

Inhalt

1	Grundlagen	1
I.	Begriff der Identität	1
1.	Divergierende Begriffe der Identität	1
2.	Begriff der Identität im rechtlichen Sinne	3
3.	Identitätsbegriff der Studie	4
4.	Begriff der Identität im technischen Sinne	5
II.	Identitätsmissbrauch und Identitätsdiebstahl	9
1.	Der Begriff des Identitätsmissbrauchs	9
2.	Der Begriff des Identitätsdiebstahls	10
3.	Schutz von Identitäten (Überblick)	11
III.	Fallgruppen des Identitätsdiebstahls und -missbrauchs	12
1.	Identitätsdiebstahl und -missbrauch ohne IT-Bezug (Überblick)	12
2.	Identitätsdiebstahl und -missbrauch mit IT-Bezug (Überblick)	14
IV.	Ähnliche Phänomene	15
2	Strukturen von Identitätsdiebstahl und -missbrauch unter Einsatz von Informationstechnologie	17
I.	Vortäuschung einer technisch nicht geschützten Identität (Spoofing)	17
II.	Diebstahl von durch Wissen geschützten Identitätsdaten	25
1.	Benutzername/Passwort, PIN	25
2.	TAN	27
3.	iTAN	28
III.	Man-in-the-Middle-Angriffe gegen den Nachweis einer Identität durch Besitz	29
1.	Hardwaretokens	30
2.	One-Time Passwords (OTP)/elektronische TANs (eTAN)	35
3.	eTAN+	35
4.	mTAN	36
5.	HBCI/FinTS	37

6.	FinTS+/Secoder	38
7.	(Qualifizierte) elektronische Signaturen	38
8.	SSL Clientzertifikate	39
IV.	Weitere Methoden zum Nachweis einer Identität	40
1.	Biometrie	40
2.	CAPTCHAs	43
V.	Man-in-the-Middle-Angriffe	48
1.	Man-in-the-Middle im Internet	48
2.	Man-in-the-Middle im PC	50
VI.	Standardsicherheitsmaßnahmen	56
1.	Antivirenprogramme	57
2.	Personal Firewall	60
3.	Firefox-Add-Ons	62
	4. Weitere Standardsicherheitsmaßnahmen	67
3	Künftige Entwicklung von Identitätsmissbrauch und Identitätsdiebstahl	71
I.	Prognose: Angriffsszenarien	71
1.	Business Cases zukünftiger Angreifer	71
2.	Umgehung von Standardsicherheitsmaßnahmen	73
3.	Umgehung spezieller softwarebasierter Schutzmechanismen	82
4.	Umgehung spezieller hardwarebasierter Schutzmechanismen (Chipkarten, HSM)	83
5.	Umgehung von Sicherheitsmechanismen auf Serverseite	84
6.	Netzwerkbasierte Angriffe	87
7.	Klassische Malware: neue Trends	92
8.	Social Engineering	96
9.	Malware + JavaScript, Web 2.0-Angriffe	101
10.	Google-Hacking	107
II.	Prognosen: Zielplattformen	111
1.	Zielplattformen	111
2.	Neue Computing-Paradigmen: Browsetechnologien	123
3.	Neue Computing-Paradigmen: Servertechnologien	126
4.	Neue Computing-Paradigmen: Kommunikationstechnologien	128
5.	Neue Computing-Paradigmen: Web 2.0 und SaaS	135
6.	Neue Computing-Paradigmen: Webservices, SOAP und Cloud Computing	138
7.	Neue Computing-Paradigmen: Single-Sign-On	141
8.	Neue Computing-Paradigmen: neue Schutzmaßnahmen	144
9.	Kombination mehrerer Angriffstechniken	145
4	Identitätsdiebstahl und neuer Personalausweis	151
I.	Einführung	151
1.	Der elektronische Identitätsnachweis	151

Inhalt	ix
2. Einsatzbereiche des elektronischen Identitätsnachweises	153
II. Technische Rahmenbedingungen	154
1. Bestandteile des Neuer-Personalausweis-Gesamtsystems	157
2. Beschreibung der Anwendungsmöglichkeiten des neuen Personalausweises	158
3. Beschreibung der Protokolle des neuen Personalausweises	164
4. Art des Chipkartenlesers	170
5. Kombination der einzelnen kryptografischen Protokolle (für Webanwendungen: SSL)	172
6. Klassifikation der Dienste auf Basis des neuen Personalausweises	174
III. Rechtliche Rahmenbedingungen des neuen Personalausweises	176
1. Überblick	176
2. Das Personalausweisgesetz	176
3. Gesetzliche Regeln zum Einsatz des Personalausweises	179
4. AGB mit Bezugnahme auf den Personalausweis	185
5. Ergebnis: Die Bedeutung des Personalausweises als Identitätsnachweis	188
IV. Verhinderung von Identitätsdiebstahl und -missbrauch durch Einsatz des neuen Personalausweises	190
1. Realistische Ziele	191
2. Mögliche Ziele	192
5 Rechtsfragen des Identitätsmissbrauchs	195
I. Überblick	195
1. Strafrechtliche Aspekte	195
2. Zivilrechtliche Aspekte	198
II. Gesetzliche Rahmenbedingungen	200
1. Grundrechtsschutz	200
2. Datenschutzrecht	203
3. Strafrecht	207
4. Zivilrecht	211
III. Aktuelle Geschäftsbedingungen	213
1. Regeln zum Identitätsmissbrauch in AGB	214
2. Risikoverteilung und Haftungsregeln in AGB	229
IV. Strafbarkeit de lege lata	233
1. Strafbarkeit des Erlangens der fremden Identität (Identitätsdiebstahl)	233
2. Strafbarkeit des Verwendens der fremden Identität (Identitätsmissbrauch)	244
3. Probleme der Rechtsanwendung	252
V. Risikotragung bei Identitätsmissbrauch	253
1. Risikoverteilung im Onlinebanking	254
2. Risikoverteilung bei Handelsplattformen	264
3. Ergebnis und Ausblick	268

VI.	Verkehrspflichten im Internet	269
1.	Verkehrspflichten der Anbieter	270
2.	Verkehrspflichten der Internetnutzer	272
VII.	Verhaltenspflichten und Haftung der Identitätsinhaber	275
1.	Grundlagen der Haftung	275
2.	Verhaltenspflichten des Identitätsinhabers in Fallgruppen	281
3.	Haftung für Pflichtverletzungen	290
4.	Haftungsbeschränkungen	292
VIII.	Verhaltenspflichten und Haftung der Anbieter	294
1.	Überblick	294
2.	Verhaltenspflichten im Onlinebanking	295
3.	Verhaltenspflichten in anderen Feldern	297
IX.	Zivilrechtliche Beweisfragen	299
1.	Überblick	299
2.	Der Beweis der Urheberschaft im gerichtlichen Verfahren	300
3.	Der Anscheinsbeweis für die Urheberschaft elektronisch übermittelter Erklärungen	303
6	Deutschland im internationalen Vergleich	317
I.	Technische Rahmenbedingungen in anderen Staaten (Überblick)	318
1.	Im Onlinebanking (eTAN+, FinTS/HBCI, Secoder, mTAN)	318
2.	In ausgewählten anderen Diensten	319
II.	Überblick zu Angriffs- und Schadensszenarien	320
1.	Vergleich der Angriffsszenarien im Bereich Onlinebanking: transaktions- vs. kontobezogene Sicherheitsmechanismen	323
2.	Vergleich der Angriffsszenarien in ausgewählten weiteren Diensten	324
III.	Rechtliche Rahmenbedingungen in anderen Staaten (Überblick) ...	325
1.	Strafbarkeit von Identitätsdiebstahl und -missbrauch (de lege lata)	325
2.	Zivilrechtliche Verantwortlichkeit für Identitätsmissbrauch	351
IV.	Die Positionierung Deutschlands im Vergleich	356
1.	Technisch: Vergleich im Bereich Onlinebanking (Überblick)	356
2.	Rechtlich: Vergleich im Bereich Onlinebanking (Überblick) ...	357
7	Handlungsoptionen/Abwehrmaßnahmen und Empfehlungen	359
I.	Technische Maßnahmen	359
1.	Empfehlungen zum Einsatz von Standardsicherheitsmaßnahmen	359
2.	Empfehlungen zum Einsatz bestimmter Technologien	360
3.	Empfehlungen zur Erstellung von Best-Practice-Richtlinien für bestimmte Einsatzszenarien	364

4. Aufzeigen gezielten Forschungsbedarfs (z. B. in den Bereichen Malware, Bot-Netze, Browsersicherheit, Betriebssystemsicherheit, kryptografische Sicherheitsmodelle für reale Applikationen)	365
II. Organisatorische Maßnahmen	367
1. Schulungsinhalte	368
2. Meldestellen für entdeckte Schwachstellen, neue Angriffe etc. mit Anreizmechanismen (nicht monetär)	373
III. Polizeiliche Maßnahmen	373
1. Zentrale Meldestelle (z. B. zur Meldung von Phishingservern)	374
2. Information zur Prävention/Aufklärung	374
IV. Gesetzliche/regulatorische Maßnahmen	374
1. Vorgaben zur Produktgestaltung	375
2. Umgang mit gespeicherten Kundendaten	376
3. Strafrechtliche Maßnahmen	377
4. Gesetzliche Haftungsregeln für Anbieter und Nutzer	379
5. Regulierung von Verhaltenspflichten	380
V. Information und Aufklärung der Nutzer	387
VI. Internationale Abkommen für das Internet (Strafverfolgung)	389
VII. Aufwandsschätzungen für die Umsetzung	390
VIII. Risiken	390
1. Gezielte Angriffe	390
2. Spionageangriffe	390
Literatur	391
I. Technik	391
II. Recht	395