ConSecur
GmbH

IT-Sicherheitsmanagement

Einführung von Intrusion-Detection-Systemen

Grundlagen

31. Oktober 2002

Version 1.0

Inhaltsverzeichnis

1 Inhalt und Zweck des Dokuments

Im vorliegenden Dokument werden Informationen zu Intrusion-Detection-Systemen (IDS) bereitgestellt, die Grundlagencharakter aufweisen. Das Dokument ergänzt den „Leitfaden zur Einführung“ durch zusätzliche Informationen.

Zunächst werden in Kapitel 2 Aufbau und Funktionsweise von IDS erläutert. Dabei wird parallel jeweils der aktuelle Entwicklungsstand reflektiert. Für den Betrieb von IDS relevante Sicherheitsaspekte und Aspekte der Nutzungsfreundlichkeit werden dargestellt. Abschließend wird kurz auf die aktuelle Marktsituation und die Standardisierung im Bereich IDS eingegangen.

Bei der Einführung von IDS ist relevant, wie IDS mit bestehenden, bereits getroffenen Sicherheitsmaßnahmen zusammenwirken. Dies wird für eine Reihe von Sicherheitsmaßnahmen (Firewalling, Virenscanning, etc.) in Kapitel 3 erläutert.

Typische Einsatzweisen von IDS werden im Rahmen von Einsatzszenarien in Kapitel 4 vorgestellt.

Basisarchitekturen für den Einsatz von IDS (Kapitel 5) betreffen die Anordnung und Einsatzweise von IDS-Komponenten in bestehenden Infrastrukturen. Dabei werden u. a. Beispielarchitekturen für konkrete Realisierungen der Einsatzszenarien beschrieben.

Kapitel 6 beschäftigt sich abschließend mit organisatorischen Aspekten des IDS Einsatzes, wie der Kalibrierung von IDS, der Integration von IDS-Alarmen in das Incident-Handling und weiteren betriebsrelevanten Aspekten.

2 IDS Grundlagen und aktueller Stand

In diesem Kapitel werden grundlegende Aspekte von Intrusion-Detection-Systemen (kurz IDS) beschrieben:

- Definition eines IDS
- Komponenten und Architektur von IDS
- Methoden der Angriffserkennung
- Intrusion-Response-Funktionen
- Sicherheitsaspekte beim Einsatz von IDS
- Nutzungsfreundlichkeit
- IDS-Markt, Kosten und Investitionsschutz
- Standardisierung und Interoperabilität

Neben der allgemeinen Beschreibung wird dabei insbesondere der jeweilige aktuelle Entwicklungsstand marktverfügbarer Produkte dargestellt.

2.1 Definition Intrusion-Detection und Intrusion-Detection-Systeme

Intrusion-Detection

Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.

Intrusion-Detection ist als Prozess zu verstehen und bedarf einer geeigneten organisatorischen Einbindung sowie der technischen Unterstützung durch geeignete Werkzeuge.

Unterstützende Werkzeuge

Intrusion-Detection bedarf einer technischen Grundlage, um überhaupt Ereignisse aufnehmen und sie dann nach interessierenden Kriterien bewerten zu können. Eine werkzeugbasierte Unterstützung kann zur Generierung von Ereignissen, zur Filterung von Ereignissen, zur Auswertung und Alarmierung sowie zur Archivierung der gefundenen Ergebnisse erfolgen.

Ob und in welcher Form Werkzeuge den Intrusion-Detection-Prozess unterstützen können, hängt im Einzelfall vom organisatorischen und technischen Einsatzumfeld, insbesondere auch vom Überwachungsziel ab. Einfache Werkzeuge, z. B. zur Generierung und zum Vergleich von Checksummen ausgewählter Dateien oder zum Vergleich von Zeichenketten bei der Analyse von Logdateien, können hierzu ebenso nützlich sein wie komplexe Werkzeuge zur Überwachung des Netzverkehrs.

Ein wirksames Intrusion-Detection bedarf daher einer angepassten und zusammenpassenden Auswahl geeigneter Hilfsmittel.

Intrusion-Detection-System

Als Intrusion-Detection-System wird eine Zusammenstellung von Werkzeugen bezeichnet, die den gesamten Intrusion-Detection-Prozess von der Ereigniserkennung über die Auswertung bis hin zur Eskala-

tion und Dokumentation von Ereignissen unterstützen. Der Großteil marktverfügbare Intrusion-Detection-Produkte weist diese integrierte Funktionalität auf. IDS können jedoch auch aus Einzelkomponenten zusammengesetzt werden. Auswahl und Zusammenstellung des IDS richten sich dabei nach den individuellen technischen und organisatorischen Gegebenheiten und Anforderungen.

2.2 Architektur und Komponenten

Heutige IDS bestehen typischerweise aus folgenden Komponenten:

- Netzsensoren (zur Überwachung des Netzverkehrs an bestimmten Punkten)
- Hostsensoren (zur Überwachung des Betriebssystem, von Applikationen und oder des hostspezifischen Netzverkehrs)
- Datenbankkomponenten
- Managementstation
- Auswertungsstation

Die Komponenten werden in den folgenden Abschnitten beschrieben. Zusätzlich sind Kommunikationsverbindungen zwischen den Komponenten vorzusehen, die in Abschnitt 2.2.6 erläutert werden.

2.2.1 Netzbasierte Sensoren

Netzbasierte Sensoren (Netzsensoren) überwachen den Netzverkehr eines Rechners oder eines ganzen Teilnetzes auf verdächtige Ereignisse. Zum Betrieb jedes Netzsensors wird typischerweise ein separater Rechner eingesetzt, so dass andere Applikationen nicht gestört werden können. Teilweise liefern Hersteller Netzsensoren nur noch in Kombination mit der zugehörigen Hardware/Software-Plattform, als sogenanntes Appliance.

Nachstehend sind Vorteile (gekennzeichnet als ↗) und Nachteile (gekennzeichnet als ↘) von Netzsensoren aufgeführt.

↗ Durch Einbringen netzbasierter Sensoren in ein Netz, werden Endsysteme (Hosts, Server) nicht zusätzlich belastet.

↗ Netzbasierte Sensoren eignen sich zur Erkennung von netzbasierten Angriffen, die sich gegen mehrere Zielsysteme richten (z. B. SYN flooding, verschiedene Arten von Denial-of-Service Angriffen). Solche Angriffe würden von einem Angriffsziel allein nicht als verteilte Angriffe interpretiert werden können.

↗ Netzbasierte Sensoren können so konfiguriert werden, dass sie für Angreifer „unsichtbar“ sind und von ihnen nicht direkt angesprochen werden können. Sie sind daher schwerer angreifbar als hostbasierte Sensoren.

↗ Netzbasierte Sensoren können über ein zusätzliches Netzwerkinterface miteinander verbunden werden, so dass ein separates IDS-Netz aufgebaut werden kann.

↘ Viele der heute verfügbaren Sensoren können Netze mit einer hohen Netzlast (ab 100Mbps) bei gleichzeitig hoher Paketdichte nicht mehr vollständig überwachen. Grund hierfür ist die zur Verarbeitung notwendige hohe Rechenleistung und hohe Performance bei Zugriffen auf die Signaturdatenbank der Sensoren, die in dedizierten Netzsensoren meist nur unter sehr hohem technischen Aufwand erbracht werden kann. Grundsätzlich nimmt die Übertragungsgeschwindigkeit der Netze schneller zu als die Geschwindigkeit, mit der netzbasierte Sensoren Daten verarbeiten können. Eine Überwachung sämtlicher Datenpakete ist daher nur in Netzen mit begrenztem Durchsatz oder begrenzter Auslastung möglich.

- In verteilten Netzen (swiched networks) oder in lastverteilten bzw. redundant ausgelegten Netzstrukturen ergeben sich zusätzliche Probleme beim Abgriff des Netzverkehrs (siehe Kapitel 3.6.2).
- Netzsensoren können das Verhalten des eigentlichen Angriffsziels nur begrenzt nachvollziehen und lediglich diejenigen Auswirkungen des Angriffsversuchs wiederspiegeln, die im Netzverkehr sichtbar sind.
- Netzsensoren können keine Ereignisse in verschlüsselten Kommunikationsdaten erkennen (vgl. auch Kapitel 3.4).
- Die Angriffserkennung durch Netzsensoren ist nicht exakt und fehlerbehaftet. Dies liegt darin begründet, dass verdächtiger Netzverkehr nicht nur durch Angriffe, sondern z. B. auch durch Konfigurationsfehler anderer Schutzkomponenten oder durch Fehlern bei der Datenübertragung verursacht werden kann.

2.2.2 Hostbasierte Sensoren

Hostbasierte Sensoren (Hostsensoren) sind dadurch gekennzeichnet, dass sie auf dem zu überwachenden System betrieben werden. Sie werden typischerweise eingesetzt, um Angriffe zu erkennen, die auf Anwendungs- oder Betriebssystemebene durchgeführt werden. Beispiele für derartige Angriffe sind Rechteüberschreitungen von Nutzern, Login-Fehlversuche oder Trojaner. Manche Hostsensoren erlauben die Überwachung des hostspezifischen Netzverkehrs.

Nachstehend werden zunächst allgemeine Vor- und Nachteile von Hostsensoren im Vergleich zu Netzsensoren aufgeführt und anschließend die verschiedenen Überwachungstypen von Hostsensoren diskutiert.

Generelle Vor- und Nachteile von Hostsensoren

- Da Hostsensoren auf dem zu überwachendem Host betrieben werden, können sie (im Gegensatz zu Netzsensoren) die tatsächliche Reaktion des Systems beobachten und auswerten.
- Hostbasierte Sensoren müssen auf jedem zu überwachendem Host installiert werden.
- Hostbasierte Sensoren sind spezieller als netzbasierte Sensoren, da sie betriebssystem- und ggf. applikationsspezifisch sind. Daher müssen für sämtliche zu überwachende Plattformen entsprechende hostbasierte Sensoren verfügbar sein und angepasst werden. Der Einsatz hostbasierter IDS ist daher im Allgemeinen kostenaufwändiger als der Einsatz reiner netzbasierter IDS.
- Im Gegensatz zu Netzsensoren können Hostsensoren nicht unsichtbar arbeiten. Angreifer können mit dem zu überwachenden System gleichzeitig auch den Hostsensor und damit das IDS angreifen.
- Der Betrieb eines Hostsensors belastet das überwachte System.

Systemüberwachung

In diesem Fall erfolgt eine Überwachung auf Prozessebene durch den IDS-Sensor selbst.

- Zugriffe auf Dateien und Applikationen sowie Systemzugänge können überwacht werden. Häufig fehlgeschlagene Anmeldeversuche, Zugriffsverletzungen und anormale Verhaltensmuster können erkannt werden. Die Überwachung erfolgt einerseits durch Auswertung der Logdaten des Systems (inkl. Kernel-Logs), andererseits durch spezialisierte IDS-Plugins, die Prozesse überwachen, regelmäßige Integritätsscans durchführen, etc.
- Erkanntes Fehlverhalten kann Nutzerkennungen zugeordnet werden.

Applikationsüberwachung

- ↗ Durch applikationsüberwachende Sensoren ist eine Überwachung spezifischer Applikationen möglich, die weder durch system- noch durch netzüberwachende Sensoren erreicht werden kann. Die Überwachung erfolgt typischerweise durch Auswertung der Logdaten der Applikation.
- ↘ IDS-Sensoren müssen jedoch applikationsspezifisch angepasst werden. Häufig werden hierzu applikationseigene Komponenten mitverwendet.

Integritätsüberwachung

Bei der Integritätsüberwachung wird in regelmäßigen Abständen (ggf. auch bei jedem Dateizugriff) überprüft, ob sich Änderungen an Dateien (Daten, Programmen) ergeben haben. Dies erfolgt typischerweise durch einen Vergleich von Checksummen mit einem definierten Sollzustand.

- ↗ Konkret erkannte Veränderungen können die Untersuchung des Vorfalls sowie die Wiederherstellung des Systems erleichtern.
- ↗ Systemüberwachende Sensoren prüfen Dateiinhalte (z. B. Logdaten) und vertrauen auf deren Integrität. Bei der Integritätsüberwachung hängt die Überwachung nicht von Dateiinhalten ab, sondern die Dateien selbst sind das beobachtete System.
- ↘ Integritätsverletzungen sind typischerweise die Auswirkung eines erfolgreichen Angriffs. Eine Frühwarnfunktion für Angriffsversuche ist durch integritätsüberwachende Sensoren daher nicht gegeben.
- ↘ Eine Erkennung von Integritätsverletzungen erfolgt aus Kapazitätsgründen in der Regel im Batch-Betrieb und nicht in Echtzeit. Die Häufigkeit der Kontrollen ist dabei kritisch, da zu häufig durchgeführte Kontrollen zu einer nicht tragbaren Belastung des System führen können und selten durchgeführte Kontrollen das Restrisiko erhöhen.

Die Integritätsüberwachung eignet sich daher nicht als alleinige Überwachungsmethode.

Überwachung des hostspezifischen Netzverkehrs

Fallweise kann es sinnvoll sein, den zu einem dedizierten System gehörenden Netzverkehr auf diesem System selbst zu beobachten und zu analysieren.

- ↗ Der ins System eingehende Kommunikationsdatenfluss kann auf sämtlichen Protokollebenen überwacht werden.
- ↗ Verschlüsselte Protokolle behindern die Überwachung nicht.
- ↗ Da das System nur entsprechend adressierte Pakete annimmt, ist das Datenaufkommen geringer. Im allgemeinen ist daher eine vollständige Prüfung des für dieses System bestimmten Kommunikationsverkehrs möglich.
- ↘ Durch die hostbasierte Überwachung werden jedoch typischerweise keine auf mehrere Ziele verteilten Angriffe erkannt[1].

[1] Die hostbasierte Erkennung verteilter Angriffe würde neben einer nachträglichen sensorübergreifenden Korrelation eine sensorübergreifende Kommunikation bereits bei der Filterung an jedem Sensor erfordern. Dies würde zu einem sehr hohen Kommunikationsoverhead führen. Marktverfügbare IDS-Produkte bieten hierfür keine ausgereifte Lösung an.

2.2.3 Datenbankkomponenten

Intrusion-Detection-Systeme erzeugen bei der Angriffserkennung Ereignisdaten, die zur späteren Weiterverarbeitung gespeichert werden müssen. Abhängig davon, wie diese Ereignisdaten weiterverwendet werden sollen, müssen sie in entsprechender Detailtiefe und über einen möglicherweise langen Zeitraum gespeichert werden.

Bei geringen Datenmengen ist eine Speicherung in Dateiform ausreichend. Abhängig von der konkreten IDS-Konfiguration können jedoch sehr große Datenmengen anfallen, die die Nutzung eines Datenbanksystems notwendig machen, um die anfallende Datenmenge aufzunehmen und zuverlässig zu verwalten sowie andererseits Zugriffszeiten zu minimieren.

Welches Datenbanksystem zum Einsatz gelangen kann, ist dabei abhängig von der Unterstützung der IDS-Hersteller. Die meisten Intrusion-Detection-Systeme beinhalten Schnittstellen zu den „gängigen“ SQL-Datenbanken.

2.2.4 Managementstation

Über die Managementstation erfolgt die Konfiguration und Kalibrierung des IDS. Dies umfasst in der Regel die folgenden Funktionalitäten:

- Aufnahme der IDS-Komponenten (Sensoren, Datenbanken, Managementstationen) in das IDS.
- Einstellen der Kommunikationsparameter der IDS-Komponenten untereinander (IP-Adressen, Namensgebung, Kryptoschlüssel, Lebenszeichen-Intervall).
- Aufnahme der zu überwachenden Objekte (Netze, IT-Systeme) in das IDS.
- Erstellung und Anpassung von Überwachungsregeln und Gruppierung dieser zu „IDS-Policies“.
- Gruppierung von IDS-Sensoren.
- Zuweisung der „IDS-Policies“ zu Sensoren oder Sensorengruppen

Die konkreten Ausführungen der Managementstationen von IDS sind unterschiedlich. Zu unterscheiden sind das Management über

- ein Kommandozeilen-Interface
- eine webbasierte Schnittstelle
- ein IDS-spezifisches GUI.

Bei einigen IDS sind Management- und Auswertungsstation in einer Komponente zusammengefasst.

2.2.5 Auswertungsstation

Die Auswertungsstation verfügt typischerweise über Funktionen zur Analyse aufgezeichneter Ereignisse und zum Reporting.

Analog zu Konfigurationsoberflächen des IDS werden auch Auswertungs- und Reporting-Tools angeboten. Auch diese sind zu unterteilen in

- Kommandozeilen-Interface
- Webbasierte Schnittstelle
- IDS-eigene Auswertungsoberfläche

Die Analysefunktionalität dient primär der Erkennung und Erstanalyse eingehender IDS-Ereignismeldungen, im Einzelnen der

- Anzeige eingehender Meldungen
- Sortierung der Ereignisse
- Klassifikation der Ereignisse
- Reaktion und Alarmierung
- Ablage der Ereignisdaten zur späteren Weiterverarbeitung

Reporting-Funktionen können sowohl zur

- Generierung von Managementreports und -statistiken als auch zur
- Langfristanalyse der Meldungen eingesetzt werden, um bislang unentdeckte Angriffe und Trends aufzuzeigen.

Wie die Managementstation kann auch die Auswertungsstation unterschiedlich ausgeführt sein (Kommandozeilen-Interface, webbasierte Schnittstelle, IDS-spezifisches GUI).

2.2.6 Kommunikation zwischen den Komponenten

Die Kommunikation der IDS-Komponenten untereinander erfolgt teils über proprietäre Protokolle, teils auch über Standardprotokolle (SSH, SCP). Dabei erfolgt eine Kommunikation typischerweise zwischen folgenden Komponenten:

- Managementstation ➔ IDS-Sensoren
  (Übertragung von Konfigurationsdaten, Kommandos und IDS-Policy, Abfrage von Statusdaten)
- IDS-Sensoren ➔ Managementstation
  (Übertragung von Lebenszeichen – Heartbeats – bei einigen IDS)
- Managementstation ➔ Datenbank
  (Übertragung von Konfigurations- und Statusdaten)
- IDS-Sensoren ➔ Auswertungsstation
  (Übertragung von Ereignisdaten und ggf. Lebenszeichen)
- Auswertungsstation ➔ Datenbank
  (Übertragung von Ereignisdaten)
- IDS-Sensoren ➔ Datenbank
  (Übertragung von Ereignisdaten – bei einigen IDS)
- Managementstation ➔ Auswertungsstation
  (Signalisierung von Konfigurationsalarmen, etwa Ausbleiben von Lebenszeichen)

Hinzu kommen Kommunikationswege

- zur Initiierung von Intrusion-Response-Funktionen (z. B. Alarmierung),
- zum Zugriff auf die Management- und Auswertungsstation sowie
- ggf. eine Kommunikation zwischen verschiedenen Auswertungsstationen.

2.3 Methoden der Angriffserkennung

In den nächsten Abschnitten wird kurz erläutert, auf welche Weise IDS Angriffe erkennen. Folgende Methoden der Angriffserkennung werden beschrieben:

- Erkennung von Angriffsmustern
- Anomalieerkennung
  - durch Protokollanalyse
  - auf Basis statistischer Daten
  - auf Basis von Künstlicher Intelligenz
  - auf Basis von Honeypots
- Korrelation von Ereignisdaten

Einsatz der Erkennungsmethoden in marktverfügbaren IDS-Produkten

Derzeit werden von fast allen Anbietern kommerzieller IDS Analysemethoden angewendet, die auf der Erkennung von Angriffsmustern oder auf Protokollanalyse beruhen. Zusätzlich bieten fast alle IDS die Möglichkeit zur manuellen statistischen Anomalieerkennung auf der Basis vom IDS erzeugter Reporte und Angriffsstatistiken. Die automatische statistische Anomalieerkennung ist im Gegensatz dazu kaum in marktverfügbare Produkte integriert und fast ausschließlich im wissenschaftlichen Bereich anzutreffen. Auch die Relevanz von IDS, deren Angriffserkennung auf Basis künstlicher Intelligenz erfolgt, beschränkt sich auf den wissenschaftlichen Bereich.

Die Anomalieerkennung auf Basis von Honeypots ist ein am Markt verfügbares Analyseverfahren. Honeypots werden von einigen Herstellern angeboten und sind auch im Open-Source-Bereich erhältlich. Eine automatische sensorübergreifende Korrelation von Ereignisdaten bieten nur wenige der marktverfügbaren IDS. Möglichkeiten zur manuellen Korrelation sind jedoch in der Regel gegeben.

2.3.1 Erkennung von Angriffsmustern

Als Signaturen werden im IDS-Kontext Muster bzw. Ereignisse bezeichnet, die auf einen bekannten Angriff oder ein missbräuchliches Systemverhalten hinweisen. Signaturen reichen dabei von einfacher Zeichenerkennung in Daten („pattern matching") bis hin zu komplexen Verhaltensmustern. So erlauben sie auch die Erkennung fehlerhafter Verhaltensweisen des Systems oder einzelner Nutzer (z. B. drei Login-Fehlversuche innerhalb von 5 Minuten).

Bei signaturgestützten IDS erfolgt die Definition des zu erkennenden Angriffs auf der Basis definierter Angriffsmuster. Das IDS alarmiert, sobald ein solches Muster zutrifft. Die meisten verfügbaren IDS gestatten das Anpassen oder Neuerstellen von Signaturen durch eine einfache Skriptsprache.

Vorteil dieser Methode ist die leichte Verständlichkeit des Vorgehens. Nachteilig ist, dass praktisch alle Angriffe (in sämtlichen Modifikationen) aufgezählt werden müssen, damit sie erkannt werden können. Zwar können ähnliche Angriffe durch dieselbe Signatur erkannt werden, wenn die Signatur entsprechend „unscharf" definiert ist. Hierdurch erhöht sich jedoch auch die Fehlalarmrate (false positives) des IDS und mit ihr der personelle Aufwand zur Analyse der IDS-Meldungen.

2.3.2 Anomalieanalyse

Als Anomalieanalyse werden Auswertungsmethoden bezeichnet, bei denen die Abweichung des Systems von seinem Normalverhalten erkannt und gemeldet wird. In den folgenden Abschnitten werden unterschiedliche Verfahren zur Anomalieanalyse kurz erläutert:

- Protokollanalyse,
- Anomalieerkennung auf Basis statistischer Daten,

- Anomalieerkennung auf Basis von Künstlicher Intelligenz,
- Anomalieerkennung auf Basis von Honeypots.

2.3.2.1 Protokollanalyse

Bei der Protokollanalyse wird der Netzverkehr auf Anomalien untersucht. Das Normalverhalten ist dabei durch Protokollspezifikationen definiert. Es wird geprüft, ob der Kommunikationsverkehr den zugrunde liegenden Protokollspezifikationen genügt. Da im Bereich von IP-basierten Netzen viele Angriffe darauf beruhen, dass von den spezifizierten Protokollen abgewichen wird, kann hierdurch eine recht zuverlässige Angriffserkennung erfolgen.

Die Methode weist eine hohe Performance auf, da im Gegensatz zur Signaturerkennung keine Vielzahl von Signaturen getestet werden muss. Nachteilig an dieser Methode ist, dass diejenigen Angriffe, die auf Unschärfen oder Fehlern in der Protokollspezifikation beruhen, nicht erkannt werden. IDS, die auf dieser Methode beruhen, beinhalten daher meist zusätzliche signaturbasierte Komponenten, um eine vollständige Angriffserkennung zu gewährleisten.

2.3.2.2 Anomalieerkennung auf Basis statistischer Daten

Bei der Anomalieerkennung auf Basis statistischer Daten wird davon ausgegangen, dass das Systemverhalten im Angriffsfall signifikant von einem durch statistische Kennwerte festgelegten Normalverhalten abweicht. Um das Normalverhalten eines Systems zu definieren, werden für unterschiedliche Objekte (Nutzer, Dateien, Anwendungen, etc.) und zugehörigen „Verhaltensweisen“ (Anzahl von Fehlversuchen bei der Anmeldung, Tageszeiten des Zugriffs, Nutzungshäufigkeit, Zugriffsdauer, etc.) statistische Kennwerte (Mittelwert, Varianz, etc.) ermittelt. Anhand der statistischen Kennwerte ermittelt das IDS, ob das aktuelle Verhalten signifikant vom Normalverhalten abweicht.

Marktverfügbare IDS bieten keine Funktionen zur automatischen Anomalieerkennung auf Basis statistischer Daten. Manuell ist eine entsprechende Anomalieerkennung in begrenzter Weise auf Basis von Reports und Angriffsstatistiken möglich. Das Vorgehen verlangt jedoch viel Intuition und ist fehlerbehaftet, da weder das Normalverhalten noch die zu suchenden Angriffe spezifiziert sind. Beispielsweise ist nicht sichergestellt, dass sich in dem durch statistische Daten beschriebenen Normalverhalten keine Angriffe verbergen, die dann als „normal“ betrachtet werden. Diese Methode eignet sich daher ausschließlich zur ergänzenden Analyse.

2.3.2.3 Anomalieerkennung auf Basis von Künstlicher Intelligenz

Analog zur manuellen Anomalieanalyse auf Basis statistischer Daten werden Verfahren der Künstlichen Intelligenz eingesetzt, um die bei manueller Analyse notwendige Intuition maschinell zu kompensieren. Hierdurch kann eine Steigerung der Verarbeitungsgeschwindigkeit erzielt werden, jedoch ist auch hier aufgrund hoher Fehlerraten eine manuelle Nachbearbeitung notwendig und intendiert. Auch diese Methode eignet sich daher nur zur ergänzenden Analyse. Sie wird derzeit nicht von IDS-Herstellern am Markt angeboten. Es gibt jedoch Individuallösungen im wissenschaftlichen Bereich.

2.3.2.4 Anomalieerkennung auf Basis von Honeypots

Honeypots sind dedizierte IT-Systeme (Server, Netze, Programme, Prozesse), die keine produktive Funktion erfüllen, sondern ausschließlich „Fallen“ für Angreifer darstellen, in dem sie produktive oder auch besonders sicherheitskritische Systeme vortäuschen. Ein Honeypot hat ein sehr einfaches Normalverhalten, das darin besteht, dass es keine oder nur eine geringe Anzahl vordefinierter Zugriffe auf das System gibt. Honeypots eignen sich sehr gut für eine Anomalieanalyse, da im Wesentlichen sämtliche

Zugriffe und Aktivitäten - ausgenommen der vordefinierten Zugriffe - als anormal einzustufen und damit beobachtenswert sind. Hierdurch lässt sich eine vollständige Aufzeichnung und Nachuntersuchung von Angriffen, aber auch dem Fehlverhalten anderer IT-Systeme realisieren.

Honeypots eignen sich jedoch grundsätzlich nicht dazu, Angriffe auf IT-Systeme außerhalb des Honeypot (z. B. Produktionssysteme) zu erkennen. Auch lässt sich aus der Analyse des Honeypot-Verhaltens nur sehr beschränkt eine Aussage auf das Verhalten von Produktionssystemen treffen. Zudem ist es möglich, dass Angriffe auf Produktionssysteme nicht zuvor oder wiederholt an parallel betriebenen Honeypots ausgeübt werden. Insbesondere bieten Honeypots daher keinen Schutz gegen Insider.

Aus diesen Gründen werden Honeypots in der Praxis nur zusätzlich zu anderen Intrusion-Detection-Maßnahmen eingesetzt. Es ist darüber hinaus bei der Installation, Wartung und Auswertung von einem hohen personellen Aufwand auszugehen. Daher gibt es für Honeypots derzeit nur wenige Anwendungsbereiche:

- Honeynet-Projekt zur wissenschaftlichen Untersuchung und Auswertung von Angriffen.
- Hersteller von Viren- und Trojanererkennungssoftware, die hierdurch versuchen, unmittelbar Zugriff auf Angriffsdaten zu erhalten.
- Bei Internet-Providern werden Pakete, die nicht ordnungsgemäß geroutet werden können, an ein spezielles System weitergeleitet, anstelle sie zu verwerfen. Anhand dieser Pakete können Scan-Versuche oder das in einigen Angriffstools vorkommende zufällige Spoofing von IP-Adressen erkannt werden.

2.3.3 Korrelation von Ereignisdaten

Die Auswertungslogik kann basieren auf Ereignissen und Daten von

- einem Sensor,
- mehreren Sensoren gleicher Art oder
- mehreren Sensoren unterschiedlicher Arten.

Die Berücksichtigung mehrerer, nicht zeitgleicher Ereignisse oder Ereignisse unterschiedlicher Sensoren durch die Auswertungslogik wird als Korrelation bezeichnet. Die Korrelation kann mit der Signaturanalyse und Anomalieanalyse kombiniert sein.

Die Korrelation von sensorübergreifenden oder langfristigen Ereignissen erfolgt in der Regel intuitiv, kann jedoch durch IDS unterstützt werden, z. B. in Form von regelmäßigen Reports.

Nicht alle am Markt erhältlichen IDS-Produkte weisen automatische Korrelationsmöglichkeiten auf. Dagegen wird eine manuelle Korrelation typischerweise durch die Möglichkeit unterstützt, auf Basis der in der Ereignisdatenbank gespeicherten Daten nach verschiedenen Kriterien zu filtern (Report-Funktionen).

Voraussetzung ist hierfür eine möglichst umfangreiche Speicherung der Ereignisdaten und Kontextinformation, da zunächst belanglos erscheinende Daten bei einer Langfrist-Analyse nachträglich an Bedeutung gewinnen können (z. B. Portscans mit einem Port pro Tag oder netzübergreifendes Scanning desselben Ports).

Die Anforderung nach umfangreicher Aufzeichnung verdächtiger Ereignisse konkurriert mit Anforderungen an den Datenschutz. Deshalb ist zu klären, welche Daten für welchen Zeitraum gespeichert werden dürfen. Ereignisdaten können im Allgemeinen auch pseudonymisiert zur Erkennung von Angriffen beitragen. Eine Pseudonymisierung der Ereignisdaten bei der Speicherung wird jedoch von marktverfügbaren IDS-Produkten in der Regel nicht unterstützt.

Die Korrelation wird in der Praxis derzeit hauptsächlich dadurch erschwert, dass einerseits ungeeignete Datenbanksysteme zur Speicherung der Ereignisdaten eingesetzt werden und andererseits aufgrund fehlender Standardisierung eine Korrelation über Sensoren verschiedener Hersteller hinweg nicht von den IDS unterstützt wird. Manuelle Korrelationen sind zwar möglich, jedoch sehr zeitaufwändig und damit kostenintensiv.

2.4 Intrusion-Response-Funktionen

Als Reaktion auf erkannte Ereignisse können verschiedene Aktionen ausgelöst werden, von der Dokumentation des Ereignisses, über die Alarmierung bis zur automatischen Aktivierung von Gegenmaßnahmen. Die von einem IDS automatisch eingeleiteten Maßnahmen werden als **Intrusion-Response** bezeichnet[2].

Die verschiedenen Intrusion-Response Funktionen werden in den nachfolgenden Abschnitten erläutert.

Welche Funktionen im Einzelnen ausgelöst werden können, ist von Produkt zu Produkt unterschiedlich. Um eine flexible Gestaltung des Intrusion-Response zu ermöglichen, bieten einige IDS die Möglichkeit, als Reaktion auf Angriffe vom Anwender vorgegebene Kommandos bzw. Skripte ausführen zu lassen. Um diese Funktion praktisch sinnvoll einzusetzen, ist es jedoch erforderlich, dass eine Parameterübergabe vom IDS an das Kommando bzw. Script bei dessen Aufruf möglich ist.

2.4.1 Dokumentation

Eine angemessene Dokumentation von Ereignissen ist die Voraussetzung zur Auswertung der Ereignisse. Typischerweise wird das Ereignis zusammen mit relevanten Parametern (Zeitpunkt des Auftretens, betroffenes System, Art des Angriffs, etc.) vom IDS protokolliert.

Daneben erlauben einige Produkte für netzbasierte Ereignisse auch eine Aufzeichnung der Rohdaten (IP-Pakete) des Angriffs. Hierdurch können Angriffe nachträglich analysiert und Dritten gegenüber dargestellt werden (Leitungsebene, Strafverfolgungsbehörden).

2.4.2 Alarmierung

Funktionen zur Alarmierung bilden die Grundlage zur Integration des IDS in Eskalationsprozesse. Entsprechend dem Stand der Kommunikationstechnik bieten die meisten IDS Funktionen zur Alarmierung per E-Mail, Signalisierung (z. B. SNMP-Traps) oder Funk (z. B. Pager, SMS).

In der Regel verfügen IDS über mehrere Alarmklassen, in die erkannte Ereignisse automatisch einsortiert werden. Hierdurch wird die Einbettung der IDS-Alarme in organisatorische Eskalationsprozeduren unterstützt.

2.4.3 Automatische Einleitung von Gegenmaßnahmen

Zusätzlich zur Alarmierung können durch das IDS **aktive Reaktionen** vorgenommen werden, wie z. B. eine automatische Beeinflussung von Netzkomponenten oder Rechensystemen. Dies erlaubt eine unverzügliche, zeitnahe Reaktion auf erkannte Angriffe. Beispiele hierfür sind

---

[2] Intrusion-Response ist von Incident-Response wie folgt abzugrenzen: Als Intrusion-Response werden Maßnahmen bezeichnet, die auf Basis erkannter Ereignisse vom Intrusion-Detection-System selbst initiiert werden. Incident-Response dagegen umfasst die technischen und organisatorischen Prozesse zum Umgang mit dem erkannten Ereignis, wie z. B. Eskalationsprozesse.

- eine temporäre Regeländerung der Firewall, um bestimmte Zugangsmöglichkeiten für Angreifer zeitweise zu sperren und Zeit für Sicherungsmaßnahmen zu gewinnen,
- das Beenden von Kommunikationsverbindungen durch aktives Einbringen von Reset-Paketen in das Netz oder
- die Sperrung von Zugriffsrechten auf einem Rechner, wenn ein Angriffs- oder Missbrauchsversuch erkannt wird.

Die automatische Einleitung von Gegenmaßnahmen auf Grundlage vom IDS erkannte Ereignisse, ist jedoch aus mehreren Gründen mit Vorsicht zu betrachten.

1. Die Angriffserkennung durch ein IDS ist unscharf. Es treten regelmäßig Fehlalarme auf. Als Reaktion auf Fehlalarme kann das Unterbinden von Kommunikationsbeziehungen oder Zugangs-/Zugriffsmöglichkeiten dazu führen, dass die Verfügbarkeit von Systemen und Applikationen ungewollt beeinträchtigt wird.
2. Zur Durchführung von Angriffen werden häufig Absenderkennungen gefälscht. Automatische Reaktionen können dann dazu führen, dass Dienste oder Applikationen für legitime Nutzer nicht mehr erreichbar sind.

Deshalb sind bei der Festlegung automatischer aktiver Reaktionen die Nutzenaspekte gegenüber den Auswirkungen der Reaktion des IDS im Falle von Fehlalarmen abzuwägen.

2.5 Sicherheitsaspekte beim Einsatz von IDS

Beim Betrieb eines IDS ist es von elementarer Bedeutung, dass die Funktionalität des IDS selbst nicht in einfacher Weise durch Angriffe außer Kraft gesetzt oder manipuliert werden kann. Nachfolgend werden die Anforderungen näher beschrieben, die in diesem Zusammenhang als relevant angesehen werden.

2.5.1 Verfügbarkeit und Stabilität

Nachstehend werden Verfügbarkeits- und Stabilitätsaspekte für netzbasierte Sensoren, hostbasierte Sensoren, Management- und Auswertungsstation sowie die Datenbank kurz diskutiert.

Netzbasierte Sensoren

Die Verfügbarkeit netzbasierter Sensoren kann durch hohe Netz- und Angriffslast, aber auch durch gezielte Angriffe sowie Programm- und Administrationsfehler eingeschränkt werden.

- Diesem wird in neueren Produkten dadurch begegnet, dass herstellerseitig Netzsensoren als Appliance angeboten werden, um eine ausreichende Hardwareausstattung sowie geeignete Softwarekonfiguration sicherzustellen.
- Durch eine Selbstüberwachung des Sensors können Störungen erkannt werden.
- Wenn Sensoren außer Betrieb gesetzt werden, so berührt dies in der Regel nicht die zu überwachenden Systeme.
- Durch regelmäßige Statusabfragen (Heartbeats) zwischen Managementstation und Sensoren können Störungen und Ausfälle von Sensoren erkannt werden.
- Eine redundante Auslegung des Netzsensors ist prinzipiell möglich. Sie wird in der Praxis jedoch kaum durchgeführt, da typischerweise keine Hochverfügbarkeitsanforderungen an Netzsensoren gestellt werden.

Hostbasierte Sensoren

Die Verfügbarkeit hostbasierter Sensoren kann sowohl durch direkte, auf den Sensor gezielte Angriffe als auch indirekt, durch erfolgreiche Angriffe auf das zu überwachende System beeinträchtigt werden. Auch Störungen und Fehlverhalten des zu überwachenden IT-Systems wirken unmittelbar auf den hostbasierten IDS-Sensor.

- ↗ Durch eine Selbstüberwachung des Sensors können Störungen erkannt werden.
- ↗ Durch regelmäßige Statusabfragen (Heartbeats) zwischen Managementstation und Sensoren können Störungen der Sensoren erkannt werden.

Umgekehrt können sich auch Störungen des Sensors auf das zu überwachende IT-System auswirken.

- ↘ Fehlverhalten oder Abstürze des Sensors können ein Fehlverhalten oder Absturz des zu überwachenden Produktionssystems nach sich ziehen.
- ↘ Der Neustart eines Sensors verlangt in der Regel administrativen Zugriff auf das zu überwachende System. Der IDS-Administrator muss demnach Root/Administratorberechtigung zum betreffenden Produktionssystem besitzen.

Im Gegensatz zu netzbasierten Sensoren kann eine redundante Auslegung hostbasierter Sensoren in der Regel nicht erfolgen.

Management- und Auswertungsstationen

Ein Ausfall der Managementstation (Konfiguration oder Auswertung) berührt in der Regel nicht die Funktion der IDS-Sensoren. Dagegen ist eine hohe Verfügbarkeit der Auswertungsumgebung wichtig, denn ein Teil der zu erkennenden Angriffe findet im Sekundenbereich (oder schneller) statt und Folgeschäden können sich schnell ausbreiten. Deshalb ist eine zeitnahe Ereigniserkennung und Reaktion notwendig.

- ↗ IDS unterstützen in der Regel eine redundante Konfiguration der Managementstationen in Form einer Cold-Standby-Konfiguration. Dabei müssen nach Ausfall einer Managementstation die Konfigurationsdaten und verwendete Kryptoschlüssel zum Ersatzsystem übertragen werden.
- ↗ Alternativ dazu können in einigen IDS die Managementstationen kaskadiert werden, so dass bei Ausfall einer Station die Konfiguration und Auswertung eines IDS weiterhin möglich ist.

Datenbank

Einige IDS sind so ausgelegt, dass sie bei Ausfall der Ereignisdatenbank die abzulegenden Ereignisse zwischenspeichern. Dies ist jedoch nicht in allen verfügbaren IDS realisiert.

Weitergehende Mechanismen zur Sicherstellung der Verfügbarkeit werden in der Regel durch das IDS nicht realisiert, sondern müssen durch das Datenbanksystem selbst erbracht werden.

2.5.2 Integrität

Netzbasierte Sensoren

- ↘ Bei hoher Netz- und Angriffslast kann ein Sensor überlastet werden, so dass nicht mehr alle IP-Pakete untersucht werden können und Angriffe möglicherweise übersehen werden.
- ↗ Einer Überlastung kann vorgebeugt werden, indem dem Sensor ausreichend dimensionierte Hardware (ggf. als Appliance) zugrundegelegt wird.
- ↗ Durch eine Selbstüberwachung des Sensors kann eine Überlastung oder sonstige Störung erkannt werden.
- ↗ Durch regelmäßige Statusabfragen (Heartbeats) zwischen Managementstation und Sensoren können Störungen erkannt werden.

- ↗ Durch Einsatz spezieller Netzadapter (TAPs) kann sichergestellt werden, dass sich ein eventuelles Fehlverhalten des netzbasierten Sensors nicht auf Systeme im Produktionsnetz auswirken kann, da jeglicher Datenverkehr vom Sensor in Richtung Produktionsnetz physikalisch blockiert wird.

Hostbasierte Sensoren

Auch hostbasierte Sensoren, die Netzverkehr überwachen, können überlastet werden und Angriffe übersehen. Zusätzlich ist beim Einsatz hostbasierter Sensoren zu bedenken, dass sich ein eventuelles Fehlverhalten des Sensors unmittelbar auf das zu überwachende Produktionssystem auswirken kann, da der Sensor typischerweise administrative Systemrechte wahrnimmt. Gezielte Angriffe auf die Integrität des IDS-Sensors (z. B. Buffer Overflows) können daher auch das Produktionssystem schädigen.

- ↘ Ein Fehlverhalten des Sensors kann ein Fehlverhalten oder den Absturz des zu überwachenden Produktionssystems nach sich ziehen.
- ↘ Die Konfiguration und der Neustart eines hostbasierten Sensors verlangen in der Regel administrativen Zugriff auf das zu überwachende System. Der IDS-Administrator muss demnach Root/Administratorberechtigung zum betreffenden Produktionssystem besitzen.
- ↘ Ein Schutz des Produktionssystems durch Trennung von Sensor und überwachtem System ist – im Gegensatz zu netzbasierten Sensoren – nicht möglich.

Die Integrität hostbasierter Sensoren kann darüber hinaus durch indirekte Angriffe auf das zu überwachende System selbst beeinträchtigt werden, denn auch Störungen und Fehlverhalten des zu überwachenden IT-Systems wirken unmittelbar auf den hostbasierten IDS-Sensor.

- ↗ Der Sensor sollte derartiges Fehlverhalten jedoch erkennen und an das IDS melden.
- ↗ Durch eine Selbstüberwachung des Sensors können Störungen des Sensors erkannt werden.
- ↗ Durch regelmäßige Statusabfragen (Heartbeats) zwischen Managementstation und Sensoren können Störungen erkannt werden.

Datenbank

Die Sicherstellung der Datenbankintegrität muss in der Regel durch diese selbst erbracht werden und erfolgt nicht durch das IDS.

2.5.3 Vertraulichkeit

Einsatz von Verschlüsselung

Die Kommunikation zwischen den einzelnen IDS-Komponenten erfolgt meist unverschlüsselt, teils nur in eine Richtung verschlüsselt. Bei einigen IDS kann die Verschlüsselung für einige der Kommunikationswege nachgerüstet werden, z. B. durch Einsatz von SSL bei webserver-basierten Managementstationen oder durch Einsatz von SSH/SCP bei der Kommunikation zwischen IDS-Management und Sensoren.

Einsatz separater IDS-Teilnetze

Einige IDS gestatten die Definition eigener physikalischer IDS-Teilnetze für die Kommunikation der IDS-Komponenten untereinander. Hierdurch kann erreicht werden, dass das IDS von Produktionsnetzen aus unsichtbar ist, d.h. ein Angreifer kann nicht durch Installation eines Sniffers die IDS-Kommunikation belauschen. Auch kann ein Angreifer Komponenten des IDS nicht interaktiv erreichen, wenn die Trennung der Netze über TAPs oder Netzwerkinterfaces erfolgt, die in einem sog. Stealth-Mode konfiguriert sind.

Eine hohe Schutzwirkung eines separaten IDS-Netzes ist jedoch nur dann gegeben, falls auch alle weiteren Netzübergänge zu Produktionsnetzen angemessen geschützt sind (vgl. Kapitel 5.3). Dies betrifft insbesondere

- eine mögliche Netzkopplung über das überwachte System beim Einsatz von Hostsensoren,
- Alarmierung per E-Mail oder SNMP zu Systemen im Produktionsnetz und
- Zugriffe auf Webseiten im Internet von der Management- und Auswertungsstation aus (Informationsgewinnung, ggf. Signatur-Updates, etc.)

2.5.4 Nachvollziehbarkeit des Zugriffs auf IDS-Komponenten

IDS-Systeme sehen typischerweise weder eine Benutzer- und Rechteverwaltung noch eine Rollentrennung vor. In der Regel müssen alle IDS-Benutzer dieselbe administrative Kennung verwenden (Passwort-Sharing). Hierdurch können administrative Zugriffe nachträglich nicht mehr konkreten Personen zugeordnet werden.

Beim Einsatz webbasierter Managementkonsolen kann der Zugriff zu diesen Konsolen durch den Webserver auf Berechtigte eingeschränkt werden. Die Zugriffskontrolle kann durch Einsatz von SSL um eine Authentisierung basierend auf X.509-Zertifikaten ergänzt werden. Eine applikationsseitige Beschränkung von Rechten erfolgt jedoch auch hierdurch nicht.

2.5.5 Schutzmaßnahmen an Netzübergängen

Wenn IDS-Komponenten über Netzgrenzen hinweg miteinander verbunden werden, so müssen an dieser Stelle die für die Netzgrenze gültigen Schutzmaßnahmen (z. B. Paketfilterung) auch für die IDS-Kommunikation angewendet werden.

Darüber hinaus ist bei webserver-basierten IDS-Konsolen ein regelmäßiges Update des zugrundeliegenden Webservers erforderlich, um Angriffe gegen das IDS auf Ebene des Webservers auszuschließen.

Weitere Sicherheitsaspekte beim Einsatz von IDS an Netzübergängen werden in den Kapiteln 3.5, 3.6 und 5 angesprochen.

2.5.6 Einsatz von JavaScript bei webserver-basierten Konsolen

In einigen IDS werden ausschließlich Webseiten mit statische Daten eingesetzt. Dies hat den Nachteil, dass neue Ereignisse erst nach clientseitigem Refresh der Webseiten, d. h. nach Betätigen des Refresh-Buttons sichtbar werden[3].

Alternativ hierzu verwenden andere IDS JavaScript-basierte Webseiten. Dies führt wiederum zu erhöhten Risiken, da webserver-basierte Konsolen in der Regel auch einen Internetzugriff aufweisen, etwa um Informationen zu Angriffen abzurufen. In diesem Fall sollten Webbrowser eingesetzt werden, die ein selektives An- und Ausschalten von JavaScript für unterschiedliche Webseiten gestatten. Wenn organisationsinterne Regelungen den Einsatz von JavaScript in Webclients verbieten, hat das Auswirkungen auf die Auswahl des IDS.

[3] Es gibt grundsätzlich die Möglichkeit, auch für statische Webseiten einen regelmäßigen Refresh zu automatisieren. Diese Funktion wird jedoch in marktverfügbaren IDS-Produkten in der Regel nicht eingesetzt.

2.5.7 Sicheres Signatur-Update

Die Qualität der Angriffserkennung wird wesentlich durch die Signaturen des IDS bestimmt. Die Funktion des IDS kann gestört werden, falls bei der Aktualisierung gefälschte oder manipulierte Signaturen in das IDS geladen werden. Deshalb sollten IDS über Funktionen zur Sicherstellung der Authentizität und Integrität von Signatur-Updates verfügen. Dies ist für einen großen Teil der marktverfügbaren IDS der Fall.

2.6 Nutzungsfreundlichkeit

Hinsichtlich der Nutzungsfreundlichkeit bestehen große Unterschiede zwischen den am Markt erhältlichen IDS. Die von den Herstellern anvisierte Zielgruppe hat dabei einen wesentlichen Einfluss auf die Gestaltung des IDS.

Die Nutzungsfreundlichkeit eines IDS wird aus technischer Sicht maßgeblich geprägt durch:

- die Stabilität und Bedienungsfreundlichkeit der Konfigurations- und Auswertungsoberflächen,
- die Übersichtlichkeit und Aussagekraft der IDS-Meldungen,
- Funktionen zur manuellen Auswertung der gemeldeten Ereignisse,
- die Möglichkeiten zur Einbindung externer Informationsquellen,
- Funktionen zur Anpassung und Konfiguration von Signaturen,
- unterstützende Funktionen zum Backup der Signaturen und
- die Funktion zum automatisierten Signatur-Update.

2.6.1 Konfiguration, Stabilität und Bedienungsfreundlichkeit

Für die Konfiguration der IDS-Komponenten werden Benutzungsschnittstellen angeboten, die sich in folgende Kategorien einteilen lassen:

- **Kommandozeilen-Interface**

  Kommandozeilen basierte IDS richten sich an technisch versierte IDS-Administratoren und Analysten. Das IDS wird durch Editieren von Konfigurationsdateien oder die Angabe von Parametern beim Start des IDS konfiguriert. Neben dem Opensource-IDS „Snort“ sind auch einige UNIX-basierte IDS auf diese Weise konfigurierbar. Hierzu ist typischerweise ein Shellzugriff (z. B. per SSH) auf die betreffenden IDS-Komponenten erforderlich. IDS, die kommandozeilenorientiert arbeiten, weisen erfahrungsgemäß eine vergleichsweise hohe Stabilität auf.

- **Webbasierte Schnittstelle**

  Die Konfigurationsoptionen werden in einem Webbrowserfenster dargestellt. Der Webbrowser greift dabei auf einen für das IDS konfigurierten Webserver zu, der in der Regel auf der Managementstation installiert ist. Hierzu wird auf Drittprodukte zurückgegriffen(z. B. Apache-Webserver bei UNIX-basierten IDS sowie Microsoft IIS bei Windows-basierten IDS). Schutzmaßnahmen wie Zugriffskontrolle und Verschlüsselung werden typischerweise auf Ebene des Webservers realisiert.

  Nachteilig ist, dass regelmäßig ein manuelles Refresh der Webseiten am Browser erfolgen muss, da neue Ereignisse erst nach einem Update der Seiten dargestellt werden. Dies wird von einigen Herstellern durch Einsatz von JavaScript oder ActiveX umgangen. Browserseitig muss dann in der Regel jedoch die Verarbeitung entsprechender aktiver Inhalte aktiviert sein.

Die Stabilität webserver-basierter Bedienoberflächen ist in hohem Maße von der Stabilität des zugrundeliegenden Webservers abhängig und nach Erfahrungswerten als sehr hoch einzustufen.

- **IDS-proprietäre Bedienoberfläche**

  Die Konfigurationsoptionen und die gemeldeten Ereignisse werden in einer proprietären Oberfläche dargestellt, die in der Regel auf der Managementstation installiert ist. Die Bedienoberflächen weisen gegenüber den anderen o. g. Bedienschnittstellen eine wesentlich höhere Komplexität auf. Der Benutzungskomfort ist bei diesen IDS erfahrungsgemäß hoch. Allerdings sind diese IDS anfälliger gegen Programmierfehler und weisen eine geringere Stabilität als IDS mit webserver-basierten oder kommandozeilen-basierten Bedienoberflächen auf. Nachteilig ist zudem, dass ein Remote-Zugriff auf die Managementstation den Einsatz von Zusatzprodukten (z. B. pcANYWHERE oder VNC) erfordert.

2.6.2 Übersichtlichkeit und Aussagekraft der IDS-Meldungen

Die Aussagekraft der IDS-Meldungen soll ausreichen, um das gemeldete Ereignis einordnen und bewerten zu können. Hierzu ist ggf. ein Rückgriff auf der Meldung zugrunde liegenden Daten (etwa aufgezeichneten Netzverkehr oder Logdateien) notwendig, die durch das IDS referenziert bzw. bereitgestellt werden sollten.

Umfang und notwendige Detailtiefe der Meldungen hängen dabei wesentlich vom Einsatzszenario des IDS sowie von der Art der zu erkennenden Ereignisse ab. Hierzu folgende Beispiele:

- Die Analyse eines IP-Paketes, mit dem Shell-Verbindungen über ICMP getunnelt werden (z. B. LOKI-Angriff), verlangt die Aufzeichnung der in Frage kommenden – auch unverdächtigen – ICMP-Pakete im fraglichen Zeitraum.
- Bei Portscans dagegen werden typischerweise nicht alle in Frage kommenden IP-Pakete, sondern nur kumulierte Daten aufgezeichnet, etwa Quell- und Zieladressen, gescannte Portnummern, Anzahl gescannter Ports.

Bei einigen IDS sind Ereignismeldungen sehr oberflächlich und in ihrer Aussagekraft begrenzt. Die Analyse des zugrunde liegenden Vorfalls und eine Nachverfolgung des Angriffs ist dadurch erschwert oder im Extremfall nicht möglich.

In den gängigen IDS typischerweise zufriedenstellend gelöst ist oder in ausreichendem Maße anpassbar, sind Funktionen zur Vorsortierung der Ereignisse und zur Zuordnung von Intrusion-Response-Funktionen.

2.6.3 Reportgenerierung

Die Generierung von Reports dient typischerweise zweierlei Zielen:

- Aufdecken neuer, noch nicht erkannter Ereignisse und Trends durch Filterung und grafische Aufbereitung langfristig gespeicherter Daten.
- Generierung von Statistiken und Grafiken für Management-Reports.

Aus technischer Sicht steht die Erkennung von neuen Ereignissen im Vordergrund, wobei diese in der Regel nur manuell erfolgt – unterstützt durch umfangreiche Such- und Filterfunktionen zu den in der Ereignisdatenbank gespeicherten Datensätzen. Die Erfahrung zeigt jedoch, dass – u. a. auch zur Rechtfertigung der hohen Kosten für Schutzmaßnahmen – die Generierung von Management-Reports und zugehörigen Grafiken ebenso große Bedeutung hat. Einige IDS-Hersteller bieten explizite Schnittstellen zu Management-Reporting-Systemen an.

2.6.4 Einbindung externer Informationsquellen

Zur Analyse von IDS-Meldungen ist es sinnvoll, extern erreichbare Quellen zu konsultieren, um Hintergrundinformationen zu Angriffen zu erhalten oder eigene Beobachtungen dorthin zu melden. Aktuelle IDS unterstützen typischerweise einen Webzugriff via Shortlink zu bekannten Informationsquellen.

2.6.5 Anpassung und Konfiguration von Signaturen

Das IDS sollte die Generierung neuer und die Anpassung bestehender IDS-Signaturen unterstützen, um eine möglichst genaue Kalibrierung des IDS zu erreichen. Sowohl bei der Kalibrierung des IDS als auch der Auswertung gemeldeter Ereignisse ist es notwendig, Details der betreffenden Signatur zu sehen, um festzustellen, warum ein Ereignis gemeldet wurde (Minimierung von Fehlalarmen). Einige am Markt erhältliche IDS unterstützen dies nur sehr eingeschränkt, so dass weder die Signatur angezeigt werden kann noch eine detaillierte technische Beschreibung verfügbar ist. Ein IDS-Administrator hat in diesem Fall bei häufigen Fehlalarmen nur die Möglichkeit, die Signatur abzuschalten, kann diese jedoch nicht an die Bedürfnisse anpassen.

2.6.6 Backup von Signaturen

Die Konfiguration des IDS (Signaturen, Kalibrierung, etc.) ändert sich häufig und sollte nach jeder Änderung gesichert werden. Für die Datensicherung des aktuellen IDS-Stands ist dabei die Sicherung der Konfigurationseinstellungen (Signaturen, Kalibrierung, etc.) ausreichend. Das IDS sollte hierzu über entsprechende Funktionen verfügen.

2.6.7 Automatisches Signatur-Update

Wie auch bei Virenscannern hängt die Qualität der Ereigniserkennung eines IDS stark von der Aktualität der Signaturen ab. Neu Signaturen sind regelmäßig einzuspielen. Dieser Vorgang kann ggf. automatisiert werden. Manuell festzulegen ist jedoch in jedem Fall, wie das IDS auf die Ereignisse reagieren soll, die durch die neuen Signaturen erkannt werden.

2.7 IDS-Markt, Kosten und Investitionsschutz

Auf dem Markt fand in den letzten zwei Jahren bereits eine Konsolidierung statt. Für einige IDS Produkte wurde die Herstellerunterstützung eingestellt (z. B. Cybercop von NAI), andere wurden nicht weiterentwickelt. Einige kleinere IDS-Anbieter wurden von größeren Firmen übernommen (etwa NetworkICE von ISS, Network Security Wizards von Enterasys, Axent von Symantec).

Im Open-Source-Bereich hat Snort zunehmend an Bedeutung gewonnen. Snort wird inzwischen auch kommerziell unterstützt. Dies betrifft sowohl die Wartung von Snort als auch die kommerzielle Produktversion OpenSnort.

Die Konsolidierung geht jedoch nicht mit einer Preissenkung der Produkte einher. Dies liegt darin begründet, dass eine fortlaufende Weiterentwicklung der Produkte erfolgte. Dies betrifft einerseits die deutliche Verbesserung der Angriffserkennung netzbasierter Sensoren in den letzten Jahren sowie andererseits die Skalierbarkeit der Systeme (Management, Verwaltung mehrerer, ggf. unterschiedlicher Sensoren, etc.).

Bei den Kosten sind Anschaffungs-, Wartungs- und Betriebskosten von IDS gleichermaßen wichtig. Daneben sind die Kosten für einen Hotline-Support durch den Hersteller zu berücksichtigen. Im Rahmen der Vorauswahl können nur die Anschaffungs- und Wartungskosten berücksichtigt werden. Der genaue

Betriebsaufwand hängt von der Nutzungsfreundlichkeit des IDS ab (vgl. Kapitel 2.6) und stellt sich daher erst im Test- bzw. Pilotbetrieb heraus.

Beim Einsatz von Open-Source-Produkten entfallen typischerweise die Anschaffungskosten. Im Gegenzug ist jedoch mit höherem Personalaufwand bei Anpassung und/oder Betrieb des IDS zu rechnen.

Für den Investitionsschutz ist zu berücksichtigen, dass ein IDS – wie Virenschutzsysteme – einer regelmäßigen Aktualisierung bedarf. Der praktische Nutzen eines IDS-Produkts verringert sich daher schnell, falls für das IDS keine neuen Signaturen mehr bereitgestellt werden.

2.8 Standardisierung und Interoperabilität

Im Bereich Intrusion-Detection gab es zahlreiche Ansätze zur Standardisierung, die den IDS-Bereich unterschiedlich weit abdeckten. Einige dieser Ansätze sind im Folgenden aufgeführt.

- Common Intrusion Detection Framework (CIDF) Projekt

  Das CIDF ist ein von der US-amerikanischen DARPA unterstütztes Projekt zur Definition von ID-Komponenten (Ereigniserkennung, Ereignisauswertung, Datenspeicherung und Reaktion) und Protokollen zur Kommunikation dieser Komponenten. Für den einheitlichen Umgang mit Ereignisdaten wurde die „Common Intrusion Specification Language“ (CISL) entwickelt.

- Intrusion Detection Working Group (IDWG) der IETF

  Die IDWG entwickelte das „Intrusion Detection Exchange Format“ (IDEF), das ein Format zur Beschreibung von Angriffen definiert. Das IDEF wurde am 15.6.2000 als Internet-Draft veröffentlicht. Eine Umsetzung in einen RFC erfolgte bislang nicht.

- Common Content Inspection (CCI) API und OPSEC von Check Point

  Das CCI API definiert eine Schnittstelle, über die von einer Firewall oder einem ID-Sensor gesichtete, „verdächtige“ Daten, die einer weiteren Untersuchung bedürfen, an eine Auswertungsstation weitergeleitet werden können. OPSEC (www.opsec.com), eine Initiative der Firma Check Point, stellt eine Reihe von APIs und Protokollen bereit, die einen Austausch auch für IDS relevanter Daten zwischen Systemen ermöglichen. Beispiele sind das „Log Export API” (LEA), das „Suspicious Activity Monitoring Protocol” (SAMP) und das „Content Vectoring Protocol” (CVP). Es hat sich eine Allianz von Herstellern gebildet, die in ihren Produkten Protokolle und APIs der OPSEC-Initiative berücksichtigen.

- Common Vulnerabilities and Exposures (CVE)

  Ziel des CVE (cve.mitre.org) ist die einheitliche Benennung und Nummerierung aller bekannten Angriffe und Schwachpunkte. CVE ist eine Initiative der Mitre Cooperation, einem US-amerikanischem Non-Profit Unternehmen, dass IT-Aufgaben von allgemeinem Interesse nachgeht. Das CVE-Register weist inzwischen über 2000 Einträge auf.

- ISO Technical Report

  ISO/IEC bereiten einen „Technical Report“ zum Thema Intrusion-Detection vor, dessen voraussichtlicher Inhalt in [N3177] wiedergegeben ist. Der Report enthält einen Überblick über das Thema IDS.

Während CIDF ein übergreifendes Framework darstellt, beschränkt sich das IDEF auf die einheitliche Beschreibung und Charakterisierung von Angriffen und CVE lediglich auf deren einheitliche Benennung.

CIDF und IDEF wurden bislang nicht in Produkte umgesetzt, die am Markt angeboten und von Herstellern unterstützt werden. Die CVE-Nummerierung wird inzwischen in den meisten IDS-Produkten berücksichtigt.

Hinsichtlich der Interoperabilität ergibt sich die Situation, dass

- von unterschiedlichen IDS gemeldete Ereignisse auf Basis ihrer CVE-Nummern verglichen werden können. Grundsätzlich ist hierdurch die Basis zur nachträglichen, IDS-übergreifenden Analyse der Verteilung von Angriffen gegeben.
- ein Austausch von Komponenten zwischen unterschiedlichen IDS bislang nicht möglich ist. Dies betrifft sowohl Sensoren als auch Signaturbeschreibungen.

Einige Hersteller planen derzeit Definition und Einsatz von „Snort-like Signatures“ in ihre IDS zu integrieren. Falls dabei der Syntax der Snort-Signaturen ohne Änderungen und Ergänzungen übernommen wird, könnte hierdurch zumindest für diese Teilmenge von Signaturen eine gewisse Austauschbarkeit erreicht werden[4].

[4] In der Vereinheitlichung von Signaturbeschreibungen besteht grundsätzlich ein hohes Rationalisierungspotenzial, da Signatur-Updates nicht länger herstellerspezifisch ausgearbeitet werden müssten, sondern vereinheitlicht und herstellerübergreifend angeboten werden könnten.

3 Zusammenspiel von IDS mit anderen Sicherheitskomponenten

Zur Sicherstellung einer wirksamen Sicherheitsgesamtfunktionalität ist von besonderer Bedeutung, wie IDS mit anderen, bereits im Einsatz befindlichen Sicherheitskomponenten zusammenspielen, deren Funktionalität ergänzen bzw. möglicherweise einschränken.

In diesem Kapitel werden Intrustion Detection Systeme im Zusammenhang mit folgenden, anderen Sicherheitskomponenten bzw. -funktionen betrachtet.

- Virenscanner,
- Content Filter,
- Vulnerability Scanner,
- Verschlüsselungskomponenten,
- Firewalls,
- Hochverfügbare Systeme.

Hierzu wird der Einsatzzweck und die Funktionsweise der Sicherheitskomponente zunächst kurz erläutert und gegenüber dem Einsatzzweck und der Funktionsweise von IDS abgegrenzt. Danach werden Möglichkeiten, Einschränkungen und ggf. Zusatznutzen der Kombination der jeweiligen Sicherheitskomponente/-funktion mit IDS erläutert.

3.1 Virenscanner

3.1.1 Kurzbeschreibung und Abgrenzung

Beim Virenscan werden Dateien auf Virenbefall untersucht. Im Vordergrund der Untersuchung stehen ausführbare Programme sowie Dateien mit aktiven Elementen. Zu letzteren gehören z. B. Word und Excel Dateien, die Makroviren enthalten können, oder HTML-Seiten, in denen aktive Elemente (ActiveX) mit Schadfunktionen eingebettet sein können. Des Weiteren werden zum Teil Prozess-Heuristiken erstellt, um “virale Prozesse” zu identifizieren

Um dem Nutzer die Anwendung zu vereinfachen binden sich Virenscanner im Allgemeinen automatisch in gefährdete Aktionen mit ein, so dass etwa

- beim Laden von Dateien von Diskette,
- bei der Installieren neuer Software oder
- beim Öffnen von E-Mail-Anhängen

automatisch eine Virenprüfung der jeweiligen Dateien erfolgt. Daneben kann z. B. ein regelmäßiges Scannen des gesamten Systems konfiguriert werden.

Virenscanner können im erweiterten Sinn als spezielle hostbasierte Sensoren betrachtet werden, die Dateien, Software und z. T. Prozess-Heuristiken analysieren. Wie bei IDS gibt es Managementstationen, Alarmierungen, aktive Reaktionen und Signaturdatenbanken für Viren, die regelmäßig aktualisiert werden müssen.

Als Reaktion erfolgt bei erkannten Viren typischerweise eine Alarmierung. In vielen Fällen erlauben Virenscanner als Reaktion auch die direkte Entfernung des Virus, d. h. das „Desinfizieren“ der befallenen Datei.

3.1.2 Zusammenspiel mit IDS

Die Funktionalitäten von IDS und Virenscannern ergänzen sich gegenseitig. Intrusion-Detection und Virenscanning können grundsätzlich unabhängig von einander eingesetzt werden. Da die Einsatzweisen von IDS und Virenscannern weitgehend übereinstimmen, besteht grundsätzlich die Möglichkeit, dieselbe Organisation (Prozesse, zuständige Mitarbeiter/Abteilungen) für den Betrieb von IDS und Virenscannern zu verwenden. Ob dies in der Praxis sinnvoll ist, sollte im Einzelfall verifiziert werden.

Da sowohl hostbasierte Intrusion-Detection Sensoren als auch Virenscanner typischerweise tief in die Systeme eingreifen, ist bei konkreten Implementierungen darauf zu achten, dass sich die verwendeten Produkte in ihrer Funktionalität nicht gegenseitig beeinträchtigen.

3.2 Content Filter

3.2.1 Kurzbeschreibung und Abgrenzung

Content filter (Inhaltsfilter) werden zur aktiven Filterung der über das Netz übertragenen Inhalte eingesetzt. Nicht gewünschte Inhalte werden blockiert, ggf. werden die übertragenen Daten transparent um nicht gewünschte Inhalte gesäubert.

Bei Intrusion-Detection-Systemen stehen dagegen die Inspektion der übertragenen Daten sowie die Alarmierung im Vordergrund. Durch IDS werden typischerweise keine Daten aus dem Netz herausgefiltert.

Beispiele für die Inhaltsfilterung:

- Beim Surfen von Mitarbeitern im Internet werden bestimmte URLs unterdrückt.
- Inhalte (Web-Content, E-Mails) werden auf bestimmte Kennwörter oder Wortsequenzen untersucht, um das Empfangen und/oder Versenden anstößiger Informationen (z. B. rassistische, radikalpolitische oder pornographische Inhalte) zu unterbinden.
- Die zentrale Prüfung von E-Mails auf Viren ist ein Spezialfall der Inhaltsfilterung. Falls in E-Mails dabei Viren entdeckt aber nicht automatisch beseitigt werden können oder falls keine Virenprüfung möglich ist, da z. B. die Daten verschlüsselt wurden, werden die entsprechenden E-Mails typischerweise in ein Quarantäneverzeichnis befördert und nicht zugestellt.

3.2.2 Zusammenspiel mit IDS

Content Filtering und Intrusion-Detection weisen sich ergänzende Funktionalitäten auf und können unabhängig voneinander eingesetzt werden.

IDS können dazu dienen, Angriffe auf IT-Systeme, die zur Inhaltsfilterung genutzt werden, zu erkennen und diese Systeme zu überwachen.

3.3 Vulnerability Scanner

3.3.1 Kurzbeschreibung und Abgrenzung

Vulnerability Scanner dienen dazu, Schwächen und offene Angriffspunkte in Netzen und Systemen vorab zu erkennen, während IDS zur Erkennung von stattfindenden Angriffen in Netzen und Systemen genutzt werden. Die Funktionalität von IDS und Scannern ist in dieser Hinsicht komplementär.

Wie bei IDS wird auch zwischen netz- und hostbasierten Scannern unterschieden. Netzbasierte Scanner kommunizieren über eine Netzverbindung mit dem Zielsystem und versuchen Schwächen und Angriffspunkte in den vom Zielsystem angebotenen Kommunikationsdiensten zu ermitteln. Hostbasierte Scanner werden auf dem zu prüfenden Rechner installiert und prüfen die Konfiguration des Betriebssystems auf Schwachstellen.

Während IDS permanent ein System bzw. Netz überwachen, erfolgt die Prüfung eines Systems oder Netzes durch Scanner typischerweise in (regelmäßigen) zeitlichen Abständen. Durch den Einsatz von Scannern werden vorhandene Systemschwächen und offene Angriffspunkte deutlich. Auf Basis der Ergebnisse des Scannings kann dann versucht werden, die identifizierten Schwachpunkte zu beheben.

3.3.2 Zusammenspiel mit IDS

Die Funktionalitäten von Vulnerability Scannern und IDS ergänzen sich.

Vulnerability Scanner können sowohl zur Überprüfung der Funktionsfähigkeit von IDS eingesetzt werden als auch die Kalibrierung eines IDS unterstützen: Dabei wird das IDS so kalibriert, dass Angriffe, gegen die das überwachte System gemäß der Ergebnisse der Vulnerability Scannings nachweislich immun ist, mit einer geringen Priorität behandelt oder ggf. vollständig unterdrückt werden, während bei Angriffen, zu denen vorhandene Systemschwächen bekannt sind, eine umgehende Alarmierung durch das IDS erfolgt.

3.4 Verschlüsselungskomponenten

3.4.1 Kurzbeschreibung und Abgrenzung

Verschlüsselung dient als Maßnahme zur Wahrung der Vertraulichkeit übertragener oder gespeicherter Daten. Dabei sind folgende Ansätze zu unterscheiden:

1. **Übertragung verschlüsselter Daten über einen ungeschützten Kommunikationskanal**. Hierunter fällt insbesondere die Ende-zu-Ende Verschlüsselung von E-Mail. E-Mails werden dabei im Client verschlüsselt und ggf. digital signiert und in dieser Form über das Internet übertragen.
2. **Übertragung (unverschlüsselter) Daten über einen gesicherten, insbesondere verschlüsselten Kommunikationskanal**. Beispiele hierfür sind SSL und IPsec. Dabei ist weiter zu unterscheiden, auf welcher Protokollschicht die Verschlüsselung erfolgt:
   - Die Sicherung per SSL erfolgt direkt unter der Anwendungsschicht.
   - Die Sicherung per IPsec erfolgt auf Ebene der IP-Kommunikation.

3.4.2 Zusammenspiel mit IDS

Die Verschlüsselung beeinträchtigt Maßnahmen zur Inhaltsfilterung und zum (zentralen) Virenscanning, da eine inhaltlichen Kontrolle nur bei unverschlüsselt vorliegenden Daten erfolgen kann. Die Auswirkungen einer verschlüsselten Kommunikation auf das Intrusion-Detection erfordern eine differenziertere Betrachtung:

Beim Einsatz netzbasierter IDS hängt der Grad der Beeinträchtigung der Angriffserkennung davon ab, welcher der oben aufgeführten Verschlüsselungsansätze gewählt wurde. Bei der ungeschützten Übertragung verschlüsselter Daten (Ansatz 1 oben) wird die Funktionalität der Überwachung praktisch kaum beeinträchtigt. Lediglich inhaltlich können die verschlüsselten Daten nicht kontrolliert werden. Bei der Übertragung von Daten über verschlüsselte Kommunikationskanäle hängt der Grad der Beeinträchtigung davon ab, auf welcher Protokollschicht die Verschlüsselung erfolgt. Da Netzsensoren typischerweise mehrere Protokollschichten analysieren, können bei SSL-gesicherten Verbindungen Angriffe auf IP-Ebene erkannt werden, während bei der Nutzung von IPsec lediglich die Protokollkonformität der übertragenen IP-Pakete geprüft werden kann.

Netzbasierte IDS weisen jedoch auch Nutzenaspekte auf, die durch Verschlüsselung nicht beeinflusst werden. Beispielsweise ist es durch Analyse des Datenflusses möglich, etwa Kommunikationsbeziehungen zwischen unberechtigten Systemen oder ein ungewöhnliches Ansteigen des Datenverkehrs zu entdecken. Darüber hinaus bedeutet das Vorhandensein verschlüsselten Datenverkehrs typischerweise nicht, dass Angriffsversuche ebenfalls verschlüsselt bzw. über den verschlüsselten Kanal erfolgen. Durch Einsatz eines netzbasierten IDS können darüber hinaus auch Fehlkonfigurationen, etwa Nachrichten, die fälschlicherweise unverschlüsselt übertragen werden, erkannt werden. Daher kann ein Einsatz netzbasierter IDS auch in Netzsegmenten sinnvoll sein, in denen typischerweise verschlüsselt kommuniziert wird.

Beim Einsatz hostbasierter IDS wird die Funktionalität der Angriffserkennung typischerweise nicht beeinträchtigt, unabhängig davon, welcher Ansatz für die Verschlüsselung genutzt wird. Erfolgt die Entschlüsslung auf dem überwachten Host, hat der Hostsensor grundsätzlich Zugriff auf die entschlüsselten Daten. Ansonsten ist durch die verschlüsselt vorliegenden Daten keine Gefährdung gegeben.

Insgesamt ist in Umgebungen, in denen eine Verschlüsselung via VPN erfolgt, eine Kombination aus netzbasierten und hostbasierten IDS-Komponenten sinnvoll, um sowohl Angriffe außerhalb des VPN-Kanals zu erkennen als auch solche, die über den verschlüsselten Kanal ausgeführt werden.

3.5 Firewalls

3.5.1 Kurzbeschreibung und Abgrenzung

Firewall-Systeme dienen zur Kontrolle des Netzverkehrs an Netzübergängen. Durch die Filterung des Datenflusses gemäß vorgegebener Regeln bieten Firewall-Systeme eine aktive Sicherheit, da nur der gemäß den eingestellten Regeln zulässige Verkehr das Firewall-System passieren darf.

IDS bieten keine aktive Sicherheit, sondern reagieren nur auf erkannte Angriffe.

3.5.2 Zusammenspiel mit IDS

Durch die unterschiedliche Art der Kontrolle und die unterschiedlichen Einsatzpunkte ergänzen sich Firewall-Systeme und IDS in ihrer Funktionalität. Kein System kann das andere ersetzten, sondern lediglich die Funktionalität des anderen Systems erweitern.

Die im Folgenden aufgeführten Beispiele verdeutlichen einige Einsatzbereiche von IDS, die von Firewall-Systemen nicht geleistet werden können. Konkrete Architekturen für den kombinierten Einsatz von Firewall-Systemen und IDS werden später in Kapitel 5 erläutert.

- **Erkennung von Angriffen aus dem internen Netz**

  Eine Firewall kann nur Angriffe abwehren, die über sie laufen. Die Firewall bietet keinen Schutz gegen Angriffe auf interne Systeme, die im internen Netz ausgelöst werden. IDS können sowohl den Datenfluss als auch Server im internen Netz überwachen.

- **Überwachung der Firewall Konfiguration**

  Als IT-Komponente ist die Firewall selbst Angriffen ausgesetzt. Daneben sind Fehlkonfigurationen der Firewall gerade in komplexen Einsatzszenarien nicht auszuschließen. Mit einem IDS kann kontrolliert werden, ob die Firewall gemäß ihrer Vorgaben arbeitet.

- **Zusätzliche Überwachung von Diensten, die aktiv nicht ausreichend kontrollierbar sind**

  Für Protokolle, für die keine Applikations-Gateways verfügbar sind, kann durch netzbasierte Sensoren die Datenflusskontrolle verbessert werden. Auch können Firewalls getunnelte und verschlüsselte Kommunikation nicht analysieren. An dieser Stelle helfen hostbasierte IDS, die die Kommunikation nach der Entschlüsselung prüfen.

- **Erkennung externer Zugänge, die nicht über die Firewall führen**

  Die Firewall bietet nur Schutz gegen über sie geleitete Kommunikation. Mit einem IDS können dagegen auch zusätzliche Zugänge (z. B. über Modems) erkannt und überwacht werden.

Sofern IDS-Komponenten über mehrere Teilnetze hinweg verteilt sind, ist darauf zu achten, dass auch die IDS-Kommunikation an den Netzübergängen entsprechend gefiltert wird.

3.6 Hochverfügbare Systeme

3.6.1 Kurzbeschreibung und Abgrenzung

Gerade für Dienstleister im Bereich eCommerce ist die ständige Verfügbarkeit der Internet-Anbindung und angebotener Dienste heute eine unumgängliche Anforderung. Bei unvollständiger Datenübertragung, der Unterbrechung von Sessions oder der fehlenden Verfügbarkeit von Web-Seiten können Kunden verloren gehen und Interessenten demotiviert werden.

Abhängig von der Höhe der Anforderungen an die Verfügbarkeit können verschiedene Ansätze zur Erhöhung der Verfügbarkeit unterschieden werden:

1. **Cold-Standby**: Im Cold-Standby wird ein Ersatzsystem deaktiv („cold“) vorgehalten, dessen Funktionalität mit dem des Produktivsystems übereinstimmt. Beim Ausfall des Produktivsystems wird dieses manuell durch das Ersatzsystem ersetzt. Cold-Standby eignet sich dann als Lösung, wenn eine gewisse Ausfallzeit (Dauer des Wechsels von Produktivsystems auf Ersatzsystem) toleriert werden kann[5].
2. **Hot-Standby**: Im Gegensatz zum Cold-Standby wird im Hot-Standby das Ersatzsystem permanent betrieben („hot“). Bei Ausfall des Produktivsystems erfolgt die Umschaltung auf das Ersatzsystem automatisch ohne Zeitverzug. Abhängig von den Anforderungen und der spezifischen Lösung wer-

[5] Cold-Standby wurde der Vollständigkeit halber mit aufgeführt. Es stellt keine Hochverfügbarkeits-Lösung dar, da mit dem Wechsel vom Produktivsystem auf das Ersatzsystem eine gewisse Ausfallzeit verbunden ist.

den bei der Umschaltung auf das Ersatzsystem bestehende Sitzungen entweder unterbrochen oder transparent übernommen.

3. **Lastverteilung (Load Balancing)**: Während im Cold/Hot-Standby das Ersatzsystem nur beim Ausfall des Produktivsystems dessen Aufgaben übernimmt, teilen sich bei der Lastverteilung mehrere Systeme die Aufgabenerbringung. Ausgefallene Systeme werden dabei erkannt und automatisch umgangen. Technisch wird der Verkehr über Lastverteiler (Load Balancer) geleitet, die ihn in Abhängigkeit bestimmter Regeln an zur Verfügung stehenden Server weiterleiten. Die Lastverteiler überwachen dabei kontinuierlich die Verfügbarkeit und Auslastung der Server und informieren sich gegenseitig hierüber.

3.6.2 Zusammenspiel mit IDS

Für die Integration von IDS in Infrastrukturen, die die oben beschriebenen Ansätze zur Erhöhung der Verfügbarkeit nutzen, werden host- und netzbasierte Sensoren getrennt betrachtet.

Integration hostbasierter Sensoren

Die Integration hostbasierter Sensoren gestaltet sich unproblematisch: Um eine vollständige Überwachung zu erzielen, sind Hostsensoren sowohl auf Produktivsystemen als auch auf Ersatzsystemen vorzusehen. In Cold-/Hot-Standby Szenarien ist dabei abhängig von den Verfügbarkeitsanforderungen an die Überwachung zu entscheiden, ob ein Einsatz von Hostsensoren auf den Ersatzsystemen erforderlich ist. Da typischerweise keine Hochverfügbarkeits-Anforderungen an IDS gestellt werden, wird im Allgemeinen vom Einsatz von Sensoren auf Ersatzsystemen abgesehen. Dies setzt jedoch voraus, das der Ausfall des Produktivsystems erkannt und behoben wird, so dass es zu keinem zeitlich längerem Einsatz eines nicht durch das IDS überwachten Systems kommt.

Falls im Cold-Standby für Ersatzsysteme ein Hostsensor vorgesehen wird, ist bei Einsatz des Ersatzsystems darauf zu achten, dass der Sensor aktiviert und bei der zugehörigen Managementstation angemeldet wird.

Integration netzbasierter Sensoren

Die Integration netzbasierter Sensoren in Hochverfügbarkeitslösungen hängt stark von der spezifischen Netzinfrastruktur ab. Netzbasierte Netzsensoren sind nur dann sinnvoll einsetzbar, wenn sie den Netzverkehr vollständig und genau einmal beobachten können. Die Integration ist insbesondere für die beiden folgenden Situationen erschwert:

1. **Kein zentraler Abgriffpunkt**: Der zu überwachende Netzverkehr ist auf mehrere physikalische Verbindungen verteilt.
2. **Multicast**[6]: Im Rahmen von Hochverfügbarkeits-Architekturen wird von Multicast gesprochen, wenn mehrere Systeme so konfiguriert werden, dass sie unter derselben Adresse (IP-/MAC-Adresse) auf Verbindungsanfragen reagieren. Die Verarbeitung eingehender Daten/Verbindungen wird zwischen den Systemen verteilt und ist für den Client transparent.

Generell ist bei der Integration zu beachten, das die Performance der eingesetzten Netzsensoren hoch genug ist, um den jeweiligen Netzverkehr zu überwachen und sich die Last bei der Überwachung mehrerer Übertragungsstrecken durch denselben Sensor vervielfacht (siehe unten Lösungsansätze 2, 3 und 4). Beispielsweise können im Duplex-Betrieb eines 100Mbps-Ethernets am Sensor bereits bis zu 200Mbps auftreten. Bei der gleichzeitigen Überwachung von zwei solcher Übertragungsstrecken ergeben sich bis

[6] Hierbei werden keine Multicast IP-Adressbereiche genutzt. Anstelle dessen werden mehrere Systeme so konfiguriert, dass sie unter derselben (Unicast) IP-Adresse und MAC-Adresse auf Verbindungsanfragen reagieren.

zu 400Mbps. Auch für die technischen Komponenten (TAPs, Switches) zum Abgriff und zur Zusammenführung des Netzverkehrs sind entsprechender Performance-Anforderungen zu beachten[7].

Kein zentraler Abgriffpunkt

Der erste Fall tritt typischerweise bei der Nutzung von Lastverteilung auf. Die Problematik kann zwar grundsätzlich auch Hot-Standby-Szenarien betreffen; hier wird jedoch üblicherweise auf die Überwachung der Standby-Verbindung verzichtet, da an das IDS keine Hochverfügbarkeits-Anforderungen gestellt werden.

Für die Überwachung von Netzverkehr, der auf mehrere physikalische Verbindungen verteilt ist, bieten sich folgende Lösungsmöglichkeiten an:

1. **Einsatz mehrerer Netzsensoren**: Für jede physikalische Verbindung wird ein separater Netzsensor vorgesehen. Dieser Ansatz hat den Vorteil, dass auch die Überwachung lastverteilt erfolgt. Da der Netzverkehr auf mehrere Sensoren verteilt wird, kann eine höhere Verkehrslast überwacht werden als beim Einsatz von nur einem Sensor. Nachteilig ist der im Vergleich zu den nachstehenden Lösungsansätzen höhere Aufwand, der sich aus dem Einsatz mehrerer Netzsensoren ergibt. Des Weiteren ist für die Angriffserkennung zu beachten, dass Zusammenhänge zwischen einzelnen Ereignissen, die von verschiedenen Sensoren erkannt wurden, erst nach deren zentraler Zusammenführung korreliert werden können. Um dieselbe Erkennungsqualität wie bei Einsatz eines einzelnen Sensors zu gewährleisten, muss die Analyse später, nach der Zusammenführung der Ereignisse erfolgen. Dies ist als Anforderung für ein auszuwählendes IDS zu berücksichtigen.

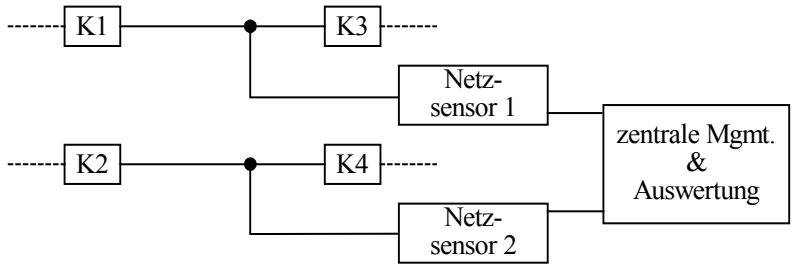

Abbildung 3-1: Einsatz mehrerer Netzsensoren

2. **Einsatz eines Netzsensors mit mehreren Netzinterfaces**: Der von den Verbindungen abgegriffene Netzverkehr wird zu separaten Netzinterfaces desselben Sensors geleitet und durch diesen ausgewertet. Im Vergleich zum Lösungsansatz 1 hat dieses Vorgehen den Vorteil, dass der Sensor den Netzverkehr insgesamt sieht und auswerten kann. Bei der Auswahl des Sensors ist jedoch darauf zu achten, dass dieser die Überwachung des Verkehrs mehrerer Netzinterfaces unterstützt und die Sensor-Performance die Überwachung des gebündelt vorliegenden Verkehrs erlaubt.

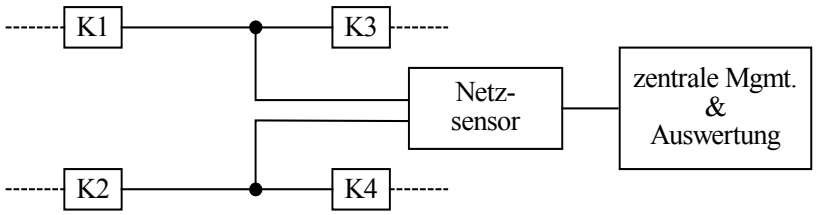

Abbildung 3-2: Einsatz eines Netzsensors mit mehreren Netzinterfaces

3. **Zusammenführung des Netzverkehrs über einen Switch**: Der von den Verbindungen abgegriffene Netzverkehr wird über einen Switch zusammengeführt und zu einem Netzsensors geleitet. Wie auch bei Lösungsansatz 2 ist der Vorteil gegeben, dass ein Sensor den Netzverkehr insgesamt sieht

[7] Z. B. gibt es 100Mbps-Switches mit einem Gigabit-Span-Port, der für Überwachungszwecke genutzt werden kann.

und auswerten kann. Bei der Auswahl des Sensors ist darauf zu achten, dass die Sensor-Performance die Überwachung des gebündelt vorliegenden Verkehrs erlaubt. Bei der Auswahl des Switches ist darauf zu achten, dass der Port, an dem die Überwachung erfolgt, so ausgelegt ist, dass er die vollständige Spiegelung des Netzverkehrs der beiden Input-Ports erlaubt.

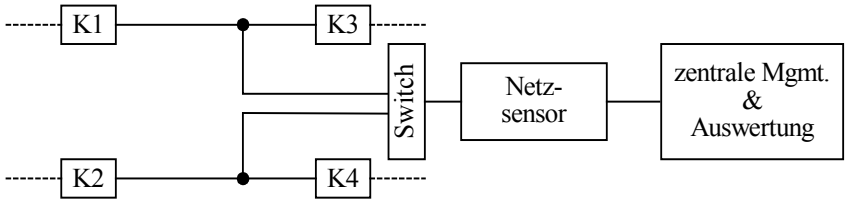

Abbildung 3-3: Zusammenführung des Netzverkehrs über einen Switch

4. **Anpassung der Konfiguration von Switches**: Falls der zu überwachende Netzverkehr über Switches auf die Zielsysteme verteilt wird, besteht ggf. die Möglichkeit, den gesamten Netzverkehr durch die Anpassung der Konfiguration der Switches zentral auf einen zusätzlichen Port eines Switches zu spiegeln. Dies hat den Vorteil, dass vorhandene Komponenten für die Zusammenführung des Verkehrs genutzt werden können. Bei der Auslegung der Switches ist wiederum darauf zu achten, dass die Last am zu überwachenden Port ein Vielfaches der Last einzelner Kommunikationsverbindungen betragen kann.

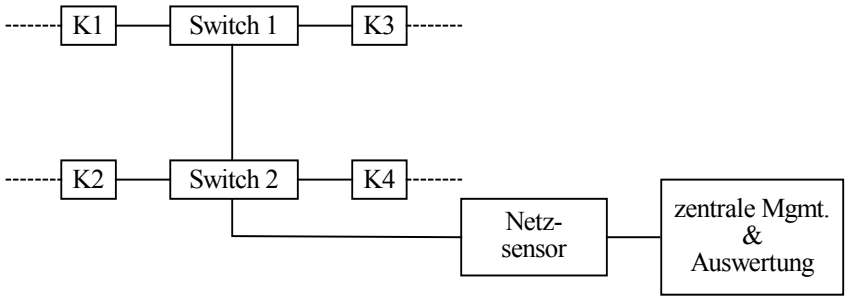

Abbildung 3-4: Abgriff des Netzverkehrs von einem Switch

Multicast

Im Rahmen von Hochverfügbarkeits-Architekturen wird von Multicast gesprochen, wenn mehrere Systeme so konfiguriert werden, dass sie unter derselben Adresse (IP-/MAC-Adresse) reagieren. Eingehender Netzverkehr erreicht sämtliche dieser Systeme parallel und wird von diesen verteilt bearbeitet. Auf der Ebene des Netzverkehrs hat dies zur Folge, dass am Netzinterface eines Systems zwar der eingehende Verkehr vollständig anliegt, der ausgehende Verkehr jedoch nur für den von diesem System bearbeiteten Teil des Verkehrs. Diese Situation ist in Abbildung 3-5 skizziert. Der eingehende Netzverkehr (A, B, C, D) wird über Switches (K1, K2) zu den Komponenten K3 und K4 gesendet. K3 und K4 teilen sich die Bearbeitung des Verkehrs (K3 bearbeitet A und B, K4 bearbeitet C und D). Die Überwachung des Verkehrs an dieser Stelle durch einen Netzsensor ist problematisch, da der Netzsensor nicht weiß, welcher Teil des eingehenden Verkehrs durch das System weiterbearbeitet wird und welcher nicht. Dies betrifft den oben diskutierten Ansatz 1 (Einsatz mehrerer Sensoren). Ein Netzsensor vor K3 würde z. B. C und D als suspekt erkennen, da auf diese (policy-konformen) Pakete von K3 keine Reaktion erfolgt.

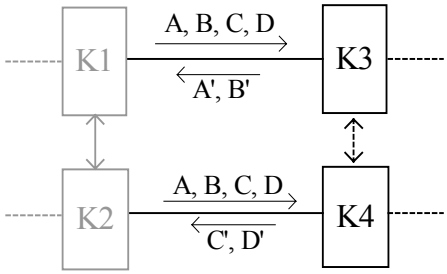

Abbildung 3-5: Skizze der Multicast-Problematik

Auch die direkte Zusammenführung des Verkehrs (oben beschriebene Ansätze 2 und 3) stellt keine Lösung dar, da im zusammengeführten Verkehr sämtliche eingehenden Pakete doppelt auftreten. Ein Filterung der doppelt auftretenden Pakete aus dem eingehenden Verkehr wäre erforderlich.

Ein Lösung der Problematik ist durch die Anpassung der Konfiguration der eingesetzten Switches möglich:

- Im oben beschriebenen Ansatz 3 wäre der Switch so zu konfigurieren, dass der Verkehr von K1 zu K3, der Verkehr von K3 zu K1 und der Verkehr von K4 zu K2 an den Netzsensor weitergeleitet würde. Nicht an den Sensor weiterzuleiten wäre der Verkehr von K2 zu K4, der aufgrund der Multicast-Konfiguration mit dem Verkehr von K1 zu K3 übereinstimmt.
- Entsprechend kann auch im oben beschriebenen Ansatz 4 über eine geeignete Konfiguration der Switches erreicht werden, dass exakt der zu überwachende Verkehr an dem Port zum Netzsensor gespiegelt wird.

4 Einsatzszenarien

In den folgenden Abschnitten werden unterschiedliche Einsatzszenarien von IDS beschrieben:

- Einsatz von IDS zur ergänzenden Absicherung von Netzübergängen und Fernwartungs-Zugängen,
- Einsatz von IDS zur Überwachung von Serversystemen,
- Einsatz von IDS zur Überwachung interner Netze.

Die Szenarien stellen Beispiele dafür dar, wie IDS typischerweise eingesetzt werden können. Beispielarchitekturen für den Einsatz von IDS gemäß der beschriebenen Szenarien sind in Kapitel 5.2 angegeben.

4.1 Ergänzende Absicherung von Netzübergängen

Im Folgenden wird der Einsatz von IDS als ergänzende Maßnahme zur Absicherung von Netzübergängen diskutiert.

Firewall-Systeme haben sich in den letzten Jahren als Standardsicherheitsmaßnahme zur Absicherung von Netzübergängen gegen unautorisierten Zugang aus weniger vertrauenswürdigen Teilnetzen etabliert. Insbesondere die Absicherung von Internet-Zugängen beruht in der Realität derzeit im Wesentlichen auf Firewall-Technologie.

Die Wirksamkeit von solchen Trenneinrichtungen hinsichtlich

- Funktionalität (insbesondere Identifizierung, Authentisierung und Datenflusskontrolle) und
- Widerstandsfähigkeit (durch Einsatz mehrstufiger Architekturen)

ist jedoch grundsätzlich begrenzt. Gründe hierfür sind z. B., dass

- entsprechend komplexe Systeme im Allgemeinen über Schwachstellen verfügen, die für Angriffe ausgenutzt werden können,
- neue Anforderungen im Hinblick auf eBusiness-Applikationen eine stärkere Öffnung von internen und externen Netzübergängen erfordern und damit auch die Risiken unautorisierter Zugänge erhöhen,
- es häufig keine geeigneten Applikations-Gateways (Anwendungsproxies) zur anwendungsbezogenen Datenflusskontrolle gibt.

Diese Randbedingungen führen zu einer Erhöhung des Restrisikos. Anforderungen zur Bereitstellung der entsprechenden Anwendungs-Funktionalität sind jedoch oft von hoher Bedeutung. Typischerweise werden daher Dienste auf Firewall-Systemen freigeschaltet, auch wenn damit ein erhöhtes Restrisiko verbunden ist.

In diesem Szenario können IDS zur Verbesserung der Absicherung von Netzübergängen eingesetzt werden. Ziel ist es, durch einen kombinierten Einsatz von Firewall-Systemen und IDS bestehende Restrisiken auf ein tragbares Maß zu reduzieren.

Die Firewall filtert den Netzverkehr auf Basis entsprechender Regeln, während das IDS insbesondere den Netzverkehr, der die Firewall passiert hat, auf bekannte Angriffsmuster überwacht und auf diese reagiert.

Durch eine entsprechende Konfiguration des IDS ist daneben gleichzeitig die Überwachung der policykonformen Konfiguration und der Funktionsfähigkeit der Firewall möglich.

4.1.1 Ergänzende Überwachung von Fernwartungs-Zugängen

In diesem Abschnitt wird der Einsatz von IDS zur verbesserten Überwachung von Fernwartungs-Zugängen diskutiert. Das Szenario ist ein Spezialfall der ergänzenden Absicherung von Netzübergängen.

Bei der Fernwartung besteht generell die Problematik konträrer Anforderungen an die Kontrolle des Datenflusses: Einerseits sollen die Aktivitäten des Fernwartenden streng kontrolliert werden. Hieraus ergeben sich grundsätzlich hohe Anforderungen an die Datenflusskontrolle. Andererseits erfordert die Wartungstätigkeit typischerweise einen möglichst unbeschränkten und transparenten Zugriff durch den Fernwartenden auf das zu wartende System. Daher können bestehende Anforderungen an die Datenflusskontrolle technisch im Allgemeinen nicht oder nur unzureichend umgesetzt werden. Eine weitere relevante Schwachstelle, die durch ein Firewall-System nur unzureichend unterbunden werden kann, ist das System-Hopping. Über das zu wartende System kann der Fernwartende versuchen, auf weitere Systeme zu gelangen.

Um diesen Schwächen entgegen zu wirken, ist daher vielfach als organisatorische Maßnahme vorgesehen, die Fernwartung lokal durch eigenes Personal begleiten und kontrollieren zu lassen. Zwischen Vorschrift und praktischer Handhabung besteht dabei in der Praxis jedoch häufig eine Lücke.

In dieser Situation kann der Einsatz von IDS helfen, um die Kontrolle der Tätigkeiten des Fernwartenden zu automatisieren. Im Gegensatz zur aktiven Überwachung der Fernwartung durch eigenes Personal sinkt dadurch der Personalaufwand drastisch. Es ist lediglich zu reagieren, falls das IDS eine Abweichung von policy-konformem Verhalten erkennt. Andererseits reduziert sich die Qualität der Überwachung auf die Ereignisse, die durch das IDS erkannt werden können.

Im Vordergrund der Überwachung steht dabei die Funktionalität von Sensoren zur Überwachung der Policy-Konformität. Über spezifische Signaturen kann kontrolliert werden, ob der Fernwartende versucht, Kommandos auszuführen oder Dienste anzusprechen, die er gemäß Policy nicht nutzen darf.

Zu beachten ist, dass die Effektivität von Schutzmaßnahmen, die auf dem zu wartenden Systems selbst ergriffen werden, bei der Fernwartung begrenzt sein kann. Falls der Fernwartende administrative Rechte besitzt, kann er Schutzmaßnahmen, wie z. B. einen hostbasierten Sensor oder einen Virenscanner, ggf deaktivieren. Diese Gefahr ist nicht gegeben, falls die Fernwartung sich auf eine spezifische Applikation (z. B. SAP) bezieht.

Wie bei der ergänzenden Überwachung von Netzübergängen ist auch hier der Einsatz eines IDS als Zusatzmaßnahme zu verstehen. Der Einsatz des IDS sollte durch ein Virenscanning und einen Integritätstest des gewarteten Systems nach Abschluss der Fernwartung flankiert werden. Um ein vom Fernwartenden versuchtes System-Hopping zu erkennen, können des Weiteren hostbasierte Sensoren auf benachbarten Serversystemen eingesetzt werden.

4.2 Überwachung von Serversystemen

Betrachtet wird das Szenario des zeitgleichen Einsatz einer Vielzahl unterschiedlicher Server und Applikationen (z. B. Webserver, Applikationsserver, Datenbank-Server, Firewall), an die hohe Anforderungen hinsichtlich Verfügbarkeit und Integrität gestellt werden. Es entsteht die Problematik, dass einerseits große Mengen von Logdaten durch die Betriebssysteme und Applikationen generiert werden, die eine manuelle Überwachung kaum zulassen, andererseits jedoch die Notwendigkeit gegeben ist, die Systeme und Applikationen möglichst permanent zu kontrollieren.

IDS können dazu dienen, die Überwachung von Servern zu automatisieren und zu zentralisieren. Aufgabe des IDS ist es dabei, Daten und Ereignissen zu überwachender Server und Applikationen zentral zusammenzuführen und auf relevante Ereignisse zu filtern. Im Vergleich zur manuellen Kontrolle liegt der

Vorteil des Einsatzes eines IDS dabei in der permanenten Überwachung mit gleichbleibender Qualität. Durch die zentralisierte Überwachung ergibt sich des Weiteren der Vorteil, dass der Blick nicht auf ein einzelnes System beschränkt bleibt, sondern Ereignisse der überwachten Systeme in Zusammenhang gebracht und gemeinsam ausgewertet werden können. Die Erkennung von Korrelationen in den Ereignissen und Daten unterschiedlicher Systeme ist möglich.

Für die Überwachung der Betriebssysteme und Applikationen stehen dabei Hostsensoren im Vordergrund, die

- anfallende Logdateien von Systemen und/oder Anwendungen auswerten,
- die Integrität spezifischer Daten/Dateien überwachen und/oder
- sonstige Systemparameter (z. B. CPU-Auslastung, verbleibender Speicherplatz, Aktivität von Rechenprozessen) kontrollieren.

Eine vollständige Überwachung erfordert jedoch zudem die Kontrolle des für die Server bestimmten Netzverkehrs. Diese kann entweder durch den zusätzlichen Einsatz von Netzsensoren oder durch den Einsatz von Hybridsensoren erreicht werden, die eine hostbasierte Überwachung des serverspezifischen Netzverkehrs erlauben.

Zur Kommunikation erkannter Angriffe ist es wichtig, entsprechende Reports und Statistiken erzeugen zu können, aus denen z. B. die Verteilung spezifischer Angriffe über definierbare Zeiträume erkannt werden kann. Dies setzt voraus, dass das IDS über skalierbare Filterfunktionen verfügt, die bei der Auswertung der aufgezeichneten IDS-Ereignisse eingesetzt werden können.

4.3 Überwachung interner Netze

In diesem Abschnitt wird der Einsatz von IDS zur Überwachung interner Netze diskutiert.

Firewall-Systeme dienen zur Kontrolle der Kommunikation an Netzübergängen. Sie erlauben jedoch keine Überwachung der Kommunikation in den Netzen selbst. Zielsetzung beim Einsatz von IDS zur Überwachung eines internen Netzes ist der Schutz der Ressourcen in diesem Netz. Als Randbedingung ist dabei der weitverbreitete Einsatz „geswichter“ Netze zu berücksichtigen.

Eine Gefährdung interner IT-Ressourcen kann unter anderem dadurch hervorgerufen werden, dass

- Mitarbeiter (Innentäter)
  - ihnen zugeordnete Rechte missbrauchen,
  - unberechtigt versuchen, Zugriff auf Dienste und Informationen zu erhalten, oder
  - Software oder Dienste - absichtlich oder unbewusst[8] - in unberechtigter Art und Weise nutzen,
- Netzübergänge nicht dokumentiert sind oder unberechtigt genutzt werden (wie z. B. der unberechtigte Einsatz von Modems) oder
- Firewall-Systeme fehlerhaft konfiguriert sind.

Für den Einsatzzweck ist insbesondere die Überwachung relevanter Netzsegmente durch netzbasierte Sensoren relevant. Diese kann durch die Überwachung kritischer Serversysteme durch hostbasierte Sensoren ergänzt werden (in diesem Punkt überschneidet sich das Szenario mit dem Szenario der Überwachung spezifischer Systeme und/oder Anwendungen).

[8] Z. B. nach einem dem Mitarbeiter unbewussten und von ihm unbeabsichtigten Download von Viren beim Surfen im Internet.

Durch netzbasierte Sensoren ist sowohl die Überwachung der Wirksamkeit des Schutzes durch die Firewalls möglich als auch die Überwachung, ob Mitarbeiter sich policy-konform verhalten:

- Erkennung von Angriffen im internen Netzverkehr,
- Erkennung unberechtigter externer Zugriffsversuche auf interne Ressourcen,
- Erkennung unberechtigter interner Zugriffsversuche auf spezifische Adressen, Ports und Dienste.

Durch hostbasierte Sensoren können darüber hinaus kritische Server und Anwendungen in die Überwachung einbezogen werden, wodurch Aktivitäten von Nutzern erkennbar werden, wie z. B.

- unberechtigte Zugriffsversuche auf Daten oder Programme,
- mehrfach fehlgeschlagene Anmeldungsversuche oder Anmeldungen zu ungewöhnlichen Tageszeiten.

Insbesondere bei der zur Überwachung interner Netze bietet der Einsatz von IDS weitreichende Missbrauchsmöglichkeiten hinsichtlich der Verhaltenskontrolle von IT-Nutzern. Daher ist gerade bei diesem Einsatzzweck eine angemessene Berücksichtigung datenschutzrechtlicher Anforderungen und Anforderungen der Arbeitnehmer-Mitbestimmung besonders wichtig.

5 Technische Basisarchitektur

In diesem Kapitel werden Basisarchitekturen für den Einsatz von IDS vorgestellt.

Voraussetzung für den Einsatz von Netzsensoren ist, dass diese den zu überwachenden Netzverkehr sehen. Der Abgriff des Netzverkehrs kann dabei technisch auf unterschiedlichen Arten erfolgen, die in Abschnitt 5.1 erläutert werden.

Im vorhergehenden Kapitel wurden Einsatzszenarien von IDS beschrieben. Zu diesen Einsatzszenarien werden in Abschnitt 5.2 Beispielarchitekturen insbesondere für die Platzierung der Sensoren vorgestellt. Die Platzierung der Managementstation und die resultierenden Kommunikationswege zwischen den IDS-Komponenten werden dediziert in Abschnitt 5.3 untersucht.

5.1 Abgriff des zu überwachenden Netzverkehrs

Die Punkte, an denen der Netzverkehr durch den Sensor abgegriffen wird, können technisch unterschiedlich ausgeprägt sein:

- **Abgriff von einem Hub**

  Ein Hub dient zur Anbindung mehrere Komponenten an dasselbe Netzsegment. Sämtliche am Hub angeschlossene Komponenten „sehen“ den gleichen Netzverkehr. Bei der Anbindung eines Netzsensors an den Hub kann von dem Netzsensor der gesamte Netzverkehr des entsprechenden Netzsegments abgehört und überwacht werden.

- **Abgriff von einem Switch**

  Im Gegensatz zum Hub kann bei einem Switch der Verkehr zwischen den unterschiedlichen Ports des Switches über Regeln gesteuert werden. Dies ermöglicht die Bildung von VLANs. So kann z. B. eine an Port 1 angeschlossene Komponente mit einer an Port 2 angeschlossenen Komponenten kommunizieren, während gleichzeitig eine an Port 3 angeschlossene Komponente mit einer an Port 4 angeschlossenen Komponenten kommuniziert. Dabei ist der Netzverkehr der Verbindungen separiert, d. h. der Verkehr auf der Port 1/3 Verbindung ist auf der Port 3/4 Verbindung nicht sichtbar und umgekehrt.

  Die Anbindung eines Netzsensors an einen Switch hat für die Überwachung des Verkehrs den Vorteil, dass über die Programmierung des Switches eingestellt werden kann, welcher Verkehr zur Überwachung zum Sensor geleitet wird. Handelsübliche Switches bieten daneben auch sog. SPAN Ports (SPAN = Switch Port Analyser) an, über die der Netzverkehr des Switches gespiegelt werden kann. Dabei ist darauf zu achten, dass der Port über eine ausreichende Bandbreite verfügt, um auch bei hoher Last den Verkehr der Switch-Ports vollständig spiegeln zu können(vgl. auch Kapitel 3.6).

- **Abgriff über einen TAP**

  TAPs dienen speziell zum Abgriff von Netzverkehr zu Überwachungszwecken. Sie sind grundsätzlich mit einem Hub (mit 3 Anschlüssen) vergleichbar, weisen jedoch an einem der Anschlüsse eine „Dioden“-Funktion auf: Über den TAP wird der Verkehr auf der Kommunikationsstrecke abgegriffen, es können jedoch keine Datenpakete in die Kommunikation hineingespielt werden. Selbst falls es einem Angreifer gelingt, über den vom Sensor überwachten Datenstrom den Netzsensor zu Fehlfunktionen zu verleiten, ist somit eine aktive Rückkopplung des Sensors auf die überwachte Strecke ausgeschlossen. Diesem Vorteil steht der Nachteil gegenüber, dass aktive Responses des Netzsensors, wie z. B. das Einspielen von Reset-Paketen, auch nicht über den TAP erfolgen können.

5.2 Architekturbeispiele für die Einsatzszenarien

Für die in Kapitel 4 beschriebenen Einsatzszenarien werden in den folgenden Abschnitten Beispielarchitekturen vorgestellt.

5.2.1 Ergänzende Absicherung von Netzübergängen

Die Einsatzarchitektur eines IDS zur ergänzenden Absicherung von Netzübergängen ist in Abbildung 5-1 am Beispiel des vom BSI empfohlenen dreistufigen Netzübergangs zum Internet (siehe [BSI 1-02]) dargestellt. Netzbasierte Sensoren können dabei an unterschiedlichen Stellen eingesetzt werden:

- Netzbasierter Sensor zwischen externem Router und Firewall

  Diese Sensorplatzierung erlaubt die Überwachung des gesamten Internet-Verkehrs des Netzübergangs an einem zentralen Punkt. An dieser Stelle ist jedoch nicht sichtbar, ob erkannte Angriffe nicht durch nachgeschaltete Schutzkomponenten abgewehrt werden. Die Platzierung eignet sich daher zur Aufzeichnung von Kontextinformationen über Angriffe, die weiter innen nicht mehr vorliegen. Das Erkennen von Angriffen auf Ressourcen in der DMZ oder im internen Netz ist jedoch effizienter durch die im Folgenden aufgeführten Platzierungen möglich.

- Netzbasierter Sensor in der DMZ

  Diese Sensorplatzierung erlaubt die gezielte Überwachung des für die DMZ freigeschalteten Netzverkehrs zu Komponenten in der DMZ (z. B. Mail-Server, Webserver oder Proxies). Sowohl Angriffe im Netzverkehr als auch die unberechtigte Nutzung von Kommunikationsdiensten können erkannt werden.

- Netzbasierter Sensor zwischen Firewall und internem Router

  Diese Sensorplatzierung erlaubt die gezielte Überwachung des Kommunikationsverkehrs, der über den Netzübergang ins interne Netz geleitet wird. Da der Verkehr bereits durch vorgeschaltete Komponenten gefiltert ist, sollten an dieser Stelle keine Angriffe mehr auftreten. Sowohl Angriffe im Netzverkehr als auch die unberechtigte Nutzung von Kommunikationsdiensten können erkannt werden.

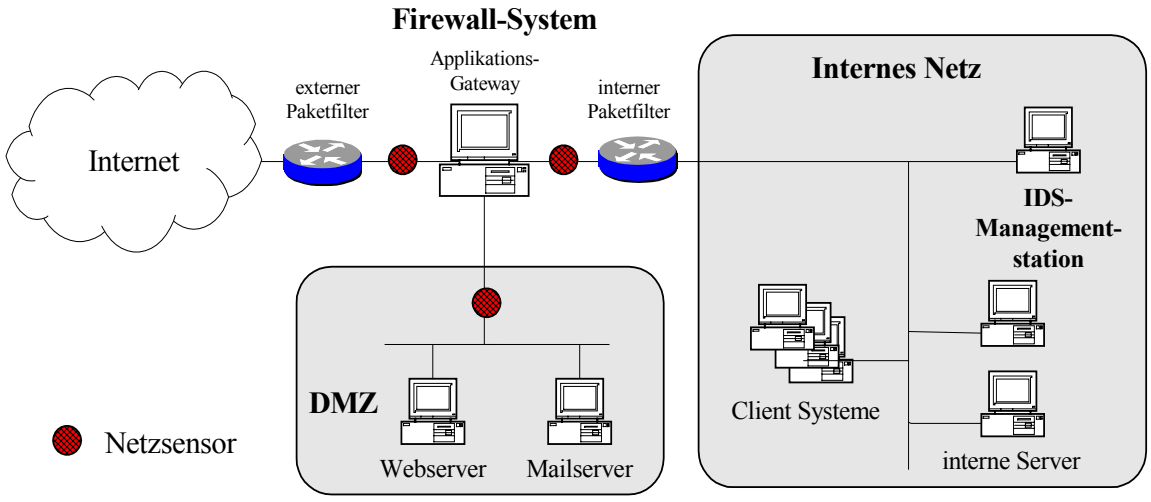

Abbildung 5-1: Einsatz des IDS zur ergänzenden Absicherung von Netzübergängen

5.2.2 Überwachung spezifischer Systeme und/oder Anwendungen

Die Einsatzarchitektur eines IDS zur Überwachung spezifischer Systeme und/oder Anwendungen ist beispielhaft in Abbildung 5-2 dargestellt. Im Beispiel wird von der Überwachung der Firewall, des Webservers in der DMZ sowie interner Server ausgegangen.

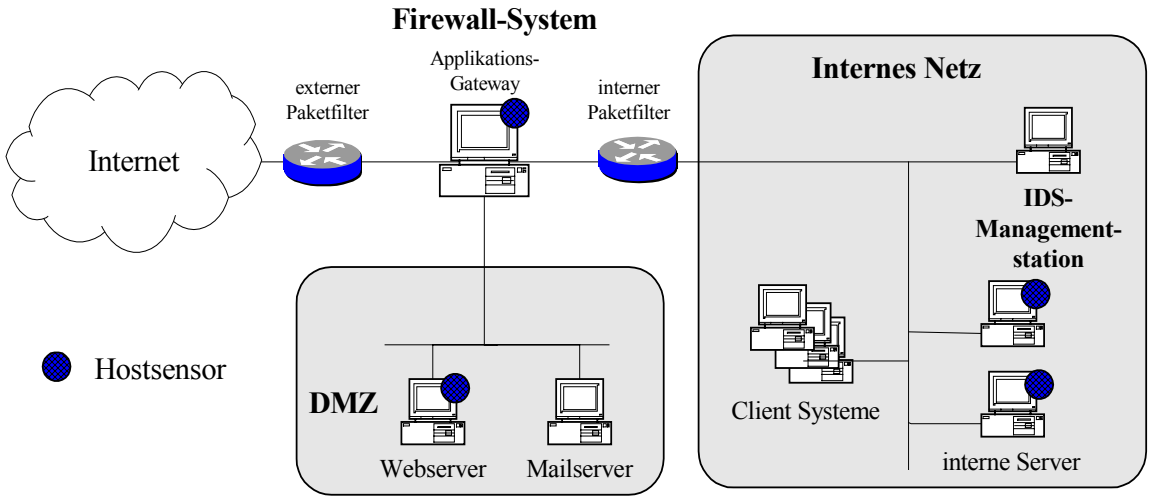

Abbildung 5-2: Einsatz eines IDS zur Überwachung spezifischer Systeme und/oder Anwendungen.

5.2.3 Überwachung interner Netze

Bei der Überwachung interner Netze sind Host- und Netzsensoren kombiniert in verschiedenen Möglichkeiten einsetzbar:

- Netzbasierter Sensoren in Netzsegmenten
- Hostbasierter Sensor auf Servern
- Hostbasierter Sensor auf Clients (z. B. Clients, die sensible Daten enthalten)

In der folgenden Abbildung ist die Einsatzarchitektur eines IDS zum Schutz des internen Netzes beispielhaft dargestellt.

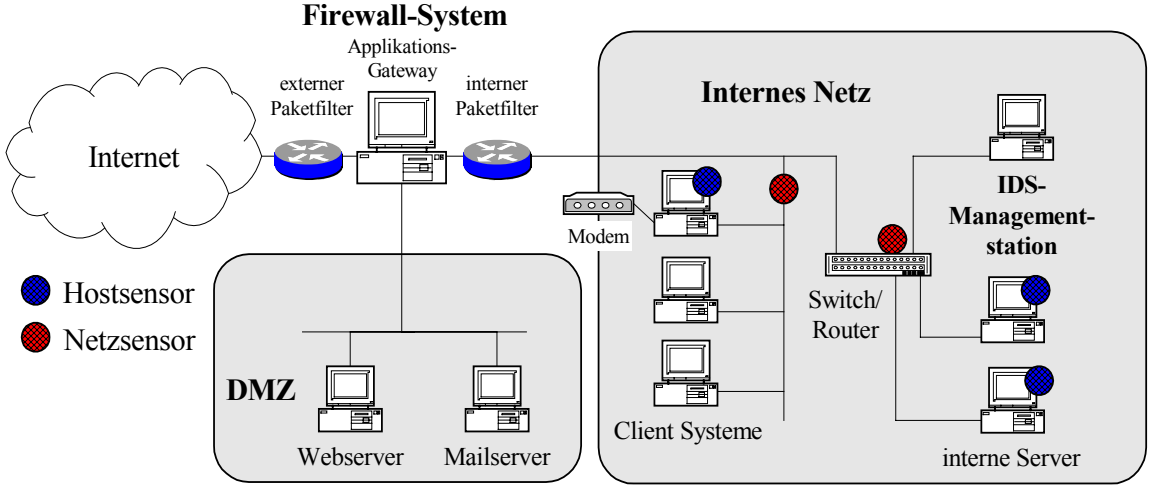

Abbildung 5-3: Einsatz eines IDS zur Überwachung des internen Netzes

Durch hostbasierte Sensoren überwacht werden dabei sowohl interne Server als auch kritische Clients. Für den Client-PC mit Modem-Anbindung ist dabei die Überwachung des Modem-spezifischen Netzverkehrs relevant.

Netzbasierte Sensoren werden zur Überwachung unterschiedlicher interner Teilnetze eingesetzt.

5.3 Kommunikation zwischen IDS-Komponenten

Während im letzten Abschnitt die Platzierung von Sensoren im Vordergrund stand, werden in diesem Abschnitt Möglichkeiten zur Platzierung der Managementstation und zur Kommunikation zwischen den IDS-Komponenten diskutiert sowie anhand von Beispielarchitekturen erläutert.

Falls die Kommunikation der IDS-Komponenten untereinander über die zu überwachenden Produktionsnetze erfolgt, können Angriffe auf Produktionsnetze auch die Funktion des IDS beeinträchtigen. Die zugrunde liegende Architektur ist in Abbildung 5-4 skizziert. IDS-Komponenten können anhand ihres Datenaustausches identifiziert und lokalisiert werden. Auf dieser Basis können nachfolgend IDS-Komponenten direkt angegriffen werden.

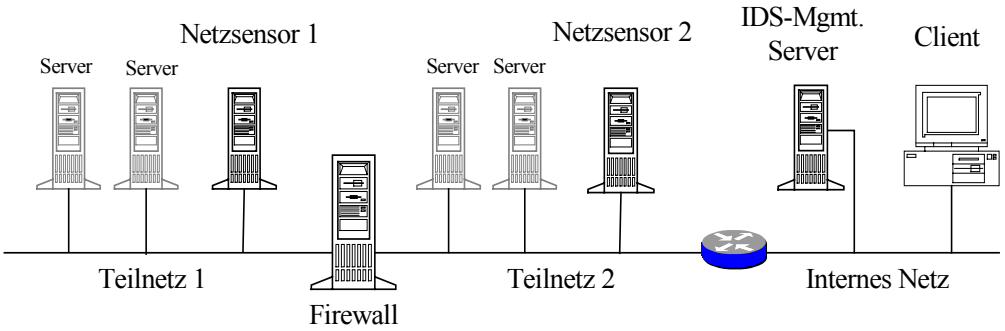

Abbildung 5-4: Nutzung von Produktionsnetzen für die IDS-Kommunikation

Um dies zu unterbinden wird häufig empfohlen, Sensoren und IDS-Managementkomponenten über ein separates Teilnetz miteinander zu verbinden, so dass eine Entkopplung der IDS-Kommunikation von der Kommunikation zu Produktionssystemen stattfindet (vgl. Abbildung 5-5).

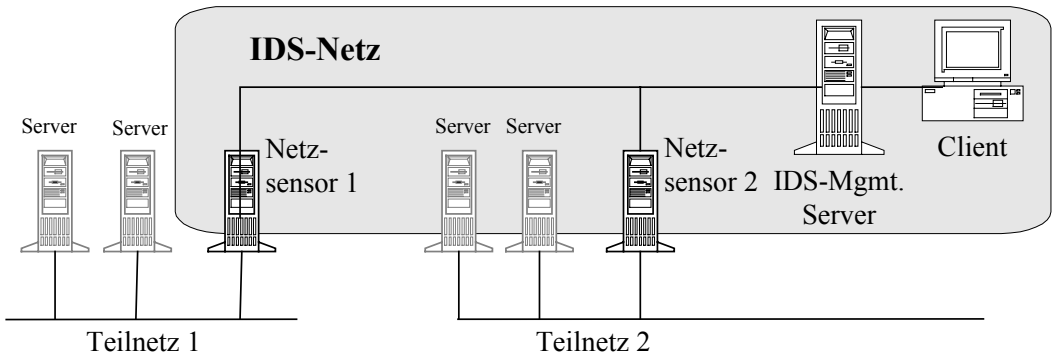

Abbildung 5-5: IDS-Kommunikation über separates IDS-Netz

Hierdurch soll sichergestellt werden, dass keine interaktive Verbindung zwischen Angreifern und IDS-Komponenten möglich ist. Darüber hinaus soll erreicht werden, dass IDS-Komponenten nicht anhand ihrer Kommunikation mit Managementsystemen erkannt oder die Kommunikation durch Denial-of-Service Angriffe (etwa Erhöhung der Netzlast) verzögert wird.

Beim Aufbau eines separaten Teilnetzes müssen jedoch einige Besonderheiten beachtet werden:

- Netzbasierte Sensoren sollten so konfiguriert werden, dass sie in dem Netz, das beobachtet werden soll, nicht sichtbar sind. Dies kann durch den Abgriff des Netzverkehrs über TAPs erfolgen oder durch die Konfiguration der betreffenden Netzinterfaces, so dass sie ohne IP-Adresse arbeiten (stealth mode), jedoch sämtlichen Netzwerkverkehr aufnehmen (promiscious mode).
- Typischerweise werden die betreffenden Netzinterfaces so eingestellt, dass sie ohne IP-Adresse arbeiten (stealth mode, Einsatz von TAPs), jedoch sämtlichen Netzwerkverkehr aufnehmen (promiscious mode).
- Wenn durch das separate IDS-Teilnetz Firewall-Komponenten (Paketfilter, Applikationsproxies) überbrückt werden, kann bei Fehlkonfiguration oder Fehlfunktion eines Sensors die jeweilige Firewall-Komponente überbrückt werden (vgl. Abbildung 5-6). Daher sollte eine gleichwertige Firewall-Komponente auch an entsprechender Stelle ins IDS-Teilnetz eingebracht werden. Beim Einsatz von Netzsensoren lässt sich die Überbrückung des Sensors vom IDS-Netz zum überwachten Teilnetz durch den Abgriff des Netzverkehrs über TAPs verhindern.

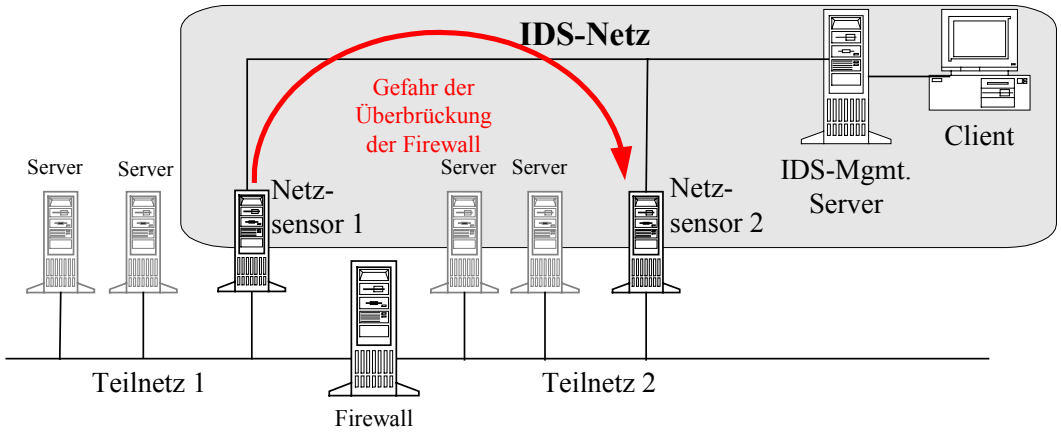

Abbildung 5-6: Überbrückung der Firewall

- Alle Übergänge zwischen IDS-Teilnetz und Produktionsnetz müssen entsprechend dem Schutzbedarf des IDS-Teilnetzes durch Firewalls gesichert werden, um zu verhindern, dass IDS-Managementkomponenten und Sensoren direkt angegriffen werden. Neben der Anbindung von Netz- und Hostsensoren treten Netzübergänge typischerweise an folgenden Stellen auf:
  - An der Kommunikationsschnittstelle zu Mailsystemen, über die eine E-Mail-Alarmierung erfolgen soll.
  - Beim Remote-Zugriff auf die Management- und Auswertungsstation (etwa vom Büro-PC des IDS-Administrators aus).
  - An der Kommunikationsschnittstelle zu Systemmanagementumgebungen, an die z. B. SNMP-Traps gesendet werden.

Um sicherzustellen, dass die Netzsicherheit nicht von der Sicherheit zusätzlicher Komponenten eines separaten IDS-Netzes abhängt, kann das bestehende Firewall-System zur Kontrolle der IDS-Kommunikation genutzt werden. IDS-Managementstation und Sensoren sind dabei über getrennte Netzinterfaces an die Firewall angebunden. Die Architektur ist beispielhaft in der nachstehende Abbildung skizziert.

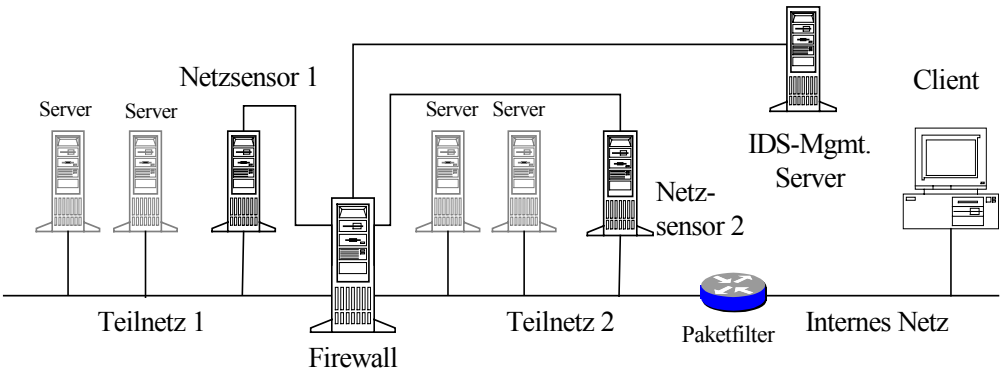

Abbildung 5-7: IDS-Kommunikation über bestehende Firewall

Im Vergleich zur Nutzung eines vollständig separaten IDS-Netzes hat diese Architektur den Vorteil, dass durch Fehlkonfiguration von IDS-Komponenten kein zusätzlicher Übergang zwischen den produktiven Teilnetzen geschaffen werden kann. Die Firewall ist das einzige Bindeglied zwischen den Teilnetzen. Des Weiteren können die o. g. sonstigen erforderlichen Übergänge zwischen Produktionsnetz und IDS-Netz zentral über die Firewall verwaltet werden.

Ob die Einrichtung eines eigenen IDS-Teilnetzes sinnvoll ist, ist im Einzelfall zu prüfen. Prinzipiell ist es sinnvoll, separate IDS-Teilnetze durch das IDS mitüberwachen zu lassen, um auch hier Angriffe zu erkennen.

6 Organisatorische Einbettung von IDS

In diesem Kapitel werden die organisatorische Aspekte beschrieben, die beim Einsatz eines IDS relevant sind.

Für den Betrieb eines IDS ist Personal erforderlich, das gute Kenntnisse sowohl über Angriffe und Systemschwächen als auch über das eingesetzte IDS selbst aufweist. Relevante Aufgaben im Betrieb eines IDS sind

- die Kalibrierung des IDS (siehe Abschnitt 6.1),
- die Auswertung und Verfolgung vom IDS gemeldeter Ereignisse und Alarme (siehe Abschnitt 6.2),
- die Anpassung des IDS bei Veränderung des Einsatzumfeldes (siehe Abschnitt 6.3),
- die regelmäßige Aktualisierung der Signaturdatenbank des IDS und der IDS-Software selbst.

Darüber hinaus sollte die Funktionsfähigkeit der Komponenten des IDS regelmäßig durch geeignete Tests überprüft werden.

Des Weiteren sind beim Betrieb von IDS rechtliche Anforderungen des Datenschutzes und der Arbeitnehmermitbestimmung zu berücksichtigen (siehe Abschnitt).

6.1 Administration und Kalibrierung

Im Rahmen der Kalibrierung erfolgt die Anpassung des IDS an die aktuelle Einsatzumgebung. Es wird eingestellt, welche Ereignisse die einzelnen Sensoren erkennen sollen und wie das IDS beim Erkennen von Ereignissen reagieren soll. Die Kalibrierung umfasst daher sowohl sog. „Sensor-Policies“ als auch die Intrusion-Response-Einstellungen des IDS. Ziel ist dabei, dass die Sensoren genau das erkennen, was sie erkennen sollen.

Um möglichst wenig Fehlalarme auszulösen, ist bei der Kalibrierung insbesondere darauf zu achten, dass „zulässiges Verhalten“ vom IDS als solches erkannt wird. Voraussetzung hierfür ist, dass das zulässige Verhalten der zu überwachenden Netze und Systeme dokumentiert vorliegt.

Der Kalibrierungsprozess der Sensoren besteht im Wesentlichen in der Festlegung, welche Ereignisse vom Sensor unterdrückt werden sollen, welche Ereignisse protokolliert werden sollen und bei welchen Ereignissen alarmiert werden soll. In der Kalibrierungsphase hat die IDS-Administration die Reaktion des IDS auf erkannte Ereignisse festzulegen.

- **Alarmierung:**
  Wenn das Ereignis einen schwerwiegenden Angriff darstellt, der zu einem Schaden führen könnte, ist eine Alarmierung durch das IDS auszulösen. Eine angemessene Konfiguration der Alarmierung ist wichtig, da zu häufige Alarmierungen zum Verlust der Sensibilität des Sicherheitspersonals führen, bei zu oberflächlicher Alarmierung dagegen relevante Angriffe übersehen werden.
- **Unterdrückung**:
  Es ist zu ermitteln, welche Ereignisse vom IDS bei normaler Netzlast gemeldet werden. Unter diesen sind die Ereignisse zu identifizieren, die nachweislich unschädlich und nicht auf Angriffsversuche zurückzuführen sind. Nach Möglichkeit ist das IDS so zu konfigurieren, dass derartige Ereignisse nicht protokolliert werden.
- **Protokollierung**:
  Sämtliche Ereignisse, die weder nachweislich als unschädlich identifiziert wurden noch schwerwiegende Alarme darstellen, sind zu protokollieren.

Bei der Einführung des IDS ist im Allgemeinen nicht für sämtliche IDS-Meldungen direkt entscheidbar, ob die korrespondierenden Ereignisse Schäden hervorrufen könnten oder ob sie tatsächlich völlig unschädlich sind. Die Menge der zu protokollierenden IDS-Meldungen fällt demnach eher groß aus.

Im Verlauf des IDS-Betriebs klärt sich nach und nach, welche konkreten Auswirkungen einzelne Ereignisse auf die zu schützende Infrastruktur haben. Auf dieser Basis kann die Kalibrierung verbessert werden. Ereignisse, die bislang protokolliert wurden, da ihre konkreten Auswirkungen unklar waren, können jetzt

- unterdrückt werden, falls sie sich als unschädlich herausgestellt haben und nicht auf relevante Angriffsversuche zurückzuführen sind,
- eine Alarmierung auslösen, falls infolge des Ereignisses Schäden aufgetreten sind, oder
- weiterhin protokolliert werden, weil kein Anlass zur Alarmierung vorliegt und
  1. das Ereignis sowohl im normalen Netzverkehr vorkommen kann als auch durch Angriffsversuche hervorgerufen werden kann und daher eine Einzelfallbetrachtung erfordert,
  2. die IDS-Meldung zu unscharf ist (d. h. auch bei anderen Ereignissen triggert) und daher eine Einzelfallbetrachtung erfordert,
  3. das Ereignis zwar unschädlich ist, jedoch ergänzende Information beinhaltet (z. B. Kontextinformationen zu Angriffen) und daher nicht unterdrückt werden soll.

Im 2. Fall ist ggf. eine Verbesserung der Kalibrierung durch die Verfeinerung bzw. Konkretisierung der entsprechenden Signaturen möglich.

Neben der laufenden Anpassung der Kalibrierung im IDS-Betrieb, ist eine Kalibrierung insbesondere in folgenden Fällen erforderlich:

1. Nach jeder Aktualisierung des IDS. Z. B. bei Einbringen neuer Signaturen in das IDS ist für diese der Intrusion-Response festzulegen bzw. die Default-Einstellung zu prüfen.
2. Änderungen in der zu schützenden Infrastruktur können dazu führen, dass bislang unschädliche Ereignisse jetzt als schadensverursachend eingestuft werden müssen oder auch umgekehrt. Eine Prüfung und Anpassung der Kalibrierung des IDS an die veränderte Einsatzumgebung ist erforderlich.

Eine vollständige Dokumentation der Kalibrierung ist aufgrund der Vielzahl von möglichen Ereignissen nur schwer zu realisieren und praktisch nicht sinnvoll möglich. Dokumentiert werden sollte, wann und weshalb Änderungen an der Kalibrierung durchgeführt wurden (Änderungshistorie). Die Inhalte der entsprechenden Änderungen sind im Rahmen von Datensicherungen festzuhalten.

6.2 Incident-Handling

IDS können sicherheitsrelevante Ereignisse erkennen und protokollieren, sowie bei deren Eintreten eine Alarmierung auslösen.

Ein sicherheitstechnischer Nutzen beim Einsatz eines IDS entsteht jedoch erst, wenn auf vom IDS gemeldete Ereignisse zeitnah und angemessen reagiert wird. Diese zeitnahe und angemessene Reaktion kann das IDS nur in Ausnahmefällen selbst leisten[9]. Es ist daher erforderlich, sowohl vom IDS protokollierte Ereignisse regelmäßig auszuwerten als auch auf IDS-Alarme zeitnah und angemessen zu reagieren.

Bei der Auswertung von IDS-Ereignissen ist insbesondere zu prüfen, welche Auswirkungen das Ereignis auf die zu schützende Infrastruktur hat.

[9] Die Möglichkeiten von IDS zur automatischen Auslösung von Gegenmaßnahmen sind mit Vorsicht zu betrachten (siehe Kapitel 2.4).

Um eine zeitnahe und angemessene Reaktion auf die IDS-Alarme sicherzustellen sind folgende Punkte festzulegen:

- Es ist ein Verfahren festzulegen, dass sicherstellt, dass IDS-Alarme angenommen und an die für die Reaktion verantwortlichen Stellen weitergeleitet werden. Hierzu sind Verantwortlichkeiten und Zuständigkeiten für die Annahme und Reaktion auf IDS-Alarme festzulegen. Des Weiteren sind Meldewege und ggf. Formvorgaben für Meldungen zu definieren.
- Es ist zu klären, ob Alarme auch außerhalb der gewöhnlichen Arbeitszeiten angenommen werden sollen. Hierfür empfiehlt es sich, eine zentrale Annahmestelle für IDS-Alarme vorzusehen.
- IDS-Alarme sind hinsichtlich der zu erwartenden Schadenswirkung zu priorisieren. Dies erfolgt typischerweise durch Definition unterschiedlicher Alarmlevel, denen die IDS-Alarme zugeordnet werden. Für die unterschiedlichen Prioritäten ist festzulegen, wie dringlich die Reaktion auf die Alarme ist und welche Stellen zu benachrichtigen sind.

Bestehende Prozesse und Vorgaben zur Problembehandlung und zum Notfall-/Krisenmanagement sollten dabei berücksichtigt werden. Ggf. können die IDS-Alarmierungen in diese Prozesse und Pläne in sinnvoller Weise integriert werden.

Das typische Vorgehen bei der Reaktion auf vom IDS gemeldete Ereignisse oder Alarme besteht darin,

- zunächst die genauen Randbedingungen des Angriffs zu klären,
- die Auswirkungen des Angriffs auf die zu schützende Infrastruktur zu ermitteln,
- bei Bedarf Maßnahmen zur Schadensbehebung oder –begrenzung zu ergreifen und
- die Kalibrierung des IDS auf Basis der neuen Erfahrungen ggf. anzupassen.

6.3 Berücksichtigung von Veränderungen der Einsatzumgebung

Die Überwachungsfunktion eines IDS steht in direktem Zusammenhang zum überwachten Einsatzumfeld. Daher ist bei Änderungen des Einsatzumfeldes zu prüfen, welche Auswirkungen sich auf die Überwachungsfunktionen des IDS ergeben.

Relevante Änderungen der Einsatzumgebung sind z. B.

- Änderungen an der Netzinfrastruktur,
- die Einführung neuer Serversysteme oder Applikationen
- die Migration von Applikationen auf andere Plattformen

In solchen Fällen ist zu prüfen,

- ob die Einsatzziele des IDS unter den veränderten Randbedingungen weiterhin erreicht werden können,
- ob sich ggf. Änderungen an der Zielsetzung des IDS ergeben und
- ob zum Erreichen der Ziele ein Einsatz des IDS in veränderter Form erforderlich ist (wie etwa die Anpassung der Kalibrierung oder die Erweiterung des IDS um zusätzliche Sensoren).

6.4 Berücksichtigung rechtlicher Anforderungen

IDS sind ein Instrument, mit dem eine weitgehende Überwachung von Netzen und Systemen möglich ist. Abhängig von der Einsatzweise des IDS können dabei

- Verhaltensmuster von Mitarbeitern bei der Nutzung von Systemen und Applikationen und/oder

- Kommunikationsdaten bei der Erkennung netzbasierter Angriffe

aufgezeichnet werden.

Beim Umgang mit solchen Daten sind die Anforderungen des Datenschutzes und der Arbeitnehmermitbestimmung zu berücksichtigen. Die spezifischen Anforderungen sind im Dokument „Einführung von Intrusion-Detection-Systemen - Rechtliche Aspekte“ beschrieben.

6.5 Outsourcing

In der Regel sind die Konfiguration eines IDS und die Auswertung der IDS-Meldungen sehr zeit- und personalaufwändig. Diese Funktionen werden daher zunehmend an spezialisierte Dienstleister ausgelagert. Gerade für kleinere Unternehmen kann ein Outsourcing kostensparend sein, wenn kein für den Betrieb spezialisiertes Personal verfügbar ist oder wenn IDS-Alarme rund um die Uhr angenommen werden sollen, im Unternehmen jedoch keine permanent besetzte Annahmestelle vorhanden ist.

Ob ein Outsourcing sinnvoll ist und welche Randbedingungen dabei zu beachten sind, hängt davon ab, welche Funktionen ausgelagert werden sollen und ob bereits andere IT-spezifische Funktionen an Dienstleister ausgelagert wurden. Dabei ist zu beachten, dass der Einsatz eines IDS als reaktive Maßnahme zur Verbesserung des Schutzes der IT-Ressourcen in erster Linie der Unterstützung des IT-Betriebs dient. Falls der IT-Betrieb an einen Dienstleister ausgelagert wurde, ist es deshalb grundsätzlich sinnvoll, dass dieser Dienstleister auch das IDS betreibt.

Nachstehend werden Aspekte zum Outsourcing für verschiedene Phasen der IDS-Einführung diskutiert:

Bedarfsfeststellung

Im Rahmen der Bedarfsfeststellung ist es wichtig, objektiv zu beurteilen, ob der Einsatz eines IDS sinnvoll ist oder nicht. Die erforderliche Neutralität ist dabei typischerweise nicht gegeben, wenn die Bedarfsfeststellung von einem Dienstleister durchgeführt wird, für den sich wirtschaftliche Vorteile (z. B. durch Verkauf oder Betrieb eines IDS) ergeben, wenn der Auftraggeber sich für den Einsatz eines IDS entscheidet. Falls die Bedarfsfeststellung an einen Dienstleister ausgelagert wird oder in Zusammenarbeit mit einem Dienstleister erfolgt, ist daher darauf zu achten, dass der Dienstleister die erforderliche Neutralität besitzt.

Konzeption und Integration des IDS

Für die Konzeption und Integration des IDS sind detaillierte Kenntnisse über die zu überwachende IT-Infrastruktur notwendig. Sie erfordern daher in jedem Fall eine enge Zusammenarbeit mit dem Betreiber der IT. Eine Zusammenarbeit mit Dienstleistern erscheint unkritisch, falls beteiligte Dienstleister zur Wahrung der Vertraulichkeit interner Informationen verpflichtet werden, die ihnen im Rahmen der Zusammenarbeit bekannt werden.

Betrieb des IDS

Bei der Auslagerung des IDS-Betriebs ist zwischen den unterschiedlichen Funktionen zu unterscheiden, die ausgelagert werden können. Hierzu werden im Folgenden Funktionen zur Annahme von Alarmen, zur IDS-Administration und zur Reaktion auf IDS-Meldungen getrennt betrachtet.

- **Annahme von IDS-Alarmen (IDS-Monitoring)**

  Ein Outsourcing der Annahme von Alarmen ist insbesondere dann vorteilhaft, falls IDS-Alarme rund um die Uhr angenommen werden sollen, im Unternehmen jedoch keine permanent besetzte Annahmestelle vorhanden ist.

Im Vergleich zur Auslagerung von Funktionen zur IDS-Administration oder zur Reaktion auf IDS-Alarme ist die Auslagerung der Annahme von IDS-Alarmen weniger sicherheitskritisch. Jedoch sollte mindestens sichergestellt werden, dass der Dienstleister keinen administrativen Zugang zum IDS und zur überwachten IT-Infrastruktur erhält, Leserechte nur für die zur Beurteilung der IDS-Alarme notwendigen Daten vergeben werden und er zur Wahrung der Vertraulichkeit der Daten verpflichtet wird, die ihm im Rahmen seiner Tätigkeit bekannt werden.

- **IDS-Administration**

  Mit dem Outsourcing der IDS-Administration erhält der Dienstleister weitgehenden Einblick in Systeme und Daten des Auftraggebers. Über Netzsensoren hat der Dienstleister grundsätzlich Zugriff auf den gesamten Netzverkehr an der überwachten Position. Zumindest bei Netzsensoren kann jedoch ein aktiver Eingriff des Dienstleisters in das Netz verhindert werden, indem der Netzverkehr über TAPs abgegriffen wird. Über Hostsensoren erhält der Dienstleister nicht nur Einblick in Systeme und Applikationen des Auftraggebers, er kann in diese auch administrativ eingreifen, da die Administration von Hostsensoren typischerweise administrative Rechte auf dem überwachten System erfordert.

  Aus den aufgeführten Gründen ist ein Outsourcing der IDS-Administration mit zahlreichen Risiken verbunden. Falls ein Outsourcing angestrebt wird, wird daher dringend empfohlen,

  - einen geeigneten Dienstleister sorgfältig auszuwählen,
  - vom Dienstleister einzuhaltende Sicherheitsmaßnahmen abzustimmen und vertraglich zu vereinbaren (Security Service Level Agreements) sowie
  - die Einhaltung der Sicherheitsmaßnahmen durch den Dienstleister regelmäßig zu kontrollieren.

- **Reaktion auf IDS-Meldungen (IDS-Incident-Response)**

  Die angemessene Reaktion auf IDS-Alarme umfasst die Prüfung der Auswirkungen des Angriffs sowie ggf. die Durchführung bzw. Einleitung von Sofortmaßnahmen zur Schadensbegrenzung oder -behebung. Bereits die Prüfung der Auswirkungen erfordert im Allgemeinen einen über den IDS-Einsatz hinausgehenden Eingriff in die zu schützende IT-Infrastruktur, z. B. um zu ermitteln, welche spezifischen Auswirkungen der Angriff auf kritische Serversysteme hatte. Aus diesem Grund kann eine angemessene Reaktion auf IDS-Alarme in sinnvoller Weise nur durch Stellen erfolgen, die auch für den Betrieb der überwachten Systeme, Applikationen und Netze zuständig sind.

7 Anhang

7.1 Glossar und Abkürzungen

DMZ	Demilitarisierte Zone
DoS	Denial of Service
hostbasierter Sensor (Hostsensor)	Sensor eines IDS, der auf dem zu überwachenden Host betrieben wird und dort das Betriebssystem, betriebene Anwendungen, die Integrität spezifischer Dateien und/oder den hostspezifischen Netzverkehr überwacht.
Hybridsensor	Hostbasierter Sensor, der neben dem System auch den serverspezifischen Netzverkehr überwacht.
ICMP	Internet Control Message Protocol
IDS	Intrusion-Detection-System
IDS-Incident-Response	Maßnahmen zur Verfolgung von IDS-Alarmen.
IETF	Internet Engineering Task Force
Incident-Handling	Das Incident-Handling umfasst sämtliche Maßnahmen zur Erkennung und Verfolgung von Sicherheitsvorfällen.
Intrusion-Response	Reaktion des IDS auf erkannte Intrusions (z. B. Protokollierung, Alarmierung).
aktive Reaktion	Als aktive Reaktion wird das automatische Einleiten von Gegenmaßnahmen durch das IDS bezeichnet, wie z. B. die Unterbrechung von Kommunikationsverbindungen oder die temporäre Rekonfiguration einer Firewall.
IT	Informationstechnik
netzbasierter Sensor (Netzsensor)	Sensor eines IDS, der auf einem separaten Rechner betrieben wird und den Netzverkehr an einer bestimmten Stelle im Netz überwacht.
RFC	Request for Comment, IETF-Standards
VLAN	Virtual Local Area Network, über Switches separierte LAN-Teilnetze.
VNC	Virtual Network Computing, Unix-Werkzeug für den Remote-Zugriff auf Rechner.

7.2 Referenzen

[BSI 1-02] „Sicherheit im Internet“ BSI Kurzinformationen zu aktuellen Themen der IT-Sicherheit, Stand Januar 2002, abrufbar unter www.bsi.de

Einführende Literatur zu IDS:

[N3177] ISO/IEC JTC 1/SC27 N3177: Final Text for ISO/IEC TR15947, Information technology – Security techniques – IT intrusion detection framework

R. Bace, P. Mell: NIST Special Publication on Intrusion Detection Systems

Bücher zum Thema Intrusion-Detection:

Stephen Northcutt, Network Intrusion Detection, 2nd Edition (New Riders 2000)

Paul E. Proctor: The Practical Intrusion Detection Handbook (Prentice Hall 2001)

Ausführlicher Vergleichstest unterschiedlicher marktverfügbarer IDS:

NSS IDS Group Test, www.nss.co.uk

CVE Nummerierung von Angriffen und Schwachstellen:

Common vulnerability enumeration, cve.mitre.org