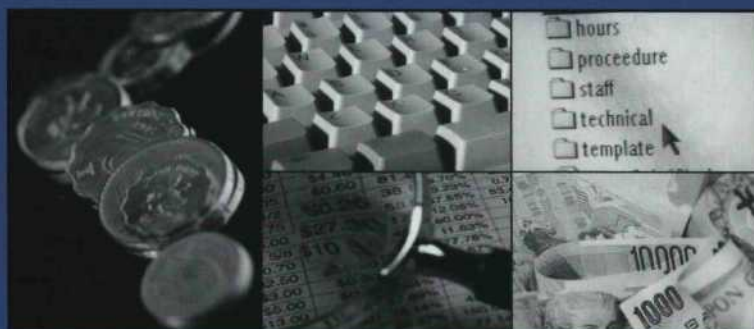


Forensic Computing



Roger Auinger
Peter R. Bitterli
Daniel Brunner
Daniel Eugster
Dr. Paul Schöbi
Stephan Schwab
Dirk Spacek
Anne-Marie Suter
Prof. Dr. Rolf H. Weber

Inhaltsverzeichnis

1	EINLEITUNG.....	14
1.1	Der grössere Kontext - Bedrohungen der Cyber-Gesellschaft.....	14
1.2	Breites Spektrum von Angriffsmöglichkeiten.....	14
1.3	Computerkriminalität, Informatikkriminalität, Cyberkriminalität.....	15
1.4	Hohes Risiko und noch mangelnde Strafverfolgung.....	16
1.5	Schlussfolgerung.....	18
2	RECHTLICHE RAHMENBEDINGUNGEN FÜR FORENSIC COMPUTING.....	19
2.1	Einleitung.....	19
2.2	Strafrecht.....	22
2.2.1	Ausgangslage: Handlung erfüllt einen Straftatbestand.....	22
2.2.2	Begriff der "Computerkriminalität".....	23
2.2.3	Spezifische Computerdelikte.....	24
2.2.3.1	Unbefugte Datenbeschaffung (Art. 143 StGB).....	24
2.2.3.2	Unbefugtes Eindringen (Hacken) in ein Datensystem (Art. 143 ^{bis} StGB).....	25
2.2.3.3	Datenbeschädigung (Art. 144 ^{bis} StGB).....	27
2.2.3.4	Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB).....	27
2.2.3.5	Erschleichen einer Leistung (Art. 150 StGB).....	28
2.2.3.6	Urkundenfälschung (Art. 251 i.V.m. Art. 110 StGB).....	29
2.2.3.7	Denial of Service-Attacken.....	31
2.2.4	Nicht spezifische Computerdelikte.....	31
2.2.4.1	Verletzung von Immaterialgüterrechten.....	32
2.2.4.2	Unlauterer Wettbewerb.....	32
2.2.4.3	Verletzung von Schweigepflichten (Geheimnisschutznormen).....	33
2.2.4.4	Pornographie (Art. 197 StGB).....	34
2.2.4.5	Unerlaubte Glücksspiele.....	35
2.2.4.6	Überwachung.....	37
2.2.4.7	Rassendiskriminierung (Art. 261 ^{bis} StGB).....	39
2.2.5	Ausnahmen von der Strafbarkeit.....	40
2.2.5.1	Gesetzliche, amtliche oder berufliche Pflichten.....	40
2.2.5.2	Agent Provocateur.....	40
2.2.5.3	Notwehr und Notstand.....	41
2.3	Persönlichkeits- und Datenschutzrecht.....	42
2.3.1	Persönlichkeitsrecht.....	42
2.3.1.1	Begriff.....	42
2.3.1.2	Spamming.....	42
2.3.1.3	Namensanmassung.....	43

2.3.1.4	Persönlichkeitsrecht im Arbeitsrecht.....	44
2.3.1.5	Klagerechte	46
2.3.2	Datenschutzrecht.....	47
2.4	Vertragsrecht.....	50
2.4.1	Allgemeine Vertragsprinzipien im Internet	50
2.4.2	EDV-Verträge.....	54
2.4.3	Ausservertragliches Haftpflichtrecht	55
2.4.4	Vereinbarung zwischen (geschädigtem) Unternehmen und Täter	56
2.5	Gesellschafts- und Bankenrecht	58
2.5.1	Gesellschaftsrechtliche Zuständigkeit für IT-Infrastruktur	58
2.5.2	Elektronischer Zahlungsverkehr	60
2.6	Beweisrecht.....	62
2.6.1	Beweismittel	62
2.6.2	Beweislast	65
3	GEFÄHRDUNGSANALYSE.....	66
3.1	Grundlagen der Gefährdungsanalyse.....	66
3.1.1	Förderliche Faktoren (<i>enabler</i>).....	67
3.1.1.1	Hohe Komplexität der Geschäftsabläufe	67
3.1.1.2	Grosses Transaktionsvolumen	67
3.1.1.3	Fehlende Sicherheitskonzepte, Richtlinien und Standards.....	68
3.1.1.4	Unwirksame oder fehlende Sicherheitsmassnahmen.....	68
3.1.1.5	Fehlendes Internes Kontrollsystem (IKS), mangelhaftes Kontrollverfahren.....	68
3.1.1.6	Fehlende Funktionentrennung	69
3.1.1.7	Fehlende Nachvollziehbarkeit (Dokumentation).....	70
3.1.1.8	Ungenügende Überwachung.....	70
3.1.1.9	Blindes Vertrauen in Technik oder Einzelpersonen	71
3.1.1.10	Fehlendes Sicherheitsbewusstsein	71
3.1.2	Warnsignale (<i>red flags</i>)	72
3.1.2.1	Storni, Korrekturbuchungen	73
3.1.2.2	Auffälligkeiten im Prozessablauf.....	74
3.1.2.3	Zahlreiche Kundenreklamationen.....	74
3.1.2.4	Anfragen der Presse/Medien.....	74
3.1.2.5	Überstunden, Wochenendarbeit, keine längeren Ferien	75
3.1.2.6	Schlüsselpersonen, ohne die es nicht geht.....	75
3.1.2.7	Lebensstil und Einkommen stimmen nicht überein.....	75
3.1.2.8	Ungewöhnliches gesellschaftliches Umfeld oder unerwartete Veränderungen	76
3.1.2.9	Unkooperatives oder sonstwie auffälliges Verhalten	76
3.1.2.10	Atypische Kundenbeziehungen	77

3.1.2.11	Warnsignale im Zusammenhang mit möglicher Geldwäscherei.....	77
3.1.3	Auslöser einer deliktischen Handlung (Trigger)	77
3.1.3.1	Schlechtes Arbeitsklima, ständige Überforderung, Zeitdruck, Leistungsdruck.....	77
3.1.3.2	Unklare Führungsstruktur, inkompetente Führung (Stil, Schwächen)	78
3.1.3.3	Hohe Personalfuktuation (auch beim Kader)	78
3.1.3.4	Androhung einer Entlassung, erfolgte Entlassung, Arbeitsplatzabbau.....	78
3.1.3.5	Überschwänglicher Lebensstil und entsprechende Bedürfnisse.....	79
3.1.3.6	Alkohol, Drogensucht und Krisen	79
3.1.4	Auslöser der Untersuchung.....	80
3.2	Durchführung der Gefährdungsanalyse.....	80
3.2.1	Einführung	80
3.2.2	Erfassung von Faktoren einer Gefährdungsanalyse	85
3.2.3	Vorgehen zum Analysieren der Gefährdungsfaktoren	85
3.2.3.1	Sammeln/Erheben.....	85
3.2.3.2	Auswerten	89
3.2.3.3	Darstellen	89
3.2.3.4	Kommunizieren.....	94
3.2.3.5	Handeln	95
3.2.4	Hilfsmittel	96
3.2.5	Unternehmensspezifische Auswahl von Faktoren.....	96
3.2.5.1	Auswahl pro Kunde/Unternehmen	96
3.2.5.2	Auswahl/Bestimmung der Faktoren	97
3.2.6	Für KMU geeignete Faktoren.....	99
4	DURCHFÜHRUNG EINER ERMITTLUNG	101
4.1	Grundsätzliche Aspekte	101
4.1.1	Ziel einer Ermittlung.....	101
4.1.2	Zusammensetzung des Ermittlungsteams.....	102
4.1.2.1	Zentrale Ermittlungsverantwortung.....	102
4.1.2.2	Kernteam.....	102
4.1.2.3	Erweitertes Team	102
4.1.3	Interne Kommunikation	104
4.1.3.1	Technische vs. Managementkommunikation	104
4.1.3.2	Führungs- & Informations-Rhythmus	104
4.1.3.3	Ermittlungsbezogene Interaktion mit Externen	104
4.1.3.4	Journalführung	105
4.1.4	Presse	105
4.1.5	Unabhängigkeit der Ermittler	106
4.1.6	Schutz der Privatsphäre in der Praxis	106

4.2	Ablauf einer Untersuchung.....	106
4.2.1	Meldungseingang.....	108
4.2.2	Überblick verschaffen.....	109
4.2.3	Sofortmassnahmen.....	111
4.2.4	Umfeld und Abhängigkeiten verstehen	112
4.2.5	Hypothese	114
4.2.6	Fachkenntnisse und Unabhängigkeit.....	114
4.2.7	Beschaffung von Beweismitteln/Daten	115
4.2.7.1	Grundsätze für die Erlangung beweiskräftiger elektronischer Informationen.....	118
4.2.7.2	Arten der Sicherstellung	120
4.2.7.3	Lagerung von elektronischen Beweismitteln.....	123
4.2.7.4	Orte von elektronischen Beweismitteln.....	123
4.2.8	Beweismittel- und Datenanalyse	125
4.2.8.1	Analyse der Beweismittel	125
4.2.8.2	Kriterien für eine hohe Beweiskraft der Beweismittel	126
4.2.9	Einvernahme	127
4.2.10	Strafanzeige.....	128
4.2.11	Nachbearbeitung und Lehren.....	128
5	TECHNISCHE ASPEKTE	129
5.1	Arten von elektronischen Spuren.....	130
5.1.1	Benutzerdateien.....	130
5.1.2	Nutzbare Daten von Anwendungen und Betriebssystem	130
5.1.2.1	Protokolldateien	131
5.1.2.2	Temporäre Files	132
5.1.2.3	Eingabehilfen	133
5.1.2.4	Konfigurationsdateien, Registry	134
5.1.2.5	Zeitangaben zu Dateien	134
5.1.2.6	Zwischenspeicher (Cache).....	135
5.1.3	Rekonstruierbare, systemnahe Datenrückstände	135
5.1.3.1	Gelöschte Dateien	135
5.1.3.2	Freier Speicherbereich (Slack Space).....	137
5.1.4	Flüchtige Spuren	139
5.1.4.1	Arbeitsspeicher (RAM).....	139
5.1.4.2	Laufende Prozesse	140
5.1.5	Physische Speicheranalyse	140
5.2	Fundorte elektronischer Spuren bei Services	140
5.2.1	eMail mit Mail-Protokollen	141
5.2.2	eMail über Web.....	142
5.2.3	Web Server.....	143

5.2.4	Surfen	147
5.2.5	Teilnahme in Foren/Chats, etc.	148
5.2.6	Drucken/Scannen/Faxen	149
5.3	Fundorte bei speziellen Aktionen und Ereignissen	150
5.3.1	Server Faking, man-in-the-middle	151
5.3.2	Trojaner, Viren.....	152
5.4	Knackpunkte in der Praxis.....	152
5.4.1	Rechner stoppen.....	153
5.4.2	Schutz vor absichtlicher und unabsichtlicher Veränderung	156
5.4.3	Rechnerzeit	157
5.4.4	Grosse Datenmengen	157
5.4.5	Zeitdruck	157
5.4.6	Identifikation der relevanten Systeme	158
5.4.7	Passwortschutz	158
5.4.8	Verschlüsselung	158
5.4.9	Alte Datenträger.....	158
5.4.10	Defekte Datenträger	159
5.4.11	Verschiedenste Hardware	159
5.4.12	Treiberproblematik	159
5.5	Hilfsmittel und Werkzeuge.....	160
5.5.1	Produkte	160
6	PRÄVENTION.....	161
6.1	Ziel der Prävention und grundsätzliches Vorgehen.....	161
6.2	Konsequente Implementierung von Grundschutzmassnahmen.....	161
6.3	Risk-Management basierend auf Gefährdungsanalyse.....	162
6.4	Konsequentes Vorgehen bei Verdachtsfällen und Strafanzeige bei Delikten.....	162
6.5	Ausgewählte präventive Informatik-Massnahmen	163
6.6	Prävention basierend auf systematischem Ansatz	164
6.6.1	Anwendung des Wirkungskreis-Modells in der Prävention.....	164
6.6.2	Konkretes Anwendungsbeispiel	164
6.6.3	Weitere präventive Massnahmen im Personalbereich.....	166
A.	BEISPIEL VERTRAULICHKEITSVEREINBARUNG.....	167
B.	LITERATURVERZEICHNIS.....	169