

Inhaltsverzeichnis

Mobile Device Management	11
Vorwort und Einleitung	11
I Mobile Device Management – Eine Übersicht	13
I.1 Mobile Endgeräte	13
I.2 Smartphones, Pads und Tablet-Computer	14
I.3 Betriebssysteme mobiler Endgeräte	16
I.3.1 »Branding«	16
I.3.2 Firmware	17
I.3.3 Apple iOS	19
I.3.4 Android	21
I.3.5 Symbian	24
I.3.6 BlackBerry OS	25
I.3.7 BlackBerry QNX	26
I.3.8 Windows Phone	26
I.4 Kommunikationsmöglichkeiten	28
I.4.1 GSM, UMTS und LTE	28
I.4.2 WLAN	29
I.4.3 Bluetooth	29
I.4.4 Near Field Communication (NFC)	30
I.4.5 Universal Serial Bus (USB)	30
I.4.6 Speicherkarten	31
I.4.7 Kamera	31
I.5 Mobile Endgeräte und ihre Appstores	32
I.5.1 Apple App Store	33
I.5.2 Windows Phone Marketplace	34
I.5.3 Nokia Store	35
I.5.4 BlackBerry App World	36
I.5.5 Google Play Store	36

2	Mobile Device Management: ISO 27001 und Grundschutz	39
2.1	Grundsätzliches	39
2.2	Sicherheits- und Kontrollmaßnahmen	43
2.3	Berücksichtigung in einer Sicherheitsleitlinie	52
2.4	Integration aller Maßnahmen in ein Sicherheitskonzept	54
2.5	Tests auf Operabilität und Wirksamkeit der Maßnahmen	56
3	Sicherheitsprobleme mobiler Endgeräte	59
3.1	Unberechtigter physischer Zugriff durch Verlust und/oder Diebstahl	60
3.2	Schadsoftware (»Malware«)	62
3.3	Phishing	65
3.4	Direkte Beobachtung (»Shoulder Surfing«)	68
3.5	Unsichere Datenablage im mobilen Endgerät	69
3.5.1	BlackBerry	70
3.5.2	iOS	70
3.5.3	Android	73
3.5.4	Symbian	73
3.5.5	WP7	74
3.6	Schwachstellen drahtloser Kommunikation	74
3.6.1	GSM/UMTS	74
3.6.2	WLAN	79
3.6.3	Bluetooth	82
3.7	Risiko Cloud Computing	83
3.8	Anwendungsprogramme mit unerwünschtem Datenabfluss	87
3.9	Aufhebung der Hersteller-Restriktionen (»Jailbreak« und »Rooten«)	96

4	Mobile Device Management	103
4.1	Grundlagen	103
4.1.1	Inventarisierung	105
4.1.2	Incident und Problem Management	105
4.1.3	Verteilung von Patches, Updates und Applikationssoftware	106
4.1.4	Überprüfung der Compliance mit Sicherheitsrichtlinien	109
4.1.5	Backup und Restore	110
4.1.6	Sperren des Geräts und Löschen sensibler Daten	111
4.1.7	Zustandsüberwachung und Auditierung der mobilen Geräte	112
4.1.8	Protokolle im Mobile Management	113
4.2	Management von RIM-BlackBerrys	115
4.3	Management über Konfigurationsdateien bei Apple iOS-Geräten	119
4.3.1	Erstellung der .mobileconfig-Dateien mit iPCU	120
4.3.2	Export von .mobileconfig-Dateien	134
4.3.3	Bereitstellung von Konfigurationsprofilen für iOS-Geräte	137
4.4	Mobile Device Management über Client-Apps	141
5	Business Continuity und Mobile Device Management	145
5.1	Business Impact Analysis	146
5.2	Präventive Maßnahmen	154
5.2.1	Ersatzgeräte	154
5.2.2	Alternative Verbindungen	155
5.2.3	Datensicherung	155
5.3	Reaktive Maßnahmen	158
5.4	Notfallübungen	159
5.5	Messung von Kennzahlen	160

6	Management einer heterogenen mobilen Infrastruktur	165
6.1	Gegensätzliche Philosophien: BYOD oder unternehmenseigene Geräte	166
6.2	MDM-Modelle	168
6.2.1	Full-Service-Anbieter	168
6.2.2	MDM von Systemmanagementanbietern	169
6.2.3	MDM von Anti-Malware-Anbietern	170
6.2.4	Gerätehersteller mit Full-Service	171
6.2.5	MDM-Startups	172
6.3	MDM-Projekt: Planung, Ausführung und Betrieb	176
6.4	Lebenszyklus eines MDM-Systems	178
6.5	MDM Rollout	184
6.6	Ausmustern der mobilen Endgeräte	185
7	Praxis: Auswahl eines Mobile Device Management Systems	187
7.1	Evaluierung von MDM-Produkten	187
7.2	Szenarien für den Einsatz der MDM-Lösung	191
7.2.1	Externe und interne Anforderungen	191
7.2.2	Risiken und Schwachstellen	191
7.2.3	Unternehmensphilosophien und Strategien	192
7.3	Szenarien	193
7.3.1	Szenario 1	193
7.3.2	Szenario 2	194
7.3.3	Szenario 3	196
7.4	Fazit	198

8	Unternehmensrichtlinien für den Einsatz mobiler Endgeräte	199
8.1	Richtlinien für mobiles Arbeiten	200
8.1.1	Sicherheitsleitlinie	200
8.1.2	Sicherheitsrichtlinie R1 (Nutzer)	202
8.1.3	Sicherheitsrichtlinie R2 (Management)	209
8.2	Intensivierung der Awareness	214
A	Quellen und Literatur	217
B	Tabellen und Abbildungen	219
C	Verwendete Abkürzungen	223
	Index	227