

# Inhalt

<b>1. Anatomie einer Attacke</b> .....	<b>15</b>
<b>1.1 Spektakuläre Angriffe aus dem Internet</b> .....	<b>15</b>
<b>1.2 Das moderne Waffenarsenal: Bedenkliche Entwicklung im Web</b> .....	<b>22</b>
<b>1.3 Aufspüren und Auskundschaften eines Systems und seiner Sicherheitslücken</b> .....	<b>28</b>
<b>1.4 Typische Angriffsszenarien auf Windows-Rechner</b> .....	<b>90</b>
<b>1.5 Typische Angriffsszenarien auf Linux-Rechner</b> .....	<b>97</b>
<b>2. Virtuelle Hacker: Viren, Würmer und Trojaner</b> .....	<b>101</b>
<b>2.1 Computerviren – effektiver Code auf kleinstem Raum</b> ....	<b>102</b>
Das Grundprinzip von Computerviren .....	102
Klassische binäre Computerviren .....	108
Viren mit passiven und aktiven Schutzfunktionen .....	118
Aufbau binärer Computerviren .....	120
Makro- und Scriptviren .....	125
<b>2.2 Würmer – Virenverbreitung im Netzwerk</b> .....	<b>134</b>
Netzwerke als Infektionswege für Viren .....	134
VBS-Mail-Würmer: Loveletter & Co. ....	137
Komplexe Würmer der neuen Generation .....	156
<b>2.3 Trojanische Pferde – die Einschleuser</b> .....	<b>159</b>
NetBus – Fernwartungs-Tool oder Trojaner? .....	160
So setzen sich Trojaner im System fest .....	165
Verbreitungskanäle von Trojanern .....	173
<b>3. Digitale Kommunikation in Zeiten des Internets</b> .....	<b>179</b>
<b>3.1 TCP/IP – Aufbau, Funktion und Arbeitsweise</b> .....	<b>179</b>
Datenübertragung im Rahmen einer TCP-Sitzung .....	203
Port unreachable .....	214
Need to frag .....	216
Time Exceeded In-Transit .....	217

<b>3.2 Analyse von Netzwerkverkehr mittels tcpdump .....</b>	<b>218</b>
Die Installation von tcpdump .....	219
Der Umgang mit tcpdump .....	220
Die Behandlung langer und großer tcpdump-Sitzungen .....	221
Die Standardausgabe von tcpdump .....	222
Die hexadezimale Ausgabe von tcpdump .....	223

## **4. Das IP-Paket als Waffe .....** **225**

<b>4.1 Warum IP-Pakete gefährlich sein können .....</b>	<b>225</b>
Das Client-/Serverprinzip .....	225
<b>4.2 Geklaute Pakete: von IP-Spoofing bis TCP-Hijacking .....</b>	<b>228</b>
Spoofing .....	228
Sniffing .....	232
TCP-Hijacking .....	236
<b>4.3 Erdrückt vom IP: von DoS und DDoS-Attacken .....</b>	<b>240</b>
Sockets aufbrauchen mittels SYN- und TCP-Connect-Flooding .....	249
Distributed Denial of Service-Attacken .....	264

## **5. Wireless LAN: Luftkrieg im Cyberspace .....** **267**

<b>5.1 Der Weg zum kabellosen Netzwerk .....</b>	<b>267</b>
Service Set Identifier (SSID) .....	270
WEP (Wired Equivalent Privacy) .....	274
Einen Schritt weiter als IEEE 802.11b .....	276
<b>5.2 Wardriving, Warflying und Warchalking .....</b>	<b>280</b>
Wardriving .....	281
Warflying .....	283
Warchalking .....	284

## **6. Angriffe auf Client- und Serverdienste .....** **287**

<b>6.1 Internet Explorer – Codeinstallation durch die Hintertür .....</b>	<b>288</b>
ActiveX-Code einschleusen .....	289
Angriffe mit Scriptsprachen .....	298
Pufferüberläufe und andere Programmierfehler .....	308
Zugriff auf lokale Dateien .....	312
Browser Helper Objects (BHO) .....	319

<b>6.2 Outlook/Outlook Express – Angriffe per E-Mail</b> .....	<b>322</b>
Programmierfehler in Outlook .....	322
HTML-Code in E-Mails einbinden .....	325
E-Mail-Nachrichten per MIME mit Dateianhängen versehen .....	326
Eine E-Mail per VBS an weitere Empfänger verschicken .....	328
<b>6.3 Media Player, Messenger &amp; Co. – Angriffe auf beliebte Internetanwendungen</b> .....	<b>330</b>
Medien-Wiedergabeprogramme für destruktive Angriffe nutzen .....	331
Messaging-Programme sabotieren und als Hintertür missbrauchen .....	336
<b>6.4 Angriffe auf Webserver</b> .....	<b>341</b>
<b>6.5 Angriffe auf andere Serverdienste</b> .....	<b>386</b>

## **7. Weitere Gefahren im Netz** ..... **397**

<b>7.1 0190-Dialer – von seriös bis illegal</b> .....	<b>398</b>
Die Technik der Dialer .....	399
Der Weg der Dialer auf den PC .....	402
So verstecken sich Dialer im System .....	409
Dialer aufspüren und entfernen .....	410
Rechtliche Mittel gegen Dialer-Gauner .....	415
<b>7.2 Spyware übermittelt Benutzerprofile</b> .....	<b>417</b>
Von Adware zu Spyware .....	418
Welche Daten werden übermittelt .....	423
Spyware aufspüren und entfernen .....	426
<b>7.3 Cookies – praktisch und gefährlich zugleich</b> .....	<b>430</b>
Das Funktionsprinzip von Cookies .....	431
So werden Cookies missbraucht .....	437
Cookies erkennen und abwehren .....	439
<b>7.4 Webbugs – die kleinen Überwachungspixel</b> .....	<b>446</b>
So arbeiten Webbugs .....	446
Das können Webbugs ausspionieren .....	447
Hier können sich Webbugs überall verstecken .....	449
Webbugs erkennen und vermeiden .....	451
<b>7.5 Spam und Flaming – wenn das Postfach platzt</b> .....	<b>455</b>
Die eigene E-Mail-Adresse tarnen .....	456
Spoofing – so leicht lassen sich E-Mails fälschen .....	460
Schutz und Gegenmaßnahmen bei Spam .....	469

<b>8. Betriebssystem Windows – das Risiko mit der Sicherheit</b> .....	<b>475</b>
<b>8.1 Offenes Scheunentor: So arbeitet Windows</b> .....	<b>475</b>
Betriebssystem unter Beschuss .....	476
Systemarchitektur .....	479
C2-Sicherheitsstandard (NT) .....	483
Kommunikation zwischen Kernel und Anwendung .....	484
Dynamic Link Libraries (DLLs) .....	488
Ausführbare Dateien .....	492
Gefahrenquelle verteilt genutzte Dateien .....	501
Einschleusen von Systemdiensten (NT) .....	503
<b>8.2 User-Management und Rechtevergabe</b> .....	<b>508</b>
Angriffsszenarien .....	509
Passwort-Spy & Co. ....	511
Notstart-CD und DOS-Diskette .....	514
Windows-Anmeldung und Benutzer-Management .....	516
Benutzer-, Gruppenkonten und SIDs .....	520
Security Access Manager .....	524
Registry und ACL-Management .....	525
Registry-Überwachung mit Regmon & Co. ....	526
NET USE und die Kommandozeile .....	531
Programmstart: Welche Rechte für was? .....	533
Systemrichtlinien (Policies) .....	535
Roaming Profiles .....	537
Vertrauensstellung zwischen Domänen .....	538
Sonderfall XP Home .....	539
NTFS versus FAT32 und weitere Dateisysteme .....	544
NT-Ereignisanzeige .....	547
<b>8.3 Windows im Web – nach allen Seiten offen</b> .....	<b>548</b>
Der Rechner als Netzwerkressource .....	549
Freigabe in verteilten Netzen .....	549
Mit oder ohne PDC? .....	554
Java, JavaScript und ActiveX .....	555
Freigaben: per ICS auch im Internet .....	558
NetBIOS und IP-Namen .....	559
<b>8.4 Das Tor zur Welt – und zum PC: der Browser</b> .....	<b>561</b>
Browser-Übersicht .....	562
Vergleich der Browser .....	568
<b>8.5 I love you – ein Virenbrutkasten namens Outlook</b> .....	<b>570</b>

---

## **9. Projekt „sicheres Windows“ ..... 573**

### **9.1 Security-Löcher stopfen – Windows besser abdichten ..... 574**

Sichere BIOS-Konfiguration .....	575
Sichere Installation von Windows NT, 2000 und XP (Professional) .....	576
Sichere Installation von Windows 9x, ME und XP (Home) .....	588
Allgemein geltende Installationsregeln .....	591
Gefährliche Dienste deaktivieren .....	598
Patches, Updates, Bugfixes .....	602
Reale oder virtuelle PCs .....	604
NT-Task-Manager .....	606

### **9.2 Minimal Risk: Internet Explorer ohne Reue ..... 608**

Internetoptionen allgemein .....	609
Sicherheit .....	610
Datenschutz .....	614
Inhalte .....	616
Verbindungen .....	617
Programme .....	618
Erweitert .....	619

### **9.3 Microsoft Outlook Express und Outlook absichern ..... 622**

Risiken und Auswirkungen .....	623
Richtige Einstellungen .....	624

### **9.4 Sandboxing ..... 638**

Java Virtual Machine .....	639
Java-Sandbox .....	640
Weitere Sandbox-Module .....	641

### **9.5 Microsoft Hailstorm-Offensive ..... 642**

Die Funktion .....	643
Die Technik .....	645
Die Sicherheit und Passport .....	646
Die Zukunft .....	647

### **9.6 .NET Framework ..... 648**

Die Funktion .....	648
Die Technik .....	649
Die Sicherheit .....	652
Die Vor- und Nachteile .....	653

## **10. Angriffe vereiteln ..... 655**

### **10.1 Passwörter, die besser sind als „geheim“ ..... 655**

Dictionary-Attacke: Angriff mit dem Wörterbuch .....	657
Hybrid Dictionary-Attacke .....	657

---

Brute Force-Attacke .....	658
Gute und schlechte Kennwörter .....	658
Passwortgeneratoren .....	663
Passworttresore .....	666
Beispiele zum Passwortknacken .....	668
<b>10.2 Small is beautiful – Gedanken zur Dienstbeschränkung .....</b>	<b>675</b>
Überkonfiguration .....	675
Begrenzte Ressourcen .....	676
Unvollständige Deinstallation .....	677
Die Sicherheit .....	678
<b>10.3 Keine Angriffspunkte liefern – anonym surfen .....</b>	<b>679</b>
Browser-Einstellungen – aber sicher .....	680
Cache, Cookies, Bookmarks und History auf Ihrem PC .....	681
IP-Adresse, die Spur zu Ihrem PC .....	687
Java Anon Proxy JAP .....	689
Anonymizer .....	694
Anonyme Proxyserver .....	696
Die anonyme E-Mail-Adresse .....	698
Key-Logger – der Spion im eigenen Haus .....	701

## **11. Firewalls & Co.: Schutz vor Angreifern ..... 707**

<b>11.1 Firewall-Systeme .....</b>	<b>707</b>
Paketfilter .....	710
Application-Gateways .....	713
SOCKS .....	720
Personal Firewalls .....	721
<b>11.2 Intrusion Detection-Systeme .....</b>	<b>722</b>
Systemarchitektur .....	723
Host- und netzwerkbasierende Intrusion Detection-Systeme .....	724
Das Zonendiagramm .....	725
Analyse von Zwischenfällen .....	726
False positives und negatives .....	729
Informationsflut in großen Umgebungen .....	730
Alerting und Response .....	731
<b>11.3 Intrusion Prevention .....</b>	<b>732</b>
<b>11.4 Security Auditing: der Test-Einbruch ins eigene Netzwerk .....</b>	<b>737</b>
Ausgangslage .....	737
Auftragsannahme .....	739
Vorbereitungen .....	741

Durchführung .....	742
Reporting .....	744
Nach dem Audit .....	746

## **12. Kryptografie – Verschlüsseln und Verstecken ..... 749**

### **12.1 Spionage schwer gemacht: Verschlüsselung ..... 753**

Symmetrische Verschlüsselung .....	753
Asymmetrische Verschlüsselung .....	758
Hash-Funktionen .....	761
Gesetzliche Auflagen und Einschränkungen .....	762

### **12.2 Steganographie – die Kunst, Daten zu verstecken ..... 764**

Die Technik .....	765
Ein Beispiel .....	767
Software zum Verstecken .....	768

### **12.3 Zertifikate, digitale Signaturen und Schlüssel ..... 769**

Die Technik .....	770
Bezugsquellen .....	774
Installation .....	777
Praktischer Einsatz .....	780
PKI (Public Key Infrastructure) .....	784

### **12.4 Quantenkryptografie ..... 786**

Die Technik .....	786
Protokolle .....	787

### **12.5 Verschlüsselungssoftware ..... 788**

Windows 2000- und XP-eigene Kryptosoftware .....	790
Kryptosoftware von Drittanbietern .....	792
Hintertüren .....	803
Exportbeschränkungen .....	806

## **13. Biometrie – die Sicherheitstechnologie der Zukunft? ..... 809**

### **13.1 Biometrische Zugangskontrollen ..... 810**

Fingerabdruckerkennung .....	810
Iris- und Retina-Erkennung .....	814
Gesichtserkennung .....	816
Dynamische Unterschriftenerkennung .....	818
Stimmerkennung .....	819
Erkennung des Tastaturanschlags .....	820
DNS-Erkennung .....	821

---

<b>13.2 Der praktische Einsatz biometrischer Zugangskontrollen</b> .....	<b>821</b>
Enrollment – Anlegen biometrischer Datensätze .....	822
Identifikation vs. Authentifizierung .....	824
Die Zuverlässigkeit von biometrischen Systemen .....	826
Biometrie als Personalausweis der Zukunft? .....	828
<b>13.3 Biometrische Zugangsverfahren knacken</b> .....	<b>829</b>
Reaktivieren von Latenzbildern .....	830
Täuschen von Bildscannern .....	832
Replay-Attacken .....	833
Manipulation der Referenzdatenbanken .....	835
 <b>Anhang</b> .....	 <b>837</b>
 <b>Stichwortverzeichnis</b> .....	 <b>862</b>

---