DECOIT

D.A.CH Security 2005

Darmstädter Zentrum für IT-Sicherheit

Intrusion Detection und Response

Anforderungen, Analysemethoden und Systemunterschiede

Dr. Kai-Oliver Detken

Business URL: http://www.decoit.de

Private URL: http://www.detken.net

Consultancy & Internet Technologies

Schwachstellen heutiger Netze

- Technische und konzeptionelle Schwachstellen
  - Lücken in Betriebssystemen (Windows, Linux etc.)
  - Lücken in Applikationen (z.B. Mail- und Webserver)
  - Lücken in Diensten
  - Lücken in Protokollen
- Personelle und organisatorische Schwachstellen
  - Lücken durch fehlenden Datenschutz
  - Fehlende personelle Regelungen
  - Social Engineering

Wesentliche Ziele eines IDS/IRS

- Integrität der zu schützenden Daten
- Verfügbarkeit dieser Daten
- Verfügbarkeit der gewünschten Dienste
- Automatische Reaktionen auf Angriffe und Einbrüche
- Justierbare Fehlertoleranz zur Vermeidung von Fehlalarmen
- Betrieb mit geringem administrativen Aufwand
- Minimale Belastung des Netzverkehrs
- Geringe Belastung der zu schützenden Systeme
- Einfache Implementierung in die bestehende Struktur
- Zuverlässiger und sicherer Betrieb

Anforderungen an ein IDS/IRS

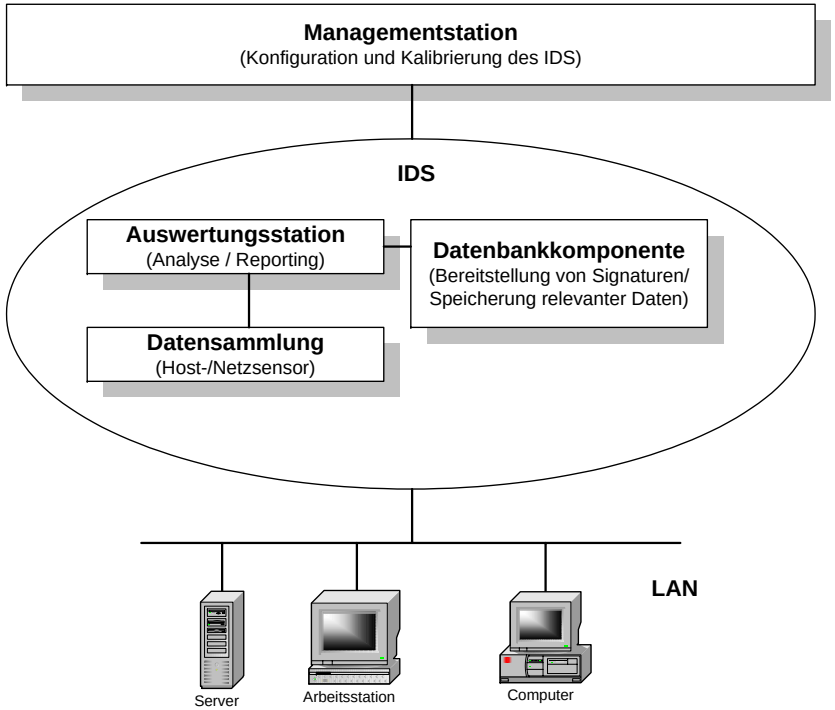
- **Echtzeitfähigkeit:** Erkennung, Alarmierung und Reaktion auf Angriffe
- **Sicherheit:** Schützes des IDS vor Angriffen und Datenverfälschung
- **Datenquellen:** Sammlung von Daten über unterschiedliche Sensoren
- **Flexibilität:** Update der Signaturdatenbank durch Hersteller/selbst
- **Adaptivität:** Anpassung an Änderungen im Nutzerverhalten
- **Betriebssystemvielfalt:** Nutzen des IDS mit bekannten OS
- **Bedienung und Komfort:** möglichst einfache Handhabung
- **Beeinflussung der Netzperformance:** möglichst geringe Auswirkung
- **Alarmierung:** unterschiedliche Alarmierungsmechanismen nutzen
- **Authentizität:** fälschungssichere Zertifizierung
- **Intrusion Response:** Aufzeichnen ausgelöster Reaktionen

IDS-Komponenten

- Netzsensoren: Die Netzsensoren dienen dazu den Netzverkehr eines Rechners bzw. eines Teilnetzwerkes auf Ereignisse zu überwachen, die in Bezug auf die Sicherheitspolitik des Unternehmens als verdächtig erscheinen.
- Hostsensoren: Sie werden eingesetzt, um Angriffe zu erkennen die sich gegen Anwendungen bzw. das Betriebssystem des jeweiligen Rechners richten.
- Datenbankkomponente: Alle Daten werden in der Datenbank abgelegt, die für das Monitoring und die Auswertung relevant sind. Hier sind auch Signaturen vorhanden, um die Rechtevergabe ablegen zu können.
- Auswertungsstation: Damit die Ereignisdaten, die während der Überwachung anfallen, zu einem späteren Zeitpunkt genauer analysiert werden können, ist es erforderlich die Daten in geeigneter Form z. B. einer Firewall zu erweitern.
- Managementstation: Damit ein IDS-System sinnvoll eingesetzt werden kann, ist es zwingend erforderlich, es an die Anforderungen des Unternehmens über eine Managementstation anzupassen.

Schematisch Darstellung eines IDS-Systems

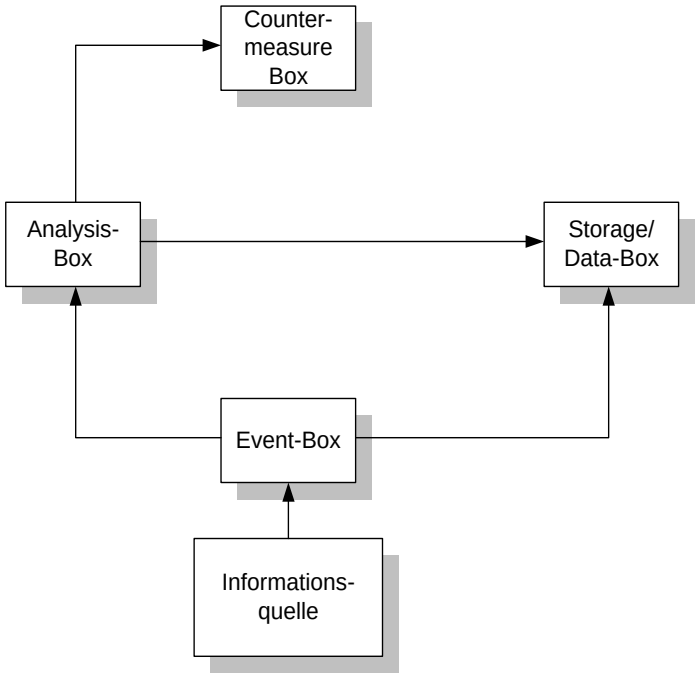
- Der Kern des IDS wird durch die Komponenten im Oval bestimmt
- Hier befinden sich die Komponenten zur Datensammlung und Datenanalyse
- Die Analysekomponente greift auf die Datenbankkomponente zu, welche die Signaturen bereitstellt und gesammelte Daten speichert
- Die Sensoren, innerhalb dieser Abbildung ein Netzsensor, greifen auf das LAN zu und filtern die passierenden Pakete



Analysemethoden von IDS

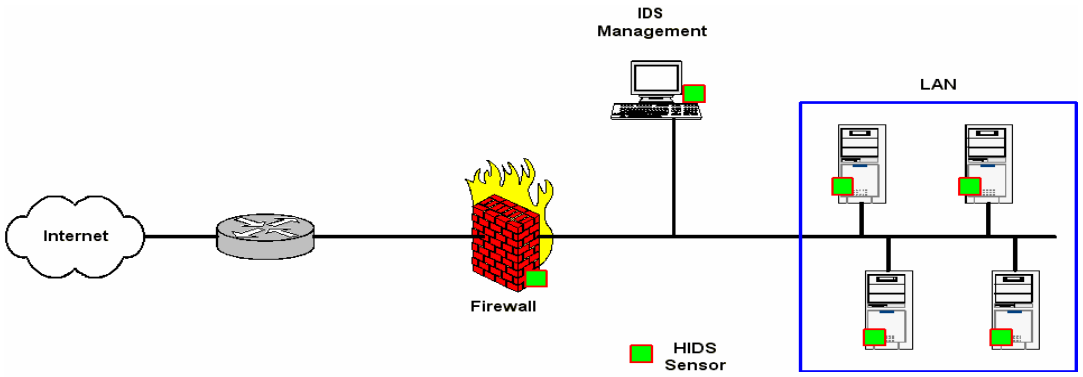
- Die Analysemethoden von Intrusion Detection Systemen unterteilen sich hauptsächlich in zwei Bereiche
  - Die Erkennung von Angriffen anhand von Signaturen
  - Die Erkennung von Abweichungen vom definierten Normalbetrieb eines Systems oder des Netzverkehrs durch Anomalieanalyse
- Heutige Systeme bevorzugen das Erkennen von Angriffen anhand von Signaturen und sind daher auch nur so gut, wie die Signaturen dies zulassen!

IDS-Verhalten



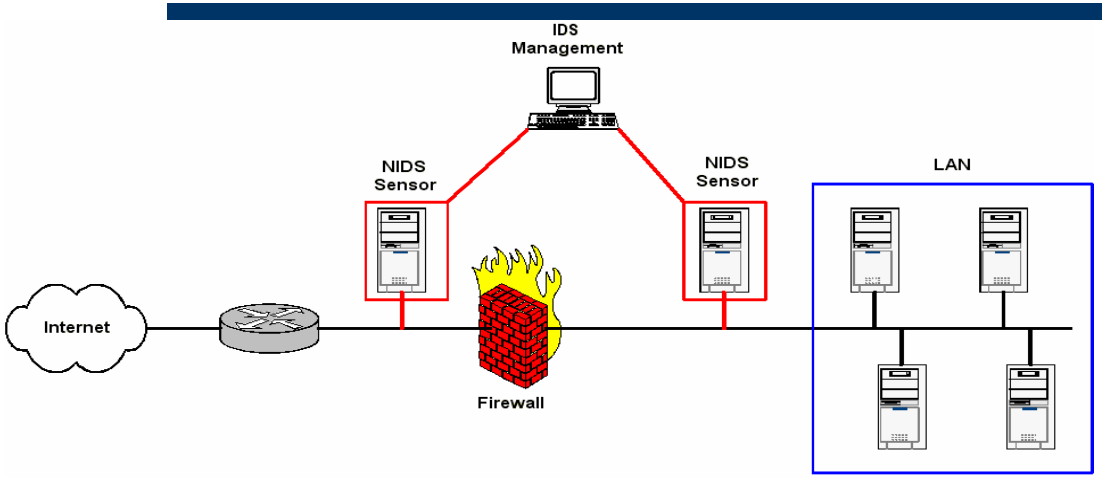
- Passives Verhalten:
  - Das Überwachungssystem reagiert lediglich mit Warnnachrichten an andere Systeme bzw. Administratoren
  - Es werden keine Versuche unternommen den Angriff in irgendeiner Form zu beenden (Trennen der Verbindung, Herunterfahren des Rechners)
- Aktives Verhalten:
  - Das System reagiert mit einem konfigurierten Verhalten auf den erkannten Angriff
  - Es kann versuchen den Angriff zu verhindern, indem das IDS z. B. die Netzverbindung trennt, den entsprechenden Port schließt oder den Rechner herunterfährt
  - Es besteht aber auch die Möglichkeit die protokollierenden Aktivitäten zu verstärken, um so mehr Informationen über diesen Angriff zu erhalten
  - Die gesammelten Informationen können dann sowohl zur Überarbeitung des Regelwerks der Firewall als auch für die technische und rechtliche Verfolgung des Angreifers eingesetzt werden

IDS-Architekturen: HIDS



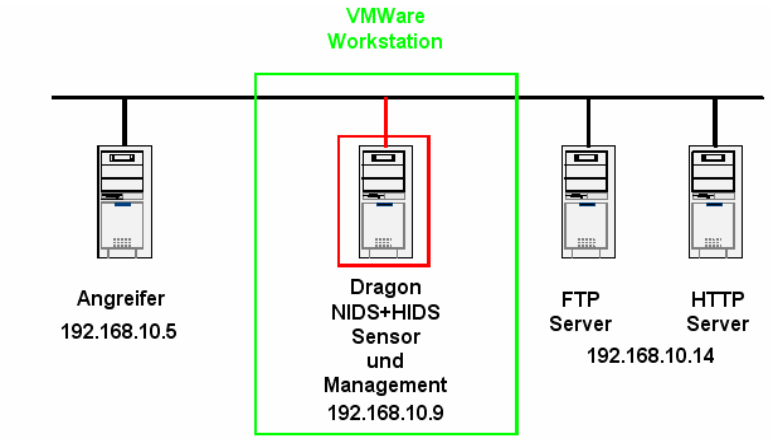
- Ein HIDS analysiert Daten, die auf einem Rechner durch das Betriebssystem oder Applikationen erzeugt werden oder das HIDS erzeugt selbst so genannte Ereignisprotokolle
- Dazu wird ein HIDS-Sensor auf dem zu überwachenden System installiert und liefert die erfassten Daten an die Analysis-Box
- Zur Überwachung mehrerer Systeme können viele HIDS in einer verteilten Struktur aus so genannten Agenten und einer zentralen Managementeinheit aufgebaut werden
- Die aufwändigste Variante von HIDS betreibt eine Echtzeitanalyse von allen System- und Dateizugriffen

IDS-Architekturen: NIDS



- Ein NIDS liest die benötigten Daten aus dem Netzwerkverkehr heraus; dazu wird ein Netzwerk-Sniffer verwendet
- Der Netzwerksensor wird dabei üblicherweise als separater Rechner oder „Appliance“ installiert, damit die produktiven Systeme nicht in ihrer Arbeit beeinflusst werden
- Die Event-Box eines NIDS liest die Daten, die über das zu überwachende Netzwerksegment transportiert werden mit und übermittelt sie dann an die Analysis-Box
- Auf Grund der Header-Informationen, wie Flags und Attribute, können DoS-Attacken oder Scans erkannt werden
- Die Daten der Payload, die vom TCP/IP-Stack an die Applikationsebene weitergereicht werden, können durch die Analysis-Box auf Angriffsmuster überprüft werden

Vergleich von IDS-Systemansätzen (1)



- Der Angriffsrechner wird durch eine Knoppix Linux Version 3.2 integriert
- Bei dem HTTP-Server handelt es sich um einen Apache Web-Server Version 1.3.23
- FTP-Server ist ein Cerberus FTP Server Version 2.1
- Beiden Server sind auf einer Windows XP Professional Plattform aufgesetzt und dienen als Angriffsziele

Vergleich von IDS-Systemansätzen (2)

- IDS Dragon von Enterasys
  - ist ein hybrides System, welches netz- und host-basierte Sensoren einsetzen kann
  - Der Hersteller hat für den Test ein ISO-Images zur Verfügung gestellt, dass beide Sensorarten integriert
  - Das System basiert auf Slackware Linux 8.0 und beinhaltete 1.788 Signaturen ausgestattet
- SNORT
  - Snort ist ein frei verfügbares NIDS, das hier in der Version 1.9.1 verwendet wurde
  - Die Signaturen werden in Regeldateien (.rules) abgelegt
  - Die Dateien sind mit den Bibliotheken beim Dragon System vergleichbar
  - Zurzeit sind im Internet ca. 1.800 Signaturen verfügbar

Planung und Durchführung der Angriffe

- Angriffe laufen unabhängig von der Kategorie immer nach dem gleichen Muster ab
  - Als Erstes beginnt der Angreifer allgemeine Informationen über das Opfersystem zusammeln
  - Die Auswahl des Angriffsziels erfolgt je nach Absicht des Angreifers gezielt (bestimmte Firma oder Institution) oder durch Scannen eines beliebigen Adressbereiches mit anschließender Auswertung des Scans nach potentiellen Opfern
  - Die technischen Methoden der Informationssammlung unterteilen sich in TCP und UDP Portscans, sowie die Ausnutzung von Systemdiensten (z.B. finger, netstat, identd)
  - Sind genügend Informationen über das Zielsystem gesammelt, geht der Angriff in die nächste Phase: Hier hat der Angreifer die Möglichkeit über verschiedene Angriffsebenen und Schwachstellen in der Systemstruktur zum Ziel zu gelangen
- Angriffe auf die Testumgebung mit Nessus
  - da dieses Tool durch die Plugin-Technik, die größten und vollständigsten Angriffsarten bereitstellt
  - Zurzeit sind über 2.000 Plugins in der Nessus-Datenbank verfügbar, die sich auf 24 Obergruppen aufteilen

Ergebnisübersicht

Angriffsmuster	Dragon	Snort
	Erkennung	Erkennung
FTP CWD ~root	Ja	Nein
FTP site exec	Ja	Nein
FTP anonymous	Ja	Nein
Teardrop	Nein	Nein
SYN Scan	Nein	Ja
FTP Server type and version	Ja	Nein
SSH protocol versions supported	Nein	Nein
Apache /server-info accessible	Nein	Nein
Apache < 1.3.27	Nein	Nein
Pocsag password	Nein	Nein
BackOrifice	Ja	Ja
Portal of Doom	Ja	Nein
Systat	Nein	Nein
Netstat	Nein	Nein
Telnet	Nein	Nein
Check for Apache vulnerability	Nein	Nein
SMB Registry	Nein	Nein
Loginversuche per ssh	Ja	Nein

Fazit

- Die Erkennungsrate der Testsysteme war sehr unterschiedlich
- Das lässt sich zum einen auf die Anzahl der Signaturen zurückführen, da nur Angriffe entdeckt werden konnten, die auch bereits bekannt waren
- Zum anderen wurden aber auch Angriffe nicht erkannt, die in der Signaturdatenbank enthalten waren
- Dies lässt darauf schließen, dass selbst eine korrekte Signatur nicht 100% vor einem Angriff schützen kann
- Die für den Test verwendeten Angriffsmuster wurden willkürlich aus dem riesigen Portfolio von Nessus ausgewählt, um keines der Systeme absichtlich stärker hervorzuheben
- Kleine IDS lassen sich mit Open-Source-Lösungen jedenfalls schneller und gezielter etablieren
- Bei größeren Einsatzgebieten ist unabhängig vom Funktionsumfang ein Vorteil für kommerzielle Produkte zu sehen

Ausblick

- Heutige IDS basieren überwiegend auf den Methoden der Signatur- und Anomalieerkennung, welche zurzeit einen hohen Konfigurationsaufwand und entsprechendes Know-how voraussetzen
- Bei der Nutzung von IDS ist die Entscheidung zwischen kommerziellen und Open Source Produkten vom gewünschten Einsatzumfang und den verfügbaren Ressourcen abhängig
- Vor dem Einsatz sollte immer eine Evaluierung verschiedener Produkte stehen, um die größte Abdeckung der individuellen Vorgaben zu ermitteln

Danke für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 1
D-28359 Bremen
Germany
Phone: +49-421-2208-185
Fax: +49-421-2208-150
E-Mail: detken@decoit.de

Darmstädter Zentrum für IT-Sicherheit

Consultancy & Internet Technologies