

Inhaltsübersicht

| | |
|--|-------|
| Inhaltsübersicht..... | XI |
| Inhaltsverzeichnis | XIII |
| Abbildungsverzeichnis..... | XXI |
| Tabellenverzeichnis..... | XXIII |
| Abkürzungsverzeichnis | XXV |
| Management Summary | XXIX |
| 1 Einleitung | 1 |
| 2 Grundlagen und Begrifflichkeiten | 13 |
| 3 Qualitätsanforderungen an das Bewertungsschema | 47 |
| 4 Vorgehensmethode zur Entwicklung des Bewertungsschemas | 57 |
| 5 Compliance-Anforderungen an Authentifizierungssysteme | 67 |
| 6 Strukturierung der Anforderungen und Herleitung der Prüfkriterien..... | 141 |
| 7 Compliance-Prüfkriterien für biometrische Authentifizierung | 161 |
| 8 Exemplarische Bewertung biometrischer Authentifizierungssysteme..... | 211 |
| 9 Evaluation des Bewertungsschemas | 225 |
| 10 Schlussfolgerungen | 233 |
| 11 Fazit und Ausblick..... | 267 |
| Anhang A: Anforderungen außerhalb der Bewertung | 273 |
| Anhang B: Referenztabellen | 277 |
| Literaturverzeichnis | XXXI |

Inhaltsverzeichnis

| | |
|---|--------------|
| Inhaltsübersicht..... | XI |
| Inhaltsverzeichnis | XIII |
| Abbildungsverzeichnis..... | XXI |
| Tabellenverzeichnis..... | XXIII |
| Abkürzungsverzeichnis | XXV |
| Management Summary | XXIX |
| 1 Einleitung | 1 |
| 1.1 Treiber für die Bedeutung der IT-Compliance | 1 |
| 1.2 Motivation der Untersuchung biometrischer Authentifizierungssysteme und die daraus resultierende Problemstellung | 3 |
| 1.3 Stand der Forschung und Einordnung der Arbeit in den aktuellen wissenschaftlichen Kontext | 4 |
| 1.4 Zielsetzung und Forschungsfragen | 5 |
| 1.5 Forschungsmethode und wissenschaftliches Vorgehen | 7 |
| 1.6 Aufbau der Arbeit | 11 |
| 2 Grundlagen und Begrifflichkeiten | 13 |
| 2.1 Grundlagen und Begrifflichkeiten der Biometrie | 13 |
| 2.1.1 Begriffe und Klassifikation der Authentifizierung | 13 |
| 2.1.2 Begriffe und Klassifikation biometrischer Verfahren..... | 14 |
| 2.1.2.1 Betriebsarten biometrischer Authentifizierungssysteme | 15 |
| 2.1.2.2 Aufbau biometrischer Systeme | 16 |
| 2.1.2.3 Biometrischer Verfahrensablauf | 16 |
| 2.1.3 Derzeitige Marktsituation der Biometrie Industrie | 19 |
| 2.2 Grundlagen der IT-Compliance..... | 21 |
| 2.2.1 Der Zusammenhang zwischen der Governance, dem Risikomanagement und der Compliance | 21 |
| 2.2.2 Herleitung des Begriffs IT-Governance..... | 23 |
| 2.2.2.1 Der Begriff Corporate Governance..... | 23 |
| 2.2.2.2 Der Begriff IT-gestützte Corporate Governance | 25 |
| 2.2.2.3 Der Begriff IT-Governance..... | 25 |
| 2.2.3 Herleitung des Begriffs IT-Risikomanagement | 27 |

| | | |
|----------|---|-----------|
| 2.2.3.1 | Der Begriff Risikomanagement | 27 |
| 2.2.3.2 | Der Begriff IT-gestütztes Risikomanagement | 29 |
| 2.2.3.3 | Der Begriff IT-Risikomanagement | 29 |
| 2.2.4 | Herleitung des Begriffs IT-Compliance | 30 |
| 2.2.4.1 | Der Begriff Corporate Compliance | 30 |
| 2.2.4.2 | Der Begriff IT-gestützte Corporate Compliance | 30 |
| 2.2.4.3 | Der Begriff IT-Compliance | 31 |
| 2.2.4.4 | Einteilung der IT-Compliance-Regelwerke | 34 |
| 2.3 | Der Begriff IT-Sicherheitsmanagement | 38 |
| 2.4 | Zusammenspiel der Begriffe | 40 |
| 2.4.1 | Chance und Risiken der IT zur Unterstützung von Compliance | 40 |
| 2.4.2 | Einteilung und Einsatzgebiete der Biometrie | 43 |
| 2.4.3 | Biometrie im Zusammenspiel mit IT-Compliance | 45 |
| 3 | Qualitätsanforderungen an das Bewertungsschema | 47 |
| 3.1 | Ableitung der Qualitätsanforderungen | 47 |
| 3.2 | Definition, Zielsetzung und Bewertbarkeit der einzelnen Anforderungen | 49 |
| 3.2.1 | Zielerfüllung | 49 |
| 3.2.2 | Vollständigkeit | 51 |
| 3.2.3 | Konsistenz | 53 |
| 3.2.4 | Redundanzfreiheit | 54 |
| 3.2.5 | Prüfbarkeit | 56 |
| 4 | Vorgehensmethode zur Entwicklung des Bewertungsschemas | 57 |
| 4.1 | Abgrenzung der IT-Compliance Regelwerke | 57 |
| 4.2 | Ergänzung um referenzierte Regelwerke | 61 |
| 4.3 | Vorgehen der Analyse der Regelwerke | 62 |
| 4.4 | Ableitung der Bewertungskriterien für biometrische Authentifizierung aus den Compliance Regelwerken | 63 |
| 5 | Compliance-Anforderungen an Authentifizierungssysteme | 67 |
| 5.1 | Gesetzliche und regulative Anforderungen an die Authentifizierung | 67 |
| 5.1.1 | Gesetzesanalyse des Sarbanes-Oxley Acts | 68 |
| 5.1.2 | Gesetzesanalyse des Euro-SOX | 74 |
| 5.1.3 | Analyse der Grundsätze ordnungsgemäßer Buchführungssysteme | 76 |

| | | |
|---------|--|-----|
| 5.1.4 | Analyse der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen..... | 80 |
| 5.1.5 | Analyse des Bundesdatenschutzgesetzes | 83 |
| 5.1.6 | Analyse des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich..... | 87 |
| 5.1.7 | Analyse der Basel II Vorschriften..... | 89 |
| 5.1.8 | Analyse der Mindestanforderungen an das Risikomanagement | 91 |
| 5.1.9 | Analyse der Richtlinie über Märkte für Finanzinstrumente..... | 93 |
| 5.1.10 | Analyse des elektronischen Signaturgesetzes und der Signaturverordnung..... | 95 |
| 5.1.11 | Analyse des Elektronischen Handels- und Genossenschaftsregisters... | 98 |
| 5.1.12 | Weitere branchenspezifische Regularien | 100 |
| 5.2 | Anforderungen der IT-Management-Standards an die Authentifizierung | 101 |
| 5.2.1 | Analyse der IT-Grundsatzkataloge | 103 |
| 5.2.2 | Analyse des Standards ISO 27001 und der Information Technology Infrastructure Library | 112 |
| 5.2.3 | Analyse der Control Objectives for Information and Related Technology..... | 117 |
| 5.2.4 | Analyse der Standards des Instituts der Wirtschaftsprüfer in Deutschland..... | 122 |
| 5.2.4.1 | IDW RS FAIT 1: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie | 123 |
| 5.2.4.2 | IDW RS FAIT 2: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce..... | 126 |
| 5.2.4.3 | IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren.... | 128 |
| 5.2.4.4 | IDW PS 951 | 129 |
| 5.2.4.5 | IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie | 129 |
| 5.2.4.6 | Zusammenfassung..... | 132 |
| 5.2.5 | Payment Card Industry Data Security Standard..... | 133 |
| 5.2.6 | Analyse des Biometric Verification Mechanisms Protection Profile . | 135 |
| 5.2.7 | Analyse des Standards ISO 38500 | 136 |

| | | |
|----------|---|------------|
| 5.3 | Zusammenfassung der resultierenden Anforderungen an Authentifizierungssysteme | 137 |
| 6 | Strukturierung der Anforderungen und Herleitung der Prüfkriterien..... | 141 |
| 6.1 | Die Einteilung in Merkmal und System zur Bewertung von Authentifizierung | 141 |
| 6.2 | Das Ziel Informationsschutz..... | 143 |
| 6.2.1 | Gefahren für den Informationsschutz..... | 144 |
| 6.3 | Das Ziel Anlegerschutz..... | 146 |
| 6.3.1 | Gefahren für den Anlegerschutz | 147 |
| 6.4 | Das Ziel Mitarbeiterschutz | 148 |
| 6.4.1 | Gefahren für den Mitarbeiterschutz | 149 |
| 6.5 | Zusammenfassung | 151 |
| 6.6 | Herleitung der Prüfkriterien..... | 151 |
| 6.6.1 | Herleitung der Merkmalskriterien..... | 152 |
| 6.6.2 | Herleitung der Systemkriterien | 154 |
| 6.6.3 | Zusätzliche Kriterien | 157 |
| 6.7 | Bewertung der Prüfkriterien | 157 |
| 6.8 | Zusammenfassung | 159 |
| 7 | Compliance-Prüfkriterien für biometrische Authentifizierung | 161 |
| 7.1 | Kriterien für die Bewertung des biometrischen Merkmals | 162 |
| 7.1.1 | Personenbindung | 162 |
| 7.1.2 | Unveränderlichkeit | 165 |
| 7.1.3 | Informationsgehalt | 166 |
| 7.1.4 | Ausspähbarkeit | 167 |
| 7.1.5 | Zeitliche Variabilität | 169 |
| 7.1.6 | Willentliche Beeinflussbarkeit | 171 |
| 7.1.7 | Universalität | 172 |
| 7.1.8 | Einmaligkeit | 173 |
| 7.1.9 | Größe der Referenzspeicherung | 174 |
| 7.1.10 | Lebenderkennung | 175 |
| 7.1.11 | Mechanismenstärke | 177 |
| 7.2 | Kriterien für die Bewertung des biometrischen Systems | 181 |

| | | |
|----------|--|------------|
| 7.2.1 | Art der Datenübertragung..... | 182 |
| 7.2.2 | Art der Referenzspeicherung..... | 184 |
| 7.2.3 | Ort der Referenzspeicherung..... | 186 |
| 7.2.4 | Authentifikationsdauer | 188 |
| 7.2.5 | Sperrmechanismus | 189 |
| 7.2.6 | Replayschutz | 191 |
| 7.2.7 | Betriebsart des Authentifizierungssystems | 192 |
| 7.2.8 | Restriktive Informationsabgabe | 193 |
| 7.2.9 | Informationsfeedback | 194 |
| 7.2.10 | Erweiterbarkeit und Kombinationsmöglichkeit | 195 |
| 7.3 | Kriterien für die Bewertung der Einsatzmöglichkeiten..... | 197 |
| 7.4 | Zusammenfassung des Bewertungsframeworks..... | 198 |
| 7.4.1 | Kriterien mit dem Ziel Informationsschutz | 199 |
| 7.4.2 | Kriterien mit dem Ziel Anlegerschutz..... | 201 |
| 7.4.3 | Kriterien mit dem Ziel Mitarbeiterschutz | 203 |
| 7.5 | Kategorisierung der Bewertungskriterien..... | 205 |
| 8 | Exemplarische Bewertung biometrischer Authentifizierungssysteme | 211 |
| 8.1 | Bewertung der BergData Fingerabdruckerkennung | 211 |
| 8.2 | Bewertung der IrisID Iriserkennung | 213 |
| 8.3 | Bewertung der Fujitsu Handvenenerkennung | 214 |
| 8.4 | Bewertung nach den drei Zielen der biometrischen Authentifizierung..... | 216 |
| 8.4.1 | Bewertung mit dem Ziel des Informationsschutzes | 216 |
| 8.4.2 | Bewertung mit dem Ziel des Anlegerschutzes | 218 |
| 8.4.3 | Bewertung mit dem Ziel des Mitarbeiterschutzes..... | 220 |
| 8.5 | Zusammenfassung der resultierenden Mängel | 222 |
| 9 | Evaluation des Bewertungsschemas | 225 |
| 9.1 | Nachweis auf Zielerfüllung | 225 |
| 9.2 | Nachweis auf Vollständigkeit..... | 226 |
| 9.3 | Nachweis auf Konsistenz..... | 228 |
| 9.4 | Nachweis auf Redundanzfreiheit | 230 |
| 9.5 | Nachweis auf Prüfbarkeit | 231 |

| | |
|--|------------|
| 9.6 Zusammenfassung der Ergebnisse..... | 231 |
| 10 Schlussfolgerungen | 233 |
| 10.1 Verbesserung von Authentifizierungssystemen | 233 |
| 10.1.1 Zielkonflikte für ein biometrisches Authentifizierungssystem | 233 |
| 10.1.2 Mögliche Verbesserung des biometrischen Authentifizierungssystems | 234 |
| 10.1.2.1 BioAPI und standardisierte Austauschformate | 234 |
| 10.1.2.2 Biometric Template Protection durch Transformation | 237 |
| 10.1.2.3 Automatisierter verteilter Löschmechanismus | 240 |
| 10.1.3 Zusammenfassung | 241 |
| 10.2 Auswirkungen auf Compliance-Vorschriften | 242 |
| 10.2.1 Gefundene Schwachstellen in den Compliance-Vorschriften | 242 |
| 10.2.1.1 Mängel in Gesetzen und Regularien | 242 |
| 10.2.1.2 Mängel in Standards und Normen | 243 |
| 10.2.2 Zusammenfassung der Mängel und Identifizierung von Weiterentwicklungspotentialen | 247 |
| 10.3 Maßnahmen für das IT-Sicherheitsmanagement | 250 |
| 10.3.1 Erweiterung und Mapping der BSI IT-Grundschutzkataloge | 250 |
| 10.3.1.1 Erweiterung der Gefahrenkataloge | 251 |
| 10.3.1.2 Erweiterung der Maßnahmenkataloge | 253 |
| 10.3.1.3 Eigenentwicklung von Maßnahmen | 263 |
| 10.3.2 Zusammenfassung der Maßnahmenkataloge | 265 |
| 11 Fazit und Ausblick..... | 267 |
| 11.1 Zusammenfassung der Ergebnisse..... | 267 |
| 11.2 Weiterentwicklungspotenziale der Bewertungskriterien | 271 |
| 11.3 Ausblick..... | 272 |
| Anhang A: Anforderungen außerhalb der Bewertung | 273 |
| Anhang A.1 Schnittstellen zur Autorisierung und zum Identitätsmanagement | 273 |
| Anhang A.2 Administrations-Management | 274 |
| Anhang A.3 Audit- und Protokoll-Funktionalität | 275 |
| Anhang B: Referenztabellen | 277 |

Anhang B.1 Gefahren..... 277

Anhang B.2 Bewertungskriterien..... 278

Anhang B.3 Vollständige Bewertungsmatrix 279

Literaturverzeichnis XXXI