

Netzwerk- und IT-Sicherheitsmanagement

Eine Einführung

von
Jochen Dinger
Hannes Hartenstein



universitätsverlag karlsruhe

Inhaltsverzeichnis

1	Einleitung	1
1.1	Was ist Management?	1
1.2	Orientierungshilfe	3
1.3	Die Vielfältigkeit der Netze und des Netzmanagements	3
1.4	Die Vielfältigkeit des IT-Sicherheitsmanagements	9
1.5	Teildisziplinen des IT-Managements	10
1.6	Strukturierung dieses Buches	12

Teil I Netzwerkmanagement

2	Aufgaben des Netzwerkmanagements	17
2.1	Einleitung	17
2.2	Fallbeispiel: Rechenzentrum der Universität Karlsruhe (TH)	17
2.3	Physische Netzstrukturen	20
2.3.1	Passive Netzkomponenten	21
2.3.2	Aktive Netzkomponenten	29
2.4	Logische Netzstrukturen	33
2.4.1	Virtuelle lokale Netze	33
2.4.2	Zugangskontrolle	35
2.4.3	Traffic Engineering in Weitverkehrsnetzen	36
2.5	Leistungsgrößen und -indikatoren von Netzen	37
2.6	Netzdienste	38
2.7	Zusammenfassung	39
3	Managementarchitekturen	41
3.1	Einleitung	41

3.2	Strukturierung der Managementarchitektur	44
3.2.1	Informationsmodell	45
3.2.2	Kommunikationsmodell	47
3.2.3	Organisationsmodell	48
3.2.4	Funktionsmodell	51
3.3	Standardisierungsorganisationen	56
3.3.1	Internationale Standardisierungsorganisationen ..	57
3.3.2	„Standardisierungsorganisationen“ des Internet ..	60
3.3.3	Industrielle Standardisierungskonsortien	62
3.4	Netzwerkmanagement-Standards im Überblick	63
3.4.1	OSI-basiertes Netzwerkmanagement	64
3.4.2	Telecommunication Management Network (TMN) ..	67
3.5	Identifikation von MOs anhand des ISO- Registrierungsbaums	68
3.6	Zusammenfassung	69
4	SNMP v1, v2 und v3	71
4.1	Einleitung und Übersicht	71
4.2	Informationsmodell	72
4.2.1	Abstract Syntax Notation One (ASN.1) und Basic Encoding Rules (BER)	73
4.2.2	Structure of Management Information (SMI)	76
4.2.3	Identifikation von Object Types	83
4.2.4	Identifikation von Object Instances	84
4.2.5	Management Information Base II (MIB-II)	84
4.3	Kommunikationsmodell	86
4.3.1	SNMPv1	86
4.3.2	SNMPv2	90
4.3.3	SNMPv3	92
4.4	Funktions- und Organisationsmodell	98
4.5	Zusammenfassung	98
5	Remote Monitoring und Netzwerkmessungen	101
5.1	Einleitung	101
5.2	RMON und SMON: Managed Objects für Network Monitoring	103
5.2.1	RMON 1	105
5.2.2	RMON 2	106
5.2.3	SMON	107
5.2.4	Resümee	109
5.3	NetFlow und IPFIX	110

5.4	Zusammenfassung	112
6	Öffentliche IP-Netzverwaltung und Domain-Namen ..	115
6.1	Einleitung	115
6.2	Zuweisung von IP-Adressen	116
6.2.1	Historie	116
6.2.2	ICANN und IANA	118
6.2.3	RIPE NCC	119
6.2.4	Struktur der Organisationen und Richtlinien	120
6.3	Registrierung von Domain-Namen	121
6.4	Basiswerkzeuge	125
6.4.1	DNS Werkzeug – nslookup	125
6.4.2	„Whois“-Dienste	126
6.5	Fallbeispiele	127
6.5.1	Verwaltung von IP-Adressen und Domains am RZ der Universität Karlsruhe (TH)	127
6.5.2	Die Registrierungsstelle für .de-Domains – DENIC	131
6.6	Zusammenfassung	132
7	Managementwerkzeuge und -plattformen	133
7.1	Einleitung	133
7.2	Klassifikation von Managementwerkzeugen	133
7.2.1	Eigenständige Managementwerkzeuge	134
7.2.2	Managementplattformen	135
7.3	Ausgewählte Werkzeuge für TCP/IP-basierte Netze	140
7.3.1	ping & traceroute	140
7.3.2	MIB-Browser	142
7.3.3	MRTG & RRDTool	142
7.3.4	Wireshark	144
7.4	Plattformen am Rechenzentrum der Universität Karlsruhe (TH)	145
7.4.1	Netzwerkmanagement	146
7.4.2	WLAN Management mit AirWave	151
7.5	Zusammenfassung	155
8	Evolution des Netzwerkmanagements	157
8.1	Einleitung	157
8.2	Informationsmodell	159
8.2.1	SMIng – Structure of Management Information Next Generation	159

8.2.2	CIM – Common Information Model	161
8.3	Kommunikationsmodell	165
8.3.1	NetConf – ein XML-basiertes Protokoll zur Netzwerk-Konfiguration	165
8.3.2	Management <i>von</i> und <i>mit</i> Web Services	169
8.4	Organisations- und Funktionsmodell	170
8.4.1	Policy-basiertes Management	171
8.5	Werkzeuge und Plattformen	173
8.6	Zukünftige Herausforderungen in drahtlosen Sensornetzen	173
8.6.1	Drahtlose Sensornetzwerke	174
8.6.2	Besonderheiten beim Management von drahtlosen Sensornetzen	176
8.7	Zusammenfassung	178

Teil II IT-Sicherheitsmanagement

9	Einführung in IT-Sicherheitsmanagement	181
9.1	Einleitung	181
9.2	IT-Sicherheit als Managementaufgabe	182
9.2.1	Definition von IT-Sicherheitsmanagement und IT-Sicherheitsmanagementsystemen	182
9.2.2	Sicherheitsleitlinie und -richtlinien	185
9.2.3	Schutzziele	188
9.2.4	Weitere Begriffsdefinitionen	188
9.3	Dimensionen des IT-Sicherheitsmanagements	189
9.3.1	Menschen	190
9.3.2	Prozesse	190
9.3.3	Technologien	191
9.3.4	Abgrenzung zum Security Engineering	191
9.4	Zusammenfassung	192
10	IT-Sicherheitsprozess – BSI-Grundschutz	193
10.1	Einleitung	193
10.1.1	Wasserfallmodell	194
10.1.2	Inkrementelles Modell	195
10.1.3	Spiralmodell	195
10.2	IT-Grundschutz-Kataloge des BSI	195
10.3	IT-Sicherheitsprozess	197
10.3.1	Strategische Ebene	197

10.3.2	Taktische Ebene.....	198
10.3.3	Operative Ebene	198
10.4	Entwicklung eines Sicherheitskonzeptes nach	
	IT-Grundschutz	198
10.4.1	Strukturanalyse	198
10.4.2	Schutzbedarfsfeststellung	200
10.4.3	IT-Grundschutzanalyse – Modellierung	201
10.4.4	IT-Grundschutzanalyse – Basischeck	202
10.4.5	Ergänzende Sicherheitsanalyse	202
10.5	Internationale Standards im Bereich ITSM	204
10.5.1	ISO 2700x Standards	204
10.5.2	The Standard of Good Practice for Information Security	205
10.6	Zusammenfassung	206
11	Zugangs- und Zugriffskontrolle.....	207
11.1	Einleitung	207
11.2	Grundlagen	207
11.2.1	Terminologie	207
11.2.2	Kryptographie	209
11.2.3	Public Key Infrastructure (PKI)	211
11.3	Zugangskontrolle	214
11.3.1	RADIUS	216
11.3.2	Kerberos	217
11.4	Zugriffskontrolle	221
11.4.1	Zugriffskontrollstrategien	221
11.4.2	Zugriffskontrollstrukturen	222
11.4.3	Zugriffskontrollmodelle	223
11.5	Zusammenfassung	224
12	Identitätsmanagement	225
12.1	Einleitung	225
12.2	Herausforderungen und Ziele des Identitätsmanagements	227
12.2.1	Betreibersicht	227
12.2.2	Nutzersicht	229
12.3	Bausteine des Identitätsmanagements	230
12.3.1	Digitale Identitäten	230
12.3.2	Identitätsspeicher	231
12.3.3	Integration von Identitätsspeichern	237
12.3.4	Identitätsmanagement-Prozesse	239
12.4	Aktuelle Entwicklungen	241

12.4.1	Föderatives Identitätsmanagement	241
12.4.2	Nutzerzentriertes Identitätsmanagement	243
12.5	Karlsruhe Integriertes InformationsManagement	246
12.6	Zusammenfassung	249
13	Sicherheitspatch-Management	251
13.1	Einleitung	251
13.2	Patch-Managementprozess	253
13.2.1	Beurteilungsphase	253
13.2.2	Bestimmungsphase	254
13.2.3	Evaluiierungs- und Planungsphase	255
13.2.4	Bereitstellungsphase	256
13.3	Zusammenfassung	256
14	Firewalls, Intrusion Detection und Prevention	257
14.1	Einleitung	257
14.2	Firewalls	257
14.2.1	Paketfilter	258
14.2.2	Proxyfilter	259
14.2.3	Applikationsfilter	260
14.2.4	Architekturen	261
14.2.5	Managementaspekte	262
14.3	Intrusion Detection Systems	263
14.3.1	Signaturbasierte Erkenner	264
14.3.2	Anomaliebasierte Erkenner	265
14.3.3	Elektronische Köder	265
14.3.4	Managementaspekte	266
14.4	Zusammenfassung	266
15	Vorfallsbehandlung	267
15.1	Einleitung	267
15.2	Aufgaben und Dienste eines CERT/CSIRT	268
15.2.1	Reaktive Dienstleistungen	268
15.2.2	Proaktive Dienstleistungen	270
15.2.3	Qualitätsmanagement für Sicherheitsdienstleistungen	271
15.3	Prozess der Vorfallsbehandlung	272
15.4	Zusammenfassung	274

16 Rechtliche Aspekte	275
16.1 Einleitung	275
16.2 Wesentliche Begriffsabgrenzungen	276
16.2.1 Datenschutz und Datensicherheit	276
16.2.2 Datenschutz und Privacy	276
16.3 Grundelemente des Datenschutzes in Deutschland	277
16.3.1 Folgerungen aus dem Grundrecht auf informationelle Selbstbestimmung	277
16.3.2 Folgerungen aus der europäischen Datenschutzrichtlinie 95/46/EG	280
16.3.3 Folgerungen aus dem Fernmeldegeheimnis Art. 10 GG bzw. § 88 TKG	281
16.4 Datenschutzgesetze	281
16.4.1 Persönlicher Anwendungsbereich eines Gesetzes .	282
16.4.2 Sachlicher Anwendungsbereich eines Gesetzes ...	282
16.4.3 Rechtsfolgenbestimmung und Zielvorgaben	290
16.4.4 Zusammenfassendes Beispiel	292
16.5 Vorratsdatenspeicherung und TK-Überwachung	293
16.6 Kontrolle und Aufsicht	294
16.7 Zusammenfassung	295
 Abkürzungsverzeichnis	 297
 Literaturverzeichnis	 301