

Inhaltsverzeichnis

Seite

Abkürzungsverzeichnis.....	XI
Anmerkung zur Zitierweise.....	XIII
A. Einführung.....	1
I. Problemstellung.....	2
II. Ziel der Arbeit und Vorgehensweise.....	3
III. Inhalt und Abgrenzung der Begriffe.....	7
a) Informationsverarbeitung im Büro.....	7
b) Integrierte Bürokommunikationssysteme.....	10
c) Informationsschutz, Informations- sicherung, Informationssicherheit.....	14
d) Informationssicherheitssystem.....	18
B. Analyse der Risiken bei integrierten Büro- kommunikationssystemen.....	20
I. Stellung der Risikoanalyse innerhalb des Risikomanagements.....	21
II. Ansätze und Methoden der Risikoanalyse.....	23
III. Analyse der Schwachstellen.....	26
a) Konzeptionelle und organisatorische Schwachstellen.....	27
b) Personelle Schwachstellen.....	30
c) Technische Schwachstellen.....	31
1) Benutzernahe Ebene.....	33
2) Netzwerkebene.....	35
3) Hintergrundebene.....	48
IV. Analyse der Gefahren.....	51
a) Zufällige Gefahren.....	52
b) Bewußt herbeigeführte Gefahren.....	54
V. Risikobewertung.....	56
a) Auswirkungen der Risikoereignisse.....	56
b) Eintrittswahrscheinlichkeiten der Risikoereignisse.....	58
c) Schadensausmaß von Risikoereignissen.....	59

C. Ziele als Maßstab des Sicherheitssystems.....	60
I. Sachziele.....	62
a) Gewährleistung von Informations- sicherheit.....	63
b) Wahrung der Schutzrechte und In- teressen der Betroffenen.....	64
c) Gewährleistung einer störungsfreien Informationsverarbeitung.....	67
d) Erkennung und Verhinderung von Ri- sikoereignissen.....	70
II. Formalziele.....	71
a) Ordnungsmäßigkeit und Rechtmäßigkeit.....	71
b) Wirtschaftlichkeit.....	75
c) Angemessenheit.....	77
d) Benutzerfreundlichkeit.....	78
III. Zielsysteme.....	80
 D. Rahmenbedingungen für die Gestaltung eines Sicherheitssystems.....	 82
I. Organisatorisch-technische Bedingungen.....	83
a) Eigenschaften des zu schützenden Informationssystems.....	83
b) Risiken und ihre Wirkungen.....	87
c) Stand der Sicherungsmethoden.....	87
d) Finanzielle Restriktionen.....	90
II. Eigenschaften der personellen Aktionsträger.....	91
a) Sicherheitsbewußtsein.....	92
b) Qualifikation der Mitarbeiter.....	93
c) Benutzerakzeptanz.....	96
III. Umweltbedingungen.....	98
a) Normen des Datenschutzes und der Datensicherung.....	99
b) Normen der Rechnungslegung.....	103
c) Sonstige Normen.....	106

E. Maßnahmenkategorien und Komponenten eines Sicherheitssystems.....	107
I. Risikovermeidung.....	108
II. Risikoverminderung.....	108
a) Systemtechnische Maßnahmen.....	109
b) Organisatorische Maßnahmen.....	112
c) Personelle Maßnahmen.....	114
III. Risikoakzeptanz.....	115
IV. Risikoüberwälzung.....	116
a) Sachversicherungen.....	116
b) Folgeschadenversicherungen.....	117
c) Personenbezogene Versicherungen.....	118
d) Umfassender Versicherungsschutz.....	119
V. Auswahl geeigneter Maßnahmen.....	120
a) Wirksamkeit von Maßnahmen.....	120
b) Wirtschaftlichkeitsanalyse.....	122
F. Organisatorische Gestaltung eines Sicherheitssystems.....	124
I. Voruntersuchung.....	125
II. Detailuntersuchung und Konzeption eines Sicherheitssystems.....	128
III. Realisierung eines Sicherheitssystems.....	129
IV. Einführung, Kontrolle und Weiterentwicklung des Sicherheitssystems.....	130
G. Schlußbetrachtung.....	132
 Literaturverzeichnis.....	135
Anhang.....	166