

Thomas Lux

Intranet Engineering

Einsatzpotenziale und phasenorientierte
Gestaltung eines sicheren Intranet in der
Unternehmung

Mit einem Geleitwort von Prof. Dr. Roland Gabriel

Deutscher Universitäts-Verlag

Inhaltsübersicht

1	Einleitung	1
1.1	Strategische Planung, Gestaltung und Einsatz eines sicheren Intranet in der Unternehmung	1
1.2	Ziel der Arbeit und Gang der Untersuchung	2
2	Einordnung und Abgrenzung des Inhouse-Netzes Intranet	7
2.1	Historische Entwicklung und Organisation des Internet	7
2.2	Begriffsabgrenzung und historische Entwicklung des Intranet	15
2.3	Abgrenzung von Internet, Extranet und Intranet	17
2.4	Gestaltungsansatz und -ebenen eines Intranet	20
3	Architekturkonzepte für den Einsatz eines Intranet in der Unternehmung	27
3.1	Referenzmodelle in der Datenübertragung zur Bildung von Kommunikationsstandards	27
3.2	Übertragungsprotokolle im Internet und Intranet	39
3.3	Architektur des Internet	44
3.4	Architekturkonzepte des Intranet	48
3.5	Externe Zugangsmöglichkeiten zum Intranet der Unternehmung	57
3.6	Zusammenfassung der Architekturkonzepte	82
4	Einsatz eines Intranet	85
4.1	Gründe für den Einsatz eines Intranet	85
4.2	Standarddienste und Anwendungen im Intranet	87
4.3	Einsatzpotenziale eines betrieblichen Intranet	95

4.4	Anbindung kommerzieller Internet-Anwendungen an das Intranet der Unternehmung	108
4.5	Praxisbeispiele für den Einsatz eines Intranet	130
4.6	Zusammenfassung der Einsatzmöglichkeiten und ihrer Sicherheitsprobleme	142
5	Anforderungen an den Einsatz eines sicheren Intranet in der Unternehmung	145
5.1	Sicherheit in der Informations- und Kommunikationstechnik	145
5.2	Normative Anforderungen an die Sicherheit im Intranet	155
5.3	Unternehmungsorientierte Anforderungen an die Sicherheit des Intranet	165
5.4	Sicherheitsmaßnahmen im Intranet	177
5.5	Sicherheitsanforderungen der Praxisbeispiele	193
5.6	Zusammenfassung der Anforderungen an ein sicheres Intranet	198
6	Phasenorientierter Gestaltungsansatz zur Einführung eines sicheren Intranet	201
6.1	Grundlegung des phasenorientierten Ansatzes im Rahmen des Intranet Engineering	201
6.2	Problemanalyse und Planung des Intranet-Einsatzes	207
6.3	Definition der Anforderungen an das Intranet	226
6.4	Entwurf des System- und Sicherheitskonzeptes	244
6.5	Implementierung des Intranet	260
6.6	Einführung des Intranet	269
6.7	Einsatz und Nutzung des Intranet	277
6.8	Zusammenfassende Bewertung des Intranet Engineering	284
7	Resümee und Ausblick	287

Inhaltsverzeichnis

Abbildungsverzeichnis	XIX
Tabellenverzeichnis	XXV
Abkürzungsverzeichnis	XXVII
1 Einleitung	1
1.1 Strategische Planung, Gestaltung und Einsatz eines sicheren Intranet in der Unternehmung	1
1.2 Ziel der Arbeit und Gang der Untersuchung	2
2 Einordnung und Abgrenzung des Inhouse-Netzes Intranet	7
2.1 Historische Entwicklung und Organisation des Internet	7
2.1.1 Entwicklung und Verbreitung des globalen Netzes Internet	8
2.1.2 Entwicklung des Internet in Europa und in Deutschland	12
2.1.3 Aufbau und Organisation des Internet	14
2.2 Begriffsabgrenzung und historische Entwicklung des Intranet	15
2.3 Abgrenzung von Internet, Extranet und Intranet	17
2.4 Gestaltungsansatz und -ebenen eines Intranet	20
2.4.1 Gestaltungsansatz (Intranet Engineering)	20
2.4.2 Gestaltungsebenen eines Intranet	21
2.4.2.1 Gestaltung der Organisation	21
2.4.2.2 Gestaltung der Informationsebene	22
2.4.2.3 Gestaltung der Anwendungsebene	23
2.4.2.4 Gestaltung der technischen Ebene	23
2.4.3 Sicherheit als Querschnittsfunktion	24

3	Architekturkonzepte für den Einsatz eines Intranet in der Unternehmung	27
3.1	Referenzmodelle in der Datenübertragung zur Bildung von Kommunikationsstandards	27
3.1.1	Das OSI-Referenzmodell der Internationalen Standardisierungs-Organisation (ISO)	28
3.1.2	Das TCP/IP-Referenzmodell	35
3.2	Übertragungsprotokolle im Internet und Intranet	39
3.3	Architektur des Internet	44
3.4	Architekturkonzepte des Intranet	48
3.4.1	Architektur eines Intranet ohne die Nutzung öffentlicher Netze	49
3.4.1.1	Externe Einwahl in das Intranet (Remote Access Intranet)	50
3.4.1.2	Verbindung von zwei oder mehreren Standorten über eine nicht-öffentliche Verbindung	52
3.4.2	Verbindung eines Intranet an mehreren Unternehmungsstandorten über ein öffentliches Netz	52
3.4.3	Nutzung eines öffentlichen Netzes zum Zugriff auf das Intranet	56
3.5	Externe Zugangsmöglichkeiten zum Intranet der Unternehmung	57
3.5.1	Leitungsgebundener Zugang über eine Wählverbindung	59
3.5.1.1	Analoge Verbindung (Analogmodem)	60
3.5.1.2	Digitale Verbindung über ISDN	61
3.5.2	Leitungsgebundener Zugang über eine Standleitung	61
3.5.2.1	Verbindung über das Stromnetz (PowerLine)	62
3.5.2.2	Verbindung über das TV-Kabelnetz	63
3.5.2.3	Multiplexing-Technologien und Glasfasernetze	64
3.5.2.4	Breitbandige ISDN-Verbindung (B-ISDN)	65
3.5.3	Nutzung einer Wählverbindung zum Aufbau einer Standleitung (Hybrider Zugang) am Beispiel von xDSL	66
3.5.4	Funktechnologien	70

3.5.4.1 Lokale Funknetze (Wireless-LAN)	70
3.5.4.2 Mobile Telekommunikationsnetze (UMTS)	73
3.5.4.3 Richtfunk	77
3.5.5 Hybride Verfahren der Funktechnologie am Beispiel satellitengestützter Funkverbindung	79
3.5.6 Leistungs- und Kostenübersicht der Zugangsarten	80
3.6 Zusammenfassung der Architekturkonzepte	82
4 Einsatz eines Intranet	85
4.1 Gründe für den Einsatz eines Intranet	85
4.2 Standarddienste und Anwendungen im Intranet	87
4.2.1 Kommunikationsdienste	87
4.2.2 Informationsdienste	90
4.2.3 Dateiübertragungsdienste	93
4.2.4 Remotedienste	95
4.3 Einsatzpotenziale eines betrieblichen Intranet	95
4.3.1 Einsatzbeispiele eines Intranet für die Informationsversorgung	96
4.3.2 Einsatz eines Intranet als Mitarbeiterportal	98
4.3.3 Einsatz eines Intranet zur Integration prozess- und gruppenorientierter Anwendungen	99
4.3.3.1 Ort und Zeit der Aufgabenerfüllung	101
4.3.3.2 Strukturierung des Arbeitsflusses	102
4.3.3.3 Art des betrieblichen Einsatzes	104
4.3.4 Das Intranet als Werkzeug für das Wissensmanagement	106
4.4 Anbindung kommerzieller Internet-Anwendungen an das Intranet der Unternehmung	108
4.4.1 Erläuterung und Abgrenzung des E-Business und des E-Commerce	108
4.4.2 Transaktionsorientierte Geschäftsmodelle	116
4.4.2.1 Anwendungen mit direkter Transaktionsorientierung	116
4.4.2.2 Anwendungen mit indirekter Transaktionsorientierung	118

4.4.3	Inhaltsorientierte Geschäftsmodelle	120
4.4.3.1	Bereitstellung von Informationen auf der Organisationsseite	121
4.4.3.2	Elektronische Portale, Suchmaschinen und Webkataloge	124
4.4.3.3	Virtuelle Communities	127
4.4.4	Einordnung eines Geschäftssystems in die Klassifikation	128
4.5	Praxisbeispiele für den Einsatz eines Intranet	130
4.5.1	Intranet eines Fachbereiches einer deutschen Universität (Uni-Net)	131
4.5.1.1	Architektur des Uni-Net	132
4.5.1.2	Inhaltliche Umsetzung und Strukturierung	132
4.5.1.3	Sicherheitsprobleme des Uni-Net	133
4.5.2	Intranet einer Immobilienunternehmung (Immo-Net)	135
4.5.2.1	Architektur des Immo-Net	135
4.5.2.2	Zugangsmöglichkeiten zum Immo-Net	136
4.5.2.3	Inhaltliche Umsetzung des Immo-Net	137
4.5.2.4	Sicherheitsprobleme des Immo-Net	139
4.5.3	Intranet des Privatkundenbereiches einer deutschen Bank (Bank-Net)	140
4.5.3.1	Architektur des Intranet Bank-Net	140
4.5.3.2	Inhaltsangebote des Intranet Bank-Net	141
4.5.3.3	Sicherheitsprobleme des Intranet-Einsatzes	141
4.6	Zusammenfassung der Einsatzmöglichkeiten und ihrer Sicherheitsprobleme	142
5	Anforderungen an den Einsatz eines sicheren Intranet in der Unternehmung	145
5.1	Sicherheit in der Informations- und Kommunikationstechnik	145

5.2 Normative Anforderungen an die Sicherheit im Intranet	155
5.2.1 Europäische und nationale Normen	156
5.2.2 Anforderungen des Wirtschaftsverwaltungsrechtes	159
5.2.2.1 Sicherheitsanforderungen aufgrund vertraglicher Regelungen	159
5.2.2.2 Sicherheitsanforderungen durch das Gesetz zur Kontrolle und Transparenz (KonTraG)	160
5.2.2.3 Anforderungen an die IT-Sicherheit durch Fremdkapitalgeber (Basel II)	161
5.2.3 Mögliche rechtliche Konsequenzen	162
5.2.4 Verantwortung für die IT-Sicherheit aufgrund rechtlicher Bestimmungen	163
5.3 Unternehmungsorientierte Anforderungen an die Sicherheit des Intranet	165
5.3.1 Ableitung der Ziele des IT-Sicherheitsmanagements aus den Zielen des Informationsmanagements	166
5.3.2 Aufgaben des IT-Sicherheitsmanagements	169
5.3.2.1 Anwendungsbeispiel für das strategische IT-Sicherheitsmanagement	172
5.3.2.2 Anwendungsbeispiel für das operative IT-Sicherheitsmanagement	174
5.3.2.3 Zusammenfassung des Anwendungsbeispiels	177
5.4 Sicherheitsmaßnahmen im Intranet	177
5.4.1 Organisatorische IT-Sicherheitsmaßnahmen	178
5.4.1.1 Aufbauorganisatorische IT-Sicherheitsmaßnahmen	178
5.4.1.2 Ablauforganisatorische IT-Sicherheitsmaßnahmen	180
5.4.2 Technische IT-Sicherheitsmaßnahmen	181
5.4.2.1 Sicherheitstechnologien zum Schutz des Netzzuganges	181
5.4.2.2 Authentifikation zwischen IT-Systemen	183
5.4.2.3 Authentifikation zwischen Benutzer und IT-System	186
5.4.2.4 Sicherheitstechnologien zum Schutz der zu übertragenden Daten	191

5.5 Sicherheitsanforderungen der Praxisbeispiele	193
5.5.1 Sicherheitsanforderungen des Uni-Net	193
5.5.2 Sicherheitsanforderungen des Immo-Net	194
5.5.3 Sicherheitsanforderungen des Intranet Bank-Net	196
5.5.4 Gegenüberstellung der Sicherheitsanforderungen der Praxisbeispiele	197
5.6 Zusammenfassung der Anforderungen an ein sicheres Intranet	198
6 Phasenorientierter Gestaltungsansatz zur Einführung eines sicheren Intranet	201
6.1 Grundlegung des phasenorientierten Ansatzes im Rahmen des Intranet Engineering	201
6.2 Problemanalyse und Planung des Intranet-Einsatzes	207
6.2.1 Ziel der Problemanalyse und Planung des Intranet- Einsatzes	207
6.2.1.1 Problemanalyse und Planung der Organisationsebene	208
6.2.1.1.1 Organisation des Projektmanagements	208
6.2.1.1.2 Planung der Rollen des Intranet-Einsatzes	212
6.2.1.2 Problemanalyse und Planung der Informationsebene	212
6.2.1.3 Problemanalyse und Planung der Anwendungsebene	215
6.2.1.4 Problemanalyse und Planung der technischen Ebene	220
6.2.2 Zusammenfassung der Ergebnisse der Problemanalyse- und Planungsphase	224
6.3 Definition der Anforderungen an das Intranet	226
6.3.1 Ziel und Aufbau der Definitionsphase	226
6.3.2 Betrachtung der Gestaltungsebenen in der Definitionsphase	229
6.3.2.1 Gestaltung der Organisationsebene	229
6.3.2.2 Definition der Anforderungen auf der Informationsebene	232
6.3.2.3 Definition der Anforderungen auf der Anwendungsebene	235

6.3.2.4	Definition der Anforderungen auf der technischen Ebene	239
6.3.3	Zusammenfassung der Ergebnisse der Anforderungsdefinitionsphase	243
6.4	Entwurf des System- und Sicherheitskonzeptes	244
6.4.1	Ziele und Aufgaben in der Intranet-Entwurfsphase	244
6.4.1.1	Tätigkeiten auf der Organisationsebene	246
6.4.1.2	Entwurf der Informationsebene	247
6.4.1.3	Entwurf der Anwendungsebene	253
6.4.1.4	Entwurf der technischen Ebene	257
6.4.2	Zusammenfassung der Ergebnisse der Intranet-Entwurfsphase	259
6.5	Implementierung des Intranet	260
6.5.1	Vorgehensweise und Ziel der Intranet-Implementierung	260
6.5.1.1	Implementierung der technischen Ebene	263
6.5.1.2	Implementierung der Informationsebene	264
6.5.1.3	Implementierung der Anwendungsebene	266
6.5.2	System- und Sicherheitstests des implementierten Intranet	268
6.5.3	Zusammenfassung der Ergebnisse der Intranet-Implementierungsphase	268
6.6	Einführung des Intranet	269
6.6.1	Aufbau und Ziel der Einführungsphase	269
6.6.1.1	Technische Intranet-Einführung (technische Integration)	273
6.6.1.2	Organisatorische Intranet-Integration	274
6.6.1.3	Intranet-Einführung auf der Informationsebene	275
6.6.1.4	Intranet-Einführung auf der Anwendungsebene	275
6.6.2	Zusammenfassung der Einführungsphase	276

6.7 Einsatz und Nutzung des Intranet	277
6.7.1 Wartung und Pflege des betrieblichen Intranet	277
6.7.1.1 Organisatorische Aufgaben bei der Wartung und Pflege des Intranet	278
6.7.1.2 Wartung und Pflege des Intranet- Informationsangebotes	281
6.7.1.3 Wartung und Pflege der Intranet-Anwendungen	282
6.7.1.4 Wartung und Pflege der technischen Infrastruktur	283
6.7.2 Zusammenfassung der Aufgaben während des Intranet- Einsatzes	283
6.8 Zusammenfassende Bewertung des Intranet Engineering	284
7 Resümee und Ausblick	287
Literaturverzeichnis	291