

Firewall-Management im Rahmen einer Prozessorganisation

Dissertation

zur Erlangung des akademischen Grades
des Doktors der Naturwissenschaften
am Fachbereich IV der Universität Trier

vorgelegt von

Diplom-Wirtschaftsinformatiker
THOMAS WAGNER

August 2009

*God, give us grace to accept with serenity
the things that cannot be changed, courage
to change the things which should be changed,
and the wisdom to distinguish the one from the other.*

Karl Paul Reinhold Niebuhr,
amerikanischer Theologe (1892-1971)

Zusammenfassung

Bedingt durch die Dynamik globaler Märkte wird Information zu einem zunehmend wertvollen Produktionsfaktor wissensgesteuerter Industrien. Die hochgradige Abhängigkeit ganzer Geschäftsprozesse von Informationen (und deren Austausch) ist in der heutigen „digitalen Welt“ unweigerlich verbunden mit der Abhängigkeit von einer funktionierenden Informationstechnik, die sämtliche Prozesse mit (Geschäfts-)Daten versorgt.

Ähnlich einer Tresortür müssen daher auch die „virtuellen Türen“ zwischen dem Internet und dem eigenen Unternehmensnetz (z.B. vor Angreifern) hinreichend geschützt werden. Die Firewall als eine Art „digitaler Torwächter“ hat sich mittlerweile als eines der umfassendsten, aber auch komplexesten Standardmittel der IT-Sicherheit etabliert, deren Pflege und Wartung in vielen Unternehmen zur Herausforderung wird. Speziell Firewalls mit großen Regelwerken können mit der vom Markt geforderten Flexibilität, die sich oft in einer hohen Änderungshäufigkeit widerspiegelt, nicht Schritt halten. Gerade deshalb ist ein effizientes Firewall-Management unverzichtbar.

Die vorliegende Arbeit setzt auf den Erkenntnissen der Studie des Autors zum Thema „Firewall Management Optimierung in Banken“ auf und analysiert zunächst den „State-of-the-Art“ im Firewall-Management. Der Fokus liegt hierbei auf dem für die Flexibilität eines Unternehmens so wichtigen Firewall-Änderungsprozess, der anschließend mit Hilfe geeigneter Kennzahlen gemessen und bewertet wird. Dabei stellt sich heraus, dass dieser Prozess (insbesondere hinsichtlich der langen Durchlaufzeit von Firewall-Änderungen) in vielen der befragten Unternehmen stark verbesserungsbedürftig ist.

Es wird gezeigt, wie dessen Optimierungspotential mit Hilfe unterschiedlicher Optimierungsmethoden — vor allem durch das Automatisieren von Prozessschritten — ausgeschöpft werden kann. Dadurch ist es möglich, den Änderungsprozess wesentlich effizienter zu gestalten, als er heute in der Praxis „gelebt“ wird.

Abstract

Driven by the dynamics of global markets, information is growing to a more and more valuable production factor for knowledge-driven industries. In today's digital world, business processes' tremendous dependance on information (exchange) is inevitably linked to a dependance on an effective operation of IT systems. Those systems provide processes with almost all relevant business data.

Similar to a vault's door, the "virtual gates" between the Internet and a company's internal network must be adequately protected (e.g. against attackers). By now, firewalls as „digital doormen“ evolved to an effective but complex IT security standard instrument whose management and maintenance effort, however, is a challenge to many companies. Especially firewalls with large rulesets are unable to satisfy the market-driven demands on flexibility, that usually leads to a high change frequency. Therefore, an efficient firewall management is indispensable.

The present research thesis is based upon its author's firewall study: "Firewall Management Optimisation in Banks" and initially examines the state-of-the-art in firewall management. Here, the focus is on the firewall change process which is essential to a company's flexibility. Subsequently, this process will be measured and evaluated by capable key figures and will finally turn out to be highly inefficient (particularly concerning long runtimes of firewall changes) in many of the respondents' companies.

By applying different optimisation steps — primarily by automation of process elements — we will see how the room for improvement can be exploited in order to generate a far more efficient process than what is used today in practice.

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation	1
1.2	Ausgangssituation — Wandel zur Informationsgesellschaft	2
1.3	Zielstellung und Aufbau der Arbeit	6
2	Bedeutung der IT-Sicherheit für die Geschäftsprozesse	8
2.1	Das Unternehmen als Prozessorganisation	8
2.1.1	Wandel in der Organisationstheorie	8
2.1.2	Übergang zur Prozessorganisation	11
2.1.3	Das Konzept der Prozessorientierung	12
2.1.4	Die Rolle der IT in der Prozessorganisation	15
2.2	IT-Sicherheit zum Schutz der Prozesse	18
2.2.1	Rahmenbedingungen der IT-Sicherheit	18
2.2.2	IT-Sicherheitsziele	19
2.2.2.1	Verfügbarkeit	19
2.2.2.2	Integrität	20
2.2.2.3	Vertraulichkeit	21
2.3	Schwachstellen und Bedrohungen	21
2.3.1	Allgemeine Fehler und Schwachstellen	22
2.3.2	Bedrohungsklassen	23
2.3.2.1	Höhere Gewalt	24
2.3.2.2	Organisatorische Mängel	24
2.3.2.3	Menschliches Fehlverhalten	25
2.3.2.4	Technisches Versagen	25
2.3.2.5	Vorsätzliche Handlung	26
2.4	Schutzbedarf	27
2.4.1	Ermittlung des Schutzbedarfs	27
2.4.1.1	Identifikation der Schutzobjekte	28
2.4.1.2	Schutzbedarfskategorien	30
2.4.1.3	Zonen mit unterschiedlichem Schutzbedarf	34
2.4.2	Schadenspotential — Wert der Schutzobjekte	35
2.4.2.1	Verluste allgemein	35
2.4.2.2	Daten als Schutzobjekte	36
2.4.2.3	Kosten und Nutzen der IT-Sicherheit	36
2.5	Schutzmaßnahmen	38

2.5.1	Kategorisierung von Sicherheitsmaßnahmen	38
2.5.2	Ausgewählte (technische) Maßnahmen	39
2.6	Zusammenfassung	42
3	Die Firewall als zentrales Element einer IT-Sicherheitsinfrastruktur	43
3.1	Die Firewall — Definition und Einführung	43
3.1.1	Definition: Firewall	44
3.1.2	Die Firewall als Zugangskontrollsystem	45
3.1.3	Die Firewall als Kontroll- und Überwachungssystem	47
3.2	Arten von Firewalls	47
3.2.1	Paketfilter (statische Filter)	48
3.2.2	Stateful Inspection Filter (dynamische Filter)	49
3.2.3	Circuit Level Gateways (Transportschicht-Gateways)	50
3.2.4	Application Level Gateways	51
3.2.5	Hybride Firewalls	51
3.3	Die Policy — „Gehirn“ einer Firewall	52
3.3.1	Aufbau und Funktionsweise einer Firewall-Policy	52
3.3.2	Dynamik eines Firewall-Regelwerkes	55
3.3.3	Komplexität eines Firewall-Regelwerkes	56
3.4	Der Firewall-Änderungsprozess	58
3.4.1	Einleitung — Beispiel einer Firewall-Änderung	58
3.4.2	Theoretische Ansätze zum Änderungsprozess	59
3.4.3	Change Management im ITIL Framework	61
3.4.3.1	Einleitung ITIL Framework	61
3.4.3.2	Change Management — Definition und Ziele	62
3.4.3.3	Der ITIL Change Prozess	63
3.4.3.4	RFC — Request for Change	66
3.4.3.5	Change Rollen	69
3.4.3.6	Genehmigung	70
3.4.4	Firewall und ITIL Change Management	72
3.5	Zusammenfassung	74
4	Untersuchung der Ist-Situation — Firewall-Studie im Bankensektor	76
4.1	Erfassung der Ist-Situation	76
4.1.1	Untersuchungsgegenstand	77
4.1.2	Analyseobjekt: Bankensektor	79
4.2	Ergebnisse und Auswertungen der Studie	81
4.2.1	Ausgangssituation im ausgewählten Analysebereich	81
4.2.1.1	Mitarbeiter-Verhältnis und Firewall-Betreuung	81
4.2.1.2	Verantwortung für die Firewall	82
4.2.1.3	Ansprechpartner für Firewall-Änderungen	83
4.2.1.4	Durchschnittliche Größe des Regelwerkes	84
4.2.1.5	Outsourcing	84
4.2.1.6	Die Änderungshäufigkeit einer Unternehmensfirewall	85

4.2.1.7	Zusammenfassung der Firewall-Rahmenbedingungen	86
4.2.2	Abläufe und Rollen im Firewall Change Prozess	87
4.2.2.1	Erstellen der Anfrage	87
4.2.2.2	Formalisierung der Anfrage	88
4.2.2.3	Vervollständigung fehlender Informationen	89
4.2.2.4	Risikobewertung der Anfrage	89
4.2.2.5	Genehmigung der Änderung	92
4.2.2.6	Umsetzung der Änderung in der Firewall	93
4.2.2.7	Rückmeldung an den Antragsteller	96
4.2.2.8	Kontrolle der Änderungen	96
4.2.3	Dokumentation der Änderungen	97
4.2.3.1	Dokumentation des jeweiligen RFC	98
4.2.3.2	Hilfsmittel zur Dokumentation	99
4.2.4	Schnittstellenprobleme und Durchlaufzeit	100
4.2.4.1	Schnittstellenprobleme zwischen IT- und Fachabteilungen	100
4.2.4.2	Prozesslaufzeit — Dauer einer Änderung	102
4.3	Modellierung des Firewall Change Prozesses	103
4.3.1	Modellierungsgrundlagen	104
4.3.2	Allgemeiner Change-Prozess	105
4.4	Zusammenfassung — Firewall-Studie	108
5	Analyse des ermittelten Firewall Change Prozesses	109
5.1	Einführung	109
5.1.1	Vorgehensweise	109
5.1.2	Eigenschaften von Kennzahlen	111
5.2	Prozessbewertung durch Prozesskennzahlen	112
5.2.1	Kennzahl: Durchlaufzeit	114
5.2.1.1	Laufzeitberechnung serieller Pfade	115
5.2.1.2	Laufzeitberechnung verzweigter Pfade	116
5.2.1.3	Berechnung der Gesamt-Durchlaufzeit	121
5.2.2	Kennzahlen: Eingehende RFC (insgesamt und pro Mitarbeiter im Firewall-Team)	129
5.2.3	Kennzahlen: Umgesetzte und abgelehnte RFC	129
5.2.4	Kennzahl: Anzahl vollständiger RFC	131
5.2.5	Kennzahl: Fehlerquote der Umsetzung	131
5.2.6	Übersicht über die ermittelten Kennzahlen	132
5.3	Prozessmodellkennzahlen	133
5.3.1	Kennzahl: Parallelität (Kohäsion)	133
5.3.2	Kennzahl: Koordinationsbedarf (Anzahl der Schnittstellen)	134
5.3.3	Kennzahl: Varianz (Entscheidungsfrequenz)	134
5.3.4	Kennzahl: Aktivitätenkomplexität	135
5.3.5	Übersicht über die Prozessmodellkennzahlen	136
5.4	Theoretische Ansätze zur Laufzeitoptimierung	137
5.4.1	Prozesslaufzeit als Funktion	137

5.4.2	Variable Verzweigungswahrscheinlichkeiten	138
5.4.2.1	Laufzeit in Abhängigkeit von p_1	138
5.4.2.2	Laufzeit in Abhängigkeit von p_2 , p_3 und p_4	139
6	Optimierung des Firewall Change Prozesses	143
6.1	Einführung und Vorgehensweise	143
6.2	Optimierung der ermittelten Kennzahlen	146
6.2.1	Zusammenfassen und Elimination von Aktivitäten	146
6.2.1.1	Zusammenlegung und Elimination im Firewall-Änderungsprozess	147
6.2.1.2	Auswirkung der Zusammenlegung auf die Gesamtlaufzeit	149
6.2.2	Parallelisieren	150
6.2.2.1	Voraussetzungen für die Parallelisierung	150
6.2.2.2	Die Design-Struktur-Matrix als Analyseinstrument	151
6.2.2.3	Parallelisierung im Firewall-Änderungsprozess	152
6.2.2.4	Untersuchung des Teilprozesses T_2	154
6.2.2.5	Auswirkung der Parallelisierung auf die Gesamtlaufzeit	156
6.2.3	Outsourcing und Standardisierung	156
6.2.3.1	Outsourcing im Firewall-Änderungsprozess	158
6.2.3.2	Auswirkung des Outsourcings auf die Gesamtlaufzeit	159
6.2.4	Automatisierung	160
6.2.4.1	Voraussetzungen für die Automatisierung	160
6.2.4.2	Workflow-Systeme — Einführung	161
6.2.4.3	Workflow-Systeme — Definition	162
6.2.4.4	Unterstützung durch ein Workflow-Tool	165
6.2.4.4.1	Elektronisch-formalisierte Erfassung	165
6.2.4.4.2	Unterstützung der Risiko- und Compliance-Prüfung	167
6.2.4.4.3	Unterstützung des Genehmigungsprozesses	169
6.2.4.4.4	Verbesserung der Umsetzung und Kontrolle	169
6.2.4.4.5	Automatisierte Dokumentation	170
6.2.4.4.6	Anpassen der Anfrage	170
6.2.4.5	Auswirkungen der Automatisierung	171
6.2.4.6	Zusammenfassung: Automatisierung	178
6.3	Zusammenfassung der Optimierungsschritte	180
6.3.1	Verbesserung der Prozesskennzahlen	180
6.3.1.1	Kennzahl: Durchlaufzeit	180
6.3.1.2	Kennzahl: Anzahl eingehender RFC	185
6.3.1.3	Kennzahl: Umgesetzte und abgelehnte RFC	185
6.3.1.4	Kennzahl: Anzahl vollständiger RFC	186
6.3.1.5	Kennzahl: Fehlerquote bei der Umsetzung	186
6.3.2	Prozessmodellkennzahlen	186
6.3.2.1	Kennzahl: Parallelität (Kohäsion)	187
6.3.2.2	Kennzahl: Koordinationsbedarf	187

6.3.2.3	Kennzahl: Varianz (Entscheidungsfrequenz)	187
6.3.2.4	Kennzahl: Aktivitätenkomplexität	188
6.3.3	Übersicht über die verbesserten Kennzahlen	189
7	Fazit	191
7.1	Zusammenfassung	191
7.2	Handlungsempfehlungen für Unternehmen	192
7.3	Ausblick und weitere Forschungsarbeit	194
A	Internet Grundlagen	196
A.1	Glossar der Netzwerktechnik	196
A.2	Komplexität einer Firewall-Änderung	201
A.3	Übersicht bekannter TCP/IP Ports	203
B	Firewall-Studie	204
B.1	Durchführung	204
B.2	Übersicht der befragten Banken	205
C	ITIL	206
C.1	Ablauf des ITIL Standard-Changes	206
C.2	Genehmigung	207
D	Laufzeitberechnung	209
D.1	Beweis zum Infimum vom $h(p_2, p_3, p_4)$	209
D.2	Laufzeitberechnung mit variablem p_4	210
D.3	Einfluss der Einzeldurchlaufzeiten auf D_{ges}	212
E	Prozessmodelle	213
E.1	„Swim Lane“-Transitionen	213
E.2	„Swim Lane“-Prozessmodell	214
E.3	„Swim Lane“-Prozessmodell — optimiert	215
E.4	Allgemeines Prozessmodell	216
E.5	Allgemeines Prozessmodell — vereinfacht	217
E.6	Allgemeines Prozessmodell — optimiert	218

Abbildungsverzeichnis

1.1	Neue Rahmenbedingungen unter dem Einfluss der IuK	4
2.1	Unterschied zwischen der funktionalen und der prozessorientierten Organisationsgestaltung	10
2.2	Wechselwirkung zwischen Geschäftsprozessen und der IT	16
2.3	Ermittlung des Schutzbedarfs und der eingesetzten Maßnahmen	28
2.4	Durchschnittliche Verluste pro Teilnehmer (1999-2008)	35
2.5	Aufwand-Nutzen Verhältnis für IT-Sicherheit	37
3.1	Protokolle im TCP/IP Stapel	48
3.2	Paketfilter im TCP/IP Schichtenmodell	49
3.3	Relaisstation (Proxy) — Schema	50
3.4	Application Layer Gateway im TCP/IP Schichtenmodell	51
3.5	Grundlegendes Change Management Verfahren nach ITIL	67
4.1	Unternehmensgröße	81
4.2	Firewall-Betreuer	81
4.3	Verantwortungsträger für die Firewall	82
4.4	Ansprechpartner für Firewall-Änderungen	83
4.5	Firewall-Regeln (LU)	84
4.6	Firewall-Regeln (DE)	84
4.7	Ausgliederte Teile des Firewall-Managements	85
4.8	Anfallende Änderungsanfragen pro Monat	86
4.9	Berechtigte Rollen zur Erstellung eines RFC	88
4.10	Formalisierungsgrad einer Firewall-Änderungsanfrage	88
4.11	Instanz zur Risiko-Beurteilung einer Änderungsanfrage	92
4.12	Wie werden neue Freischaltungen in der Firewall eingefügt?	95
4.13	Wer informiert den Antragsteller?	96
4.14	Änderungskontrolle LU	97
4.15	Änderungskontrolle DE	97
4.16	In Änderungsanfragen dokumentierte Angaben	98
4.17	Hilfsmittel zur Dokumentation der Firewall-Regeln	99
4.18	Schnittstellenprobleme (Deutschland)	101
4.19	Durchschnittliche Dauer zur Umsetzung einer Änderungsanfrage	102
4.20	Modellierung des Firewall Change-Prozesses	107
5.1	Regelkreis einer kontinuierlichen Prozessverbesserung	110

5.2	Teilprozess T_1 — „Aufnahme der Anfrage“	115
5.3	Beispiel: Auftragsfertigung Schreinerei	117
5.4	Teilprozess T_4 — „Umsetzung, Kontrolle und Dokumentation“	118
5.5	Firewall-Änderungsprozess (vereinfachte Darstellung)	123
5.6	Teilprozess T_2 : Risiko- und Compliance-Prüfung	125
5.7	Durchlaufzeit in Abhängigkeit von p_1	139
5.8	Durchlaufzeit in Abhängigkeit von $p_2 = p_3$ und p_4	140
6.1	Beziehungen von Aktivitäten in einem DSM	151
6.2	Informationsbeziehungen in Firewall Change-Prozess	152
6.3	Parallelisierter Teilprozess T2: „Risiko- und Compliance-Prüfung“	155
6.4	Ablauf und Verteilung im Workflow	163
6.5	Aufbau eines Workflow-Mangement-Systems	164
6.6	Informationsabfrage aus einer Inventardatenbank	166
C.1	Change Ablauf für einen Standard-Change	206
C.2	Beispiel eines möglichen Genehmigungsprozesses	207
D.1	$f(p_2, p_3, p_4)$ mit $p_4=0,2$	210
D.2	$f(p_2, p_3, p_4)$ mit $p_4=0,3$	210
D.3	$f(p_2, p_3, p_4)$ mit $p_4=0,4$	210
D.4	$f(p_2, p_3, p_4)$ mit $p_4=0,5$	210
D.5	$f(p_2, p_3, p_4)$ mit $p_4=0,6$	211
D.6	$f(p_2, p_3, p_4)$ mit $p_4=0,7$	211
D.7	$f(p_2, p_3, p_4)$ mit $p_4=0,8$	211
D.8	$f(p_2, p_3, p_4)$ mit $p_4=0,9$	211
E.1	Prozessmodell mit „Swim Lanes“	214
E.2	Optimiertes Prozessmodell mit „Swim Lanes“	215
E.3	Modellierung des Firewall Change-Prozesses	216
E.4	Firewall Change-Prozess — vereinfachte Darstellung	217
E.5	Optimiertes Prozessmodell	218

Tabellenverzeichnis

1.1	Untersuchungsaspekte	7
2.1	Definition: „Prozess“	12
2.2	Definition: „Geschäftsprozess“	13
2.3	Mögliche Gruppierungen von Schutzobjekten	30
2.4	Mögliche Einteilung der Schutzbedarfskategorien	31
2.5	Schutzbedarfsermittlung für Software und Daten	32
2.6	Schutzbedarfsermittlung für Hardware	32
2.7	Schutzbedarfsermittlung für bauliche Elemente	33
2.8	Schutzbedarfsermittlung für Verbindungen	33
2.9	Schutzobjekt: Daten — Wert aller Daten	36
2.10	Von den Befragten eingesetzte Sicherheitstechnik	39
2.11	Firewall und Anti-Virus Software als Standardmittel der IT-Sicherheit	40
2.12	Effektivität bewährter Schutzmaßnahmen zur Abwehr weit verbreite- ter Bedrohungen	41
3.1	Attribute eines RFC (nach ITIL)	68
3.2	Übertragung des ITIL Änderungsablaufs auf Firewall-Änderungen . .	72
3.3	Zusätzliche Attribute eines Firewall-RFC	73
4.1	Elemente ereignisgesteuerter Prozessketten (EPK)	104
4.2	Regeln zur Ausführung des Firewall Change Requests	106
5.1	Kennzahlengruppen und Kennzahlen	114
5.2	Laufzeiten der Einzelaktivitäten (in Minuten)	122
5.3	Pfadwahrscheinlichkeiten der XODER-Verzweigungen	124
5.4	Laufzeiten der Aktivitäten für T_4	126
5.5	Kennzahlengruppen und Kennzahlen — Ergebnisse	132
5.6	Übersicht über die Prozessmodellkennzahlen	136
6.1	Übersichtsmatrix für die potentielle Zusammenlegung von Aktivitäten	147
6.2	Gründe gegen eine Zusammenlegung von Aktivitäten	147
6.3	Übersichtsmatrix für den Teilprozess T_2	148
6.4	Design-Struktur-Matrix für den Firewall Change-Prozess	153
6.5	Abhängigkeiten der Aktivitäten	153
6.6	DSM für den Teilprozess T_2	155
6.7	Strategische und taktische Werte bei der Outsourcing-Entscheidung .	157

6.8	Eignung der Aktivitäten zum Outsourcing	158
6.9	Einsparung durch Outsourcing der Aktivitäten	159
6.10	Verbesserung durch die elektronisch-formalisierte RFC-Erfassung . . .	173
6.11	Unterstützung der Risiko- und Compliance-Prüfung	174
6.12	Unterstützung und Verbesserung des Genehmigungsprozesses	175
6.13	Verbesserung der Umsetzung und Kontrolle	176
6.14	Automatisierte Dokumentation	177
6.15	Verbesserung der RFC-Anpassung	178
6.16	Verbesserte Aktivitätenlaufzeiten	178
6.17	Auswirkung der geänderten Wahrscheinlichkeiten	179
6.18	Auswirkungen der einzelnen Optimierungsschritte auf die Aktivitäten	180
6.19	Kombination der Optimierungsschritte (ohne Outsourcing)	181
6.20	Kombination der Optimierungsschritte (mit Outsourcing)	182
6.21	Zusammenfassung der kumulierten Optimierungen	184
6.22	Übersicht der Prozesskennzahlen nach der Optimierung	189
6.23	Übersicht der Prozessmodellkennzahlen nach der Optimierung	189
A.1	Einige bekannte TCP/IP Portnummern und ihre Funktion	203
B.1	Die in der Firewall-Umfrage befragten Banken	205
D.1	Auswirkung der Einzellaufzeiten auf die Gesamtlaufzeit	212
E.1	allgemeines Modell	213
E.2	optimiertes Modell	213

Kapitel 1

Einleitung

*Ich habe keine besondere Begabung,
sondern bin nur leidenschaftlich neugierig.*

Albert Einstein

1.1 Motivation

In einem globalen Umfeld, in dem Märkte zusammenwachsen, Geschäfte niemals ruhen, Menschen aus nahezu allen Teilen der Erde zusammenarbeiten und Schnelligkeit ein entscheidender Erfolgsfaktor ist, wird eine Ressource zu einem immer wichtigeren Gut: Information. Wie nie zuvor wird mit Informationen gehandelt, sie entscheiden über Erfolg oder Misserfolg von Unternehmen und werden sogar als strategische Instrumente eingesetzt. Dank des Internets und der ständig steigenden Kapazität von „High-Speed“-Datenkanälen sind Informationen weltweit, jederzeit und nahezu unverzüglich verfügbar. Doch die Informationstechnik (IT), die diesen Austausch überhaupt erst möglich macht, birgt nicht nur enorme Potentiale, sondern auch viele Risiken und Gefahren.

Je stärker die Geschäftsprozesse in Unternehmen von der IT abhängen, desto größer und weitreichender kann das Ausmaß eines potentiellen Schadens sein. Besonders in Wirtschaftszweigen, in denen die Wertschöpfung zum Großteil aus Informationen besteht, sind Werte wie Verlässlichkeit und Stabilität der zugrunde liegenden IT-Systeme wichtiger denn je. Eine Störung oder Kompromittierung der IT wirkt sich letztlich auf das operative Geschäft aus und kann so zu gravierenden wirtschaftlichen Schäden führen.

Es liegt daher nahe, dass die Systeme, die einen der wichtigsten Produktionsfaktoren vieler Unternehmen speichern, verarbeiten und transportieren, in einem hinreichenden Maße geschützt werden müssen. Ebenso wie ein produzierendes Unternehmen seine Güter und Maschinen schützt, muss ein Unternehmen, dessen Kapital auf Informationen basiert, diese vor Gefahren (wie z.B. „Einbrecher“, „Spione“ und „Diebe“) bewahren. Der Unterschied besteht jedoch darin, dass diese potentiellen Täter von nahezu jedem Ort der Welt agieren können und der Transport des „Diebesgutes“ vergleichsweise einfach ist. Welche drastischen Auswirkungen z.B. der Diebstahl sen-

sibler Informationen haben kann, zeigt die sog. „Liechtenstein-Affaire“, die Anfang 2008 wochenlang die Medien beschäftigte. Der Verlust der Vertraulichkeit (eines der wichtigsten Ziele der Informationssicherheit) führte in diesem Fall zu einer Vertrauenskrise des gesamten Staates.

Unzählige Fälle von Einbrüchen und Datenspionagen zeigen immer wieder, wie unzureichend die Informationen auch heute noch geschützt sind und wie wichtig der Einsatz angemessener Schutzmaßnahmen ist.

Eine der ältesten und bis heute umfassendsten Schutzmaßnahmen stellt der Betrieb einer *Firewall*¹ dar, die Zugriffe auf das eigene Unternehmensnetz kontrolliert und so potentielle Einbrüche und unerlaubte Zugriffe abwehren kann. In der einschlägigen Literatur mangelt es dabei nicht an Anweisungen, Richtlinien und Verfahren zum Aufbau eines umfassenden Firewall-Konzepts. Die Verwaltung und der sichere Betrieb dieser kritischen Komponenten werden jedoch weitaus seltener diskutiert. Insbesondere die Pflege einer großen Unternehmensfirewall ist eine sehr komplexe Aufgabe, die tief im Aufbau und Ablauf einer Organisation verankert sein sollte. Die Bedeutung der Firewall in der unternehmerischen Gesamtsicht wird zudem oft unterschätzt. Die Konfiguration der Firewall wirkt sich auf fast alle Bereiche und Abteilungen des Unternehmens aus, sie kontrolliert den Informationsfluss sowohl zwischen dem Unternehmen und der „Außenwelt“ als auch innerhalb der Unternehmensgrenzen. Sie schützt dessen Netzwerk, dessen Systeme und dadurch letztlich auch dessen Informationen.

In einem sich ständig ändernden Umfeld ist es schwierig, die ohnehin sehr komplexen Regeln einer Unternehmensfirewall effizient und sicher zu verwalten. Die Schnelllebigkeit der Märkte zwingt die Unternehmen schneller und flexibler zu reagieren. Dieser Dynamik muss auch die Firewall nachkommen, was eine schlanke und unkomplizierte Änderungs politik erfordert. Dabei darf jedoch die Sicherheit nicht vernachlässigt werden, die bei jeder Änderungsentscheidung berücksichtigt werden muss. Ein Abwägen der Risiken erfordert allerdings häufig eine detaillierte Analyse der Auswirkungen und damit Zeit.

Sowohl in der Literatur als auch in der Praxis scheinen die diesbezüglichen Sicherheitsprozesse unzureichend untersucht zu sein. Die mit dem Firewall-Management zusammenhängenden Prozesse bergen möglicherweise ein deutliches Optimierungspotential. Die kritische Analyse des Managements dieser komplexen Sicherheitskomponenten in einer hochdynamischen Umwelt sowie die Herausarbeitung der Verbesserungsmöglichkeiten bis hin zur Vorstellung eines optimierten Prozesses, sind Ziele dieser Arbeit.

1.2 Ausgangssituation — Wandel zur Informationsgesellschaft

Die Rahmenbedingungen für Unternehmen haben sich in den letzten Jahrzehnten drastisch geändert. Durch den „Siegesszug“ der IT, die sich im Laufe des vergangenen Jahrhunderts von lagerhallengroßen Maschinen zu einer alle Lebensberei-

¹ Definition vgl.: Kap. 3.1.1.

che durchdringenden Alltagsunterstützung entwickelt hat, boten sich Unternehmen Möglichkeiten, ihre Geschäfte mit Hilfe dieser Technik zu unterstützen und in neue Geschäftsfelder vorzudringen. Kai Lehmann spricht vom „digitalen Wandel des Wissens“ in einer Welt, in der Informationen unabhängig von Grenzen und Informationsmonopolen verfügbar sind.²

Das Internet hat die Wertschöpfungskette weitgehend unabhängig von Ort und Zeit gemacht — es entstehen neue Produkte, Geschäftsprozesse und Dienstleistungen. Märkte wachsen zusammen und der globale Gedanke stellt Wettbewerber vor neue, nie da gewesene Herausforderungen.

Neben den klassischen Industrien sind hiervon vor allem solche Unternehmen betroffen, bei denen Informationen und Kapital in direktem Maße zusammenhängen: Banken. Die Globalisierung lässt Banken mehr denn je zu Mitspielern des weltweiten Finanzmarktes werden und die IT ermöglicht es, den Kunden ein breiteres Angebot und speziell auf sie zugeschnittene Produkte und Dienstleistungen zu generieren.³ Die kontrollierte Rücknahme staatlicher Eingriffe (Deregulierung) im Zusammenhang eines einheitlichen europäischen Wirtschaftsraumes und die Globalisierung durch grenzüberschreitende Aktivitäten schaffen neue Anbieterstrukturen.⁴ Die Markteintritts- und Handelsbarrieren werden durch die Informations- und Kommunikationstechnik (IuK) zunehmend abgebaut und die Branchengrenzen verwischen mehr und mehr. Viele größere Unternehmen dringen in klassische Bankbereiche vor oder gründen selbst konzerneigene Banken.⁵ Die Entstehung neuer Märkte, die Integration der Weltmärkte und die Internationalisierung von Geschäftsprozessen haben den Wettbewerb globalisiert. Damit einher gehen unter anderem kürzere Produktlebenszyklen, kürzere Reaktionszeiten sowie eine beschleunigte Wettbewerbsdynamik.⁶

Durch die Innovationen der IuK sind auch die Ansprüche der Kunden gestiegen. Neben dem Online-Banking (nicht nur von zu Hause, sondern mittlerweile auch von mobilen Endgeräten aus) sind vor allem die Erwartungen in neue Finanzdienstleistungen und individuelle Produkte gestiegen.⁷ Zudem verschwindet Dank der Technologie zunehmend die Informationsasymmetrie⁸ zwischen Kunde und Bank, was

² Vgl.: Lehmann und Schetsche (2005).

³ Vgl.: Group of Ten (2001), S. 71 u. 73.

⁴ Vgl.: Moormann (2001), S. 5. Vor dem Hintergrund der sich abzeichnenden Finanz- und Wirtschaftskrise sollte jedoch bedacht werden, dass bereits vielerseits wieder eine stärkere Regulierung gefordert wird. (Vgl. z.B.: <http://www.zeit.de/2008/07/Bankentransparenz>, <http://www.manager-magazin.de/unternehmen/artikel/0,2828,542097,00.html>, <http://www.spiegel.de/wirtschaft/0,1518,579381,00.html>.) Im Vergleich zu der von Moormann angesprochenen vorherigen Situation wird eine solche Regulierung (falls und wie auch immer sie realisiert werden würde) vermutlich eher international ausgerichtet sein.

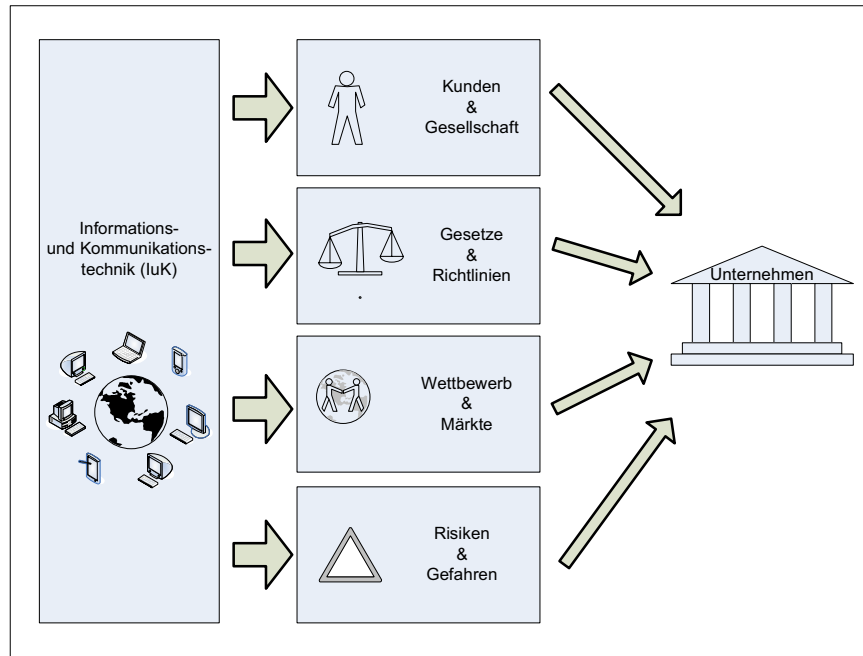
⁵ Vgl. z.B.: GE Money Bank, Mercedes-Benz Bank, Volkswagen-Bank, Postbank etc.

⁶ Vgl.: Wolf (2005), S. 9.

⁷ Vgl.: Group of Ten (2001): S. 71 u. 73.

⁸ Im klassischen Bankbetrieb verfügt der Kundenberater i.d.R. über ein spezifisches Fachwissen, welches der Kunde nicht besitzt. Es sei angenommen, die Informationsbeschaffung verursache dem Kunden gewisse Kosten. Sind diese höher als die Gebühren des Beraters, wird der Kunde versuchen, die Kosten der Informationsbeschaffung zu vermeiden und muss dann den Empfehlungen des Betreuers vertrauen. Vgl.: Krcmar (2008): *Informationsasymmetrie*.

Abbildung 1.1: Neue Rahmenbedingungen unter dem Einfluss der IuK



Quelle: Eigene Erstellung.

zu einer gesunkenen Kundenloyalität führt.⁹ Moormann spricht von einer „Emanzipation“ und einem „mehrdimensionalen Anspruchsdenken“¹⁰ der Kunden, wie z.B. hinsichtlich eines möglichst niedrigen Preises bei hoher Qualität und umfassender Dienstleistung. Die Banken stehen damit vor der Aufgabe, den neuen Ansprüchen der Kunden gerecht zu werden und gleichzeitig die Kundenbetreuung zu rationalisieren.¹¹

Im Zuge des technologischen Wandels stehen den Unternehmen nicht nur neue Möglichkeiten offen, sondern sie müssen sich auch einer Reihe neuer Gefahren und Risiken stellen. Die zunehmende Bedeutung von Information als Produktionsfaktor und als Basis zur Erringung von Wettbewerbsvorteilen zwingt Unternehmen daher zur Investition in IuK-Systeme sowie in Methoden und Techniken, diese wichtigen Ressourcen zu schützen.

Die Vernetzung birgt zusätzliche Risiken und Gefahren¹² für interne Informationssysteme der Unternehmen. Während die IT früher eine Wissenschaft war, mit der nur wenige Experten vertraut waren, gehört sie heute längst zum Alltag. Bereits in Kindergärten wird der Kontakt zwischen „Mensch und Maschine“ hergestellt und das fachspezifische IT-Wissen ist mittlerweile weit verbreitet. Auch die Kosten für die Ausrüstung stellt für einen potentiellen Angreifer kein Problem mehr dar — ein „normaler“ PC mit Internetanbindung kann mit entsprechendem „Know-How“

⁹ Vgl.: Wolf (2005), S. 8.

¹⁰ Moormann (2001), S. 6.

¹¹ Vgl.: Ebenda.

¹² Die Systeme sind auch ohne eine Vernetzung bereits gewissen Risiken (wie z.B. Viren, Ausfälle, Nach- und Fahrlässigkeit, Höhere Gewalt etc.) ausgesetzt. Vgl.: Kap. 2.3.2.

Ausgangspunkt für Angriffe von fast jedem Punkt der Erde sein.¹³

Doch mit der Technologie sind auch neue Gesetze und Vorschriften mit Bezug zur Informationsverarbeitung entstanden, die die Verantwortungspflicht der Unternehmen und deren Managern in die digitale Welt übertragen. Die Geschäftsführung eines Unternehmens ist z.B. verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Dies schließt auch die Beachtung ausreichender und anerkannter Sicherheitsmaßnahmen für das eigene Unternehmensnetz mit ein. Es existieren in Deutschland verschiedene Gesetze, aus denen sich Handlungs- und Haftungsverpflichtungen zu Risikomanagement und IT-Sicherheit ableiten.¹⁴

Als wichtigste Beispiele seien hier das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) sowie das Aktiengesetz (AktG) genannt. Daneben existieren in vielen Branchen weitere spezifische Gesetze und Vorschriften. Für die Bankenbranche stellen dabei die vom Basler Ausschuss für Bankenaufsicht entworfenen Eigenkapitalvorschriften (kurz „Basel II“)¹⁵ eine der wichtigsten Grundlagen dar. Basel II gilt seit Anfang 2007 für alle EU-Mitgliedstaaten.¹⁶

In Reaktion auf diverse Bilanzskandale¹⁷ wurde durch den Sarbanes-Oxley Act (SOX)¹⁸ im Jahr 2002 auch in den USA ein neues Gesetz zur stärkeren Regulierung des Bankenmarktes erlassen. Da alle an US-Börsen gehandelten Firmenwerte unter die Anwendung dieses Gesetzes fallen, müssen auch viele deutsche Firmen dessen Vorschriften folgen. Daraus ergeben sich z.B. spezielle Haftungs- und Kontrollpflichten, die sich nicht nur auf das Geschäft, sondern auch auf die IT auswirken.¹⁹

Die jeweilige Gesetzeslage hängt meist von der Art der Institution bzw. der von ihr betriebenen Geschäftsprozesse und Dienstleistungen ab und kann von Land zu Land variieren.²⁰ Allerdings lassen sich trotz der Vielzahl an Vorschriften keine eindeutigen und konkreten Sicherheitsanforderungen unmittelbar ableiten. Vielmehr orientiert sich die Gesetzgebung am Stand der Technik als Bewertungsgrundlage für den Grad der erreichbaren Sicherheit.²¹

¹³ Vgl.: Müller (2005), S. 1.

¹⁴ Vgl.: BSI (2008), G 2.105, S. 480.

¹⁵ Die Aspekte der IT-Sicherheit fallen hierbei unter den Punkt „Operationelles Risiko“. Diese betreffen die „Gefahr von Verlusten, die in Folge der Unangemessenheit des Versagens von internen Verfahren, Menschen und Systemen [...] eintreten“. Vgl.: BASEL II (2004).

¹⁶ Vgl.: Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates, Amtsblatt der Europäischen Union, Abschnitt L 177, S. 249. Die deutsche Umsetzung ist verankert in den Verordnungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), konkret in den „Mindestanforderungen an das Risikomanagement“ (MaRisk) und der Solvabilitätsverordnung (SolvV).

¹⁷ Als Beispiele seien die Firmen „Enron“, „Tyco International“ oder „WorldCom“ genannt, deren Finanzskandale Verluste im hohen Milliardenbereich zur Folge hatten.

¹⁸ „The Sarbanes-Oxley Act of 2002“, Pub.L. 107-204, 116 Stat. 745, 30.07.2002, vgl.: <http://www.sec.gov/about/laws/soa2002.pdf>.

¹⁹ Vgl.: Robles, u.a. (2009), S. 85f.

²⁰ Vgl.: BSI (2008), G 2.105, S. 480.

²¹ Vgl.: Ebenda, S. 481.

1.3 Zielstellung und Aufbau der Arbeit

Unter der Hypothese, das Management von Firewall-Änderungen in einer hochdynamischen Umwelt sei sowohl unzureichend erfasst als auch deutlich optimierungsfähig, besteht das Ziel dieser Arbeit in der Erfassung, Analyse und Verbesserung des bestehenden Firewall-Änderungsprozesses. Mit der Ausarbeitung konkreter Handlungsempfehlungen soll es Unternehmen ermöglicht werden, ihr Firewall-(Änderungs)Management zu verbessern, um so schneller und flexibler auf Änderungen im Umfeld der IT-Landschaft zu reagieren.

Im ersten Schritt (Kapitel zwei) ist es dazu wichtig, die Bedeutung der IT speziell für die Geschäftsprozesse zu unterstreichen. Da die Geschäftsprozesse im Wesentlichen auf Informationen basieren, die durch die IT-Systeme transportiert, verarbeitet und gespeichert werden, ist der Schutz dieser Systeme unerlässlich. Um adäquate Schutzmaßnahmen anwenden zu können, müssen zunächst die Bedrohungen und Gefahren für die IT-Landschaft klassifiziert und die potentielle Schadensausmaße quantifiziert werden. In diesem Zusammenhang wird sich die Firewall als eines der effektivsten und komplexesten Standard-Mittel der IT-Sicherheit herausstellen.

Kapitel drei beschreibt die Grundlagen und die Arbeitsweise von Firewalls. Als „Gehirn“ der Firewall erweist sich die Policy nicht nur als ein sehr komplexes Konfigurationsinstrument, sondern unterliegt, bedingt durch verschiedene externe und interne Einflüsse, einem ständigen Wandel. Die Auslöser von Dynamik und Komplexität werden vorgestellt. Von zentraler Bedeutung ist hierbei der Firewall-Änderungsprozess, der vor dem Hintergrund bestehender Ansätze und Empfehlungen der Literatur diskutiert wird.

Zur Feststellung der Ist-Situation des Firewall-Managements wurde eine Firewall-Studie im Bankenumfeld durchgeführt. Diese Studie hatte die Erfassung der „Best Practices“ sowie des allgemeinen „State-of-the-Art“ des Firewall-Managements zum Ziel. Kapitel vier fasst die wichtigsten Aussagen der Studie zusammen, mit Hilfe derer ein allgemeiner Firewall-Änderungsprozess modelliert werden kann. Dieser Prozess dient als Ausgangsbasis für die weiteren Untersuchungen.

Eine kritische Analyse und Bewertung des modellierten Prozesses ist nur dann sinnvoll möglich, wenn bestimmte Eigenschaften gemessen (und später verglichen) werden können. Kapitel fünf befasst sich deshalb mit der Erfassung von Kennzahlen, die Eigenschaften wie z.B. Prozessqualität, -produktivität und -effizienz quantifizieren. Das Hauptaugenmerk liegt dabei auf der Gesamtdurchlaufzeit als wichtigste Kennzahl der Prozesseffizienz. Die Ermittlung der Kennzahlen ist eine notwendige Voraussetzung, um die Effektivität von Optimierungsschritten bewerten zu können. Eine mathematische Betrachtung der Prozess-Laufzeit sowie die Ermittlung der theoretisch minimalen Laufzeit schließt das Kapitel ab.

Die eigentliche Optimierung des Prozesses erfolgt im sechsten Kapitel. Den Empfehlungen der Fachliteratur²² folgend, werden verschiedene Optimierungsschritte auf den Firewall-Änderungsprozess angewandt und deren Auswirkungen (bzw. Verbesserungspotentiale) mit Hilfe der Prozesskennzahlen gemessen. Die Optimierung fokussiert sich hauptsächlich auf die Prozesslaufzeit, wobei zunächst Auswirkungen

²² Vgl.: Kap. 6.1.

der einzelnen Optimierungsschritte isoliert betrachtet werden, bevor diese im Rahmen ihrer praktischen Realisierbarkeit miteinander kombiniert werden. Abschließend wird der optimierte Firewall-Änderungsprozess vorgestellt und die verbesserten Kennzahlen werden mit denen der Ist-Situation verglichen.

Das siebte und letzte Kapitel fasst die Ergebnisse der Untersuchung zusammen und bezieht sich dabei auf die Ausgangshypothese. Mit konkreten Handlungsempfehlungen werden (basierend auf den Ergebnissen des Untersuchungshergangs) zusammenfassend Maßnahmen vorgeschlagen, mit denen Unternehmen ihr eigenes Firewall Change²³ Management (teilweise sehr deutlich) verbessern können. Ein kritischer Ausblick mit Vorschlägen zu weiterer Forschungsarbeit schließt die vorliegende Arbeit ab. Tabelle 1.1 fasst die einzelnen Untersuchungsaspekte zusammen.

Tabelle 1.1: Untersuchungsaspekte

Kap.	Hauptaspekt	Untersuchungsaspekte
2	Grundlagen und Bedeutung der IT-Sicherheit	<ul style="list-style-type: none"> • Bedeutung der IT(-Sicherheit) für die Geschäftsprozesse • Bedrohungen für die Unternehmensgüter (allgemein) • Schutzbedarf (schützenswerte Objekte) • Schadenspotential (in Zahlen) • Effektive Maßnahmen und Mittel zum Schutz vor diesen Bedrohungen (Firewall als effektive Schutzmaßnahme)
3	Grundlagen zum Firewall (Change) Management	<ul style="list-style-type: none"> • Erfassung der Wichtigkeit einer Firewall für die IT sowie die darauf basierenden Geschäftsprozesse • Firewall-Änderungen und der Änderungsprozess • Untersuchung der Literaturempfehlungen zu Best Practices im Firewall-Änderungsmanagement
4	Erfassung des Ist-Zustandes	<ul style="list-style-type: none"> • Auswertung der Firewall-Umfrage • Feststellung des Change-Prozesses • Modellierung des Change-Prozesses
5	Untersuchung des Ist-Prozesses	<ul style="list-style-type: none"> • Auswahl und Bestimmung der Prozesskennzahlen • Auswahl und Bestimmung der Prozessmodellkennzahlen
6	Optimierung des erfassten und bewerteten Firewall Change-Prozesses	<ul style="list-style-type: none"> • Bestimmung der Optimierungsschritte • Verbesserung der Prozesskennzahlen • Verbesserung der Prozessmodellkennzahlen • Konsolidierung der einzelnen Schritte
7	Schlussfolgerungen	<ul style="list-style-type: none"> • Handlungsempfehlungen für Unternehmen • Weitere Forschungsarbeit

Quelle: Eigene Erstellung.

²³ Der Begriff „Änderung“ und der aus der englischsprachigen Fachliteratur stammende Begriff „Change“ werden im Folgenden synonym verwendet.

Kapitel 4

Untersuchung der Ist-Situation — Firewall-Studie im Bankensektor¹

*Wenn du eine weise Antwort verlangst,
musst du vernünftig fragen.*

Johann Wolfgang von Goethe

4.1 Erfassung der Ist-Situation

Firewalls haben sich längst als zentrales und effektives IT-Sicherheitsselement zum Schutz des eigenen Netzwerkes etabliert. Im vorigen Kapitel wurde gezeigt, dass der Betrieb und die Pflege einer Unternehmensfirewall einen sehr komplexen und dynamischen Prozess bilden. In der Literatur werden zwar grundlegende Verfahren zum Aufbau oder zur Validierung einschlägiger IT-Sicherheitsstrategien diskutiert, jedoch fehlen konkrete Praktiken und Empfehlungen zum effektiven Firewall-Management.² Interne Richtlinien und Vorgehensweisen zum Firewall-Management sind sicherheitstechnisch äußerst sensibel. Kaum ein Unternehmen ist daher geneigt, Informationen zu Management-Prozessen ihrer Sicherheitspolitik öffentlich preis zu geben, insbesondere wenn es sich um eine sensible Kernkomponente der Sicherheitsarchitektur wie die Firewall handelt. Unternehmen (speziell solche, deren Informationen einem hochgradigen Schutzbedarf unterliegen) geben demzufolge nur sehr wenige, lückenhafte oder veraltete Informationen nach außen. Die Zurückhaltung dieser Informationen ist aus Sicherheitsgründen durchaus nachvollziehbar (und z.T. auch berechtigt³), verhindert jedoch andererseits auch eine wissenschaftliche Untersuchung sowie eine dadurch ggf. mögliche Optimierung bestehender Prozesse. Der Mangel an verwertbaren und aktuellen Informationen legt eine genauere Untersuchung des „State-of-the-Art“ im Firewall-Management in Unternehmen mit stark schutzbedürftigen Informationsbeständen nahe.

¹ Teile dieses Kapitels wurden bereits veröffentlicht in: Wagner (2007).

² Vgl.: Kap. 3.4.2.

³ Der Austausch mit Kollegen anderer Unternehmen kann jedoch durchaus hilfreich sein.

Vor dem Hintergrund dieser Probleme wurde vom Autor der vorliegenden Arbeit eine Studie zum Firewall-Management in Banken durchgeführt. Die Studie hatte zum Ziel, Informationen zum Ist-Zustand des Firewall-Managements in Unternehmen zu finden, deren Daten eine hohe Sensibilität und daher einen hohen Schutzbedarf aufweisen. Im weiteren Verlauf der Arbeit soll zunächst die Ist-Situation erfasst werden, bevor diese auf mögliches Optimierungspotential untersucht werden kann.

4.1.1 Untersuchungsgegenstand

In Kapitel 3.4.3.6 wurde verdeutlicht, dass am Firewall-Management-Prozess viele Personen aus unterschiedlichen Abteilungen beteiligt sind. Soll ein Mitarbeiter beispielsweise Zugriff auf das Internet über eine spezielle Anwendung erhalten, ist in der Regel eine Freischaltung in der Firewall erforderlich. Vermutlich wird sich der Mitarbeiter zunächst an seinen Vorgesetzten (oder an einen dedizierten Betreuer der entsprechenden Applikation) wenden, um den Änderungswunsch vorzubringen. Der Änderungsantrag muss dann geprüft, genehmigt und schließlich getestet werden. Bei der Umsetzung müssen Aspekte wie Aufbau und Strukturierung des Regelwerkes berücksichtigt werden, damit dieses auch nach zahlreichen Änderungen für die jeweiligen Administratoren überschaubar bleibt und keine ungewollten „Cross-Zugriffe“ entstehen.⁴

Zur Gewährleistung der Nachvollziehbarkeit muss jede Änderung letztlich so weit dokumentiert werden, dass auch im Nachhinein alle relevanten Informationen (wie z.B. der Antragsteller, die Art und der Zweck der Änderung, sowie die am Genehmigungsprozess beteiligten Personen) erhalten bleiben. Im Idealfall sollten Regelwerk, Genehmigung und Umsetzung aller Änderungen vollständig protokolliert sein, so dass für jeden Zugriff eine schriftliche Historie mit allen wichtigen Informationen existiert.

Neben diesen Aspekten sind auch die Rahmenbedingungen, unter welchen eine Firewall betrieben wird, wichtige Untersuchungsobjekte. Hierzu gehören u.a. die Größe der betrachteten Regelwerke, die Dauer des Änderungsvorgangs, die Restriktivität und die Abbildungsschärfe des Netzes im Firewall-Regelwerk sowie die Rollenverteilung und Verantwortlichkeiten im Firewall-Management.

In der durchgeführten Studie wurden sechs Untersuchungsbereiche definiert, deren Ziel und Intention im Folgenden kurz erläutert werden.

1. Ausgangssituation im ausgewählten Analysebereich

Ziel des einleitenden Frageblocks war es, die generelle Situation im betroffenen Standort zu hinterfragen. Hierbei waren neben primären Größen wie Mitarbeiterzahl, Größe des Firewall-Teams oder die Anzahl der Firewall-Regeln auch die grundlegende Verankerung der Firewall-Verantwortung im Unternehmen von besonderem Interesse. Aspekte der Kompetenzen sind nicht nur in der Kontrolle der Zugriffsrechte enthalten, sondern zeichnen sich auch durch den Grad der nach außen gegebenen Zuständigkeiten aus. Daher sollte festgestellt

⁴ Vgl.: Beispiel zur Umsetzung einer Firewall-Änderung im Anhang A.2.

werden, ob und in welchem Maße außenstehende Personen am Prozess des Firewall-Managements beteiligt sind.

2. Abläufe und Rollen im Firewall-Änderungsmanagement

Im darauf folgenden Teil stand der Firewall-Änderungsprozess im Vordergrund. Ziel war es, einen umfassenden Einblick in den Ablauf von Firewall-Änderungen mit allen beteiligten Instanzen, Personen und Praktiken zu erhalten. Dieser Änderungsprozess steht im Zentrum des weiteren Untersuchungsergebnisses. In den Kapiteln fünf und sechs soll dieser Prozess näher analysiert und schließlich mit Hilfe geeigneter Optimierungsschritte verbessert werden.

3. Prozessschnittstellen und Prozessablauf im Change Management

Zur Analyse des Änderungsprozesses sind neben den Durchlaufzeiten der einzelnen Aktivitäten auch mögliche Probleme an den Prozessschnittstellen (wie zum Beispiel zwischen Fach- und IT-Abteilung) von Interesse. Treten dort häufig Probleme auf, kann dies den Prozess verzögern. Bei einer Optimierung müssen daher die potentiellen Probleme möglichst beseitigt werden (z.B. durch einen hohen Grad an Standardisierung). Die entsprechenden Fragen der Firewall-Studie dienten der Untersuchung dieser Probleme und der damit zusammenhängenden Laufzeit.

4. Wartung und Pflege des bestehenden Regelwerkes

Im vierten Teil des Fragebogens wurde untersucht, wie die Banken die Komplexität ihrer Firewall-Regeln in Grenzen halten. Die Umwelt der Firewall unterliegt einem ständigen Wandel. Die Belegschaft fluktuiert, Abteilungen fusionieren oder werden aufgelöst, Hard- und Softwarekomponenten werden ersetzt, Prozesse optimiert und Abläufe geändert. Die Änderungen an der Firewall sind ein Zeugnis dieser sich ständig ändernden Umwelt. Damit die Firewall mit dieser Dynamik Schritt halten kann und nicht zu einem unüberschaubaren, „historisch gewachsenen“ Gebilde mutiert, müssen Änderungen koordiniert und das Regelwerk in gewissen Abständen einem technischen Review unterzogen werden. Darüber hinaus müssen nicht mehr benötigte Zugriffe sowie sicherheitskritische Regeln identifiziert und möglichst eliminiert werden.⁵ Hinsichtlich einer Optimierung ist die Suche nach logisch gruppierbaren Regeln sinnvoll, um dem ständig wachsenden Regelwerk entgegenzuwirken.⁶

5. Nachvollziehbarkeit und Dokumentation

Eine hinreichende Dokumentation ist unverzichtbar, um sowohl bei regelmäßiger Revision, als auch bei allgemein auftretenden Problemen und Änderungen die Nachvollziehbarkeit zu gewährleisten.⁷ Ebenso wie jeder Regel in der Firewall bestimmte Informationen (z.B. der „Geschäftszweck“ (Business Need) oder die verantwortlichen Personen) zugeordnet sein sollen, ist auch bei jeder

⁵ Freischaltungen werden zunächst zu einem bestimmten Zweck benötigt und in der Firewall als Regeln umgesetzt. Es ist jedoch anzuzweifeln, dass nicht mehr benötigte Regeln mit der gleichen „Energie“ vom Antragsteller wieder deaktiviert werden.

⁶ Vgl.: Fritsch und Gundel (2005), S. 249.

⁷ Vgl.: Müller (2005), S. 247.

Änderung dafür Sorge zu tragen, dass ausreichende Informationen dokumentiert werden. Nur kann vermieden werden, dass Inkonsistenzen in der Firewall entstehen, die meist nur mit großem Aufwand beseitigt werden können.

6. Struktur und Restriktivität der Firewall-Regelwerke

Gemäß des „Prinzips der minimalen Rechte“ darf die Firewall jedem „Nutzer“ nur genau die Zugriffe gewähren, die dieser zum Ausführen seiner Arbeit mindestens benötigt. Dadurch wird einerseits die Sicherheit erhöht: Die Realität wird schärfer abgebildet und minimale Freigaben bieten weniger Angriffspunkte für Missbrauch. Andererseits nehmen Komplexität und Dynamik des Regelwerkes zu, da für jeden Zugriff eigene Einträge vorgenommen werden und daher bereits kleine Änderungen der Infrastruktur Anpassungen der Firewall erfordern. Im letzten Frageteil der Studie standen die Strukturierung des Regelwerkes sowie der Restriktivitätsgrad und dessen Umsetzung im dynamischen Firewall-Regelwerk im Vordergrund.

Hauptsächlich fokussiert sich die weitere Forschungsarbeit der vorliegenden Arbeit auf die Ausgangssituation (1.), den eigentlichen Firewall-Änderungsprozess, inklusive der Schnittstellenproblematik (2. und 3.) sowie die Dokumentation (5.). Die für die Analyse des Firewall-Änderungsprozess interessanten Aspekte der Untersuchungsbereiche 4. und 6. werden an den entsprechenden Stellen erwähnt, jedoch nicht gesondert untersucht.⁸

4.1.2 Analyseobjekt: Bankensektor

Vor der Durchführung der Firewall-Studie wurde der zu untersuchende Objektbereich⁹ im Hinblick auf Unternehmen mit hochgradig schützenswerten Informationsbeständen festgelegt. Es ist anzunehmen, dass Unternehmen, die weitaus mehr auf den Schutz ihrer Informationen angewiesen sind als Unternehmen anderer Branchen, eine restriktivere Informationssicherheit benötigen und demgemäß ihre schützenswerten Informationen durch eine restriktive Firewall vom Internet abschirmen. Als Analyseobjekt wurde für die betrachtete Studie der Bankensektor herangezogen, da das operative Bankgeschäft fast ausschließlich mit immateriellen Gütern (d.h. Informationen) arbeitet. Insbesondere Kunden- und Kontodaten stehen hierbei unter speziellem Schutz, der meist sogar im Gesetz verankert ist. Eine unzureichende Absicherung dieser Informationen kann für ein Kreditinstitut mit enormem Schaden sowohl materieller als auch immaterieller Natur verbunden sein. In kaum einer anderen Branche stehen IT- und operative Risiken in einem solch engen Zusammenhang, wie in Banken.

Speziell standen Großbanken im Augenmerk der Untersuchung. Einerseits wird dort sowohl eine hinreichend große Komplexität, als auch eine ausreichend hohe Dynamik des Regelwerkes erwartet, um darauf die späteren Optimierungsanalysen aufbauen

⁸ Die Durchführung der regelmäßigen Komplettrevision einer Firewall ist Ziel weiterer Forschungsarbeit (vgl.: Kap. 7.3).

⁹ Vgl.: Schnell u.a. (1999), S. 252.

zu können.¹⁰ Zum anderen stellt die internationale Präsenz eines Bankkonzerns aus firewalltechnischer Sicht ebenfalls einen interessanten Faktor dar: Bei einer Vernetzung mehrerer internationaler Standorte müssen die jeweilig geltenden, spezifisch auf den Bankensektor ausgerichteten gesetzlichen Bestimmungen berücksichtigt werden. Dabei müssen nicht nur die Kommunikationswege des Unternehmens nach außen, sondern u.U. auch die länderübergreifenden Verbindungen gesondert geschützt werden. So sind z.B. die am Bankenplatz Luxemburg geltenden Gesetze teilweise noch restriktiver als in Deutschland, sodass viele luxemburgische Filialen internationaler Banken sich sogar von ihren eigenen Muttergesellschaften per Firewall absichern.¹¹ In der betrachteten Firewall-Studie wurden primär die 25 nach Bilanzsumme größten deutschen Banken befragt.¹² Da in der Studie neben den Auswirkungen der Mitarbeiterzahl ebenfalls die Auswirkungen der unterschiedlichen Gesetzeslagen auf das Management der Firewall untersucht werden sollten, wurden zudem die Tochtergesellschaften der o.g. Banken am Finanzplatz Luxemburg befragt (sofern vorhanden).¹³ Eine Auflistung aller befragten Banken befindet sich im Anhang B.2. Die Studie wurde mit Hilfe von postalisch versandten Fragebögen durchgeführt und die Antworten anonym ausgewertet. Hauptsächlich waren die Fragebögen an Ansprechpartner aus dem Umfeld der IT-Sicherheit bzw. des „Information Risk Managements“ adressiert, von denen angenommen wurde, dass sie den gesamten Prozess des Firewall-Managements übersehen und zugleich hinreichend am Alltagsgeschäft involviert sind, um den Stand ihres Firewall-Managements zu kennen. Insgesamt wurden 37 Fragebögen versandt, von denen 26 ausgefüllt zurückgesandt wurden. Die sich daraus ergebende Teilnahmequote von ca. 70% lässt gerade vor dem Hintergrund der Sensibilität der gesamten Sicherheitsthematik auf ein großes

¹⁰ Diese Annahme ist ebenfalls ein Aspekt der Untersuchung.

¹¹ Vgl.: Wagner (2004), S. 2.

¹² Bei der Definition der Grundgesamtheit mussten einige wichtige Aspekte berücksichtigt werden. Zum einen sind die (speziell den Datenschutz betreffenden) Gesetzgebungen in den verschiedenen Ländern z.T. sehr unterschiedlich, sodass auch die Umsetzung der IT-Sicherheitsmaßnahmen (und des Firewall-Managements) nur bedingt vergleichbar ist. Zum anderen sind die Bankgesellschaften international durch verschiedene Arten von Gesellschaftsformen vertreten, die dem jeweils geltenden nationalen Recht unterliegen. Die Frage, ob und ab welcher Größe sich eine Tochtergesellschaft von der Muttergesellschaft insofern abgrenzt, dass sie als gesondertes Element in die Grundgesamtheit aufgenommen werden muss, ist nicht definitiv zu beantworten. Vgl.: Wagner (2007), S. 3f.

¹³ Die Auswahl der zu befragenden Banken gemäß deren Bilanzsummen stellt in der empirischen Sozialforschung keine Zufallsauswahl dar und schließt dadurch repräsentative Schlüsse auf die Grundgesamtheit aller Banken aus. Schnell u.a. (2005) bezeichnen die hier vorgenommene Auswahl als „Bewusste Auswahl“ typischer bzw. extremer Fälle. Die in Abschnitt 4.1.2 genannten Gründe stellen kleine bzw. lokal agierende (Privat)Banken z.B. als weniger interessant für die Studie dar, da diesen die für das Firewall-Management problematische Komplexität fehlt. Die Entscheidung gegen eine Zufallsauswahl fiel daher bewusst und wohl wissentlich, dass repräsentative Schlüsse auf eine Grundgesamtheit nicht möglich sein werden. Diese Art Schlüsse waren jedoch weder Ziel der Studie noch der auf ihr basierenden Untersuchungen. Ziel der Studie war es, einen Überblick über die Ist-Situation des Firewall-Managements deutscher Großbanken zu erhalten, um in der Praxis übliche Handhabungen (*best practices*) mit der Theorie zu vergleichen (falls möglich) und darauf aufbauend Maßnahmen und Handlungsempfehlungen für ein effektives und praktikables Firewall-Management erarbeiten zu können.

Interesse seitens der Banken an diesem Themengebiet schließen.¹⁴

4.2 Ergebnisse und Auswertungen der Studie

Die im Folgenden vorgestellten Ergebnisse (und Auswertungen) der Firewall-Studie bringen interessante und wichtige Erkenntnisse hervor. Sie tragen zum besseren Verständnis des „State-of-the-Art“ im Firewall-Management deutscher Großbanken bei und liefern (teilweise offensichtliche) Ansätze zur Verbesserung des Firewall-Managements. Diese Optimierungsansätze werden schließlich in den Kapiteln fünf und sechs diskutiert.

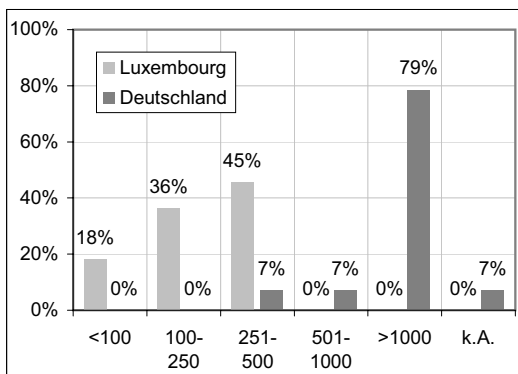
4.2.1 Ausgangssituation im ausgewählten Analysebereich

Im ersten Abschnitt der Firewall-Studie wurde hauptsächlich das organisatorische Umfeld der Firewall untersucht. Diese „Rahmenbedingungen“ einer Firewall lassen bereits erste Schlüsse auf die Zusammenhänge und Anforderungen des Firewall-Managements zu.

4.2.1.1 Mitarbeiter-Verhältnis und Firewall-Betreuung

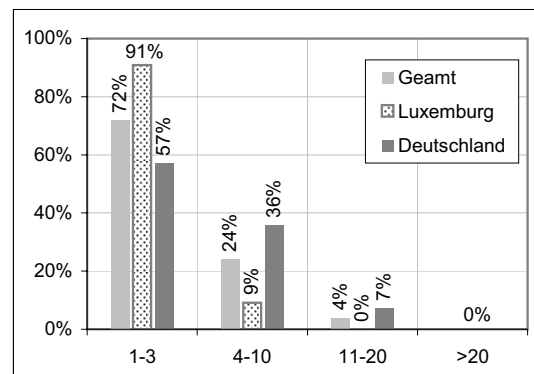
Die Mitarbeiterzahl ist ein wichtiges Indiz für die Komplexität der Firewall-Verwaltung, da eine große Mitarbeiterzahl ggf. auch eine höhere Fluktuation und Dynamik im vorhandenen Regelwerk bedeuten kann. In Deutschland wurden überwiegend die Konzernzentralen befragt. Die Ergebnisse (vgl.: Abb. 4.1) zeigen, dass die in Deutschland befragten Banken größtenteils wesentlich mitarbeiterstärker sind, als deren Filialen in Luxemburg. Die dort befragten Banken haben eine Beschäftigtenzahl von maximal 500 Mitarbeitern, während die untersuchten Banken in Deutschland (bis auf wenige Ausnahmen) mehr als 1000 Mitarbeiter aufweisen.

Abbildung 4.1: Unternehmensgröße



Quelle: Wagner (2007), S. 15.

Abbildung 4.2: Firewall-Betreuer



Quelle: Wagner (2007), S. 15.

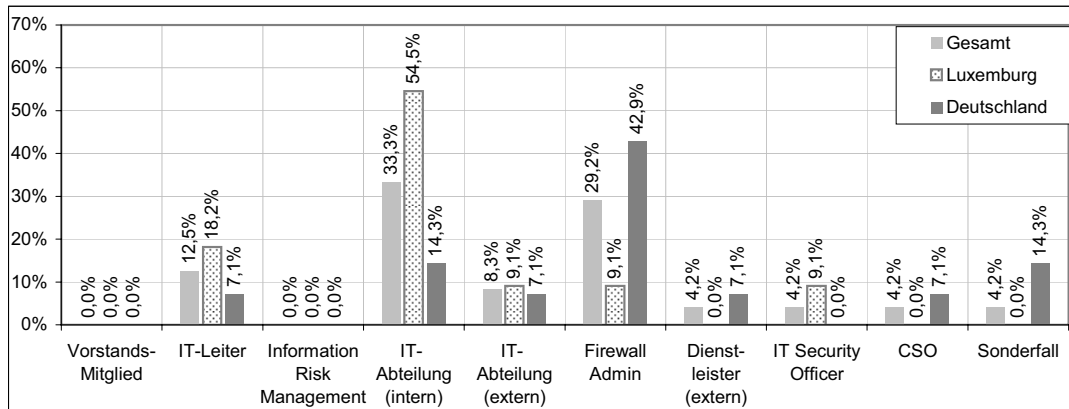
¹⁴ Die Resonanz aus den persönlichen Gesprächen mit mehreren Firewall-Zuständigen während der Durchführung der Studie hat diese Vermutung bestärkt.

Weiterhin zeigt sich, dass die Betreuung der Firewall in knapp drei von vier befragten Banken in den Händen eines maximal dreiköpfigen Teams liegt. In Luxemburg ist dieser Trend noch deutlicher: Nur eines aller dort befragten Unternehmen gab an, mehr als drei Personen für die Betreuung der Firewall einzusetzen (vgl.: Abb. 4.2).

4.2.1.2 Verantwortung für die Firewall

Die umfassende Gesamtsicherheit eines Unternehmensnetzwerkes hängt in erster Linie von der erfolgreichen Umsetzung der erforderlichen IT-Sicherheitsmaßnahmen ab. Für alle Informationen, Anwendungen und IT-Komponenten muss festgelegt werden, wer die Verantwortung für deren Sicherheit trägt.¹⁵ Dies gilt ebenso für die Firewall.

Abbildung 4.3: Verantwortungsträger für die Firewall¹⁶



Quelle: Wagner (2007), S. 17.

Im Gesamtbild zeigt sich, dass sich die Verantwortung für die Firewall im Wesentlichen auf Mitarbeiter der IT-Abteilung (in jedem dritten befragten Unternehmen) und den Firewall-Administrator (in jedem vierten befragten Unternehmen) verteilt. Damit wird deutlich, dass die Verantwortung auf einer ausführungsnahen Hierarchieebene (wenn nicht sogar mit dieser gleichauf) liegt, statt, wie vermutet, eher auf höherer Ebene verankert ist.

In Luxemburg hingegen ist ein spezieller Firewall-Administrator lediglich in Einzelfällen für die Firewall verantwortlich. In mehr als der Hälfte aller dort befragten Banken trägt ein Mitarbeiter aus der internen IT-Abteilung die Firewall-Verantwortung. Der IT-Leiter folgt an zweiter Stelle. Möglicherweise ist das Ergebnis auf die in Luxemburg knappen personellen Ressourcen zurückzuführen, sodass dort ein spezieller Firewall-Administrator u.U. nicht existiert. Externe Verantwortungsträger wurden nur in einem Fall genannt, die Hauptverantwortung für die Firewall bleibt

¹⁵ Vgl.: BSI (2008), M 2.225, S. 1557.

¹⁶ Die Kategorien „IT Security Officer“ und „Chief Security Officer (CSO)“ wurden von den Befragten selbst genannt. In den beiden Sonderfällen wurde ein Team aus „IT-Spezialist“ und „Firewall-Administrator“ sowie ein „externer Dienstleister mit Durchführungsverantwortung“ angegeben.