

# Inhaltsverzeichnis

1	Gefahren, Mitspieler & Merkwürdigkeiten.....	1
1.1	Angreifer und Angriffsmethoden.....	3
1.2	Die Ursachen.....	11
1.3	Recht oder rechtsfreier Raum?.....	14
2	Kommunikation: Internet-Protokolle.....	19
2.1	Transport- und Organisationsschichten.....	19
2.1.1	Programmiertechnik.....	22
2.1.2	Lokale Organisation, Transport- und Verbindungsprotokolle.....	39
2.1.2.1	Netzwerkaufbau und lokale Adressauflösung (ARP, DHCP). 39	
2.1.2.2	Transport- und Verbindungsschichten.....	51
2.1.3	Organisationsprotokolle.....	70
2.1.3.1	Externe Adressauflösung: Domain Name Service.....	70
2.1.3.2	Übertragungswege, Routing-Protokolle.....	81
2.1.3.3	Gemeinsame Funktionen: Remote Procedure Call.....	85
2.1.3.4	Maschinenorganisation, Netzwerkmanagement.....	93
2.1.4	Geräteerkennung.....	108
2.2	Dateiübertragung.....	114
2.3	Email-elektronische Post.....	131
2.3.1	Der Aufbau von Email-Dokumenten.....	131
2.3.2	Das Versenden von Emails.....	136
2.3.3	Postverwaltung.....	142
2.3.3.1	Postfachabruf.....	142
2.3.3.2	Postablageverwaltung.....	144
2.3.3.3	Sicherheitsanalyse und Spam-Filter.....	150
2.3.4	Helpdesk-Management.....	173
2.4	Webseiten: Programmierung und Nutzung.....	176
2.4.1	Das „Hypertext Transfer Protocol“ HTTP.....	176
2.4.2	Dokumentformatierung: HTML.....	193
2.4.3	Aktive und interaktive HTML-Dokumente.....	207
2.4.3.1	Formulare.....	207
2.4.3.2	Links auf Dokumente und Programme.....	213
2.4.3.3	Applets.....	214

2.4.3.4	Skripte.....	222
2.4.3.5	Sicherheitsanalyse: ActiveX.....	230
2.4.4	Programmierung des Serversystems.....	237
3	Kommunikationssicherung.....	249
3.1	Verschlüsselungsalgorithmen.....	250
3.2	Kennworte.....	263
3.3	Sichere Emails und Zertifikate.....	267
3.3.1	Sicherungsergänzungen des SMTP - Protokolls.....	267
3.3.2	Öffentliche Zertifikate.....	272
3.3.3	Technisches zum Zertifikatzugriff: LDAP-Protokoll.....	281
3.3.4	S/MIME und PGP.....	294
3.4	Sichere HTTP-Verbindungen: HTTPS.....	313
3.4.1	Verschlüsselte Verbindungen: SSL/TLS.....	313
3.4.2	Vereinfachte Anmeldeprozeduren für Anwender.....	329
3.4.3	Kritische Systeme.....	334
3.5	Interne Authentifizierung.....	337
3.6	Sichere Mehrkanalverbindungen: SSH.....	342
3.7	IPsec, gesicherte private Netzwerke (VPN).....	357
3.8	Funknetze.....	367
3.8.1	Mobilfunknetze.....	367
3.8.2	Wireless LAN.....	377
4	Netzwerk- und Systemsicherung.....	385
4.1	Einführung in die Problematik.....	385
4.2	Systeminfektionen.....	390
4.2.1	Typen und wirtschaftliche Bedeutung.....	390
4.2.2	Infektion mit „Anwenderunterstützung“.....	397
4.2.3	Funktionalität der Angriffsprogramme.....	408
4.2.4	Infektion über „Sicherheitslücken“.....	414
4.3	Internet und Intranet.....	435
4.4	Filtern von Datenströmen.....	439
4.4.1	Kontrolle des Datenflusses.....	442
4.4.2	Systemprotokolle.....	453
4.4.3	Informationskontrolle.....	458
4.4.4	Kontrolle von Seiteninhalten.....	479
4.5	Protokollierung und Gegenmaßnahmen.....	484
4.6	Systemintegrität.....	493
4.6.1	Erkennen von Infektoren.....	493
4.6.1.1	Direkte Suche nach Infektorcode.....	495
4.6.1.2	Untersuchung des Systemverhaltens.....	510

---

4.6.1.3 Virensan im Netzwerk.....	515
4.6.2 Integritätsprüfung des Systems.....	516
4.7 Sicherung der Kontrollprogramme und „Lock Down“.....	524
5 IT-Sicherheitspolitik im Unternehmen.....	531
5.1 Design des Netzwerkes.....	531
5.2 Netzwerkkomponenten und Störfälle.....	546
5.2.1 Organisation der Komponentenverwaltung.....	546
5.2.2 Störfallmanagement.....	558
5.3 Allgemeine Sicherheitspolitik.....	564
5.4 Private Key Infrastructure.....	570
5.4.1 Verschlüsselung des Netzwerk-Datenverkehrs.....	571
5.4.2 Anwenderverwaltung.....	576
5.4.3 System- und Netzwerkmodell.....	581
5.5 Dokumentenmanagement.....	587
5.5.1 Verwaltungskriterien für Dokumente.....	587
5.5.2 Ein einfacher Dokumenten-Manager.....	589
5.5.3 Versionsmanagement.....	598
5.5.4 Vertraulichkeit und Inhalt von Dokumenten.....	607
5.5.5 Urheberrechtsicherung an Dokumenten.....	617
5.6 Poststellenmanagement.....	632
5.7 Daten- und Programm-Management.....	642
5.7.1 Systemupdates.....	644
5.7.2 Backup-Strategien.....	651
5.8 Objektidentifizierung.....	653
5.8.1 Radio Frequency Identification RFID.....	658
5.8.2 Chipkartensysteme.....	664
5.8.3 Fingerabdruck-Identifikation.....	674
5.8.4 Videokontrollen.....	680
5.9 Geschäftsabwicklung im Internet.....	691
5.10 Lauschangriffe und Informationsauswertung.....	702
5.11 Elektronische Wahlen.....	712
Literaturhinweise.....	719
Stichwortverzeichnis.....	721