

Diplomarbeit

Modellbasiertes Management
von Sicherheitsdiensten:
Integrale Durchsetzung von Policies
in Firmennetzen

Gereon Geist

Diplomarbeit
am Fachbereich Informatik
der Universität Dortmund
Lehrstuhl IV

Betreuer:
Prof. Dr. Heiko Krumm
Dipl. Inform. Ingo Lück

Inhaltsverzeichnis

1	Einleitung	1
2	Sicherheit in Firmennetzwerken	4
2.1	Sicherheitsdienste, Verfahren und Produkte.....	4
2.2	Ausgewählte Verfahren für die Herstellung von Sicherheit in Firmennetzen	6
2.2.1	X.509	6
2.2.2	SSL	7
2.2.3	VPN	8
2.2.4	IPSec	8
2.2.5	Firewalls	9
2.2.6	http-Proxy-Server	10
2.2.7	Network-Address-Translation.....	10
2.2.8	Radius	11
2.3	Zusammenfassung	11
3	Sicherheitsdienste und Policy-Durchsetzung	12
3.1	Policy-basiertes Management.....	12
3.2	Modellbasiertes Management.....	14
3.3	Metamodell und Basis-Metamodell.....	16
3.3.1	Entwurfsziele	17
3.3.2	Ausgewählte Basisklassen der Ebene Roles & Objects	18
3.3.3	Ausgewählte Basisklassen der Ebene Subject & Ressources	19
3.3.4	Ausgewählte Basisklassen der Ebene Processes & Hosts.....	20
3.3.5	Security-Vektoren	22
3.3.6	Abbildung eines Services auf Ebene S&R.....	23
3.3.7	Abbildung von Benutzerinformationen im Modell unter Berücksichtigung von RBAC	23
3.3.8	Behandlung großer Datenmengen im Modell: Typisierte Folder	28
3.3.9	Anwendung des Metamodells, Modellierung von Firmennetzwerken und deren Betrieb	28
3.4	Schrittweise Verfeinerung, Ableitungsprozesse, Umsetzung der Policy-Durchsetzung	29
3.4.1	Realisierbarkeit der automatischen Erzeugung einer Policy-Hierarchie.....	30
3.4.2	Precondition „structural consistency“ der Access-Permission.....	31
3.4.3	Precondition „structural consistency“ der Service-Permission	32
3.4.4	Lösungsansatz beim Auftreten von Widersprüchen – ungültige Modelle	33
3.4.5	Preconditions im Bereich der RBAC-Modellierung	33
3.4.6	Die Verfeinerungs-Relationen ref1, ref2 und ref3	34
3.5	Das Werkzeug MoBaSec.....	38
3.5.1	Metamodell und Modell.....	39
3.5.2	Ebenen Roles & Objects, Subjects & Ressources und Processes & Hosts	39
3.5.3	Automatische Ableitung von Permissions und Konfigurationen: Policy-Refinement.	40
3.6	Zusammenfassung	40
4	Pfadermittlung	41
4.1	Ziele.....	42
4.2	Ermittlung relevanter Prozesse.....	43

4.3	Pfadermittlung	44
4.3.1	Basisalgorithmus	44
4.3.2	Definition einer geeigneten Datenstruktur für den Algorithmus.....	45
4.3.3	Definition des Besuchskriteriums	48
4.3.4	Abbruchkriterien	49
4.4	Design der Path-Description.....	50
4.5	Gültige Modelle.....	50
4.6	Sichere und unsichere Pfade.....	51
4.7	Zusammenfassung	51
5	Implementierung	52
5.1	Architektur des Werkzeugs MoBaSec.....	53
5.2	Design und Implementierung der Metamodellklassen	54
5.3	Funktionserweiterungen im Bereich der typisierten Folder.....	55
5.3.1	Graphische Benutzerunterstützung	55
5.3.2	Graphische Darstellung der Folder-Zugehörigkeit	56
5.3.3	Problem der Transienz und Persistenz	56
5.3.4	Prüfung von Kardinalitäten sowie Durchführung von Assoziationen.....	56
5.3.5	Ermittlung von connected objects.....	60
5.4	Allgemeine Erweiterung von StView	60
5.4.1	Erweiterung von StView um Kanten zur Darstellung von gerichteter Kommunikation	60
5.4.2	Benutzermenu	61
5.5	Implementierung der Methoden im Kontext des automatischen Policy-Refinements	61
5.5.1	Erweiterung des Werkzeugs im Bereich Transformation und Konfiguration	62
5.5.2	Erweiterungen des Werkzeugs im Bereich spezieller Modellobjekt-Methoden	63
5.6	Zusammenfassung	64
6	Szenarien	65
6.1	Klassifikation von Sicherheitsdiensten.....	65
6.1.1	Datendurchflusspunkte bzw. Transit-Dienste	66
6.1.2	Verteilte Dienste	66
6.1.3	Datenstrom-orientiert wirkende Sicherheitsdienste	67
6.2	Zugriff auf einen Web-Server via SSL in einer Firewall-Architektur	67
6.2.1	Szenario	67
6.2.2	Analyse der Wechselwirkungen	68
6.2.3	Ziel.....	68
6.2.4	Lösungsansätze	69
6.2.5	Zusammenfassung	71
6.3	Einsatz von VPN und Firewall	71
6.3.1	Szenario	71
6.3.2	Analyse der Wechselwirkungen	73
6.3.3	Ziel.....	74
6.3.4	Lösungsansätze	74
6.3.5	Zusammenfassung	81
6.4	Wechselwirkung durch Address-Translation-Services.....	82
6.4.1	Szenario	82
6.4.2	Analyse der Wechselwirkungen	83
6.4.3	Ziel.....	84
6.4.4	Lösungsansätze	85
6.4.5	Zusammenfassung	89
6.5	Auswirkungen eines Proxy-Servers im Netzwerk	89
6.5.1	Szenario	89
6.5.2	Analyse der Wechselwirkungen	90
6.5.3	Ziel.....	91
6.5.4	Lösungsansätze	91
6.5.5	Zusammenfassung	92
7	Integrierte Policy-Durchsetzung - Teilmodelle	94
7.1	Beispielhafte Modellierung des Zugriffs auf einen Web-Server via SSL in einer Firewall-	

Architektur.....	94
7.1.1 Modellierung auf der Ebene P&H	95
7.1.2 Modellierung des Beispielszenarios auf der Ebene S&R.....	96
7.1.3 Modellierung des Beispielszenarios auf der Ebene R&O.....	98
7.1.4 Durchführung der Ableitungsprozesse.....	98
7.2 Beispielhafte Modellierung des gemeinsamen Einsatzes von VPN und Firewall	101
7.2.1 Modellierung auf der Ebene P&H	102
7.2.2 Modellierung des Beispielszenarios auf der Ebene S&R.....	103
7.2.3 Modellierung des Beispielszenarios auf der Ebene R&O.....	104
7.2.4 Durchführung der Ableitungsprozesse.....	105
7.3 Beispielhafte Modellierung der Wechselwirkungen durch Address-Translation-Services	108
7.3.1 Modellierung auf der Ebene P&H	108
7.3.2 Modellierung des Beispielszenarios auf der Ebene S&R.....	110
7.3.3 Modellierung des Beispielszenarios auf der Ebene R&O.....	111
7.3.4 Durchführung der Ableitungsprozesse.....	111
7.4 Beispielhafte Modellierung der Auswirkungen eines Proxy-Servers im Netzwerk	113
7.4.1 Modellierung auf der Ebene P&H	114
7.4.2 Modellierung des Beispielszenarios auf der Ebene S&R.....	115
7.4.3 Modellierung des Beispielszenarios auf der Ebene R&O.....	115
7.4.4 Durchführung der Ableitungsprozesse.....	117
8 Modellierung einer umfassenden Sicherheitsinfrastruktur eines möglichen realen Netzwerkes	119
8.1 Szenario	119
8.1.1 Kommunikationsfluss	121
8.2 Modellierung des Netzwerkes	123
8.2.1 Modellierung auf der Ebene P&H	123
8.2.2 Modellierung auf der Ebene S&R.....	127
8.2.3 Modellierung des Netzwerkes auf der Ebene R&O.....	131
8.2.4 Policies und Modellierung der Access-Permissions	132
8.2.5 Anwendung von ref1 zur Erzeugung von Service-Permissions.....	134
8.2.6 Anwendung von ref2 und ref3 zur Erzeugung von allgemeinen Protocol-Permissions	134
8.2.7 Anwendung von ref3' zur Erzeugung der technischen Protocol-Permissions und der Path-Description-Ketten	135
8.3 Zusammenfassung	138
9 Schluss	140
A Modelle und Klassendokumentationen	iv
A.1 Übersicht über das Modell des Firmennetzwerks.....	iv
A.2 Klassendiagramm des Metamodells	v
A.3 Metamodell der Service-Klassen.....	vi
B Ausgewählte Implementierungen	vii
B.1 Implementierung ref2().....	vii
C Abbildungsverzeichnis	x
D Literaturverzeichnis	xiv
E Glossar	xvi

1 Einleitung

Der Einsatz von elektronischen Kommunikationsmedien in Unternehmen hat in den vergangenen Jahren immer größere Bedeutung angenommen. Wesentliche Geschäftsprozesse von Firmen bauen auf elektronischer Kommunikation auf und es entsteht eine immer weiter wachsende Abhängigkeit von Computer- und Netzwerkintegration.

Eine Störung der computergestützten Kommunikation hat nicht selten unmittelbare Auswirkungen auf den Geschäftserfolg von Unternehmen. Das Beispiel des Management-Werkzeugs SAP, das direkt den Geschäftsverlauf eines Unternehmens steuert, kontrolliert und dokumentiert, sei hierbei nur als ein Beispiel von vielen genannt.

Nachfolgende Abbildungen dokumentieren die stetig wachsende Integration eines Informationsdienstes zur Recherche von Kontaktdaten, wie Telefonnummern, Raumnummern oder E-Mail-Adressen in einem internationalen Konzern mit ungefähr 350.000 Mitarbeitern. Es ist zu erkennen, dass die Nutzung dieses Informationsdienstes von ca. 150.000 Zugriffen pro Monat im Jahr 1997 bis auf ca. 35 Mio. Zugriffe im Jahr 2003 kontinuierlich angestiegen ist. [Sie03]

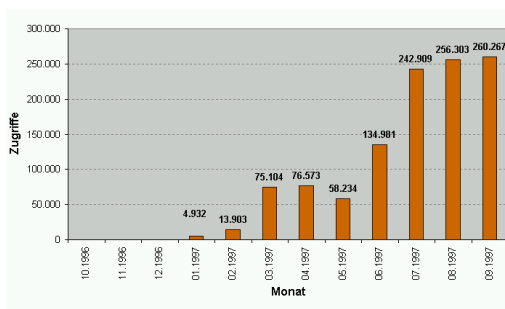


Abbildung 1: [Sie03] Zugriffsstatistik 1996/1997

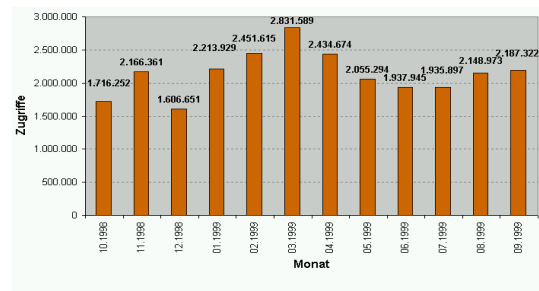


Abbildung 2: [Sie03] Zugriffsstatistik 1998/1999

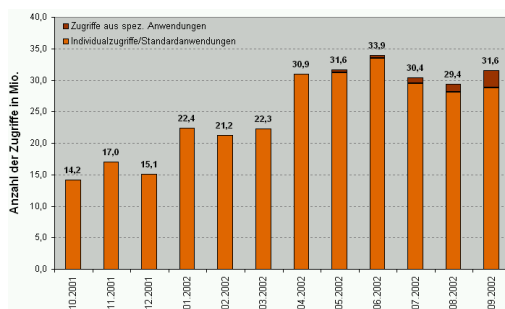


Abbildung 3: [Sie03] Zugriffsstatistik 2001/2002

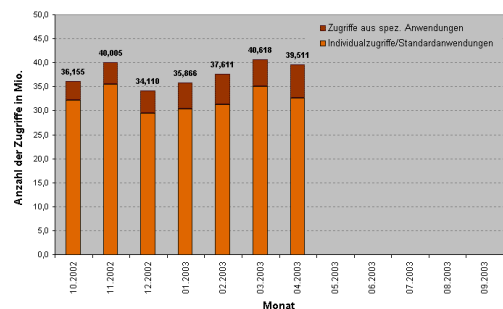


Abbildung 4: [Sie03] Zugriffsstatistik bis April 2003

Es ist offensichtlich, dass Systemausfälle bereits bei diesem einfachen Informationsdienst direkte Auswirkungen auf die Produktion der Unternehmensinhalte haben, da durch den Verlust der Kommunikationsdatenrecherche beispielsweise die telefonische Erreichbarkeit der Mitarbeiter drastisch eingeschränkt wird.

Die Wichtigkeit der Funktionsfähigkeit derartiger Systeme steht somit im Mittelpunkt von Managementzielen einer Unternehmensführung. Aber nicht nur die Verfügbarkeit solcher Kommunikationssysteme ist für den Unternehmenserfolg entscheidend. Auch der Schutz vor unsachgemäßer Nutzung oder Verfälschung ist hier zu nennen. Dies stellt einen unmittelbaren Bezug zu der allgemeinen Problematik der Sicherheitsangriffe auf Kommunikationssysteme von Firmen her, wobei nicht zuletzt Firmenspionage oder Sabotage sehr ernstzunehmende Faktoren darstellen.

Das CERT Coordination Center des amerikanischen Carnegie Mellon Software Engineering Institute veröffentlicht auf seinen Internet-Seiten die aktuellen Statistiken über die Anzahl von Sicherheits-Störungen, die dem Institut gemeldet werden. Es ist deutlich zu erkennen, dass die Anzahl von Vorfällen pro Jahr kontinuierlich ansteigt. [Cer03]

Year	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	1Q 2003
Incidents	6	132	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	52,658	82,094	42,586

Abbildung 5: An das CERT gemeldete Sicherheits-Störungen, <http://www.cert.org/stats/>, [Cer03]

Die wachsende Notwendigkeit, Unternehmensnetze vor allgemeinen Sicherheits-Störungen zu schützen rückt den Begriff des Sicherheits-Managements in den Mittelpunkt. Die vorliegende Diplomarbeit behandelt, durch dieses Umfeld motiviert, den Einsatz einer Methode zum Management von Sicherheitsdiensten in Firmennetzwerken: Das modellbasierte Management.

Gegenstand der Methode ist, aus den Unternehmenszielen abgeleitete abstrakte Sicherheitsanforderungen aufzunehmen und über Automatisierungsschritte zu konkreten Konfigurationen von Sicherheitsdiensten zu überführen. Ziel ist es hierbei, die Methode aus dem Blickwinkel von realen oder realitätsnahen Unternehmen zu analysieren und entsprechend anzuwenden, um somit eine sichere Administration von Sicherheitsdiensten in Firmennetzwerken zu ermöglichen.

Firmennetzwerke sind im Allgemeinen komplexe und heterogene Systeme mit einer Vielzahl von unterschiedlichen Funktionen, Techniken und Anwendungen. Es ist daher verständlich, dass auch auf eine Vielzahl von Verfahren zurückgegriffen werden muss, um Sicherheit im Bereich von Firmennetzen herzustellen. Als Beispiele für derart unterschiedliche Anforderungen und Verfahren sei der Einsatz einer Firewall zum Schutz eines Firmennetzwerks vor Internet-Zugriffen einerseits genannt und andererseits stellt Email-Verschlüsselung die Vertraulichkeit und Integrität auf einem völlig anderen Bereich der Firmenkommunikation her. Durch den gemeinsamen Einsatz derartiger verschiedener Sicherheitstechniken in Firmennetzwerken ergeben sich Wechselwirkungen, welche die Administration von komplexen Netzwerken im Bereich der Sicherheit deutlich erschweren.

Innerhalb dieser Arbeit werden somit die folgenden Themen aus dem Bereich des Sicherheitsmanagements analysiert und entsprechende Lösungen präsentiert:

- ? Nach einer kurzen Diskussion von Sicherheitsdiensten, Verfahren und Produkten, die in Firmennetzen Anwendung finden sowie einer kurzen Vorstellung von konkreten Verfahren zur Herstellung von Sicherheitsdiensten in Kapitel 2, wird im Kapitel 3 das Prinzip des Policy-basierten und des modellbasierten Managements vorgestellt.
- ? Kapitel 4 untersucht das Problem der Ermittlung von Kommunikationspfaden in heterogenen Netzwerken. Der Schwerpunkt liegt dabei auf der Berücksichtigung von Sicherheits- und Netzwerkdiensten, die allgemein Einfluss auf Kommunikationswege in Firmennetzen haben.

- ? Kapitel 5 präsentiert den Werkzeugbezug dieser Arbeit. In diesem Umfeld wurde eine intensive Software-Entwicklung vorgenommen. Im Mittelpunkt der Tätigkeiten standen dabei Erweiterungen des Werkzeugs MoBaSec, das am Lehrstuhl innerhalb von verschiedenen Diplomarbeiten entwickelt worden ist und die Methoden des modellbasierten Managements unterstützt.
- ? Es folgt eine Analyse der Wechselwirkung von Sicherheitsdiensten in Firmennetzwerken. Ziel dieses Teils der Arbeit ist es, eine möglichst repräsentative Auswahl von Sicherheitsdiensten zu treffen, die sich beim gemeinsamen Einsatz in Netzwerken gegenseitig beeinflussen. Hier werden Szenarien vorgestellt, die trotz Wirklichkeitsbezug auf die wesentlichen Elemente reduziert wurden, so dass für die extrahierten Problemsituationen konkrete Lösungen präsentiert werden. Dies geschieht in Kapitel 6
- ? Auf die vorgestellten Szenarien wird nun in Kapitel 7 die Methode des modellbasierten Managements real angewendet. Mit Hilfe des Werkzeugs MoBaSec werden die Lösungen des vorigen Kapitels erprobt und die Schwierigkeiten der diskutierten Wechselwirkungen automatisiert gelöst.
- ? Kapitel 8 zeigt nun, dass die zuvor extrahiert betrachteten Inhalte im Kontext von Firmennetzwerken angewendet werden können. Die zuvor erstellten Ergebnisse werden hier an einem realitätsnahen Firmennetz gemeinsam angewendet und eine beispielhafte modellbasierte Administration der Sicherheitsdienste dieses Firmennetzes vorgenommen.

Im Anschluss an diese Einführung wird eine Übersicht über Sicherheitsdienste, Verfahren und Produkte gegeben.