

Inhaltsverzeichnis

Vorwort	5
1 Einleitung	17
1.1 Die Bedeutung der Sicherheit im IT-Bereich.	17
1.2 Vorgehen bei der Risikobewältigung	19
1.2.1 Beispiele aus der Praxis.	19
1.2.2 Usancen bei der Risikobewältigung.	22
1.3 Ursachen «schlechter Lösungen».....	24
1.3.1 Mangelndes Problembewusstsein	24
1.3.2 Probleme bei der Funktionstrennung.	25
1.3.3 Probleme bei der Informationsbeschaffung.	26
1.3.4 Probleme bei der Finanzierung.	26
1.4 Ziel der Arbeit.	27
1.5 Abgrenzung.....	28
1.6 Gliederung der Arbeit	29
2 Grundbegriffe	32
2.1 Entscheidungstheoretische Grundlagen	32
2.1.1 Die Entscheidung als Auswahlprozess	32
2.1.2 Delegation von Entscheidungen	34
2.1.3 Einflussfaktoren im Entscheidungsprozess	35
2.1.4 Idealtypische Risikohaltungen	37
2.2 Der Sicherheitsbegriff allgemein	38
2.3 Der Sicherheitsbegriff im IT-Bereich	39
2.3.1 Datenschutz - Datensicherheit.....	40
2.3.2 Datensicherheit aus Benutzersicht	41
2.3.3 Datensicherheit aus der Sicht des Systembetreibers	41
2.3.4 Datensicherheit aus der Sicht des Systemingenieurs	41
2.3.5 Definition «Sicherheit»	41
2.4 Der Risikobegriff	42
2.4.1 Definition «Risiko»	42
2.4.2 Risikoarten	43
2.4.3 Risikobewertung, Schätzverfahren	44
2.4.4 Praxisnahe Risikobewertung	47
2.4.4.1 Der Mittelwert als Risikomass	48
2.4.4.2 Probable und Possible Maximum Loss	49
2.4.4.3 Die Varianz als Risikomass.....	51
2.4.4.4 Die graphische Darstellung des Risikos	54
2.4.4.5 Intervallschätzung	57
2.4.5 Prognose des Schadensausmasses	57
2.4.6 Risiko im IT-Bereich	59
2.4.7 Bemerkungen zum Risikobegriff	60

2.5	Der Begriff «Risk Management»	61
2.6	Der Begriff «Sicherheitspolitik»	63
2.7	Portfoliotheorie	65
2.7.1	Grundlagen	65
	Exkurs A: Das (μ, σ) -Prinzip	65
	Exkurs B: Kovarianz und Korrelation	68
2.7.2	Historische Entwicklung, Anwendungsgebiete	71
2.7.3	Portfolio Management	72
2.7.4	Diskussion	72
2.8	Portfoliotechnik im Strategischen Management	72
2.9	Sicherheitsmassnahmen	74
2.10	Risikobewältigung im aufbauorganisatorischen Kontext	74
2.11	Zusammenfassung	76
3	Bestehende Konzepte zur Risikobewältigung im IT-Bereich	77
3.1	Standards und Sicherheitskriterienkataloge	77
3.1.1	Das «Orange Book»	78
3.1.2	Der IT-Sicherheitskriterienkatalog	80
3.1.3	Kriterien des britischen Handelsministeriums	82
3.1.4	Information Technology Security Evaluation Criteria	82
3.1.5	Zusammenfassung	83
3.2	NBS Guideline for Automatic Data Processing Risk Analysis	83
3.3	Checklisten	85
3.4	Fallstudien	86
3.5	Computer Aided Risk Analysis/Management	86
3.5.1	Quantitative Methoden	86
3.5.1.1	RiskCalc	86
3.5.1.2	LRAM	86
3.5.1.3	CompuDARE	87
3.5.2	Qualitative Methoden	87
3.5.2.1	RANK-IT.	87
3.5.2.2	RiskPac.	87
3.5.3	MARION	88
3.5.4	Expertensysteme	89
3.5.4.1	KEEPER	89
3.5.4.2	COSSAC	91
3.6	Zusammenfassung	92
4	Portfoliomethode zur Risikobewältigung	94
4.1	Formulierung der Sicherheitspolitik	94
4.1.1	Ziel einer Sicherheitspolitik	95
4.1.2	Erstellung eines Risikobildes	95
	Exkurs C: Funktionaler Ansatz zur Risikoidentifikation ...	97

4.1.3	Allgemeine Grundsätze einer Sicherheitspolitik	99
4.1.3.1	Abdeckung existenzgefährdender Risiken	100
4.1.3.2	Erfüllung behördlicher Auflagen	101
4.1.3.3	Tolerierbare Risiken selbst tragen	101
4.1.3.4	Kopplung verbleibender Risikobewältigung an die unternehmerische Investitionsstrategie	102
4.1.4	Risikoklassifikation	102
4.1.5	Finanzierung von Sicherheitsmassnahmen	103
4.2	Anwendung der Sicherheitspolitik	104
4.2.1	Die Auswahl von Sicherheitsmassnahmen	109
4.2.1.1	Risikobeurteilung	109
4.2.1.2	Massnahmenbeurteilung	111
4.2.1.2.1	Massnahmenklassifikation	112
4.2.1.2.2	Merkmale von Sicherheitsmassnahmen	117
4.2.1.2.3	Grundsätze bei der Implementation ...	124
4.2.1.3	Effektive Sicherheitsmassnahmen	129
4.2.1.4	Generierung von Portfolios	131
4.2.1.4.1	Substitutive Portfolios	131
	Exkurs D: Diskussion	135
4.2.1.4.2	Simultane Portfolios	137
4.2.1.5	Berechnung der Effizienz	138
4.2.1.6	Auswahl des optimalen Portfolios	140
4.2.1.7	Nebeneffekte	140
4.2.2	Überprüfung des implementierten Portfolios	141
4.2.2.1	Grundsätze bei der Überprüfung	142
4.2.2.2	Konsequenzen aus Überprüfungstätigkeiten	145
4.3	Zusammenfassung	146
5	Fallstudie I: «Hacking»	147
5.1	Risikobeurteilung	147
5.1.1	Risikoanalyse	147
5.1.1.1	Risikoidentifikation	147
5.1.1.2	Risikoabgrenzung	147
5.1.1.3	Bestimmung der Risikofaktoren	148
5.1.1.4	Diskussion	148
5.1.2	Risikobewertung	149
5.1.2.1	Quantifizierung der Risikofaktoren	149
5.1.2.2	Risikoklassifikation	150
5.2	Bestimmung effektiver Massnahmen	150
5.2.1	Suche nach Massnahmenalternativen	150
5.2.2	Bestimmung kausaler Zusammenhänge	151
5.2.3	Schätzung des Restrisikos	151

5.2.4	Berechnung der Effektivität	152
5.3	Generierung von Portfolios	153
5.3.1	Überprüfung auf Vollständigkeit	153
5.3.2	Auflistung der Portfolios	154
5.4	Berechnung der Effizienz	155
5.4.1	Anschaffungs- und laufenden Kosten	155
5.4.2	Bestimmung der Effizienz	156
5.5	Interpretation der Ergebnisse	159
5.6	Interaktive Optimierung	159
5.6.1	Portfolioberechnung	160
5.6.1.1	Modellierungssprachen	160
5.6.1.2	Modellierung und Lösung	162
5.6.2	Das Modell	163
5.6.3	Diskussion	172
5.6.4	Der Modellierungsvorgang	174
5.6.5	Ein heuristischer Ansatz	175
5.7	Diskussion der Resultate	176
5.7.1	Kostenminimierung	176
5.7.2	Maximierung der Rendite	179
5.7.3	Risikominimierung	184
5.8	Diskussion des quantitativen Portfolioansatzes	189
6	Fallstudie II: Computerviren	191
6.1	Szenarium	191
6.2	Risikobeurteilung	191
6.2.1	Risikoanalyse	191
6.2.1.1	Risikoidentifikation	192
6.2.1.2	Risikoabgrenzung	192
6.2.1.3	Bestimmung der Risikofaktoren	194
6.2.2	Risikobewertung	197
6.2.2.1	Zerlegung des Risikos in Teilrisiken	197
6.2.2.2	Qualitative Risikoausprägungen	197
6.2.2.2.1	Gruppenbildung	197
6.2.2.2.2	Kritische Systemkomponenten	199
6.2.2.2.3	Unbewusste Einbringung	201
6.2.2.2.4	Grad der Öffentlichkeit	202
6.2.2.2.5	Ausmass der Bedrohung	203
6.2.2.2.6	Konsequenzen	203
6.2.2.2.7	Risikoschätzung	204
6.2.2.3	Risikoklassifikation	205
6.3	Bestimmung effektiver Massnahmen, Effizienz	205
6.4	Rahmenbedingungen	211
6.5	Realisierung	212

6.5.1	Massnahmen in «öffentlichen Bereichen»	212
6.5.2	Massnahmen in «geschlossenen Bereichen».....	213
6.6	Risikosituation nach Realisierung der Massnahmen.	218
6.6.1	Erfahrungen auf Universitätsebene.	219
6.6.2	Erfahrungen auf Institutsebene.	219
6.7	Zusammenfassung.	223
7	Schlussbemerkungen und Ausblick	224
7.1	Unternehmenspolitische Grundsätze	224
7.2	Vergleich mit bestehenden Ansätzen der Risikobewältigung	227
7.3	Kritische Beurteilung der Methode	228
7.4	Möglichkeiten der Weiterentwicklung	231
7.4.1	Methoden zur Risikobewältigung	231
7.4.2	Offizielle Produktbewertungen	234
Anhang A:	Beispiele zu «Preloss»- und «Postloss»-Massnahmen ..	236
A.1	«Preloss»-Massnahmen	236
A.2	«Postloss»-Massnahmen	238
Anhang B:	Listing des GAMS-Modells gegen Hackingversuche	240
Anhang C:	Computeranomalien und -viren	245
C.1	Logischer Aufbau eines Virusprogramms	245
C.2	Der Infektionsvorgang	246
C.3	Die Schadensfunktion	247
C.4	Besondere Probleme bei der Virenprophylaxe	248
C.5	Motivation der Autoren von Virusprogrammen.....	249
C.6	Virusgefahr durch Gruppenbildungen	249
Literatur		254
Weitere Literatur		261
Glossar		264
Abkürzungen und Akronyme		272
Index		274