

## 2 IT-Sicherheit und Intrusion Detection

Eine der wichtigsten Entwicklungstendenzen der letzten Jahre ist der rasche Vormarsch moderner Kommunikations- und Informationstechnologien in vielen gesellschaftlichen Bereichen. Insbesondere mit dem rasanten Wachstum des Internets findet eine zunehmende Verlagerung wirtschaftlicher und privater Werte auf leistungsfähige informationstechnische Systeme statt. Die somit immer stärker werdende Abhängigkeit vieler gesellschaftlicher Prozesse von IT-Systemen sowie deren zunehmende technologische Komplexität fördern jedoch auch ein stetig steigendes Bedrohungspotential, das diese Systeme gefährdet. Gleichzeitig wächst die Attraktivität der Systeme für gezielte Missbräuche. Dadurch gewinnen Aspekte der IT-Sicherheit<sup>1</sup> immer mehr an Bedeutung. Während in der Praxis bisher hauptsächlich präventive IT-Sicherheitsmechanismen eingesetzt wurden, zeigen die Entwicklungen, dass Sicherheitsziele nicht allein durch Prävention erreicht werden können. Vielmehr müssen präventive Verfahren um reaktive Mechanismen ergänzt werden. Voraussetzung jedes reaktiven Verfahrens ist die Erkennung von Sicherheitsvorfällen.

In diesem Kapitel führen wir grundlegende Begriffe der IT-Sicherheit ein und geben einen Überblick über existierende Sicherheitsmechanismen. Die Rolle der im Weiteren betrachteten Erkennungsmechanismen wird diskutiert und ihre Notwendigkeit motiviert.

### 2.1 IT-Sicherheit

Aufgabe der IT-Sicherheit ist der Schutz von informationstechnischen Werten und Gütern. Um den Begriff der IT-Sicherheit fassen zu können, wird typischerweise betrachtet, wie informationstechnische Güter kom-

---

<sup>1</sup> Im Englischsprachigen Raum werden zur Unterscheidung von intentionalen und nichtintentionalen Beeinträchtigungen von Systemen überwiegend die Begriffe Security und Safety gebraucht (vgl. [Die04]), die im Deutschen mit demselben Wort, nämlich Sicherheit, übersetzt werden. Wir betrachten Security-Aspekte von Systemen und der Begriff IT-Sicherheit wird ausschließlich in dieser Bedeutung gebraucht.

promittiert werden können bzw. welche Schutzziele verfolgt werden. Im Allgemein werden die folgenden vier Schutzziele unterschieden (vgl. [Wo+00, Eck02]):

- *Vertraulichkeit* - Schutz vor unautorisierter Kenntnisnahme von Informationen.
- *Integrität* - Schutz vor unautorisierter unbemerkter Modifikation von Informationen.
- *Verfügbarkeit* - Schutz vor unautorisierter Vorenthaltung von Informationen oder Ressourcen.
- *Zurechenbarkeit* - Verursacher von Aktionen und Ereignissen sind ermittelbar.

Für spezifische Dienste existieren verschiedene Konkretisierungen dieser Schutzziele. Beispielsweise werden Vertraulichkeitsziele bei Kommunikationsdiensten ausgehend von den zu schützenden Gegenständen (Kommunikationsinhalte vs. Kommunikationsumstände) in Vertraulichkeit und Verdecktheit (Kommunikationsinhalte) sowie Anonymität und Unbeobachtbarkeit (Kommunikationsumstände) unterschieden (vgl. [Wo+00]). Ziel der IT-Sicherheit ist die Erreichung von Schutzzielen trotz der Präsenz intelligenter Angreifer.

*Bedrohungen*, wie z. B. der Verlust der Vertraulichkeit, beschreiben Situationen oder Ereignisse, die die Sicherheit eines Systems potentiell beeinträchtigen. Unter *Verwundbarkeiten* von IT-Systemen werden Schwächen der Systeme verstanden, die ausgenutzt werden können, um IT-Sicherheitsverletzungen durchzuführen. Bedrohungen sind das Ergebnis der Ausnutzung einer oder mehrerer Verwundbarkeiten [Ba00]. Anleitungen, Prozeduren bzw. Programme zur gezielten Ausnutzung von Verwundbarkeiten werden als *Exploits* bezeichnet.

Die Kontrolle, Steuerung und Autorisierung von Zugriffen auf informationstechnische Ressourcen setzt die Existenz einer *Sicherheitspolitik* voraus, die eine Menge von Regeln enthält, die festlegen was erlaubt und was verboten ist. Unter (*IT*-)*Sicherheitsverletzungen*, *Angriffen*, *Attacken* bzw. *Einbrüchen* (*Intrusions*) werden alle Aktionen oder Ereignisse verstanden, die den Regeln der Sicherheitspolitik zuwiderlaufen. Diese vier Begriffe werden in diesem Buch synonym verwendet.

## 2.2 Sicherheitsmechanismen

Zur Durchsetzung der Schutzziele werden IT-Systeme mit Sicherheits- bzw. Schutzmechanismen versehen. Eine grobe Unterteilung der Sicherheitsmechanismen unterscheidet zwischen

- präventiven und
- reaktiven Verfahren.

*Präventive* Mechanismen realisieren Maßnahmen, die eine Beeinträchtigung von informationstechnischen Ressourcen verhindern. Verschiedene präventive Verfahren zur Durchsetzung der Schutzziele sind in Tabelle 2-1 dargestellt. Präventive Mechanismen zur Gewährleistung der Vertraulichkeit von Informationen sind z. B. Verschlüsselungsverfahren, Zugriffskontrollverfahren oder Zugangskontrollen wie Firewalls (vgl. [Eck02, Sta03]). Angemerkt sei, dass Verfahren zur Prüfung der Integrität von Informationen, z. B. Digitale Signaturen, entsprechend dem verbreiteten Integritätsbegriff (s. o.) präventive Verfahren sind. Ihr Ziel ist es, zu *verhindern*, dass Informationen *unbemerkt* unautorisiert modifiziert werden.

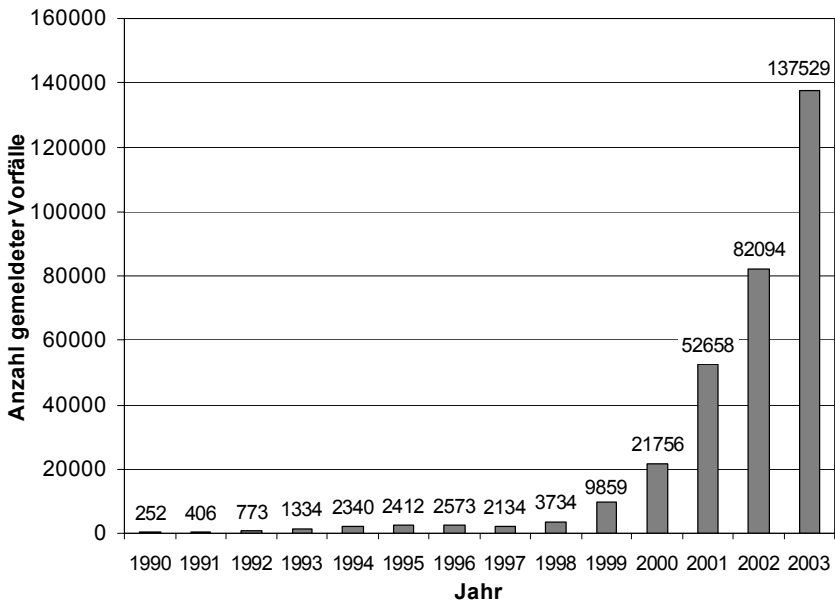
**Tabelle 2-1.** Beispiele für präventive Sicherheitsmechanismen

Schutzziele	Präventive Mechanismen
Vertraulichkeit	Verschlüsselungsverfahren, Zugriffskontrollverfahren, Zugangskontrollen (Firewalls)
Integrität	Zugriffs- und Zugangskontrollverfahren, Digitale Signaturen
Verfügbarkeit	Zugriffs- und Zugangskontrollen, Redundante Auslegung von Ressourcen
Zurechenbarkeit	Digitale Signaturen, Protokollierung sicherheitsrelevanter Aktivitäten

Zum Schutz von IT-Systemen wurden bisher hauptsächlich präventive Verfahren verwendet. Der rapide Zuwachs an Sicherheitsvorfällen macht jedoch deutlich, dass durch präventive Sicherheitsmechanismen allein nur ein gewisses Maß an Schutz geboten werden kann. Trotz verstärkter Anwendung dieser Verfahren war in den letzten Jahren ein jährlicher Anstieg der beim US-amerikanischen CERT/CC (Computer Emergency Response Team / Coordination Center) gemeldeten Vorfälle um mehr als 50% zu beobachten (vgl. Abb. 2-1, [CE05])<sup>1</sup>. Präventive Mechanismen können

<sup>1</sup> Das CERT/CC bemerkt zu diesen Statistiken: „Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore,

keinen Schutz vor missbräuchlichen Aktionen von autorisierten Nutzern, so genannten Insidern (vgl. [So99]), bieten oder durch Verwundbarkeiten aufgrund von fehlerhaften Implementierungen oder Konfigurationen in Systemen umgangen werden (vgl. [Bü01]). Daher sind präventive Mechanismen um reaktive Verfahren zu ergänzen.



**Abb. 2-1.** Entwicklung beim CERT/CC gemeldeter Sicherheitsvorfälle

Ziel *reaktiver* Maßnahmen ist die Begrenzung und Beseitigung von verursachten Schäden sowie die Identifikation verantwortlicher Akteure. Sie sind Voraussetzung für eine Bestrafung von Verantwortlichen oder der Geltendmachung von Schadensersatzansprüchen. Unter Umständen werden bei Ihrer Umsetzung Abschreckungseffekte erreicht, die zusätzlich präventiv wirken [So99, Go99]. Voraussetzung für reaktive Maßnahmen ist eine zuverlässige Erkennung von Sicherheitsverletzungen. Zur automatischen Erkennung von Sicherheitsverletzungen werden *Intrusion-Detection-Systeme (IDS)* [Ba00, Mc01] verwendet. Um die Möglichkeiten der Systeme zur automatischen Reaktion auf erkannte Attacken zu unterstreichen

---

as of 2004, we will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics,...“ [CE05].

chen, wird auch von *Intrusion-Detection-and-Response-Systemen (IDRS)* gesprochen<sup>1</sup>.

## 2.3 Intrusion-Detection-Systeme

Ziel des Einsatzes von Intrusion-Detection-Systemen ist eine möglichst frühzeitige Erkennung von Angriffen, um den Schaden zu minimieren und Angreifer identifizieren zu können. Darüber hinaus erlauben IDS das Sammeln von Informationen über neue Angriffstechniken, die zur Verbesserungen präventiver Maßnahmen genutzt werden können. Dazu analysieren IDS Daten über Abläufe und Zustände von IT-Systemen. Im Folgenden wird der allgemeine Aufbau von IDS beschrieben.

Die *Defense Advanced Research Projects Agency (DARPA)* initiierte ein Projekt, in dem die Kooperation von und Kommunikation zwischen verschiedenen IDS bzw. IDRS ermöglicht werden sollte [Tu99]. Dadurch sollte auch eine Wiederverwendung von IDS-Komponenten erreicht werden. Ergebnis der Standardisierungsbemühungen ist das *Common Intrusion Detection Framework (CIDF)* [Ka+98], das u. a. mögliche Architekturen von IDS beschreibt. Das CIDF sieht vier Arten von IDS-Komponenten vor (vgl. Abb. 2-2):

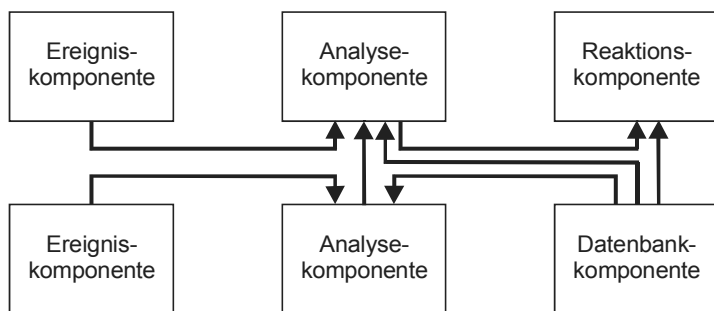
- *Ereigniskomponenten* stellen Informationen über das zu schützende System bereit. Systemfunktionen zur Protokollierung sicherheitsrelevanter Aktivitäten sind Beispiele für Ereigniskomponenten.
- *Analysekomponenten* realisieren die eigentliche Erkennung von Angriffen und analysieren dazu die von den Ereigniskomponenten protokollierten Informationen.
- *Datenbankkomponenten* speichern weitere zur Analyse erforderliche Informationen sowie Zwischenergebnisse.
- *Reaktionskomponenten* führen auf Veranlassung durch andere Komponenten Gegenmaßnahmen durch.

Abb. 2-2 veranschaulicht exemplarisch eine mögliche Anordnung verschiedener Komponenten sowie den Informationsaustausch zwischen ihnen.

---

<sup>1</sup> In letzter Zeit sind viele kommerzielle Anbieter dazu übergegangen ihre IDS- bzw. IDRS-Produkte als *Intrusion-Prevention-Systeme (IPS)* zu vermarkten. In den meisten Fällen handelt es sich dabei um *reaktive* IDRS. Vereinzelt werden auch *präventive* Zugangs- bzw. Zugriffskontrollsysteme (z.B. Firewalls) mit diesem Schlagwort beworben. Wir verwenden diesen irreführenden Begriff nicht.

Inspiziert durch die CIDF-Aktivität wurden zwischenzeitlich verschiedene Standardisierungsbemühungen der *Intrusion Detection Working Group (IDWG)* der *Internet Engineering Task Force (IETF)* initiiert [Tu99, Be01], deren Ziel es ist, Formate und Protokolle für den Informationsaustausch zu entwickeln. Nachfolgend werden die Funktionen der verschiedenen CIDF-Komponenten sowie verwendete Verfahren diskutiert.



**Abb. 2-2.** Informationsaustausch verschiedener CIDF-Komponenten

### 2.3.1 Ereigniskomponenten und Audit

Voraussetzung für eine automatische Erkennung von Sicherheitsverletzungen ist die Aufzeichnung von Informationen über sicherheitsrelevante Abläufe oder Zustände des zu schützenden IT-Systems. Im Zusammenhang mit diesen Verfahren wird der Begriff *Audit* mit verschiedenen Bedeutungen verwendet. Verschiedene Autorengruppen [Pri97, So99, Bi03] fassen unter diesem Begriff Verfahren

- zur Protokollierung,
- zur Analyse oder
- zur Protokollierung und Analyse

zusammen. Wir schließen uns der ersten Gruppe an und verwenden den Begriff *Audit* in diesem Buch allein für Verfahren zur Protokollierung von sicherheitsrelevanten Abläufen oder Zuständen von IT-Systemen.

Entscheidend für die Möglichkeiten und die Qualität der Erkennung von Sicherheitsverletzungen ist der Informationsgehalt der erhobenen Audit-Daten. Andererseits muss die Menge gesammelter Informationen handhabbar bleiben. Das Problem, genügend aber nicht zuviel Audit-Daten zu sammeln, wird etwas humorvoll beschrieben durch „You either die of thirst, or you are allowed a drink from a fire hose ...“ [Ax98]. Aus diesem

Grund verfügen Audit-Funktionen von IT-Systemen typischerweise über umfangreiche Konfigurationsmöglichkeiten, die es dem Systemadministrator ermöglichen die Protokollierung an die Erfordernisse des Einsatzumgebung des Systems anzupassen. Prinzipiell können zwei Arten von Audit unterschieden werden: zustandsbasiertes Audit und transitions- bzw. aktionsbasiertes Audit (vgl. [Bi03]).

Beim *zustandsbasierten Audit* werden, typischerweise regelmäßig, Informationen über den Zustand bzw. über Teilzustände des IT-Systems, z. B. die Auslastung bestimmter Ressourcen, aufgezeichnet. Durch eine spätere Analyse dieser Informationen werden die Zustände des IT-Systems als sicherheitskonform oder sicherheitsverletzend klassifiziert. Problematisch bei diesem Ansatz ist, dass eine periodische vollständige Aufzeichnung des Zustandes eines IT-Systems zu großen schwer handhabbaren Datenmengen führt. Aus diesem Grund werden in der Praxis nur Informationen über kritische oder signifikante Teilzustände aufgezeichnet. Ein Beispiel für diese Vorgehensweise ist die regelmäßige Protokollierung der Auslastung eines Netzwerkes, eines Prozessors oder eines Pufferspeichers.

Ein *transitions- bzw. aktionsbasierter Audit-Mechanismus* zeichnet Informationen über sicherheitsrelevante Aktivitäten im IT-System auf. Typischerweise umfassen diese Informationen

- wer,
- wann,
- welche Aktion,
- wie (erfolgreich bzw. erfolglos)

ausgeführt hat sowie aktionsspezifische Zusatzinformationen wie z.B. Parameter (vgl. [So99]). Durch Analyse dieser Audit-Daten wird später entschieden, ob durch die protokollierten Aktionen ein sicherheitskritischer Systemzustand erreicht wurde. Beispiele für (hauptsächlich) transitionsbasiertes Audit sind die Audit-Funktionen der Betriebssysteme Solaris [Sun02] und Windows NT / 2000 / XP [Ju+98] aber auch Netzmonitore wie TCPDUMP [Ja+89]. Problematisch am transitionsbasierten Audit ist, dass auf der Grundlage der Daten nicht in jedem Fall zuverlässig entschieden werden kann, ob ein sicherheitskritischer Zustand erreicht wurde. Dies gilt insbesondere dann, wenn sich das IT-System bereits zu Beginn der Protokollierung in einem kritischen Zustand befindet [Bi03]. Aus diesem Grund wird häufig eine Kombination aus zustands- und transitionsbasiertem Audit realisiert.

Die protokollierten Informationen werden typischerweise als *Audit-Records* in einer zeitlich geordneten Sequenz organisiert, die als *Audit-Trail*

bezeichnet wird. Unsere weiteren Betrachtungen gehen von folgenden selten explizit genannten jedoch üblichen Annahmen hinsichtlich der Audit-Funktion des IT-Systems aus:

- Zu Beginn des transitionsbasierten Audits befand sich das zu schützende System in einem zur Sicherheitspolitik konformen Zustand.
- Die Audit-Trail enthält durch zustands- und transitionsbasiertes Audit generierte Audit-Records.
- Die Audit-Records in der Audit-Trail sind zeitlich geordnet.
- Die Integrität der Audit-Daten ist sichergestellt.

### 2.3.2 Analyse- und Datenbankkomponenten

Analysekomponenten führen die eigentliche Erkennung von Sicherheitsverletzungen durch. Je nach verwendeter Analysetechnik werden dazu zusätzliche Informationen verwendet, die in den Datenbankkomponenten organisiert werden. Mittels entsprechender Verfahren werden die in den Audit-Daten dokumentierten Beobachtungen analysiert, um den Zustand des überwachten Systems als sicherheitskonform oder sicherheitsverletzend zu klassifizieren. Zur Diskussion und Bewertung dieser binären Klassifikationsverfahren werden typischerweise vier Werte herangezogen:

- *Wahr-Positive (True Positives)*: Beobachtungen, die korrekt als positiv (sicherheitsverletzend) klassifiziert wurden.
- *Wahr-Negative (True Negatives)*: Beobachtungen, die korrekt als negativ (sicherheitskonform) klassifiziert wurden.
- *Falsch-Positive (False Positives)*: Beobachtungen, die inkorrekt als positiv (sicherheitsverletzend) klassifiziert wurden.
- *Falsch-Negative (False Negatives)*: Beobachtungen, die inkorrekt als negativ (sicherheitskonform) klassifiziert wurden.

Insbesondere werden die Häufigkeiten bzw. Raten inkorrekt klassifizierungsergebnisse betrachtet. Falsch-Positive von IDS beschreiben Fehlalarme, also sicherheitskonforme Zustände, die als Sicherheitsverletzungen angezeigt wurden. Falsch-Negative stellen Sicherheitsverletzungen dar, die nicht als solche erkannt wurden.

Es existieren zwei allgemeine Analysetechniken zur Einbruchserkennung, die sich sowohl in der Vorgehensweise als auch durch die verwendeten Referenzinformationen unterscheiden:

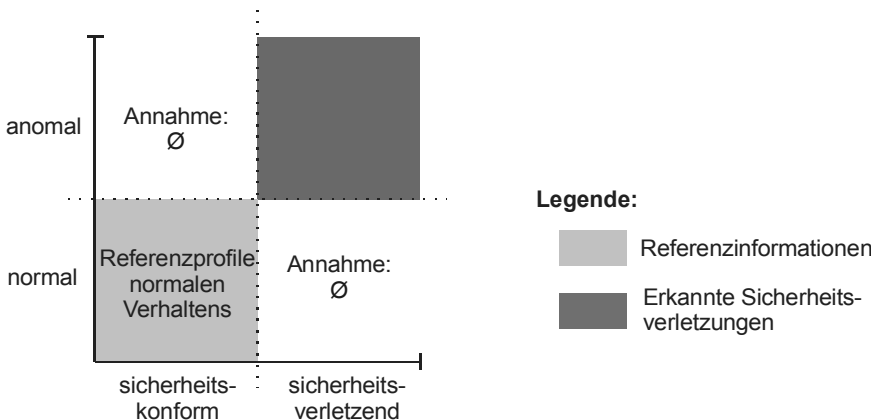


- Anomalieerkennung und
- Missbrauchserkennung bzw. Signaturanalyse.

### Anomalieerkennung

Der *Anomalieerkennung* (*Anomaly Detection*) liegt die Annahme zugrunde, dass Abweichungen von Normen, so genannte Anomalien, auf Sicherheitsverletzungen hindeuten [Ba00]. Neben der Konformität zur Sicherheitspolitik wird hier eine zweite Klassifikationsebene eingeführt (vgl. Abb. 2-3), die zwischen normalen und anomalen Abläufen und Zuständen unterscheidet. Darüber hinaus wird unterstellt, dass weder normale sicherheitsverletzende noch anomale sicherheitskonforme Aktivitäten existieren. Dementsprechend werden durch Audit-Daten dokumentierte Aktionen und Zustände als normal bzw. anomal klassifiziert und auf sicherheitskonforme respektive sicherheitsverletzende Aktivitäten geschlossen.

Bei der Anomalieerkennung wird angenommen, dass ein normales Verhalten existiert und geeignet mess- oder beschreibbar ist. Diese Analysetechnik verwendet Referenzinformationen über normales Verhalten und vergleicht diese mit den in Audit-Daten dokumentierten Ereignissen. Abweichungen werden als Sicherheitsverletzungen angezeigt. Abb. 2-3 veranschaulicht die Grundidee der Anomalieerkennung anhand der zugrunde liegenden Klassifikationsebenen.



**Abb. 2-3.** Klassifikationsebenen der lern- bzw. messbasierten Anomalieerkennung (nach [So99])

Zur Erzeugung der erforderlichen Referenzinformationen, die normales Verhalten repräsentieren, werden zwei grundlegende Ansätze unterschieden:

- das Erlernen bzw. Messen normalen Verhaltens und
- die Spezifikation normalen Verhaltens.

Zur Umsetzung des ersten Ansatzes ist eine Lernphase des Systems erforderlich, in der Referenzprofile normalen Verhaltens erhoben werden. Da sich insbesondere nutzerbezogenes Verhalten über die Zeit verändern kann, wiederholen verschiedene IDS, die diesen Ansatz realisieren, regelmäßig oder kontinuierlich diese Phase. Problematisch hierbei ist, dass die Sicherheitskonformität des gemessenen Verhaltens während der Lernphase durch andere Mechanismen sicherzustellen ist, um auszuschließen, dass Sicherheitsverletzungen in die Referenzprofile normalen Verhaltens einfließen. Techniken, die zur Umsetzung dieses Ansatzes zum Einsatz kommen, umfassen statistische Methoden [Ja+91], neuronale Netze [De+92], genetische Algorithmen [Mé96], Support Vector Machines [La+04], Methoden des Data Minings [Le+99] und Analogien zum menschlichen Immunsystem [Fo+96].

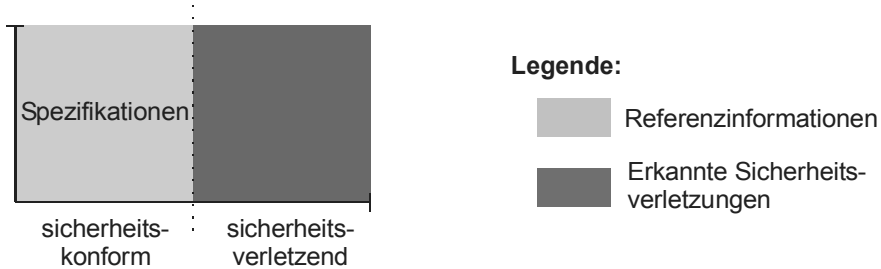
Der zweite auch als *spezifikationsbasierte Anomalieerkennung* bezeichnete Ansatz basiert auf der expliziten häufig formalen Spezifikation normalen Verhaltens. Dieser Ansatz wird oft auch ohne Bezug auf die Klassifikationsebene normal-anomal realisiert, indem explizit sicherheitskonforme Aktionen und Zustände spezifiziert werden.<sup>1</sup>

Die spezifikationsbasierte (Anomalie-)Erkennung eignet sich insbesondere zum Schutz von Systemen für die bereits Spezifikationen des möglichen Verhaltens bzw. möglicher Aktionen und Zustände vorliegen, wie dies bei Kommunikationsprotokollen häufig der Fall ist. Beispiele für IDS, die diesen Ansatz realisieren sind *DPEM (Distributed Program Execution Monitor)* [Ko+94, Ko96] und *ANIDA (Aachen Network Intrusion Detection Architecture)* [Bü+99, Bü01]. Die verwendeten Techniken erinnern an die Compiler-Technik: die verwendeten Spezifikationen repräsentieren eine Grammatik und ein entsprechender Parser überprüft die Konformität beobachteter Aktionen und Zustände zu den Spezifikationen. Abb. 2-4 veranschaulicht die Grundidee der spezifikationsbasierten (Anomalie-)Erkennung: sämtliche sicherheitskonformen Aktivitäten sind durch die Refe-

---

<sup>1</sup> Aus diesem Grund betrachten verschiedene Autoren die spezifikationsbasierte Erkennung nicht als Art der Anomalieerkennung sondern als eigenen dritten Analyseansatz [Bi03]. Wieder andere Autoren unterscheiden nur Anomalieerkennung und politikbasierte Erkennung, die ausgehend von der Art der zugrunde liegenden Sicherheitspolitik in Default-Permit- (Missbrauchserkennung) und Default-Deny- (spezifikationsbasierte Erkennung) Verfahren unterteilt werden [Ax98].

renzdaten spezifiziert und jegliche Abweichung wird als Sicherheitsverletzung klassifiziert.



**Abb. 2-4.** Grundidee der spezifikationsbasierten (Anomalie-)Erkennung

### Missbrauchserkennung

Bei der *Missbrauchserkennung (Misuse Detection)*, die auch als *Signaturanalyse (Signature Analysis)* bezeichnet wird, suchen die Analysekomponenten nach konkreten Sicherheitsverletzungen. Dazu verwenden sie definierte Angriffsmuster, die als Signaturen bezeichnet werden. Während der Analyse werden die Audit-Daten auf Übereinstimmung mit den spezifizierten Signaturen untersucht und die Übereinstimmungen als Sicherheitsverletzung angezeigt (vgl. Abb. 2-5). Voraussetzung für die Erkennung eines Angriffs ist das Vorliegen einer entsprechenden Signatur. Dementsprechend können mit diesem Ansatz nur bekannte Angriffsarten erkannt werden.



**Abb. 2-5.** Grundidee der Missbrauchserkennung

Zur Umsetzung der Missbrauchserkennung werden verschiedene Techniken wie z. B. Expertensysteme eingesetzt. *EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances)* [Po+97], *CMDS (Computer Misuse Detection System)* [Pro94], *AID (Adaptive Intrusion Detection system)* [So+96] sind Beispiele für IDS, die diesem Ansatz folgen. Andere IDS, wie z. B. *STAT (State Transitions Analysis Technique)*

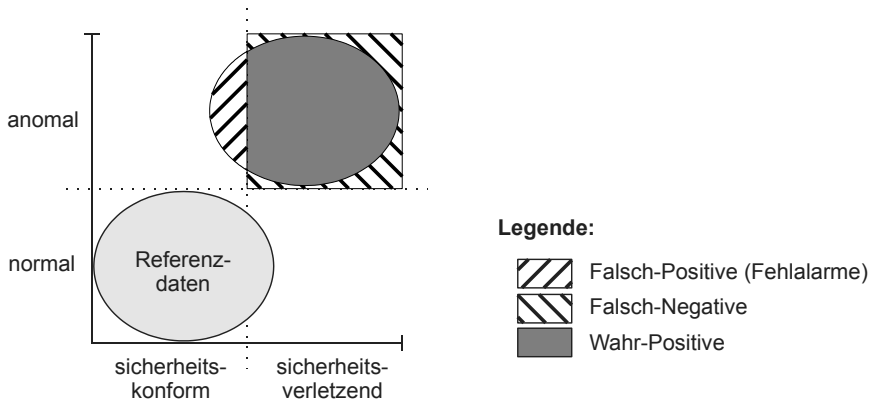
[Vi+00] oder *IDIOT (Intrusion Detection In Our Time)* [Ku95], verwenden dedizierte Verfahren zur Überprüfung von Zustandsänderungen. Auf diese Techniken wird im weiteren Verlauf genauer eingegangen.

### **Vergleich und Bewertung der Analyseansätze**

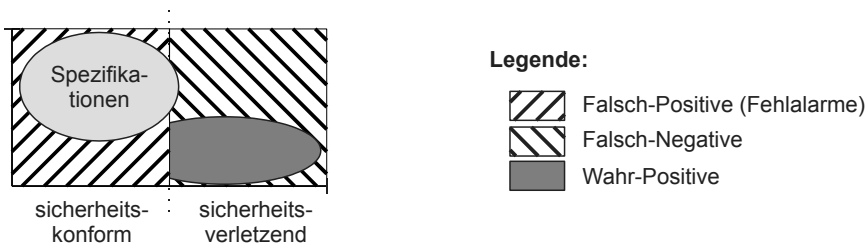
Der Hauptvorteil der lern- bzw. messbasierten Anomalieerkennung besteht darin, keine expliziten Festlegungen hinsichtlich sicherheitskonformer oder sicherheitsverletzender Aktionen und Zustände treffen zu müssen. Im Unterschied zur Missbrauchserkennung ist es mit diesem Ansatz prinzipiell möglich, neue bzw. unbekannte Sicherheitsverletzungen zu erkennen. Diese Vorteile werden jedoch durch eine Reihe von Nachteilen relativiert. Dies ist zum einen die grundsätzliche Schwierigkeit, geeignete verhaltensspezifische Merkmale zu finden und zum anderen das Problem der Veränderbarkeit des (Nutzer-)Verhaltens über längere Zeiträume. Die gesamte Vorgehensweise weist oftmals eine signifikante inhärente Unschärfe auf, was in der praktischen Anwendung häufig zu unakzeptablen Fehlalarmraten führt (vgl. Abb. 2-6). Ein weiteres Problem der Anomalieerkennung besteht in der Notwendigkeit, die Sicherheitskonformität des Systems während der Lernphase durch andere Mechanismen (z. B. unter Verwendung von Missbrauchserkennungssystemen) sicherzustellen. Außerdem basiert der Ansatz (lediglich) auf der Hypothese, dass sich Sicherheitsverletzungen in anomalem Verhalten manifestieren. Aus diesen Gründen besitzen existierende Anomalieerkennungssysteme eine nicht zu vernachlässigende Falsch-Negativ-Rate (vgl. Abb. 2-6). Darüber hinaus zeigen die von Anomalieerkennungssystemen gelieferten Ergebnisse zunächst nur Anomalien im System an, von denen nicht ohne weiteres auf konkrete stattgefundene Sicherheitsverletzungen geschlossen werden kann. Dadurch sind vor der Einleitung von Gegenmaßnahmen weitere Untersuchungen erforderlich. Das Leistungsvermögen existierender Anomalieerkennungssysteme wird durch Abb. 2-6 veranschaulicht. Die Größe der dargestellten Flächen hat dabei keinen quantitativen sondern nur existentiellen Charakter.

Die lern- bzw. messbasierten Anomalieerkennung liefert unscharfe Analyseergebnisse (z. B. Abweichungen eines numerischen Anomalieindicators). Im Unterschied dazu zeigt die spezifikationsbasierte (Anomalie-)Erkennung typischerweise an, gegen welchen Teil der Spezifikationen verstoßen wurde. Allerdings ist es auch hier nicht in jedem Falle möglich, konkret die aufgetretenen sicherheitsverletzenden Aktionen oder Zustände zu benennen. Technisch ist dieses Problem teilweise vergleichbar mit der Schwierigkeit für Compiler, geeignete Fehlermeldungen zu erzeugen. Hauptproblem bei diesem Ansatz ist jedoch die Notwendigkeit einer fehlerfreien vollständigen Spezifikation aller normalen bzw. sicherheitskon-

formen Aktivitäten, da dies für komplexere Systeme nicht oder nur mit sehr großem Aufwand möglich ist. Deshalb treten auch bei spezifikationsbasierten Verfahren sowohl Fehlalarme als auch Falsch-Negative auf (vgl. Abb. 2-7).

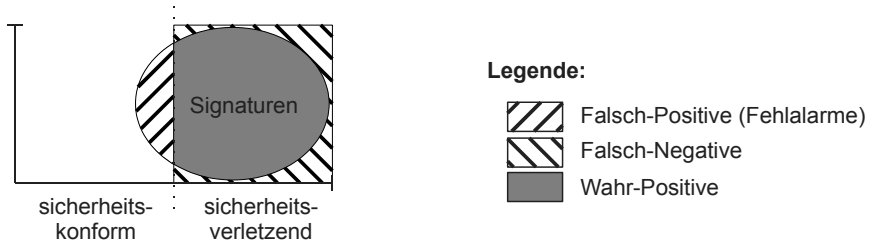


**Abb. 2-6.** Leistungsvermögen von Anomalieerkennungssystemen



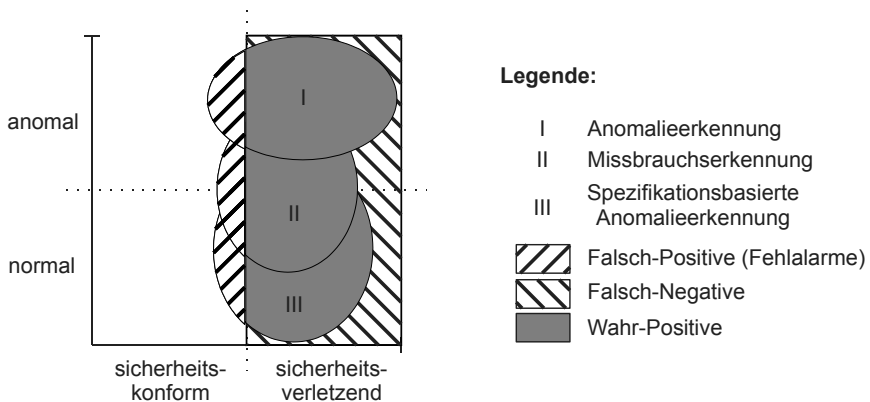
**Abb. 2-7.** Leistungsvermögen spezifikationsbasierter Anomalieerkennungssysteme

Ein Hauptvorteil der Missbrauchserkennung liegt in den scharfen und nachvollziehbaren Ergebnissen, durch die konkret aufgetretene Sicherheitsverletzungen beschrieben werden können. Das Leistungsvermögen von Missbrauchserkennungssystemen steht und fällt jedoch mit dem Umfang und der Qualität der verwendeten Signaturbeschreibungen. Durch die kontinuierliche Weiterentwicklung von IT-Systemen, z. B. durch so genannte Patches aber auch die regelmäßige Entdeckung neuer Verwundbarkeiten, besteht hier ein permanentes Unvollständigkeitsproblem. Aufgrund der Komplexität der Signaturentwicklung und daraus resultierender Entwicklungszeiten kommen neue Signaturen typischerweise erst einige Zeit nach dem Auftauchen entsprechender Exploits zum Einsatz [Li+02]. Aus diesen Gründen weist in der Praxis auch die Missbrauchserkennung Falsch-Negative auf (vgl. Abb. 2-8).



**Abb. 2-8.** Leistungsvermögen von Missbrauchserkennungssystemen

Da in der Praxis jeder der drei Analyseansätze jeweils nur für das Finden bestimmter Teilmengen von Sicherheitsverletzungen geeignet ist, wird zunehmend eine Kombination der Ansätze angewandt. Wie die Veranschaulichung in Abb. 2-9 suggeriert, kann durch eine Kombination der Ansätze eine Verringerung der Falsch-Negativ-Rate erreicht werden. Hingegen scheint eine Minimierung der Falsch-Positiv-Rate (Fehlalarmrate) durch eine einfache Kombination der Ansätze nicht erreichbar.



**Abb. 2-9.** Kombiniertes Leistungsvermögen der Analyseansätze

### 2.3.3 Reaktionskomponenten

Nachdem Sicherheitsverletzungen durch Analysekomponenten erkannt wurden, werden die Reaktionskomponenten des IDS veranlasst entsprechende Reaktionen durchzuführen. Grundlegend wird zwischen *passiven* und *aktiven* Reaktionen unterschieden. Passive Reaktionen liefern Informationen an den Nutzer des IDS und überlassen diesem die Ergreifung weiterer Maßnahmen. Aktive Reaktionen umfassen das automatische oder halbautomatische Auslösen von Aktionen. Möglich sind hierbei gezielte

Aktionen gegen den Angreifer, z. B. das Blockieren bestimmter Netzwerkdienste, die Benachrichtigung umgebender Systeme und die Sammlung zusätzlicher Informationen. Eine ausführliche Diskussion möglicher Gegenmaßnahmen findet sich in [Ba00].

## 2.4 Fazit

Mit der wachsenden Abhängigkeit unserer Gesellschaft von der Zuverlässigkeit informationstechnischer Systeme gewinnen Fragen der IT-Sicherheit an Bedeutung. Während bisher vorrangig präventive Sicherheitsmechanismen im Vordergrund standen, zeigt sich zunehmend, dass IT-Sicherheit nicht allein durch Prävention erreicht werden kann. Vielmehr stellt Prävention einen Grundpfeiler dar, neben dem ergänzend die reaktiven Aspekte der IT-Sicherheit stehen. Dem Nachweis von aufgetretenen IT-Sicherheitsverletzungen kommt dabei eine wachsende Bedeutung zu. Auf der Grundlage mittels Audit protokollierter Informationen über sicherheitsrelevante Zustände und Aktionen in IT-Systemen können IDS eingesetzt werden, um automatisch IT-Sicherheitsverletzungen zu erkennen und Reaktionen zu veranlassen. IDS setzen dazu verschiedene Verfahren ein, von denen die mess- bzw. lernbasierte und die spezifikationsbasierte Anomalieerkennung hinsichtlich der Erkennung unbekannter bzw. neuer Attacken eine Reihe von Vorteilen bieten. Diese werden jedoch durch die inhärente Unschärfe der von diesen Verfahren gelieferten Ergebnisse relativiert, so dass diese Auswertungsansätze nur ergänzend von Interesse sind. Entsprechend stellt die Missbrauchserkennung, die auf der Grundlage von definierten Angriffsmustern scharfe Ergebnisse liefert, ein unverzichtbares Basisanalyseverfahren dar.

Intrusion Detection effektiv!

Modellierung und Analyse von Angriffsmustern

Meier, M.

2007, XIV, 209 S. Mit CD-ROM., Hardcover

ISBN: 978-3-540-48251-2