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

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]

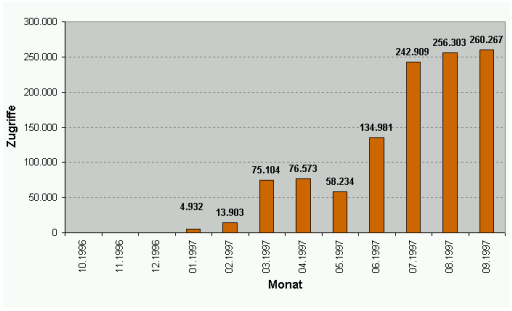

Abbildung 1: [Sie03] Zugriffsstatistik 1996/1997

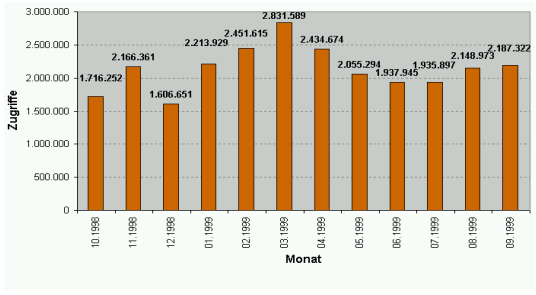

Abbildung 2: [Sie03] Zugriffsstatistik 1998/1999

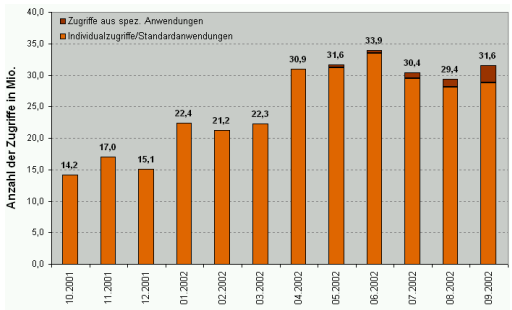

Abbildung 3: [Sie03] Zugriffsstatistik 2001/2002

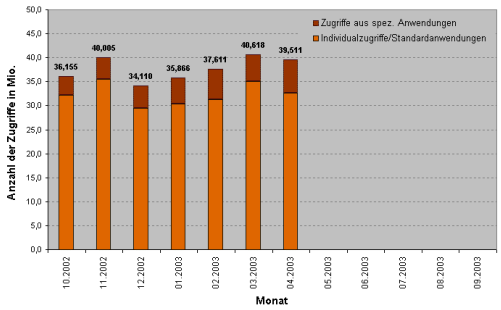

Abbildung 4: [Sie03] Zugriffsstatistik bis April 2003

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 trotzt 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.