Inhaltsverzeichnis

1 Einleitung 1
1.1 Der CEO-Fraud 3
Quellen 8

2 Grundlagen 9
2.1 Erkennen von Sicherheitsvorfällen 17
2.1.1 Methoden zur Erkennung von Sicherheitsvorfällen 20
2.1.2 Fazit: mehrere Werkzeuge einsetzen 29
2.1.3 Reaktion auf Sicherheitsvorfälle 30
2.1.4 Aus dem Schaden anderer lernen 32
Quellen 33

3 Was als normaler Angriff beginnt und in professioneller Spionage endet 35
3.1 Die Kontaktaufnahme 35
3.2 Erste Aktionen 37
3.3 Analysephase 44
3.4 Auswerten der Maßnahmen und Einleiten weiterer Schritte 45
3.5 Nach dem Incident ist vor der Haftung 49
Quellen 61

4 Wenn digitale Forensik an Grenzen stößt 63
4.1 Die Kontaktaufnahme 63
4.2 Erste Aktionen 65
4.3 Analysephase 65
4.4 Auswerten der Maßnahmen und Einleiten nächster Schritte 74
4.4.1 Analyse möglicher Fremdzugriffe 74

5 Massenangriff oder gezielter Angriff, die Grenzen verschwimmen 85
5.1 Die Kontaktaufnahme 85
5.2 Erste Aktionen 87
5.3 Analysephase 91
Quellen 100

6 Der eigene Administrator als Angreifer 101
6.1 Die Kontaktaufnahme 101
6.2 Erste Aktionen 103
6.3 Analysephase 105

6.4 Auswerten der Maßnahmen und Einleiten weiterer Schritte 106
Quellen 113

7 **Vorbereitung auf den Ernstfall** 115
7.1 Sicherheitsvorfälle, die schiefgelaufen sind 116
7.1.1 Der Mitarbeiter, der Daten entwendete und dann selbst zum Opfer wurde 116
7.1.2 Die Konkurrenz hört mit 119
7.2 Grundlagen der organisatorischen Sicherheit 122
7.2.1 Das Fundament der organisatorischen Sicherheit 125
7.2.2 Teamwork makes the dream work 134
7.3 Sogar das billigste Hotel hat einen Feuerfluchtplan, aber die wenigstens Unternehmen einen IT-Incident-Guide 154
7.4 Definition Sicherheitsvorfall 155
7.5 Erkennen von Ernstfällen 156
7.5.1 Die Erkennung von Angriffen im Detail 157
7.6 Verantwortlichkeiten 169
7.7 Eskalationsstrategie 171
7.7.1 Schritt 1: Festlegung der Eskalationswege 174
7.7.2 Schritt 2: Entscheidungshilfe für Eskalation 174
7.7.3 Schritt 3: Art und Weise der Eskalation 175

7.8 Train hard, win easy 176
Quellen 179

8 Schlusswort 181