

Inhaltsverzeichnis

| | | |
|----------|--------------------------------------------------------|-----------|
| | Data Leakage Prevention | 9 |
| | Einleitung | 9 |
| | Inhalt des Buches | II |
| I | Überblick | 13 |
| I.1 | Definitionen | 14 |
| I.2 | Sensible Daten | 15 |
| I.3 | Arten von Data Leakage Prevention | 17 |
| I.3.1 | Kommunikationsbezogenes DLP | 17 |
| I.3.2 | Medienbezogenes DLP | 18 |
| I.3.3 | Personenbezogenes DLP | 21 |
| I.3.4 | Inhaltsbezogenes DLP | 22 |
| I.4 | Zusammenfassung | 24 |
| 2 | Ursachen für Data Leakage | 27 |
| 2.1 | Ursache 1: der »Faktor Mensch« | 27 |
| 2.1.1 | Nicht-vorsätzliches Handeln | 27 |
| 2.1.2 | Vorsätzliches Handeln | 30 |
| 2.2 | Ursache 2: Unzulänglichkeiten und Versagen der Technik | 32 |
| 2.3 | Ursache 3: Angriffe von »außen« | 35 |
| 2.3.1 | Cybercrime | 35 |
| 2.3.2 | Wirtschaftsspionage | 37 |
| 3 | Kanäle für Datenabflüsse | 41 |
| 3.1 | Datenabflüsse durch Speichermedien | 41 |
| 3.1.1 | Halbleiterspeicher | 43 |
| 3.1.2 | Datenabflüsse durch mobile Endgeräte | 53 |
| 3.1.3 | Unsichere Datenablage im mobilen Endgerät | 60 |

| | | |
|--------|-----------------------------------------------------------------------|-----|
| 3.1.4 | Datenabflüsse durch drahtlose Netze | 63 |
| 3.1.5 | Fernwartungszugänge | 74 |
| 3.2 | Multimediale Kommunikation | 76 |
| 3.2.1 | E-Mail | 76 |
| 3.2.2 | Instant Messaging | 77 |
| 3.2.3 | »Peer to Peer« | 78 |
| 3.2.4 | Hypertext Transfer Protocol (HTTP/HTTPS) | 78 |
| 3.2.5 | FTP/SCP | 79 |
| 3.2.6 | Drucker | 80 |
| 3.2.7 | »Embedded WebServer« | 80 |
| 3.2.8 | Audio- und Videokonferenzen | 82 |
| 3.2.9 | Der »Faktor Mensch« | 83 |
| 3.2.10 | »Sin of Admin« | 84 |
| 3.3 | Verdeckte Speicher- und Zeitkanäle | 85 |
| 3.3.1 | Speicherkanäle | 88 |
| 3.3.2 | Zeitkanäle | 89 |
| 3.3.3 | Verdeckte Kanäle | 90 |
| 3.3.4 | Informationsflusskontrolle | 94 |
| 4 | DLP: Recht, Organisation und Personal | 97 |
| 4.1 | Rechtliche Maßnahmen | 97 |
| 4.1.1 | Arbeitsverträge | 97 |
| 4.1.2 | Datenschutz | 102 |
| 4.1.3 | Outsourcing-Verträge | 103 |
| 4.1.4 | Wartungs- und andere Supportfunktionen | 105 |
| 4.1.5 | Lizenzierungs- und Update-Funktionen | 106 |
| 4.2 | Organisatorische Maßnahmen | 108 |
| 4.2.1 | Bestandsaufnahme und Klassifikation von sensiblen Daten | 108 |
| 4.2.2 | Inventarisierung aller Speicherstellen | 112 |
| 4.2.3 | Aufstellung von Richtlinien und Regeln zur Verwendung sensibler Daten | 115 |
| 4.2.4 | Einschränkung von Benutzergruppen | 116 |
| 4.3 | Personelle Maßnahmen | 118 |

| | | |
|----------|--------------------------------------------------|------------|
| 5 | DLP: Leitlinien, Konzepte und Richtlinien | 121 |
| 5.1 | Grundsätzliches | 121 |
| 5.1.1 | Leitungsfunktion | 122 |
| 5.1.2 | Sicherheitsmanagement | 124 |
| 5.2 | DLP in der Sicherheitsleitlinie | 129 |
| 5.3 | DLP in einem Sicherheitskonzept | 134 |
| 5.4 | DLP in Sicherheitsrichtlinien | 139 |
| 5.4.1 | DLP-Richtlinie für Anwender | 140 |
| 5.4.2 | Auswirkung auf andere Richtlinien | 147 |
| 5.4.3 | Management | 149 |
| 5.5 | DLP in ISO 27001 und IT-Grundschutz | 150 |
| 5.5.1 | ISO 27001 | 150 |
| 5.5.2 | IT-Grundschutz | 157 |
| 6 | DLP in der Praxis | 165 |
| 6.1 | Zwei Arten von DLP-Systemen | 165 |
| 6.2 | Vorbereitungen zur Einführung eines DLP-Systems | 167 |
| 6.3 | DLP-Policy | 168 |
| 6.4 | Prinzipielle Funktionsweise eines DLP-Systems | 170 |
| 6.5 | Netzwerkbasiertes DLP-System | 173 |
| 6.6 | Hostbasierte DLP-Systeme | 177 |
| 6.6.1 | Hostbasierte DLP-Agenten | 179 |
| 6.6.2 | DLP und DRM (Digital Rights Management) | 182 |
| 6.7 | Multi-Level-Systeme | 184 |
| 7 | DLP-Management-Server | 189 |
| 7.1 | Erstellung der Richtliniendatenbank (DLP-Policy) | 190 |
| 7.2 | Standardrichtlinien | 192 |
| 7.3 | Definition der Informationstypen | 197 |

| | | |
|-------|-----------------------------------------------|-----|
| 7.4 | Rollenbasierte Administration des DLP-Servers | 199 |
| 7.4.1 | Master DLP-Administrator | 199 |
| 7.4.2 | DLP-Administrator | 200 |
| 7.4.3 | DLP-Auditor | 201 |
| 8 | Auswahl von DLP-Systemen und Ergänzendes | 203 |
| 8.1 | Anbieter von DLP-Systemen | 203 |
| 8.2 | Auswahl von DLP-Systemen | 206 |
| 8.3 | Rollout des DLP-Systems | 208 |
| 8.4 | Begleitende Maßnahmen | 209 |
| 8.5 | Kontroll- und Prüfmaßnahmen | 210 |
| 8.5.1 | Vorgaben | 210 |
| 8.5.2 | Korrekte Umsetzung | 211 |
| 8.5.3 | Awareness | 212 |
| 8.5.4 | Einhaltung organisatorischer Vorgaben | 215 |
| 8.5.5 | Grad der Überwachung | 216 |
| 8.5.6 | Prüfungen der Wirksamkeit | 217 |
| 9 | Ausblick | 219 |
| A | Quellen und Literatur | 223 |
| B | Abbildungen und Tabellen | 225 |
| C | Verwendete Abkürzungen | 229 |
| | Index | 233 |