

# Inhaltsverzeichnis

Vorwort .....	III
Inhaltsverzeichnis .....	V
Abbildungsverzeichnis .....	VI
1 Einleitung .....	1
2 Hacking, Friendly-Hacking, Compliance und Risikomanagement .....	5
2.1 Hacking versus Friendly-Hacking .....	5
2.2 Compliance und Compliance-Risiken .....	7
2.3 Risikomanagement .....	7
3 Compliance-Risiko 1: §202 a StGB – Ausspähen von Daten .....	11
3.1 Bisherige und aktuelle Strafbarkeit durch §202 a StGB .....	11
3.2 Auswirkungen des §202 a StGB für Unternehmen .....	19
3.3 Auswirkungen des §202 a StGB für die interne IT-Abteilung .....	20
3.4 Auswirkungen des §202 a StGB für externe IT-Berater .....	20
4 Compliance-Risiko 2: §202 b StGB – Abfangen von Daten .....	23
4.1 Aktuelle Strafbarkeit durch §202 b StGB .....	23
4.2 Auswirkungen des §202 b StGB für Unternehmen .....	27
4.3 Auswirkungen des §202 b StGB für die interne IT-Abteilung .....	28
4.4 Auswirkungen des §202 b StGB für externe IT-Berater .....	28
5 Compliance-Risiko 3: §202 c StGB – Vorbereiten des Ausspähens von Daten ...	29
5.1 Aktuelle Strafbarkeit durch §202 c StGB .....	29
5.2 Auswirkungen des §202 c StGB für Unternehmen .....	33
5.3 Auswirkungen des §202 c StGB für die interne IT-Abteilung .....	35
5.4 Auswirkungen des §202 c StGB für externe IT-Berater .....	35
6 Handlungsmaßnahmen zur Prävention der Strafbarkeit .....	39
6.1 Handlungsmaßnahmen für das Management .....	39
6.2 Handlungsmaßnahmen für die interne IT-Abteilung .....	41
6.3 Handlungsmaßnahmen für externe IT-Berater .....	44
7 Fallbeispiele .....	47
7.1 Fallbeispiel 1: Interner Penetrationstest .....	47
7.2 Fallbeispiel 2: IT-Abteilung ohne Dokumentation .....	48
7.3 Fallbeispiel 3: Engagierter IT-Mitarbeiter .....	49
7.4 Fallbeispiel 4: IT-Berater mit allgemeinem Auftrag .....	50
7.5 Fallbeispiel 5: Vertriebsorientierter IT-Berater .....	51
8 Ausblick und Fazit .....	53
Quellenverzeichnis .....	57