einen Angriff es wird als solcher gewertet und ein Alarm ausgelöst
- Application Based Intrusion Detection

System Call Interception

- Soll manipulierte Systemaufrufe identifizieren
- Bevor der Systemaufruf zugelassen wird, wird überprüft wer diesen Aufruf gestartet hat und ob dieser zugelassen wird
  - wer hat den Systemcall aufgerufen (welches Prog...) ?
  - unter welcher User - Autorität läuft der Prozess (root...) ?
  - auf was versucht der Systemcall zuzugreifen ?

HIDS

- Hostbasierte Intrusion Detection Systeme
- System (Sensor) wird auf dem zu überwachenden System installiert. Dient zur Auswertung nach fehlgeschlagenen Logins, Angriffsversuchen, Viren, versuchte oder erfolgte Rechteüberschreitung usw.

HIDS (Vorteile)

- Tatsächliche Reaktion kann erfasst werden
- Gezielte Reaktion möglich es wird nur 1 System erfasst
- Es können auch verschlüsselte Verbindungen erfasst werden
- Integritätscheck für Dateien möglich
- Es können z.B. NT-Events erfasst werden

HIDS (Nachteile)

- Auf jedem Host zu installieren
- Es kann natürlich nur ein Host überwacht werden
- Keine Erkennung von Protokollfehlern
- Betriebssystemabhängig
- Kann der Host übernommen werden ist auch der Sensor komprommitiert
- Kostenintensiv Lizenzen pro Host

NIDS

- Networkbasierte Intrusion Detection Systeme
- Überwachen den Netzwerkverkehr eines IP Bereiches oder Netzwerks.
- I.d.R- Plazierung an bestimmten Punkten innerhalb des Netzes (vor und hinter einer Firewall)

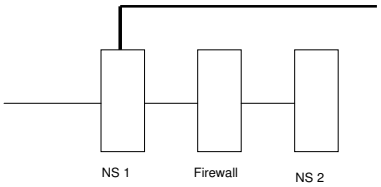
NIDS (Vorteile)

- Es wird der gesamte Netzwerkverkehr überwacht
- Erkennen von Protokollfehlern
- Promiscous Mode möglich
- Betriebssystemunabhängig
- Keine Beeinträchtigung der anderen Systeme

NIDS (Nachteile)

- Keine Überwachung von verschlüsseltem Verkehr
- Hohe Performanceansprüche bei 100Mb Netzen
- Keine Information über die Auswirkungen des Angriffs auf das Zielsystem

Netzwerksensor vor der Firewall

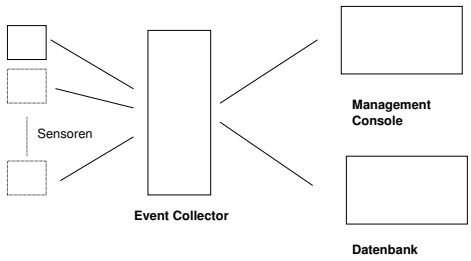


Bei einem schlecht konfigurierten NS kann die Firewall ggf. umgangen werden.

Produkte

- Real Secure (ISS)
  - Teuer (!), Sensoren für W2K, Linux und Solaris
  - alle möglichen Datenbankformate
- Dragon (Enterasys)
  - günstiger als Real Secure
  - MySQL als DB
  - Perl basierend
- Snort
  - Freeware

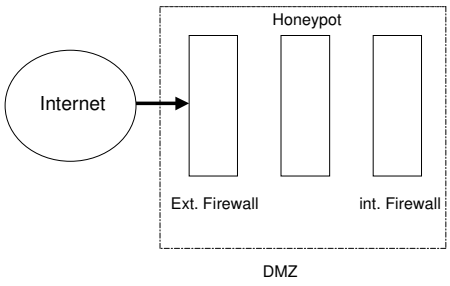
Prinzip Real Secure



Honeypot

- Honeypots are programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Schematisch



Aufgabe

- Der Honeypot ist nach aussen hin ungeschützt und protokolliert und analysiert aber jeden Netzwerkverkehr der ankommt.
- Da der Pot normalerweise nicht erreicht werden kann, ist prinzipiell jede Verbindung verdächtig