

X.systems.press

X.systems.press ist eine praxisorientierte Reihe zur Entwicklung und Administration von Betriebssystemen, Netzwerken und Datenbanken.

Michael Meier

Intrusion Detection effektiv!

Modellierung und Analyse von
Angriffsmustern

Mit 104 Abbildungen, 16 Tabellen
und CD-ROM

Dr. Michael Meier
Fachbereich Informatik
Universität Dortmund
44221 Dortmund
michael.meier@udo.edu

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISSN 1611-8618
ISBN-13 978-3-540-48251-2 Springer Berlin Heidelberg New York

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsge setzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Springer ist nicht Urheber der Daten und Programme. Weder Springer noch der Autor übernehmen die Haftung für die CD-ROM und das Buch, einschließlich ihrer Qualität, Handels- und Anwendungseignung. In keinem Fall übernehmen Springer oder der Autor Haftung für direkte, indirekte, zufällige oder Folgeschäden, die sich aus der Nutzung der CD-ROM oder des Buches ergeben.

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

© Springer-Verlag Berlin Heidelberg 2007

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Text und Abbildungen wurden mit größter Sorgfalt erarbeitet. Verlag und Autor können jedoch für eventuell verborgene fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Satz: Druckfertige Daten des Autors
Herstellung: LE-T_EX, Jelonek, Schmidt & Vöckler GbR, Leipzig
Umschlaggestaltung: KünkelLopka Werbeagentur, Heidelberg
Gedruckt auf säurefreiem Papier 33/3100 YL - 5 4 3 2 1 0

Widmung

Meinen Eltern.

Vorwort

In dem Forschungsgebiet *Intrusion Detection* wird seit Mitte der 80er Jahre gearbeitet. Seit einigen Jahren sind kommerzielle *Intrusion-Detection-Systeme (IDS)* verfügbar, die ergänzend zu präventiven Sicherheitsmechanismen zum Schutz von informationstechnischen Systemen eingesetzt werden können. Die Wirksamkeit zurzeit verfügbarer Systeme bleibt jedoch weit hinter den Erwartungen der Nutzer zurück. Ursache dafür ist eine große Zahl von Fehlalarmen sowie eine schwer zu beziffernde Zahl von unerkannten Sicherheitsverletzungen, durch die der tägliche Einsatz von IDS geprägt ist. Darüber hinaus wird es aufgrund der anfallenden Datenvolumen zunehmend schwieriger in modernen leistungsfähigen Systemen zeitnah Sicherheitsverletzungen zu erkennen.

Dieses Buch betrachtet diese Problemfelder. Dabei werden systematisch fundiert die folgenden Fragestellungen diskutiert und entsprechende Lösungen dargestellt:

- Was sind die relevanten Charakteristika von Sicherheitsverletzungen, die in Angriffsmustern spezifiziert werden müssen, um eine exakte Erkennung zu ermöglichen?
- Wie können komplexe Angriffsmuster geeignet modelliert und beschrieben werden?
- Wie kann die Erkennung der Angriffsmuster effizient(er) realisiert werden?

Dem Leser werden dabei Werkzeuge zur Bewertung existierender und Konstruktion neuer IDS vorgestellt. Schwerpunkte sind dabei die systematische Betrachtung sowie exakte Modellierung und Beschreibung von Angriffsmustern. Darüber hinaus werden existierende Analyseverfahren zur Erkennung von Angriffsmustern beschrieben und ein hinsichtlich Effizienz optimiertes Verfahren vorgestellt.

Dieses Buch ist zum größten Teil während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl Rechnernetze und Kommunikationssysteme der Brandenburgischen Technischen Universität Cottbus entstanden. Für die wissenschaftliche Betreuung meiner Arbeiten, die eingeräum-

ten Freiräume sowie die in vielerlei Hinsicht angenehme Arbeitsatmosphäre an seinem Lehrstuhl danke ich Hartmut König. Meine Arbeiten zu diesem Buch profitierten unter anderem von der fruchtbaren Zusammenarbeit mit Ulrich Flegel. Während zahlloser Treffen auf Workshops und Konferenzen sowie Besuchen in Dortmund und Cottbus diskutierten wir die Ausdrucksstärke von Modellierungsansätzen für Angriffssignaturen. Als Ergebnis unserer Zusammenarbeit entstand ein allgemeiner Ansatz zur Modellierung von Angriffssignaturen. Mario Schözel gilt besonderer Dank für seine Unterstützung bei der formalen Definition von Signaturnetzen. Niels Bischof, Christian Rohr und Sebastian Schmerl danke ich für ihre Arbeiten und ihre konstruktiven Ideen zu den Sprachen SHEDEL und EDL sowie den Werkzeugen SAM und SEG, die auf beiliegender CD-ROM enthalten sind.

Dortmund, im November 2006

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIII
1 Einleitung.....	1
2 IT-Sicherheit und Intrusion Detection.....	5
2.1 IT-Sicherheit	5
2.2 Sicherheitsmechanismen.....	7
2.3 Intrusion-Detection-Systeme	9
2.3.1 Ereigniskomponenten und Audit	10
2.3.2 Analyse- und Datenbankkomponenten	12
2.3.3 Reaktionskomponenten.....	18
2.4 Fazit	19
3 Missbrauchserkennung	21
3.1 Systemmodell und Informationsarten	22
3.2 Aktuelle Herausforderungen	25
3.2.1 Fehlalarme	26
3.2.2 Effiziente Erkennung	27
3.2.3 Fazit	28
4 Beispiele	29
4.1 Beispielumgebung Solaris	29
4.1.1 Schwachstellen.....	29
4.1.2 Audit-Funktion.....	31
4.2 Beispielattacken	32
4.2.1 Login-Attacke	33
4.2.2 PATH-Attacke	35
4.2.3 Link-Attacke	37
4.2.4 Nebenläufige Link-Attacke.....	39
5 Semantische Aspekte von Angriffssignaturen.....	41
5.1 Aktive Datenbanksysteme	42
5.1.1 Ereignisse in aktiven Datenbanken.....	42
5.1.2 Unterschiede zum Signaturkonzept	43

5.2	Ereignisse – Begriffseinführung	44
5.3	Dimensionen der Semantik von Signaturen.....	49
5.4	Ereignismuster	51
5.4.1	Typ und Reihenfolge	52
5.4.2	Häufigkeit	53
5.4.3	Kontinuität	56
5.4.4	Nebenläufigkeit.....	56
5.4.5	Kontextbedingungen	57
5.5	Selektion der Schrittinstanzen.....	57
5.6	Konsum von Schrittinstanzen	59
5.6.1	Aktionsfolgen und Aktionssemantik.....	60
5.6.2	Auswahl von Schritt kombinationen.....	60
5.6.3	Schritt kombinationen.....	62
5.7	Zusammenfassung	65
6	Modell für Angriffssignaturen.....	67
6.1	Signurnetze – Das allgemeine Modell	67
6.2	Modellierungselemente im Detail.....	69
6.2.1	Plätze.....	69
6.2.2	Transitionen	70
6.2.3	Kanten.....	72
6.2.4	Token	72
6.2.5	Schaltregel	75
6.2.6	Charakteristische Netztopologien	80
6.3	Eine Beispielsimulation	86
6.4	Formale Definition eines Signurnetzes	89
6.5	Ausdrucksstärke	98
6.5.1	Ereignismuster	98
6.5.2	Instanzselektion	106
6.5.3	Instanzkonsum	106
6.6	Verwandte Ansätze	108
6.6.1	Automatenbasierte Signaturmodellierung	108
6.6.2	Graphenbasierte Signaturmodellierung	110
6.6.3	Netzbasierte Signaturmodellierung.....	110
6.7	Zusammenfassung	111
7	Beschreibung von Angriffssignaturen.....	113
7.1	Signaturentwicklung	113
7.2	Regelbasierte Signaturbeschreibung	115
7.2.1	Expertensysteme	116
7.2.2	Expertensystembasierte Missbrauchserkennung	117

7.2.3	Probleme expertensystembasierter Missbrauchs-erkennung.....	119
7.2.4	Regelbasierte Signaturbeschreibung.....	123
7.3	SHEDEL – Eine einfache ereignisbasierte Beschreibungssprache.....	123
7.3.1	Beschreibungselemente von SHEDEL	124
7.3.2	Beispiele.....	127
7.3.3	Diskussion.....	131
7.4	EDL.....	132
7.4.1	Basiskonzepte	132
7.4.2	Beispiel	139
7.4.3	Diskussion.....	141
7.5	Alternative Beschreibungszugänge.....	142
7.6	Zusammenfassung	144
8	Analyseverfahren	147
8.1	Stand der Technik	148
8.1.1	Abbildung in separate Programm-Module.....	148
8.1.2	Expertensystembasierte Analysen	151
8.2	Optimierungsstrategien	159
8.2.1	Strategie 1: Ereignistypbasierte Transitionsindizierung	159
8.2.2	Strategie 2: Tokenunabhängige Prüfung von Intra-Ereignis-Bedingungen	160
8.2.3	Strategie 3: Wertebasierte Tokenindizierung.....	161
8.2.4	Strategie 4: Gemeinsame Ausdrücke	164
8.2.5	Strategie 5: Kostenbasierte Bedingungspriorisierung.....	165
8.2.6	Diskussion.....	166
8.3	Das Analysewerkzeug SAM	168
8.4	Experimentelle Evaluierung.....	170
8.4.1	Testszenario	171
8.4.2	Vorgehensweise und Messumgebungen	176
8.4.3	Messergebnisse und Diskussion	177
8.5	Zusammenfassung	182
9	Zusammenfassung und Ausblick.....	185
10	Anhang.....	187
10.1	Signatur der nebenläufigen Link-Attacke in EDL	187
Index.....	193	
Literatur	197	

Abkürzungsverzeichnis

AID	Adaptive Intrusion Detection system
ANIDA	Aachen Network Intrusion Detection Architecture
ASAX	Advanced Security audit trail Analyzer on uniX
BSM	Basic Security Module
CC	Coordination Center
CERT	Computer Emergence Response Team
CIDF	Common Intrusion Detection Framework
CLIPS	C Language Integrated Production System
CMDS	Computer Misuse Detection System
CPA	Coloured Petri Net Automaton
DARPA	Defense Advanced Research Projects Agency
DPEM	Distributed Program Execution Monitor
ECA	Event Condition Action
EDL	Event Description Language
EGID	Effektive Gruppen-ID
EMERALD	Event Monitoring Enabling Responses to Anomalous Live Disturbances
ET	Ereignis-Token
EUID	Effektive User-ID
FL	Failed Login
FRT	Fire Ready Tokens
GID	Gruppen-ID
GUI	Graphical User Interface
ID	Identifikator
IDIOT	Intrusion Detection In Our Time
IDMEF	Intrusion Detection Message Exchange Format
IDRS	Intrusion Detection and Response System
IDS	Intrusion-Detection-System
IDWG	Intrusion Detection Working Group
IETF	Internet Engineering Task Force
Inter-EB	Inter-Ereignis-Bedingung
Intra-EB	Intra-Ereignis-Bedingung
IP	Internet Protokoll
IPS	Intrusion-Prevention-System

IT-	Informationstechnisch (im Zusammenhang)
MIDAS	Multics Intrusion Detection and Alerting System
MuSig	Misuse Signature
OID	Objekt-ID
P-BEST	Production-Based Expert System Toolset
PID	Reale Prozess-ID
RGID	Reale Gruppen-ID
RUID	Reale User-ID
RUSSEL	RULE-baSED Sequence Evaluation Language
SAM	Signature Analysis Module
SEG	Snoopy-based EDL GUI
SHEDEL	Simple Hierarchical Event DEscription Language
STAT	State Transition Analysis Technique
StraFER	Straight Forward Event Recognition
SUID	Set-User-ID
TT	Token-Token
UID	User-ID

1 Einleitung

Die moderne Informationsgesellschaft basiert auf komplexen informationstechnischen Infrastrukturen, die einen zunehmenden Grad an Vernetzung aufweisen. Immer mehr private und öffentliche Institutionen verwenden *informationstechnische Systeme (IT-Systeme)*, um ihre Dienste effektiver und effizienter anbieten und abwickeln zu können. Durch die globale Vernetzung wird der Zugang zu Diensten in Zukunft für jedermann, zu jederzeit und von jedem Ort möglich sein. Die Vorteile dieser Entwicklungen sind unbestritten. Sie bringen jedoch auch Nachteile mit sich. Aus der Verlagerung vieler gesellschaftlicher Prozesse auf IT-Systeme resultiert eine direkte Abhängigkeit unserer Gesellschaft von diesen Systemen. Darauf gewinnt der Schutz von IT-Systemen zunehmend an Bedeutung.

Klassische Sicherheitsmechanismen, z. B. kryptographische Verfahren und Zugangskontrollsysteme, wie beispielsweise Firewalls, sind notwendige Komponenten zum Schutz von IT-Infrastrukturen und heute weit verbreitet. Während bisher vorrangig präventive Maßnahmen und Mechanismen im Vordergrund standen, wird zunehmend deutlich, dass die Sicherheit von IT-Systemen nicht allein durch Prävention erreichbar ist. Vielmehr stellt Prävention einen Grundpfeiler dar, neben dem reaktive Aspekte der Sicherheit von IT-Systemen stehen.

Um in der Lage zu sein, auf Sicherheitsverletzungen reagieren zu können, sind Mechanismen zur Erkennung von Sicherheitsverletzungen erforderlich. Seit Mitte der 80er Jahre hat sich daher das Forschungsgebiet der *Angriffserkennung (Intrusion Detection)* entwickelt. Seit einiger Zeit sind kommerzielle *Intrusion-Detection-Systeme (IDS)* verfügbar, die ergänzend zu präventiven Sicherheitsmechanismen zum Schutz von IT-Systemen eingesetzt werden können.

Die in diesem Gebiet entwickelten Verfahren zur Erkennung von Sicherheitsverletzungen können grob in Anomalieerkennung und Missbrauchserkennung unterteilt werden. Verfahren zur *Anomalieerkennung* basieren auf der expliziten Definition von normalem Verhalten und erkennen Abweichungen von dieser Norm. Problematisch bei diesen Verfahren sind die inhärente Unschärfe der gelieferten Ergebnisse sowie die Frage, ob jede Anomalie eine Sicherheitsverletzung darstellt.

Zur *Missbrauchserkennung* ist das Vorliegen expliziter Definitionen von Angriffsmustern in Form von Signaturen erforderlich. Beobachtete Aktionen werden auf Übereinstimmung mit den Signaturen überprüft. Prinzipiell sind Verfahren zur Missbrauchserkennung bezüglich der Erkennungsgenauigkeit sehr robust und liefern scharfe Ergebnisse, auf deren Grundlage Reaktionen auf Angriffe veranlasst werden können. Die Missbrauchserkennung stellt daher ein unverzichtbares Basisauswertungsverfahren von IDS dar, das um Anomalieerkennung ergänzt werden kann. Naturgemäß sind Verfahren zur Missbrauchserkennung jedoch auf die Erkennung von bekannten, durch Signaturen repräsentierten Angriffen beschränkt.

Obwohl die Notwendigkeit von Systemen zur Missbrauchserkennung unwidersprochen bleibt, ist der Einsatz derzeit verfügbarer Systeme mit einer Reihe von Problemen verbunden. Eines der Hauptprobleme ist die Vielzahl der von den Systemen erzeugten Alarme. Häufig werden tausende von Alarmen pro Tag erzeugt, von denen 99% Fehlalarme sind. Aufgrund dieser Alarmflut ist es schwierig die Alarme zu identifizieren, die tatsächlich Sicherheitsverletzungen anzeigen. Dadurch wird der Nutzen von IDS infrage gestellt.

Unter der Voraussetzung einer korrekten Spezifikation von Signaturen, können Fehlalarme durch Missbrauchserkennungssysteme ausgeschlossen werden. Missbrauchserkennungssysteme erkennen genau die Muster, die in den Signaturen beschrieben sind. Die Ursache für hohe Fehlalarmraten ist dementsprechend auf der Ebene der Spezifikation der Signaturen zu suchen. Zum einen fehlt eine Systematik zur Betrachtung der relevanten Aspekte von Angriffssignaturen. Mit verschiedenen existierenden Sprachen zur Beschreibung von Signaturen sind unterschiedliche Mengen von Signaturen beschreibbar. Vielfach können Signaturen mit den zur Verfügung stehenden Sprachmitteln nicht exakt spezifiziert werden. Zum anderen führt die Komplexität von Angriffssignaturen zu einem Fehlerpotential bei ihrer Entwicklung. In existierenden Sprachen fehlen geeignete Mittel, um den Signaturentwickler bei der Beherrschung dieser Komplexität zu unterstützen.

Die steigende Leistungsfähigkeit von IT-Systemen führt zu einem weiteren Problem für die Missbrauchserkennung. Der damit einhergehende Anstieg des Datenaufkommens führt existierende Missbrauchserkennungssysteme an die Grenzen ihrer Leistungsfähigkeit. Die aus der zunehmenden Komplexität der IT-Systeme resultierende Steigerung der Anzahl zu analysierender Angriffsmuster verschärft dieses Problem zusätzlich. Aktuelle Systeme zur Missbrauchserkennung setzen verschiedene Standardverfahren zur Analyse ein. Der Entwicklung und Untersuchung optimierter Analyseverfahren zur Missbrauchserkennung wurde bisher kaum Auf-

merksamkeit geschenkt. Dadurch wird eine zeitnahe Erkennung von Angriffen schwieriger. Es ist notwendig, effiziente Analyseverfahren zur Missbrauchserkennung zu entwickeln.

Zur Steigerung der Wirksamkeit von IDS müssen Missbrauchserkennungssysteme effizient korrekte Ergebnisse liefern. Insbesondere ist die Zahl der Fehlalarme zu reduzieren. Dazu ist zunächst eine systematische Betrachtung von Angriffsmustern erforderlich. Des Weiteren werden Werkzeuge zur Modellierung und Beschreibung von Signaturen benötigt, die eine effiziente und fehlerfreie Entwicklung von Signaturen erlauben. Aufgrund der resultierenden kürzeren Entwicklungszeiten für Signaturen wird es möglich, nach dem Auftreten bzw. bekannt werden neuer Sicherheitslücken kurzfristig entsprechende Signaturen zu erstellen. Dadurch können die betroffenen Systeme vor entsprechenden Angriffen geschützt werden, bis die Sicherheitslücken behoben werden. Effiziente Analyseverfahren erlauben es, einen Angriff zeitnah zu erkennen und geeignete Ge- genmaßnahmen einzuleiten, beispielsweise indem Aktivitäten des Angreifers blockiert werden.

Im Kapitel 2 geben wir zunächst eine grundlegende Einführung in den Bereich IT-Sicherheit. Eine Einordnung des Gebiets Intrusion Detection wird vorgenommen. Verschiedene Verfahren zur Angriffserkennung werden vorgestellt und diskutiert. Vertiefend werden in Kapitel 3 Verfahren zur Missbrauchserkennung behandelt und aktuelle Herausforderungen an diese Technologie herausgearbeitet. Beispiele für ein konkretes IT-System und verschiedene Attacken, auf die in diesem Buch Bezug genommen wird, werden in Kapitel 4 vorgestellt.

In Kapitel 5 wird ein Modell für die Semantik von Angriffssignaturen entwickelt, das systematisch die semantischen Aspekte von Signaturen betrachtet. Es bildet die Grundlage für Vergleiche der Ausdrucksstärke von Signaturbeschreibungssprachen. Kapitel 6 führt einen Ansatz zur Modellierung von Signaturen ein, bevor in Kapitel 7 zwei Sprachen zur Beschreibung von Signaturen vorgestellt werden.

Im Kapitel 8 untersuchen wir Analyseverfahren zur Missbrauchserkennung. Es werden Optimierungsstrategien zur Steigerung der Analyseeffizienz entwickelt und experimentell evaluiert. Im abschließenden Kapitel 9 werden eine Zusammenfassung und ein Ausblick gegeben.

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-Sicherheit¹ 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-

¹ 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 unbemerkt Modifikation von Informationen.
- *Verfügbarkeit* - Schutz vor unautorisierter Vorenhaltung 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 Schutzzieilen 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 Emergence Response Team / Coordination Center) gemeldeten Vorfälle um mehr als 50% zu beobachten (vgl. Abb. 2-1, [CE05])¹. Präventive Mechanismen können

¹ 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.

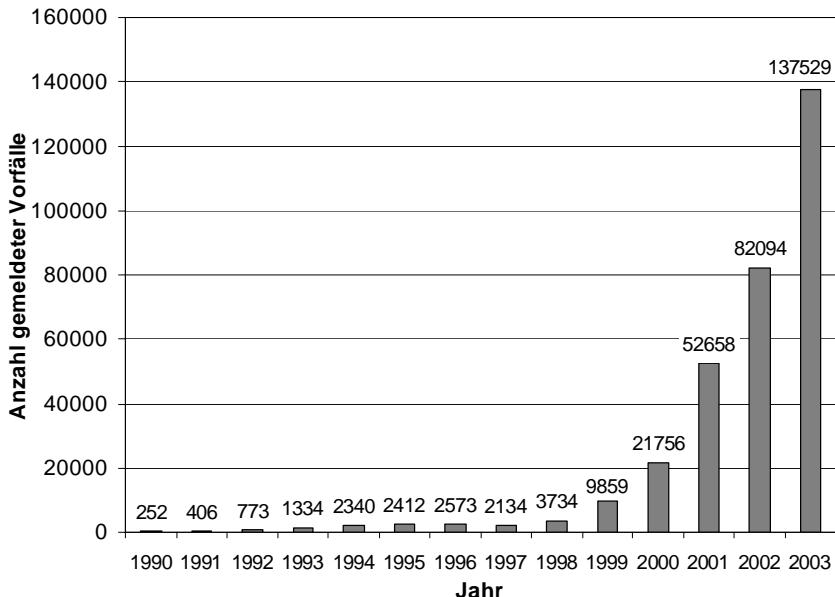


Abb. 2-1. Entwicklung beim CERT/CC gemeldeter Sicherheitsvorfälle

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)* gesprochen¹.

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.

¹ 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.

Inspiriert durch die CIDEF-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 CIDEF-Komponenten sowie verwendete Verfahren diskutiert.

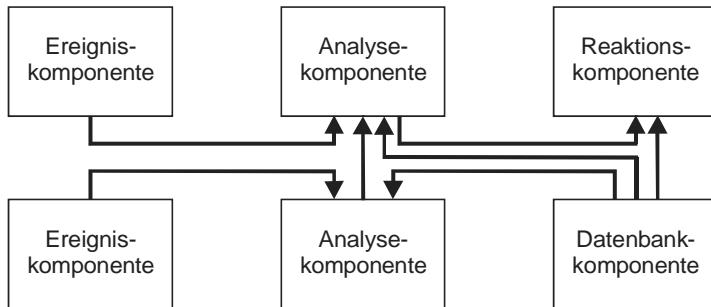


Abb. 2-2. Informationsaustausch verschiedener CIDEF-Komponenten

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 Klassifikationsergebnisse 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: