

Inhalt

Vorwort.....	7
Einleitung.....	9
1. Beispiele aus der Praxis	23
1.1 Einführung	23
1.2 Einzelaspekte bei speziellen Systemen.....	24
1.3 Bewegliche Datenträger.....	34
1.4 Berechtigungen und Kontrollen.....	40
1.5 Programme mit Schadenfunktionen.....	55
1.6 Beweissicherung	61
1.7 Abstrahlsicherheit	62
1.8 Verfügbarkeit und Datensicherung.....	62
1.9 Datenübertragung, lokale und öffentliche Netze	66
2. Grundbegriffe.....	71
2.1 Informationen, Daten, Verarbeitung, IV- und IT-System	71
2.2 Ordnungsmäßigkeit, IV-Sicherheit, IT-Sicherheit.....	72
2.3 Verfügbar, vertraulich, integer, verbindlich	75
2.4 Analysen von Bedrohungen, Risiken und Schäden	79
2.5 Subjekte, Aktionen, Objekte.....	80
2.6 Unterschiedliche Modellvorstellungen von Sicherheit.....	84
3. Sicherheitsfunktionen	87
3.1 Grundsätzliches.....	87
3.2 Zugriffsschutzmodelle	105
3.3 Funktionalitätsklassen.....	120
3.4 Praxis der Funktionalitätsklassen.....	134
4. Das Sicherheitsniveau.....	137
4.1 Grundsätzliches.....	137
4.2 Sicherheitsniveaus in Kriterienwerken	140
5. Entwicklung.....	155
5.1 Grundsätzliches.....	155
5.2 Vorgehensmodell	157
5.3 Produkt-Entwicklung.....	157
5.4 Qualitätssicherung	170
5.5 Konfigurationsmanagement.....	173

Inhalt

5.6 Werkzeuge	176
5.7 Wartung	179
6. Evaluierung	181
6.1 Reduktion der Komplexität	182
6.2 Dokumentation	185
6.3 Der Evaluierungsprozeß	188
6.3 Produktion, Auslieferung und Verteilung	191
6.4 Release-Wechsel und Weiterentwicklung	192
6.5 Kombinationen evaluierter Produkte	194
6.6 Bewertungsbeispiele für Mechanismen	196
7. Anwendungen	205
7.1 Einleitung	205
7.2 Strategien der IT-Sicherheit	206
7.3 Konzeptionelles Vorgehen	212
7.4 Strategie der Vertrauenswürdigkeit	216
7.5 Aufgaben für praktische Analysen	223
7.6 Kritik und Ausblick	225
Anhang A. Quellen	227
Anhang B. Zertifizierte Produkte	231
B.1 Orange Book	231
B.2 ITSEC	234
B.3 UKL	235
B.4 IT-Sicherheitskriterien	237
Anhang C. Glossar	239
Anhang D. Abkürzungen	263
Anhang E. Stichwortverzeichnis	265