

## Inhaltsverzeichnis

<b>1 IT-Security .....</b>	<b>5</b>
1.1 Computer- und Netzwerksicherheit .....	5
1.2 Hacker, Cracker und Skriptkiddies .....	5
1.3 Zehn Gesetze der IT-Sicherheit .....	6
1.4 Phasen eines Angriffs .....	6
<b>2 Scanning.....</b>	<b>7</b>
2.1 Sniffer .....	7
2.2 Scan-Methoden .....	7
2.2.1 TCP connect()-Scan .....	7
2.2.2 TCP SYN Scan .....	8
2.2.3 TCP FIN/Xmas/Null Scan .....	8
2.2.4 TCP Idlescan .....	8
2.3 Portscanner .....	9
2.3.1 NMap .....	9
2.4 DNS-Lookup Tools .....	10
2.5 Network Tracing Tools .....	11
2.6 Firewall Probing Tools .....	11
2.7 Penetrationstests .....	11
<b>3 Analyse der Informationen und Auswertung von Schwachstellen .....</b>	<b>12</b>
3.1 Herausfinden der verwendeten Betriebssysteme und -versionen .....	12
3.1.1 NMap .....	12
3.1.2 Nessus (UNIX) .....	13
3.2 Denial-of-Service-Attacken .....	13
<b>4 Man-in-The-Middle-Angriffe (MITM-Angriffe) .....</b>	<b>15</b>
4.1 ARP-Spoofing, ARP Poison Routing (APR) .....	15
4.1.1 ARP Spoofing mit Cain & Abel .....	15
4.1.2 ARP Spoofing mit WinARPSpoof .....	26
4.2 Maßnahmen gegen Man-in-the-Middle-Attacken .....	29
<b>5 Angriffe auf Websites .....</b>	<b>31</b>
5.1 Cross Site Scripting (XSS) .....	31
5.2 Cross Site Request Forgery (CSRF, XSRF) .....	31
5.3 SQL Injection .....	31
5.4 LDAP Injection .....	32
5.5 Phlashing – Angriffe auf Embedded Systems .....	32
<b>6 Firewalls .....</b>	<b>33</b>
6.1 Firewall-Technologien .....	33
6.1.1 Paketfilter .....	33
6.1.2 Stateful Inspection .....	33
6.1.3 Application Layer Firewall / Proxy Firewall .....	34
6.2 Marktübersicht .....	34
6.2.1 Firewall-Software .....	34
6.2.2 Firewall-Appliances .....	34
<b>7 Authentifizierung und Erhöhung der Privilegien .....</b>	<b>36</b>
7.1 Cracken von Kennwörtern (Brute-Force-Attacken) .....	36
7.1.1 L0phtcrack .....	37
7.1.2 Shadow Security Scanner .....	37

<b>8 Malware.....</b>	<b>38</b>
8.1 Viren .....	38
8.1.1 Allgemeines.....	38
8.2 Trojaner, Backdoors und Rootkits.....	40
8.2.1 Back Orifice (Backdoor).....	40
8.2.2 Sub7Legends (Backdoor) .....	40
8.2.3 Hacker Defender .....	41
8.3 Sicherheitsvorkehrungen.....	41
<b>9 Patch-Management, MBSA, WSUS .....</b>	<b>45</b>
<b>10 WLAN-Security .....</b>	<b>49</b>
10.1 Knacken von WEP-Schlüsseln.....	49
10.1.1 Airsnort.....	49
10.2 WLAN-Sniffer .....	49
10.2.1 NetStumbler .....	49
10.3 Gegenmaßnahmen .....	50
<b>11 Mailhygiene und Anti-Spam-Maßnahmen .....</b>	<b>51</b>
11.1 Spam (UBE, Unsolicited Bulk E-Mail) .....	51
11.2 Sammeln von E-Mail-Kontoinformationen.....	51
11.3 Anti-Spam mit Exchange Server 2010 .....	52
11.3.1 Installieren der AntiSpam-Agents auf einem Hub Transport Server.....	53
11.3.2 Antispamaktualisierungen verwenden .....	53
11.3.3 IP-Sperrlistenanbieter (Blacklists).....	56
11.3.4 Absenderfilterung .....	59
11.3.5 Absenderzuverlässigkeitsfilterung .....	59
11.3.6 Inhaltsfilterung (Content Filter).....	62
11.3.7 Ausnahmen für Content Filter festlegen .....	65
11.3.8 Anzeigen des SCL-Wertes in Outlook .....	65
11.4 Forefront Protection 2010 für Exchange Server .....	72
11.5 Antispam-Drittanbieterprodukte .....	85
<b>12 Intrusion Detection-Systeme (IDS) .....</b>	<b>87</b>
12.1.1 Snort.....	87
12.1.2 Honeypots .....	87
<b>13 Verschiedene Tools und Websites .....</b>	<b>88</b>
<b>14 Quellenangaben.....</b>	<b>90</b>