

Inhalt

1.	Grundlagen	1
1.1	Zielsetzung	1
1.2	Definitionen	1
1.3	Aufbau der Studie	3
1.4	Abgrenzung	4
2.	Management Summary	5
2.1	Die Bedrohungen für mobile Firmengeräte	5
2.2	Grundvoraussetzung: Der Schutz der mobilen Firmengeräte selbst	6
2.3	Bedrohungen aus den Kommunikationstechnologien	6
2.3.1	Details der Kommunikationsschwachstellen	8
2.4	Angriffe auf mobile Geräte	9
2.5	Wichtige Empfehlungen	12
2.6	Die Nutzung von (unsicheren) Fremdgeräten	13
3.	Potentielle Angreifer und ihre Zielsetzung	14
3.1	Reine Amateure	14
3.2	Hacker-Amateure	14
3.3	Die Profis	15
4.	Angriffsmöglichkeiten und daraus resultierende Schäden	17
4.1	Firmengeräte in fremden Händen (Verlust oder Diebstahl)	17
4.2	Elektronische Angriffe gegen mobile Geräte (z.B. Notebooks)	20
4.3	Angriffe auf die mobile Kommunikation (Man-in-the-Middle)	21
4.4	Geräte mit aktiven drahtlosen Schnittstellen im Firmennetz	23
4.5	Angriffe über unsichere Fremdgeräte gegen das Firmennetz	24
4.6	Social Engineering Angriffe	25
4.7	Spezielle Angriffe auf Smartphones	26

5.	Vorgehensweise bei einer Risikoabschätzung	30
5.1	Das Konzept des „Attack Trees“	30
5.2	Grundsätzliche Struktur der Kommunikation mit dem Firmennetz	31
5.3	Die Nutzung sicherer mobiler Geräte über unsichere Verbindungen	32
5.3.1	Exponierung im Internet auf Layer 3 des OSI-Modells	33
5.3.2	Exponierung im gleichen lokalen Netz	34
6.	Technische Anbindungsmöglichkeiten und ihre Bewertung	35
6.1	Details zu WLAN	35
6.1.1	Technologie-Überblick	35
6.1.2	Das WLAN-Sicherheitskonzept	35
6.1.3	WLAN-Schwächen der Übertragungssicherheit / Verschlüsselung	36
6.1.4	WLAN-Schwachstellen bzgl. Netz-Angriffen auf das Gerät	39
6.1.5	WLAN-Schwachstellen in Bezug auf DoS-Angriffe	40
6.1.6	WLAN-Access Points auf dem Firmengelände	42
6.1.7	Bewertung der WLAN-Technik	43
6.2	Details für Bluetooth	44
6.2.1	Relevanz	44
6.2.2	Technologie-Überblick	44
6.2.3	Das Bluetooth-Sicherheitskonzept	45
6.2.4	Bluetooth-Schwächen der Übertragungssicherheit / Verschlüsselung	48
6.2.5	Bluetooth-Schwachstellen bzgl. Netz-Angriffen auf das Gerät	48
6.2.6	Bluetooth-Schwachstellen in Bezug auf DoS-Angriffe	50
6.2.7	Gerätespezifische Bluetooth-Schwachstellen	51
6.2.8	Bewertung der Technik	53
6.3	Details für GSM / EDGE	54
6.3.1	Technologie-Überblick	54

6.3.2	Das GSM-Sicherheitskonzept	54
6.3.1	GSM-Schwächen der Übertragungssicherheit / Verschlüsselung	55
6.3.2	GSM-Schwachstellen bzgl. Angriffen auf das Gerät	56
6.3.3	GSM-Schwachstellen in Bezug auf DoS-Angriffe	57
6.3.4	Bewegungsprofile über GSM-Geräte	57
6.3.5	Bewertung der GSM-Sicherheitstechnik	58
6.4	Details für GPRS	59
6.4.1	Technologie-Überblick GPRS	59
6.4.1	Das GPRS-Sicherheitskonzept	60
6.4.2	GPRS-Schwächen der Übertragungssicherheit / Verschlüsselung	60
6.4.3	GPRS-Schwachstellen bzgl. Angriffen auf das Endgerät	61
6.4.4	GPRS-Schwachstellen in Bezug auf DoS-Angriffe	62
6.4.5	Bewertung der Technik	63
6.5	Details für UMTS	64
6.5.1	Technologie-Überblick UMTS	64
6.5.2	Das UMTS-Sicherheitskonzept	64
6.5.3	UMTS-Schwächen der Übertragungssicherheit / Verschlüsselung	65
6.5.4	UMTS-Schwachstellen bzgl. Netz-Angriffen auf das Gerät	66
6.5.5	UMTS-Schwachstellen in Bezug auf DoS-Angriffe	67
6.5.6	Bewertung der UMTS-Technik	68
6.6	Details für öffentliche LANs, z.B. Hotel-LAN	69
6.6.1	Technologie	69
6.6.2	Das Sicherheitskonzept von öffentlichen LANs	69
6.6.1	LAN-Schwächen der Übertragungssicherheit / Verschlüsselung	69
6.6.2	LAN-Schwachstellen bzgl. Netz-Angriffe auf das Gerät	70
6.6.3	LAN-Schwachstellen in Bezug auf DoS-Angriffe	70

6.6.4	Bewertung der Sicherheit in öffentlichen LANs	71
6.7	Bedrohung durch Geräte mit aktiven drahtlosen Schnittstellen	72
6.7.1	Relevanz	72
6.7.2	Angriffsszenario	72
6.7.3	Bewertung des Risikos durch Geräte mit aktiven drahtlosen Schnittstellen	73
7.	Schutzkonzepte	74
7.1	Das Konzept „Schutz in Schichten“	74
8.	Generelle Schutzmaßnahmen	76
8.1	Maßnahmen für den Fall von Verlust oder Diebstahl	76
8.2	Schutz des Gerätes im Internet - Gerätesicherheit	77
8.3	Schutz der Geräte durch korrektes Verhalten	80
8.4	Schutz des Firmennetzes	81
8.5	Schutzmaßnahmen für mobile Geräte mit WLAN	82
8.6	Schutzmaßnahmen für Bluetooth-Geräte	83
8.7	Schutzmaßnahmen für GSM-Geräte	85
8.8	Schutzmaßnahmen für GPRS-Geräte	86
8.9	Schutzmaßnahmen für UMTS-Geräte	87
8.10	Schutzmaßnahmen für die IR-Schnittstelle	88
9.	End-to-End Absicherungen	89
9.1	Überblick und Konzept	89
9.2	IPsec-VPN	90
9.2.1	Spezialfall Fernwartung über VPN	91
9.3	SSL-VPN	92
9.4	Terminalserver- Lösungen	94
9.5	Absichern von PDA-Synchronisationen	94
9.6	Blackberry und die RIM-Kommunikationsschnittstelle	96

9.6.1	Die Blackberry-Architektur	97
9.6.2	Zusätzliche Absicherungsmaßnahmen für Blackberry-Kunden	99
9.6.3	Bewertung	100
9.7	Outlook-Web-Access (OWA)	102
	Unsichere Geräte: Internetcafé, Privat-PC, Kunden-PC	105
10.	Entscheidungskriterien	107
10.1	Mögliche Lösungsansätze und Entscheidungshilfe	107
10.2	Weiterführende Überlegungen	108
10.2.1	Outlook Web-Access (OWA)	108
10.2.2	Die Nutzung unsicherer Geräte	109
10.2.3	IPsec-VPN- versus SSL-VPN	109
11.	Endnotes	112