

# Inhaltsverzeichnis

## 1. Die Notwendigkeit

1.1 Alles nur Hacker?.....	2
1.2 Die Risiken.....	4
1.3 Was bedeutet Sicherheit?.....	9
1.4 Die Verkettung von Hardware und Software.....	10

## 2. Einige spektakuläre Fälle..... 13

2.1 Deutsche Hacker für den KGB.....	14
2.1.1 Nur ein kleiner Fehler in der Buchhaltung?.....	14
2.1.2 Der Beginn einer langen Jagd.....	17
2.1.3 Wohin führt die Spur?.....	20
2.1.4 Die Falle.....	26
2.1.5 Ein Ausflug nach Ostberlin.....	29
2.1.6 Eine Analyse.....	30
2.2 Der Morris-Wurm.....	34
2.2.1 Technik und Ausbreitung.....	35
2.2.2 Die Reaktion.....	38
2.3 Das falsche Satellitenprogramm.....	40

## 3. Die Bedrohung unserer Ressourcen..... 43

3.1 Opfer und Täter.....	44
3.2 Die Zielgruppen.....	46
3.2.1 Die Banken.....	46
3.2.2 Das Militär und seine Zulieferer.....	51
3.2.3 Die Industrie.....	53
3.2.4 Persönliche Daten.....	56
3.2.5 Das Gesundheitswesen.....	57
3.2.6 Computer und Politik.....	59
3.3 Die Täter.....	62
3.3.1 Die Hacker - Mythos und Wirklichkeit.....	62
3.3.2 Anarchisten und Terroristen.....	67
3.3.3 Kriminelle aller Couleur.....	68
3.3.4 Agenten und Spione.....	69

---

3.3.5 Insider.....	69
3.4 Der Zielkonflikt zwischen Kommunikation und Sicherheit.....	70
3.5 Angriff mit konventionellen Mitteln.....	70
3.5.1 Sabotage.....	71
3.5.2 Diebstahl und Erpressung.....	72
3.5.3 Das Anzapfen von Leitungen ( <i>wiretapping</i> ).....	73
3.5.4 Leakage.....	74
3.5.5 Piggybacking.....	75
3.5.6 Impersonation.....	75
3.6 Die Bedrohung durch Software.....	76
3.6.1 <i>Data Diddling</i> oder Datenveränderung.....	76
3.6.2 Zeitdiebstahl.....	78
3.6.3 Salamataktik.....	79
3.6.4 Trojanische Pferde.....	81
3.6.5 Trapdoors.....	84
3.6.6 Zeitbomben ( <i>logic bombs</i> ).....	84
3.6.7 Asynchronous Attack.....	85
3.6.8 Superzapping.....	87
3.6.9 Viren.....	87
3.6.10 Würmer.....	102
3.6.11 Scavenging.....	103
3.6.12 Simulation und Modellbildung.....	104
3.7 Software im Einsatz.....	104
3.7.1 Die Richtigkeit der Daten.....	104
3.8 Die Verwundbarkeit der Netze.....	106
<b>4. Die Möglichkeiten zum Schutz unserer Ressourcen.....</b>	<b>107</b>
4.1 Einleitung.....	108
4.2 Herkömmliche Maßnahmen.....	109
4.2.1 Lage und Ausstattung der EDV-Räume.....	110
4.2.2 Zugangskontrolle.....	119
4.2.3 Ständige Überwachung und Kontrolle.....	123
4.3 Hilfe durch die Behörden.....	124
4.4 Die Rechner.....	127
4.4.1 Architekturen.....	127
4.4.2 Ausfallsichere und fehlertolerante Systeme.....	127
4.4.3 Cluster.....	133
4.5 Datensicherung und <i>Back-up</i> .....	135
4.5.1 Datensicherung.....	135
4.5.2 Das Vorhalten zusätzlicher Ressourcen.....	139

---

4.6 Die vorhandenen Schutzmechanismen des Betriebssystems.....	143
4.6.1 Identifikation und Zugangskontrolle.....	148
4.6.2 Paßworte.....	148
4.6.3 Anforderungen an Paßworte.....	149
4.6.4 Die Ausweitung des Konzepts.....	152
4.6.5 Ähnliche Verfahren.....	153
4.6.6 Persönliche Daten.....	154
4.6.7 Algorithmische Verfahren.....	155
4.6.8 Rückruf.....	156
4.6.9 Zustände des Betriebssystems und Privilegien.....	156
4.6.10 Das Vergeben der Zugriffsrechte.....	158
4.6.11 Spezielle Schutzrechte.....	161
4.6.12 Kommunikation zwischen Programmen und Prozessen.....	162
4.7 Die Verwaltung der Programme und Daten.....	165
4.7.1 Das Inventar.....	165
4.7.2 Die Rolle des Konfigurationsmanagements.....	168
4.8 Abwehr von Attacken durch Software.....	170
4.8.1 Die Dividende eines geregelten Software-Entstehungs- prozesses.....	170
4.8.2 Verifikation und Validation von Software.....	174
4.9 Sicherheit als Funktion der Software.....	177
4.9.1 Maßnahmen gegen <i>Scavenging</i> und <i>Asynchronous Attack</i> .....	177
4.10 Gefährliche Werkzeuge.....	180
4.11 Abwehr von Viren und Würmern.....	184
4.11.1 Die Schwächen der Viren.....	186
4.11.2 Die Strategie zur Abwehr von Viren.....	187
4.12 Wie hält man Hacker draußen?.....	194
4.12.1 Alarme und Monitore.....	195
4.13 Wie sichert man die Richtigkeit der Daten?.....	200
4.13.1 Defensive Programmierung.....	201
4.13.2 Sicherheitsfunktionen.....	202
4.14 Schutzmöglichkeiten bei verbreiteten Computern und Betriebs- systemen.....	206
4.14.1 UNIX.....	206
4.14.2 VAX/VMS.....	212
4.14.3 Der PC.....	214
4.15 Zusätzliche Maßnahmen.....	217
4.15.1 Kryptographie.....	217
4.15.2 Der DES-Algorithmus.....	218
4.15.3 Der RSA-Algorithmus.....	220
4.15.4 Digitale Unterschrift.....	222

4.15.5 Datenkompression.....	224
4.15.6 Die Vor- und Nachteile.....	224
4.16 Schutz von Computern am Netz.....	225
4.16.1 Das Übertragungsmedium.....	225
4.16.3 Lokale Netze.....	228
4.16.4 Großflächige und globale Netze.....	231
4.16.5 Redundanz im Netz.....	232
4.16.6 Isolation.....	234
4.16.7 Die Empfangsstation.....	235
4.17 Schutzmaßnahmen im Bereich der Banken.....	235
4.18 Besonders gefährdete Installationen.....	237
4.19 Behördliche Auflagen.....	239
4.19.1 <i>Orange Book</i> und IT-Sicherheitskriterien.....	239
<b>5. Die Aufgaben der Organisation und des Managements.....</b>	<b>243</b>
5.1 Organisatorische Maßnahmen.....	244
5.2 Die kritische Rolle des Managements.....	245
5.3 Die beteiligten Gruppen.....	245
5.4 Die Vorgehensweise bei der Einführung eines Sicherheitssystems.....	245
5.4.1 Die Bestandsaufnahme.....	248
5.4.2 Bewertung der Risiken.....	250
5.4.3 Das Konzept.....	251
5.4.4 Durchführung und Anpassung.....	252
<b>6. Der Stand der Technik.....</b>	<b>253</b>
6.1 Eine Beurteilung.....	254
6.2 Notwendige Verbesserungen.....	256
<b>7. Epilog.....</b>	<b>259</b>
7.1 Wohin führt uns der Weg?.....	260
<b>Anhang.....</b>	<b>265</b>