Inhaltsübersicht

Erster Teil Einleitung und Grundlagen

A.	Einleitung	29
B.	Begrifflichkeiten und Grundlagen der Kommunikation über das Internet- Netzwerk	40
C.	Kryptologische Grundlagen	55
	Zweiter Teil Informationstechnologische Analyse	
D.	Einleitung	69
E.	Der Zugriff auf den Datenverkehr eines lokalen Funknetzwerks	72
F.	(Inhaltliche) Untersuchung des Netzwerkverkehrs	113
G.	Folgerungen für die nachfolgende rechtliche Analyse	142
	Dritter Teil Rechtliche Analyse	
H.	Einleitung	149
I.	Die Überwachung lokaler Funknetzwerke ("WLAN-Catching")	152
J.	Analyse der einzelnen Kategorien von Ermittlungsmaßnahmen	186
	Vierter Teil Ergebnisse und Zusammenfassung	
K.	Kernaussagen des Buches	339

L.	Erge	onisse der informationstechnologischen Analyse	341
M.	Zusa	mmenfassung der rechtlichen Analyse	345
N.	Schlı	ussfolgerung und thesenartiger Überblick	352
Anhaı	ng A	Einzelheiten zu der informationstechnologischen Untersuchung und Umsetzung	355
Anhai	ng B	Detailinformationen zur Arbeitsweise des Internet-Netzwerks	378
Anhar	ng C	Kryptologischer Hintergrund	400
Anhar	ng D	Mathematische Grundlagen und Zeichenkodierung	491
Quelle	en im	World Wide Web	510
Zitiert	te Ent	scheidungen	523
Litera	turver	zeichnis	525
Stichv	vortre	gister	537

Inhaltsverzeichnis

Erster Teil

Einleitung und Grundlagen

Α.	Einl	eitung
	I.	Einführung
	II.	Theorie und Realität der Überwachung moderner Kommunikation .
		1. Der "Staatstrojaner"
		2. Die Alternativlosigkeit des "Staatstrojaners"
		3. Eine Alternativmöglichkeit
		a) Die Alternativmöglichkeit aus technologischer Sicht
		b) Die Alternativmöglichkeit in der Praxis
		c) Die Alternativmöglichkeit aus rechtlicher Sicht
	III.	Methodik
		1. Informationstechnologische Analyse
		2. Rechtliche Analyse
	IV.	Gang der Darstellung
3.	Beg	rifflichkeiten und Grundlagen der Kommunikation über das Internet-
	Netz	zwerk
	I.	Das Internet-Netzwerk
	II.	Die Netzwerkprotokolle des Internet-Netzwerkes
		1. Referenzmodelle
		2. TCP/IP-Referenzmodell
		a) Aufbau des TCP/IP-Referenzmodells
		b) Die einzelnen Schichten des TCP/IP-Referenzmodells
		aa) Anwendungsschicht
		bb) Transportschicht
		cc) Internetschicht
		dd) Netzzugangsschicht (Sicherungs- und Bitübertragungs-
		schicht)
		(1) IEEE 802.11 (WLAN) als Beispielprotokoll der
		Netzzugangsschicht
		(a) Betriebsmodus
		(b) Assoziierung
		(c) Begleiterscheinungen der Funkübertragung
		(d) Authentifizierung/Verschlüsselung
		(aa) Sicherheitsmechanismen

		(bb) WPA2-Personal und WPA2-Enterprise	49
		(e) Adressierung	50
		(2) Address Resolution Protocol	50
		(a) Intra-Netzwerk-Niveau	51
		(b) Inter-Netzwerk-Niveau	51
		3. Art der Übermittlung	52
	III.	Protokolldateneinheiten: Überblick und Termini	52
C.	•	ptologische Grundlagen	55
	I.	Kryptologie: Termini und Aufgaben	55
		1. Termini	55
		2. Aufgaben der Kryptologie	55
	II.	Elementares Instrumentarium der Kryptographie	56
		1. Kryptographischer Algorithmus	56
		2. Schlüssel	57
		3. Kryptosystem, Verschlüsselungsverfahren, Algorithmus	57
		4. Symmetrische Algorithmen – Secret-Key-Verfahren	57
		a) Prinzip des symmetrischen Algorithmus	57
		b) Problem des Schlüsselaustausches	58
		5. Asymmetrische Algorithmen – Public-Key-Verfahren	59
	***	6. Hybride Algorithmen	61
	III.	Kryptanalyse	62
		1. Angriffsarten	62
	13.7	2. Man-in-the-Middle-Angriff	63 64
	IV.	Public-Key-Infrastrukturen	65
			65
	V.		66
	V. VI.	Digitale Signaturen	67
		Zweiter Teil	
		Informationstechnologische Analyse	
D.		eitung	69
	I.	Erläuterung und Eingrenzung des Untersuchungsgegenstandes 1. Eigenständigkeit und lokaler Ansatzpunkt der Überwachungs-	69
		maßnahme	69
		2. Vorgehen ohne Eindringen in das informationstechnische Endgerät	70
		3. Überprüfbarkeit des Vorgehens als methodische Voraussetzung .	70
		4. Aktualität der Untersuchung	71
	II.	Gang der Analyse	71
E.		Zugriff auf den Datenverkehr eines lokalen Funknetzwerks	72
	I.	Einführung	72
	II.	Der Zugriff auf lokale Funknetzwerke (Wireless LAN)	72
		Lokalisieren und Zuordnen des Access Points	73
		a) Grundlagen	73 74
		aar Aknyes ind dassives ocannen	74

	(1) Service Set Identifier (SSID)
	(2) Aktives Scannen
	(3) Passives Scannen
	bb) Beacon-Frame und Probe-Response-Frame
	b) Lokalisieren funkbasierter Netzwerke
	c) Hidden Network
	d) Zuordnung zum Ziel der Infiltration
	e) Zusammenfassung: Lokalisieren und Zuordnen des Access Points 7
2.	Der Zugang zum (fremden) Wireless LAN
	a) WLAN ohne Sicherheitsvorkehrungen
	aa) Authentifizierung und Assoziierung
	bb) Access Control List
	cc) Zusammenfassung: WLAN ohne Sicherheitsvorkehrungen 8
	b) WEP-verschlüsseltes WLAN
	aa) Verschlüsselung bei WEP
	(1) Shared Key
	(2) WEP-Seed/Gesamtschlüssel (=RC4-Schlüssel) 8
	(3) Verschlüsselungsvorgang 8
	(4) Versendeter Datenteil bei WEP 8
	bb) Authentifizierung und Assoziierung bei WEP 8
	(1) Verfahren
	(2) Fake Authentication
	cc) Attacks on WEP
	(1) FMS/KoreK-Method
	(a) FMS
	(b) KoreK
	(2) PTW-Method
	(a) Klein- bzw. Jenkins-Korrelation 8
	(b) Extension to Multiple Key Bytes
	(3) Schätzung der ersten 16 Bytes des RC4-Schlüsselstroms 8.
	(4) Umsetzung einer WEP-Attack 8
	dd) Zusammenfassung: WEP-verschlüsseltes WLAN 8
	c) WPA/WPA2-verschlüsseltes WLAN (Pre-Shared-Key) 8
	aa) Verschlüsselung bei WPA/WPA2
	(1) WPA – Temporary Key Integrity Protocol 8
	(2) WPA2 – AES-CCMP
	bb) Schlüsselmanagement in WPA/WPA2
	cc) Authentifizierung und Assoziierung bei WPA/WPA2 90
	dd) Attacks on WPA/WPA2
	(1) Brute-Force-Attack 9
	(a) Offline-Dictionary-Attack (als Ausprägung der
	Brute-Force-Attack) 9
	(b) Dictionary Files
	(c) Precomputed Hash Files (Rainbow Tables) 9.
	(d) Erfolgsaussichten eines Dictionary-Angriffs
	auf WPA/WPA2
	(e) Erweiterung: Deauthentication attack 94
	(f) Umsetzung der Brute-Force-Attack 9.

		(2) Schwachstelle: Vorkonfigurierter w PA/w PAZ-Schlüssel (PSK)	ı 95
		(3) Schwachstelle: Wi-Fi Protected Setup (WPS)	96
		(4) Schwachstelle: Router-Remote Management	98
		(5) Sonstige Attacken auf WPA/WPA2	99
		(a) WPA-TKIP	99
		(aa) Beck/Tews	99
		(bb) Beck und Vanhoef/Piessens	100
		(cc) Umsetzung	101
		(b) WPA2	101
		(aa) Hole196 Vulnerability	101
		(bb) KRACK	101
		ee) Zusammenfassung: WPA/WPA2-verschlüsseltes WLAN	102
		d) Evil-Twin-Attack	102
		e) Zusammenfassung: Der Zugang zum (fremden) Wireless LAN	105
		Mitschneiden des Datenverkehrs im Wireless LAN	105
		a) Sniffen des unverschlüsselten Netzwerkverkehrs (WLAN	103
		ohne Sicherheitsvorkehrungen)	106
		b) Sniffen des WEP-verschlüsselten Netzwerkverkehrs	106
		c) Sniffen des WPA/WPA2-verschlüsselten Netzwerkverkehrs .	107
		d) Sniffen am Evil Twin	109
		e) Zusammenfassung: Mitschneiden des Datenverkehrs im	107
		Wireless LAN	109
	III.	Zusammenfassung: Der Zugriff auf den Datenverkehr	110
	111.	Lokalisieren und Zuordnen des Access Points	110
		Der Zugang zum (fremden) Wireless LAN	111
		Mitschneiden des Datenverkehrs im Wireless LAN	111
_			
F.		altliche) Untersuchung des Netzwerkverkehrs	113
	I.	Einführung und Eingrenzung	113
	II.	Bestimmung des anvisierten Endgerätes	113
	III.	Auswerten der Daten und Herausfiltern der Kommunikationsinhalte	114
		1. Methoden des Mitschneidens und Speicherns der Daten	115
		2. Inhaltsdaten und Zugangsdaten	115
		a) Inhaltsdaten	115
		b) Zugangsdaten/Passwörter	115
		3. E-Mails	116
		a) E-Mail-Client	116
		aa) E-Mails versenden: Simple Mail Transfer Protocol	116
		bb) E-Mails empfangen: POP3/IMAP	116
		b) Webmail	116
		4. Soziale Netzwerke/Webforen/Sonstiges HTTP	117
	***	5. Instant Messaging/Chat	117
	IV.	Besonderheit: Verschlüsselung oberhalb der Netzzugangsschicht	118
		1. Verschlüsseltes World Wide Web	119
		a) Transport Layer Security (SSL/TLS)	119
		b) HTTP über eine SSL/TLS-Verbindung (HTTPs)	121
		c) Angriffe auf HTTPs	121
		aa) Ausgangspunkt: Man-in-the-Middle-Angriff	123

			(1) Address Resolution Protocol Spoofing	123
			(2) Domain Name System Spoofing	124
			SSL-Stripping	125
		cc)	Man-in-the-Middle-Angriff über eigene digitale Zertifikat	te 126
			SSL/TLS-Session-Cookie-Hijacking	129
		ee)	Schutzmaßnahmen: HSTS und HPKP	131
			(1) HTTP Strict Transport Security (HSTS)	131
			(a) Funktionsweise von HSTS	131
			(b) Schwachstellen und Verbreitung von HSTS	132
			(2) HTTP Public Key Pinning (HPKP)	133
		ff)	Weitere Beispiele für Schwachstellen und Zero-Day-Explo	its 134
			(1) BEAST	135
			(2) POODLE	136
			(3) RC4-Verzerrungen	137
			Sonstige Angriffe (Spear-Phishing, Brute-Force-Attack) .	138
		2. Weiter	e offene Forschungsfelder beim Einsatz von Verschlüsselu	ng 139
	V.		nfassung	140
			rten der Daten und Herausfiltern der Kommunikationsinhal	ite 140
		2. Versch	ılüsseltes World Wide Web	140
			Dritter Teil Rechtliche Analyse	
			·	
Н.		eitung		149
	Ι.	Einführung		149
	II.	Abgrenzun	ng zu Quellen-TKÜ und Online-Durchsuchung	150
I.	Die I	Überwachuı	ng lokaler Funknetzwerke ("WLAN-Catching")	152
	I.		ung lokaler Funknetzwerke aus technischer Perspektive	152
			enzierende Betrachtungsweise des Vorgangs	152
			erung der unterschiedlichen Maßnahmen	155
			tliche Betrachtungsweise des Vorgangs?	160
	II.		ung lokaler Funknetzwerke aus rechtlicher Perspektive	162
	11.		e) Erläuterung der maßgeblichen Normen	162
			Bgebliche Grundrechte	162
			Recht auf informationelle Selbstbestimmung, Art. 2 I	102
		uu)	i.V.m. Art. 1 I GG	163
		bb)	Brief-, Post- und Telekommunikationsgeheimnis, Art.	103
		00)	10 I GG	163
		cc)	Gewährleistung der Vertraulichkeit und Integrität infor-	103
		(3)	mationstechnischer Systeme (GVIiS), Art. 2 I i.V.m. Art.	
			1 I GG	164
		44)	Unverletzlichkeit der Wohnung, Art. 13 I GG	165
			Bgebliche strafprozessuale Normen	166
			erste) rechtliche Einordnung	167
			gemeines	167

		b) Die Primärmaßnahme: Mitschneiden und Speichern des	
		Datenverkehrs eines lokalen Funknetzwerks (Abhören des	
		WLAN) inkl. Überwachung des Surfverhaltens	169
		c) Sekundärmaßnahmen	171
			1/1
		aa) Sekundärmaßnahmen I: Maßnahmen ohne Überwin-	
		dung von Sicherheitsvorkehrungen	172
		bb) Sekundärmaßnahmen II: Maßnahmen zur Überwindung	
		von Sicherheitsvorkehrungen (insb. Verschlüsselung)	173
		cc) Sekundärmaßnahmen III: "Informationstechnologische	
		Täuschungen" im Rahmen der Überwachung lokaler	
		Funknetzwerke	175
	TIT		
	III.	Überwachung lokaler Funknetzwerke in Lit. und Rspr	175
		1. Jordan	176
		2. Kleih	179
		3. Weitere Erwähnungen	183
		4. Fazit	185
J.	Ana	llyse der einzelnen Kategorien von Ermittlungsmaßnahmen	186
	I.	Die Primärmaßnahme	186
		1. Erläuterung der Ermittlungsmaßnahme	186
		2. Verfassungsrechtliche Vorgaben	187
		a) Telekommunikationsgeheimnis, Art. 10 I GG	189
		aa) Reichweite des Schutzbereichs des Telekommunikati-	10)
		onsgeheimnisses	189
			105
		(1) Die Übermittlung von Informationen (die Trans-	
		portkomponente des Telekommunikationsgeheim-	
		nisses)	189
		(a) Beginn/Ende/Unterbrechung des Übermittlungs-	
		vorganges (Behandlung der beim Provider zwi-	
		schengespeicherten E-Mails)	190
		(b) Übertragung der Vorgaben auf Daten in lokalen	
		Funknetzwerken (Netzbetreiberlose Telekom-	
		munikation)	192
		(aa) Technologische Aspekte	192
		(bb) Rechtliche Aspekte	192
		(2) Die Überwachung des gesamten Surfverhaltens	
		(die Kommunikationskomponente des Telekom-	
		munikationsgeheimnisses)	194
		(a) Die Kommunikationskomponente in der Defi-	
		nition des $BVerfG$	195
		(b) Abgrenzung von Individual- und Massenkom-	
		munikation	196
		(aa) Subjektives Kriterium	196
		(bb) Objektives Kriterium	196
		(cc) Beschränkung auf klassische, interperso-	170
			107
		nale Kommunikation?	196
		(c) Potentielle Betroffenheit von interpersonaler	
		Kommunikation	199
		(d) Nichtannahmebeschluss des BVerfG	199

		(e) Drohender Wertungswiderspruch	200
		(3) Zusammenfassung: Reichweite des Schutzbereichs	
		des Telekommunikationsgeheimnisses	201
		bb) Eingriff in das Telekommunikationsgeheimnis	202
	b)	Gewährleistung der Vertraulichkeit und Integrität informati-	
			202
			203
		(1) Netzwerkkomponenten als informationstechnisches	
			203
		· ·	204
		· · · · · · · · · · · · · · · · · · ·	205
			205
			20e
		(2) Nutzung der gesamten Bandbreite des Internet-	_00
			207
		dd) Zusammenfassung: Gewährleistung der Vertraulichkeit	
		und Integrität informationstechnischer Systeme, Art. 2 I	
			209
	c)		209
		Recht auf informationelle Selbstbestimmung, Art. 2 I i.V.m.	
	/		212
	e)		212
3.			214
		-	215
			215
		bb) Behandlung der beim Provider zwischengespeicherten	
			217
		cc) Übertragung der Vorgaben auf andere Daten und diffe-	
			218
	b)	Anwendbarkeit von § 102 StPO?	218
			218
	d)	Anwendbarkeit der §§ 99, 100 StPO?	219
		aa) Behandlung der beim Provider zwischengespeicherten	
		E-Mails in der Rechtsprechung durch das BVerfG und	
			220
		bb) Übertragung der Vorgaben auf andere Kommunikations-	
		e	222
		cc) Bewertung der von der Rechtsprechung entwickelten	
		2	222
		, , ,	224
		(1) Gewahrsam des Providers an den Daten im lokalen	
			224
		, ,	225
	e)	v	226
			227
			227
		(2) Definition des Rundesgerichtshofs	225

(3) "Genuin stratvertanrensrechtliche Begriffsbestim-	
mung" – Beschränkung auf zwischenmenschliche	
(interpersonale) Kommunikation?	229
(a) Einschränkende Auslegung in der Literatur	229
(b) Weites Verständnis in der Literatur	231
(c) Rechtsprechung	231
(4) Schlussfolgerung unter Orientierung am grund-	
rechtlichen Schutz durch Art. 10 GG	232
(5) "Telekommunikation" und das Abhören des WLAN	
(WLAN-Catching)	233
(a) Betroffenheit des gesamten Surfverhaltens	234
(b) Übertragungsweg beendet/noch nicht begonnen?	235
(c) Betroffenheit von Datenpaketen, die nur inner-	
halb des lokalen Netzwerks zirkulieren	237
bb) "Überwacht und aufgezeichnet"	238
(1) Zulässigkeit der selbständigen Durchführung einer	
Überwachungsmaßnahme durch die Strafverfol-	
gungsbehörden im Rahmen von § 100a I S. 1 StPO	238
(2) "Überwacht und aufgezeichnet"	240
cc) "Auch ohne Wissen"	240
dd) "Betroffene"	240
ee) Sonstige Anordnungsvoraussetzungen von § 100a I S. 1	
StPO	242
ff) Zusammenfassung: Anwendbarkeit von § 100a I S. 1	
StPO für das Mitschneiden und Speichern des Datenver-	
kehrs eines lokalen Netzwerks (Abhören des WLAN)	
inkl. Überwachung des Surfverhaltens	243
f) Anwendbarkeit von § 100a I S. 2 StPO?	244
aa) Strafprozessuale Begriffsbestimmung des Merkmals "in	
informationstechnische Systeme eingegriffen"	245
bb) Ergänzende Anhaltspunkte aus dem Verfassungsrecht? .	247
cc) Ergänzende Anhaltspunkte durch die Begriffsbestim-	
mung in § 20l II BKAG?	248
dd) Übertragung auf die Primärmaßnahme	248
g) Anwendbarkeit von § 100a I S. 3 StPO?	249
h) Anwendbarkeit von § 100b I StPO?	250
4. Exklusive Wahrnehmung von WLAN-Verkehrsdaten	250
a) Technologische Einzelheiten	250
b) Rechtliche Einordnung	252
aa) Erhebung <i>zusätzlich</i> zu der inhaltlichen Wahrnehmung	250
nach § 100a I S. 1 StPO	252
bb) Separate Erhebung <i>anstelle</i> der inhaltlichen Wahrnehmung	253
(1) Verfassungsrechtliche Vorgaben	253
(2) Strafprozessuale Zulässigkeit	254
(a) Strafprozessuale Zulässigkeit der selbständi-	22.
gen Erhebung von Verkehrsdaten	254
(b) Erhebung nicht beim Erbringer öffentlich zu-	
gänglicher Telekommunikationsdienste, § 100g	25.
V StPO	254

		(c) Kategorien von Verkehrsdaten, § 100g I - III StPO	255
	5.	Zusammenfassung: Zulässigkeit des Mitschneidens und Spei-	
		cherns des Datenverkehrs eines lokalen Funknetzwerks (Abhö-	
			257
II.	Sel		259
11.	1.	Sekundärmaßnahmen I: Maßnahmen ohne Überwindung von	23)
	1.		259
		, 6	259
		b) WLAN lokalisieren und zuordnen; Ermittlung der MAC-	
			260
		, 8	260
			261
		(1) Verfassungsrechtliche Vorgaben	261
		(2) Strafprozessuale Zulässigkeit	263
		c) Maschine-zu-Maschine-Kommunikation: Ermittlung der MAC-	
		Adressen der assoziierten Endgeräte mittels passiver Scanner;	
		•	263
			263
		,	264
		(1) Verfassungsrechtliche Vorgaben	264
			266
			266
			267
		d) Das Senden von Datenpaketen an den Access Point: Verwen-	2.00
			268
			268
			269
		()	269
			272
		e) Zusammenfassung: Sekundärmaßnahmen I: Maßnahmen	
		ohne Überwindung von Sicherheitsvorkehrungen	272
	2.	Sekundärmaßnahmen II: Maßnahmen zur Überwindung von	
			273
		— · · · · · · · · · · · · · · · · · · ·	273
			274
		c) Alleiniges Überwinden von Sicherheitsvorkehrungen von	
			276
			277
			279
			219
		(1) Überwinden der Verschlüsselung von Telekommu-	
		nikation als "Überwachen und Aufzeichnen" i.S.v.	250
		v .	279
		(2) Überwinden der Verschlüsselung von Telekommu-	
		nikation als Annexkompetenz zu § 100a I S. 1	
		StPO?	281
		d) Eingriffe in den Datenverkehr einer Netzwerkinfrastruktur	
			285
			285
			205

		(2)	GVIiS und Abgrenzung zum Telekommunikations-	
			geheimnis	287
		(3)	Sonstige Grundrechte	289
1	bb)	Straf	prozessuale Zulässigkeit	289
		(1)	Anwendbarkeit von § 100a I S. 1 StPO?	290
		(2)	Anwendbarkeit von § 100a I S. 2 StPO?	291
			(a) "Die Überwachung und Aufzeichnung der Te-	
			lekommunikation darf auch in der Weise erfolgen"	292
			(b) "Eingreifen in informationstechnische Systeme"	292
			(c) "Mit technischen Mitteln"	293
			(d) "Von dem Betroffenen genutzte" (informati-	
			onstechnische Systeme)	294
			(e) "Wenn dies notwendig ist, um die Überwa-	
			chung und Aufzeichnung insbesondere in un-	
			verschlüsselter Form zu ermöglichen"	294
			(f) Voraussetzungen des § 100a V und VI StPO	295
			(g) Schlussfolgerung	296
		(3)	Anwendbarkeit von § 100a I S. 3 StPO?	296
		(4)	Anwendbarkeit von § 100b I StPO?	296
			(a) "Eingreifen in ein informationstechnisches System"	297
			(b) "Erheben von Daten aus dem informations-	
			technischen System"	298
			(c) Verhältnis von § 100b StPO zu § 100a StPO? .	299
			(d) Schlussfolgerung	301
e) l	Maß	3nahn	nen mit Auswirkungen auf IT-Endgeräte (aber ohne	
]	Infil	tratio	on) zur Überwindung von Sicherheitsvorkehrungen .	301
ä	aa)	Verf	assungsrechtliche Vorgaben	301
		(1)	Aussagen des BVerfG	302
			(a) Urteil zum "IMSI-Catcher"	302
			(b) Urteil zum NWVerfSchG	302
			(c) Urteil zu den neuen Befugnissen im BKAG	305
			(d) Schlussfolgerung	308
		(2)	Übertragung auf die WLAN-Überwachungsmaßnahme	
			mit Auswirkungen auf IT-Endgeräte (aber ohne	
			Infiltration)	308
			(a) Ausschließlich punktuelle Veränderung am IT-	
			System	308
			(b) Ausschließliche Betroffenheit von Daten mit	
			Bezug zu einer laufenden Telekommunikation .	310
		(3)	Schlussfolgerung	310
I	bb)		Sprozessuale Zulässigkeit	311
		(1)	Anwendbarkeit von § 100a I S. 1 StPO?	311
		(2)	Anwendbarkeit von § 100a I S. 2 StPO?	312
			(a) Auswirkungen der verfassungsrechtlichen Vor-	212
			gaben auf § 100a I S. 2 StPO	312
			(b) Notwendigkeit einer verfassungskonformen	212
			Auslegung von § 100a I S. 2 StPO?	313
			(c) Übertragung auf Maßnahmen mit Auswirkun-	21.
			gen auf IT-Endgeräte	314

Zusamm	nenfassung der rechtlichen Analyse	345
Ergebnis	sse der informationstechnologischen Analyse	341
Kernaus	Ergebnisse und Zusammenfassung sagen des Buches	339
	Vierter Teil	
4.	Zusammenfassung: Sekundärmaßnahmen	336
		336
	(4) Sonstige Anordnungsvoraussetzungen von § 100b StPO	335
	(3) Weitere Merkmale	334
	schen System"	334
		333
	,	333
		332
	ee) Schlussfolgerung	331
	mationelle Selbstbestimmung	329
	dd) Konkurrenzverhältnis von GVIiS und Recht auf infor-	
	i.V.m. Art. 1 I GG	327
	Integrität informationstechnischer Systeme, Art. 2 I	
		223
		325
		<i>32</i> 4
		324 324
	,	224
		322
	b) Verfassungsrechtliche Vorgaben	321
	a) Erläuterung der Ermittlungsmaßnahme	320
	schungen" im Rahmen der Überwachung lokaler Funknetzwerke	320
3.	Sekundärmaßnahmen III: "Informationstechnologische Täu-	
	zur Überwindung von Sicherheitsvorkehrungen	318
	f) Zusammenfassung: Sekundärmaßnahmen II: Maßnahmen	
	(e) Schlussfolgerung	318
		317
		510
		316
		315
		315
		314
	(3) Anwendbarkeit von § 100a I S. 3 StPO?	314
	4. Kernaus Ergebnis	(4) Anwendbarkeit von § 100b I StPO? (a) "Eingreifen in ein informationstechnisches System" (b) "Erheben von Daten aus dem informationstechnischen System" (c) Weitere Merkmale (d) Sonstige Anordnungsvoraussetzungen von § 100b StPO (e) Schlussfolgerung f) Zusammenfassung: Sekundärmaßnahmen II: Maßnahmen zur Überwindung von Sicherheitsvorkehrungen 3. Sekundärmaßnahmen III: "Informationstechnologische Täuschungen" im Rahmen der Überwachung lokaler Funknetzwerke a) Erläuterung der Ermittlungsmaßnahme b) Verfassungsrechtliche Vorgaben aa) Telekommunikationsgeheimnis, Art. 10 I GG bb) Recht auf informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG (1) Staatliche Identitätstäuschungen (2) Übertragung auf "informationstechnologische Täuschungen" im Rahmen der Überwachung lokaler Funknetzwerke cc) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG dd) Konkurrenzverhältnis von GVIiS und Recht auf informationelle Selbstbestimmung ee) Schlussfolgerung c) Strafprozessuale Zulässigkeit aa) Anwendbarkeit von § 100b I StPO? (1) "Eingreifen in ein informationstechnisches System" (2) "Erheben von Daten aus dem informationstechnischen System" (3) Weitere Merkmale (4) Sonstige Anordnungsvoraussetzungen von § 100b StPO d) Zusammenfassung: Sekundärmaßnahmen III: "Informationstechnologische Täuschungen" im Rahmen der Überwachung lokaler Funknetzwerke 4. Zusammenfassung: Sekundärmaßnahmen

	1.	Zulassigkeit der Primarmaßnanme	340
		1. Verfassungsrechtliche Vorgaben	346
		2. Strafprozessuale Zulässigkeit	347
	II.	Zulässigkeit der Sekundärmaßnahmen I	348
	III.	Zulässigkeit der Sekundärmaßnahmen II	349
	IV.		
	IV.	Zulässigkeit der Sekundärmaßnahmen III	350
N.	Schl	ussfolgerung und thesenartiger Überblick	352
	I.	Schlussfolgerung für durchgeführte Maßnahmen des	
		"WLAN-Catchings" vor dem 24.08.2017	352
	II.	Thesenartiger Überblick	353
A nha	na A	Einzelheiten zu der informationstechnologischen Untersuchung	
Anha	ng A		355
	т	und Umsetzung	
	I.	Der Zugriff auf den Datenverkehr eines (fremden) lokalen Netzwerks	355
		1. Lokalisieren und Zuordnen des Access Points	355
		a) Abbildung eines Beacon-Frames und Probe-Response-Frames	355
		b) Beacon- und Probe-Response-Frame bei einem Hidden Network	
		2. Der Zugang zum (fremden) Wireless LAN	356
		a) WEP-verschlüsseltes WLAN	356
		aa) Versendeter Datenteil bei WEP mit unverschlüsseltem	
		Initialisierungsvektor	356
		bb) Einzelheiten zu den Angriffen auf WEP	356
		(1) Fluhrer/Mantin/Shamir	356
		(2) <i>KoreK</i>	359
		(3) Umsetzung einer WEP-Attack	359
		b) WPA/WPA2 (PSK)-verschlüsseltes WLAN	361
		aa) WPA mit Temporary Key Integrity Protocol	361
		(1) RC4-Schlüsselgenerierung (per Frame) in TKIP	361
		(2) (Weitere) Auswirkungen der neuen Schlüsselgene-	501
		rierung	361
		bb) WPA2 mit AES-CCMP	361
		(1) AES-Counter Mode	361
			362
		cc) Einzelheiten zum Schlüsselmanagement	362
		dd) Einzelheiten zur Authentifizierung und Assoziierung	200
		bei WPA/WPA2	363
		ee) Attacks on WPA/WPA2	364
		(1) Brute-Force-Attack	364
		(a) Funktionsweise der Brute-Force-Attack	364
		(b) Erstellen eigener Dictionary Files und Rainbow	
		Tables	365
		(c) Umsetzung der Brute-Force-Attack	365
		(2) Realisierung einer Evil-Twin-Attack	368
	II.	(Inhaltliche) Untersuchung des Netzwerkverkehrs	371
		1. Auswerten der Daten und Herausfiltern der Kommunikationsinhalte	
		a) Tools	371
		aa) Wireshark	371

	bb) Dsniff	371
	b) E-Mails	372
	aa) E-Mails versenden per Simple Mail Transfer Protocol	372
	bb) E-Mails empfangen: POP3/IMAP	372
	cc) Verschlüsseltes World Wide Web	372
	(1) Einzelheiten zur Funktionsweise von SSL/TLS	372
	(1) Emizemental zur Funktionsweise von SSE/TES	312
Anhang B	Detailinformationen zur Arbeitsweise des Internet-Netzwerks	378
I.	Details zu den einzelnen Schichten des TCP/IP-Referenzmodells	378
	Anwendungsschicht	378
	a) SMTP als Beispielprotokoll	378
	aa) Grundlegendes	378
	bb) Kontaktaufnahme	378
	2. Transportschicht	380
	a) TCP als Beispielprotokoll	380
		380
	aa) Grundlegendes	
	bb) Verbindungsorientierung	380
	3. Internetschicht	382
	a) IP(v4) als Beispielprotokoll	382
	aa) Grundlegendes	382
	bb) Adressierung	382
	(1) IP-Adressen	383
	(2) Network Address Translation	384
	cc) Routing und Weiterleitung	385
	dd) Fragmentierung	386
	4. Netzzugangsschicht (Sicherungs-/Bitübertragungsschicht)	386
	a) Ethernet als Beispielprotokoll der Netzzugangsschicht	386
	aa) Grundlegendes	387
	bb) Adressierung	387
	b) IEEE 802.11 (WLAN) als Beispielprotokoll der Netzzu-	
	gangsschicht	388
	aa) Die IEEE 802.11-Protokollfamilie	388
	bb) Medienzugriff	388
	cc) WPA2-Personal (PSK) vs. WPA2-Enterprise (802.1X) .	389
	(1) Authentifzierung	389
	(2) Verschlüsselung	390
II.	Aufbau einzelner Protokolldateneinheiten	390
	1. Überblick	390
	2. Aufbau einer Nachricht am Beispiel von SMTP	391
	3. Aufbau eines Segments am Beispiel von TCP	393
	4. Aufbau eines Datagramms am Beispiel von IPv4	394
	5. Aufbau eines Frames am Beispiel von Ethernet	396
	6. Aufbau eines Frames am Beispiel des 802.11-Protokolls	398
	•	
Anhang C	Kryptologischer Hintergrund	400
I.	Kryptographische Algorithmen	400
	1. Symmetrische Algorithmen	400

a) Einführung	400
aa) Permutation und Substitution	400
bb) Blockchiffren vs. Stromchiffren	401
cc) Produktchiffren/Substitutions-Permutationschiffren	402
dd) Vernam-Chiffre/One-Time-Pad	402
b) Ausgewählte Blockchiffren	403
aa) Feistel-Chiffre	403
bb) Data Encryption Standard (DES)	405
(1) Überblick über die Funktionsweise von DES	405
(2) Die Erzeugung der Rundenschlüssel	407
(3) Eine Runde des DES-Algorithmus	408
(a) Die Rundenfunktion f	408
(aa) Expansionspermutation und	
XOR-Verknüpfung	408
(bb) S-Box-Substitution	410
(cc) P-Box-Permutation	412
(b) Verbindung von linker und rechter Hälfte	412
(4) Die weiteren Teilschritte	412
(a) Anfangspermutation	412
(b) Schlusspermutation	413
(5) Entschlüsselung mit DES	413
(6) Sicherheit von DES	413
(7) Triple-DES	414
cc) Advanced Encryption Standard (AES)	415
(1) Einordnung von AES	415
(2) Überblick über die Funktionsweise von AES	415
(3) Eine Runde des AES-Algorithmus	416
(a) Die Rundenfunktion f	418
(aa) Der endliche Körper $GF(2^8)$	418
(bb) Polynome	419
(cc) Byte-Substitution (SubBytes-Operation) .	420
(dd) Zeilenverschiebung (ShiftRows-Operation)	421
(ee) Spaltentransformation (MixColumns-Op.)	422
(b) XOR-Verknüpfung mit Rundenschlüssel (Key-	122
Addition)	423
(4) Erzeugung der Rundenschlüssel (Schlüsselexpansion)	423
(5) Entschlüsselung mit AES	424
(6) Sicherheit von AES	425
dd) International Data Encryption Algorithm (IDEA)	425
c) Betriebsmodi der Blockchiffren	426
aa) ECB-Mode	426
bb) CBC-Mode	427
cc) CTR-Mode	427
dd) CFB-Mode	428
ee) OFB-Mode	428
d) Ausgewählte Stromchiffren	429
aa) Allgemeines Prinzip von Stromchiffren	429
bb) RC4/Arcfour	430
(1) Überblick über die Funktionsweise von RC4	430
(1) Obelotick does die Pulikuolisweise von RC4	TJ 1

	(2	KSA-Algorithmus	431
		(a) Die einzelnen Schritte des Algorithmus	431
		(b) Beispielrechnung (KSA)	432
	(3		433
		(a) Die einzelnen Schritte des Algorithmus	433
		(b) Beispielrechnung	434
	(4		435
	(5		436
	cc) W	Veitere Stromchiffren	436
2.	Asymmet	trische Algorithmen	437
		nrung in die Public-Key-Kryptographie	437
		inwegfunktion	437
	bb) Tr	rapdoor-Einwegfunktion	438
	cc) M	Tathematische Umsetzung	438
	(1		438
	(2		439
	b) Der RS	SA-Algorithmus	439
	aa) Da	as zugrunde liegende Prinzip	440
	bb) M	lathematische Umsetzung des Prinzips	441
		orüberlegungen	443
	(1		443
	(2	Voraussetzungen	444
	(3		444
	(4	Ausgabe des Geheimtextes als darstellbarer Text	446
	(5) "Berechnung" der Primzahlen	447
	dd) Di	ie einzelnen Schritte des Algorithmus	448
		eispiel eines RSA-Verschlüsselungsvorganges	450
	ff) Si	cherheitsprinzip von RSA	457
	(1		457
	(2	Entschlüsseln ohne geheimen Schlüssel durch In-	
		vertieren	458
	(3		459
	c) Diffie-	Hellman-Schlüsselvereinbarung	459
		as zugrunde liegende Prinzip	459
	bb) Pa	arameterauswahl	461
	(1		461
	(2		461
	(3	Geheimer Exponent x	462
	cc) Di	ie einzelnen Schritte des Algorithmus	462
	dd) Be	eispielrechnung	463
		Tathematische Umsetzung des Prinzips	464
	ff) Si	cherheitsprinzip von Diffie-Hellman	465
	(1		465
	(2	Rückschluss auf den Schlüssel direkt	466
	gg) M	lehrpersonen	466
	d) Elgam	al-Algorithmus	467
	aa) Da	as zugrunde liegende Prinzip	467
	bb) Di	ie einzelnen Schritte des Algorithmus	468
		aicnialrachnung	460

	dd) Mathematische Umsetzung des Prinzips	472
	ee) Sicherheitsprinzip von Elgamal	473
II.	Public-Key-Infrastrukturen	474
	1. Elemente einer PKI	474
	a) Digitale Zertifikate	474
	b) Certification Authority (CA)	474
	c) Root-CA	475
	d) Registration Authority (RA)	475
	e) Directory Service	475
	f) Certificate Revocation List	476
	2. Vertrauensmodelle	476
	a) Direct Trust	476
	b) Web of Trust	476
	c) Hierarchical Trust	477
	aa) Einstufige Hierarchie	477
	bb) Mehrstufige Hierarchie	477
	cc) Cross-Zertifizierung	477
***	3. Lösung des Man-in-the-Middle-Problems durch eine PKI?	478
III.	Digitale Signaturen	480
	1. RSA als Signaturverfahren	480
	2. Elgamal-Signaturverfahren	482
	a) Die einzelnen Schritte des Signaturverfahrens	482
	b) Sicherheit des Elgamal-Signaturverfahrens	483 484
	Digital Signature Algorithm (DSA)	484
	b) Sicherheit des Elgamal-Signaturverfahrens	486
IV.	Kryptologische Hashfunktionen	486
1 V.	Überblick über die Funktionsweise von Hashfunktionen	486
	Allgemeine Sicherheitsaspekte von Hashfunktionen	487
	Wichtige (eigenständige) Hashfunktionen	488
	a) MD5	488
	b) SHA-Familie	488
	c) RIPEMD-160	489
	4. Message Authentication Codes (MAC)	489
Anhang D	Mathematische Grundlagen und Zeichenkodierung	491
I.	Mathematische Grundlagen	491
	1. Natürliche und ganze Zahlen	491
	2. Gruppen und Körper	492
	a) Gruppen	492
	b) Ringe	493
	c) Körper	493
	3. Die multiplikative Inverse	494
	4. Teilbarkeit und Primzahlen	494
	a) Teiler	494
	b) Größter gemeinsamer Teiler	495 495
	c) Die Euler'sche φ-Funktion	495
	d) Primzahlen	493

Inhaltsverzeichnis

	e) Die Euler'sche ϕ -Funktion und Primzahlen
	f) Primfaktorzerlegung
	5. Modulare Arithmetik
	a) Division mit Rest
	b) Kongruenzen
	c) Restklassen, Restklassengruppe, Restklassenring 49
	d) Euklidischer Algorithmus
	e) Vielfachsummendarstellung 50
	aa) Erweiterter euklidischer Algorithmus 50
	bb) Die multiplikative Inverse modulo einer Zahl 50
	6. Der kleine Fermat und der Satz von Euler-Fermat 50
	a) Der kleine Satz von Fermat
	b) Der Satz von Euler-Fermat
	7. Berechnung großer Potenzen
	a) Square-and-Multiply-Algorithmus 50
	aa) Allgemein
	bb) Modulo-Rechnung
	b) Binäre Modulo-Exponentiation
	8. Exklusives Oder bzw. XOR-Verknüpfung 50
II.	Zeichenkodierung
Quellen im	World Wide Web
Zitierte Ent	scheidungen
Literaturver	rzeichnis
Stichwortre	gister