



Computer & Literatur Verlag GmbH

DIE KUNST DER DIGITALEN VERTEIDIGUNG

Thomas Werth

Widmung

Wenn aus Liebe Leben wird, trägt das Glück einen Namen:

– Maya –

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopie, Mikrofilm oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

Der Verlag macht darauf aufmerksam, daß die genannten Firmen- und Markenzeichen sowie Produktbezeichnungen in der Regel marken-, patent-, oder warenzeichenrechtlichem Schutz unterliegen.

Die Herausgeber übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren, Programme oder Schaltungen.

1. Auflage 2009

© 2009 by C&L Computer und Literaturverlag
Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: <http://www.CuL.de>

Coverdesign: Hawa & Nöh, Neu-Eichenberg
Satz: C&L-Verlag
Druck: PUT i RB DROGOWIEC
Printed in Poland

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN 978-3-936546-59-0

INHALT

Vorwort
Seite 11

Geleitwort
Seite 16

Kapitel 1
Bedrohungen und Risiken
Seite 17

| | |
|--|-----------|
| 1.1 Schützenswerte Güter und Bedrohungsarten | 18 |
| 1.1.1 Potentielle Angreifer | 19 |
| 1.1.2 Hardwareausfall | 22 |
| 1.2 Angriffsarten | 23 |
| 1.3 Angriffsvektoren | 28 |
| 1.3.1 Windows-Client fernsteuern..... | 32 |
| 1.3.2 Mobile Endgeräte kapern | 37 |
| 1.3.3 Drahtlosen Netzverkehr abhören | 40 |
| 1.3.4 Angriffe auf Server | 51 |
| Angriffe auf interne Server | 51 |
| Angriffe auf öffentliche Server | 62 |
| 1.3.5 Angriffe auf Anwendungsebene | 71 |
| 1.3.6 Telefongespräche mitschneiden..... | 76 |
| 1.3.7 Datenverkehr im Internet abfangen (Man in the Middle)..... | 79 |
| 1.4 Zusammenfassung | 82 |

Kapitel 2

Gefahrenabwehr

Seite 85

| | |
|---|------------|
| 2.1 IT-Sicherheitsrichtlinien | 85 |
| 2.2 Netzwerkzugang von extern | 90 |
| 2.2.1 Virtuelles Privates Netzwerk (VPN) | 91 |
| 2.2.2 Stunnel..... | 93 |
| 2.3 Netzwerke sichern | 95 |
| 2.3.1 Firewallsystem installieren..... | 97 |
| Zugriff auf Webseiten über HTTP-Proxy..... | 102 |
| Anbinden des internen E-Mailservers..... | 103 |
| Zugriff auf FTP-Server über einen FTP-Proxy..... | 104 |
| Einrichten einer DMZ..... | 105 |
| Firewall-Regeln konfigurieren..... | 106 |
| Optionale Konfiguration | 108 |
| 2.3.2 Angriffserkennung | 109 |
| Intrusion-Detection-Systeme (IDS) | 110 |
| Honeypots | 114 |
| ARP-Spoofing abwehren..... | 121 |
| 2.3.3 Systemmeldungen zentral sammeln und verwalten | 123 |
| 2.3.4 Netzwerkverfügbarkeit überwachen..... | 127 |
| 2.3.5 Virtuelle LANs..... | 129 |
| 2.4 Drahtlose Netzwerke (WLAN) sichern..... | 136 |
| 2.4.1 WLAN-Reichweite erhöhen..... | 137 |
| 2.4.2 WPA-Enterprise einrichten..... | 139 |
| 2.5 Server sichern | 147 |
| 2.5.1 Server härten..... | 147 |
| 2.5.2 Webserver härten | 148 |
| 2.5.3 Microsoft Internet Information Services absichern | 158 |
| 2.5.4 Sicherheitsleitfaden für Microsoft Exchange | 160 |
| 2.5.5 Windows Server Update Services installieren | 162 |
| 2.5.6 Serverintegrität überwachen..... | 170 |
| 2.5.7 Sicherer Terminalzugriff auf Server..... | 173 |
| 2.5.8 Eigene Zertifizierungsstelle für das Intranet..... | 174 |
| 2.6 Clients sichern | 175 |
| 2.6.1 Desktop-Firewalls | 176 |
| 2.6.2 Browser sichern | 179 |
| Internet Explorer..... | 183 |
| Firefox | 186 |
| Seamonkey..... | 190 |
| Galeon, Epiphany, K-Meleon, Flock und Co. | 190 |
| Opera | 193 |

| | |
|---|------------|
| Safari | 194 |
| Chrome | 194 |
| Konqueror | 195 |
| Versteckte Browser | 197 |
| 2.6.3 Das TOR-Netzwerk | 197 |
| 2.6.4 Virenschutz | 198 |
| 2.6.5 Schutz vor Buffer Overflows | 200 |
| 2.6.6 Arbeiten mit eingeschränkten Rechten | 201 |
| 2.6.7 Vermeiden von Standardsoftware | 201 |
| 2.6.8 Kommunikation verschlüsseln | 201 |
| 2.6.9 Daten- und Datenträgerverschlüsselung | 201 |
| 2.6.10 Sichere Passwörter | 202 |
| 2.6.11 Autostart deaktivieren | 203 |
| 2.6.12 Anwenderschulung | 204 |
| 2.7 Virtuelle Maschinen sichern | 205 |
| 2.7.1 Gefährdungslage | 209 |
| 2.7.2 Planung des VM-Hosts | 213 |
| 2.7.3 Sicherheitsvorkehrungen auf Netzwerkebene | 214 |
| 2.7.4 Konfiguration | 215 |
| 2.7.5 Administration | 216 |
| 2.8 Sichere PDAs | 218 |
| 2.9 Daten verschlüsseln | 222 |
| 2.9.1 Daten verschlüsselt ablegen | 223 |
| 2.9.2 E-Mails verschlüsseln | 225 |
| 2.10 Datensicherung | 226 |
| 2.11 Online-Banking | 229 |

Kapitel 3

Schwachstellenerkennung

Seite 237

| | |
|--|------------|
| 3.1 Unsichere Serverzugriffe erkennen | 237 |
| 3.2 Programmfehler finden | 239 |
| 3.2.1 Speicherüberläufe (Buffer-Overflows) | 241 |
| Stack Buffer-Overflow | 242 |
| Off-by-One Buffer-Overflow | 259 |
| BSS Buffer-Overflow | 267 |
| Heap Buffer-Overflow | 274 |
| 3.2.2 Integer-Overflow | 282 |
| 3.2.3 Formatstring-Overflows | 288 |

| | |
|---|------------|
| 3.2.4 Fortgeschrittene Exploit-Techniken..... | 296 |
| Return-into-PLT | 302 |
| Stack Juggling..... | 309 |
| 3.2.5 Zusammenfassung | 312 |
| 3.3 Penetration Testing | 314 |
| 3.3.1 Programme für Sicherheitsanalysen..... | 315 |
| Nmap..... | 316 |
| Metasploit Framework 3..... | 323 |
| John the Ripper..... | 325 |
| Hydra | 327 |
| Chaosreader..... | 329 |
| Ettercap | 329 |
| Cain | 332 |
| Aircrack-NG | 333 |
| Nikto | 335 |
| Web Application Attack and Audit Framework (W3AF) | 338 |
| Damn Vulnerable Linux..... | 338 |
| Backtrack..... | 339 |
| 3.3.2 Penetration-Testsystem aufsetzen..... | 340 |
| 3.3.3 Methodiken der Sicherheitsanalyse..... | 345 |
| 3.3.4 Schritt-für-Schritt-Sicherheitsanalysen | 361 |
| Konfigurationsfehler aufspüren..... | 361 |
| Bruteforce-Angriffe durchführen | 371 |
| Exploits | 382 |
| Webanwendungen untersuchen..... | 395 |
| 3.3.5 Zusammenfassung | 408 |

Kapitel 4

Digitale Forensik

Seite 413

| | |
|---|------------|
| 4.1 Reverse Engineering..... | 413 |
| 4.1.1 Kryptoanalyse..... | 420 |
| 4.1.2 Patchanalyse | 434 |
| 4.2 Systemanalyse | 444 |
| 4.2.1 Image anlegen | 445 |
| 4.2.2 Image untersuchen | 446 |
| 4.2.3 Datei-wiederherstellung | 448 |
| 4.2.4 Virtuelle Maschinen untersuchen | 449 |
| 4.2.5 Systeminfektion untersuchen | 451 |
| Dateianalyse unter Windows | 451 |
| Live-Systemanalyse unter Windows..... | 455 |

| | |
|--|------------|
| Dateianalyse unter Linux..... | 459 |
| Live-Systemanalyse unter Linux | 461 |
| 4.2.6 Backtracking | 468 |
| 4.3 Forensische Analyse nach dem SAP-Modell..... | 471 |
| 4.3.1 Sichern | 471 |
| 4.3.2 Analysieren | 472 |
| 4.3.3 Präsentieren..... | 473 |
| 4.3.4 Protokollieren..... | 474 |
| 4.3.5 Datenschutz | 474 |
| 4.3.6 Sicherstellung der Untersuchungsumgebung..... | 475 |
| 4.3.7 Juristische Verwertbarkeit der Beweise..... | 480 |
| 4.3.8 Incident-Response-Vorbereitung im Unternehmen..... | 484 |
| 4.3.9 Zusammenfassung | 487 |

Kapitel 5 Nachwort Seite 489

| | |
|---|------------|
| 5.1 Die Gesetze der Sicherheit | 489 |
| 5.2 Trends..... | 503 |

Anhänge Seite 507

| | |
|--|------------|
| A Disassembler-Crashkurs | 507 |
| A.1 Funktionsumfang von Assembler | 507 |
| A.2 Statische Analyse..... | 515 |
| A.3 Laufzeitanalyse..... | 519 |
| A.4 Patchen..... | 521 |
| A.5 Antidebugging | 522 |
| A.6 Shellcode disassemblieren..... | 524 |
| B Softwareentwicklung und IT-Sicherheit..... | 531 |
| B.1 Sicheres Programmieren..... | 531 |
| B.2 Entwicklung eines Sicherheitsprüfprogramms | 544 |
| C Programmlistings..... | 569 |
| C.1 Das Programm Encrypt_Password | 569 |
| C.2 Das Programm convert | 573 |

| | |
|---|-----|
| C.3 Puffer für die Kryptoanalyse | 575 |
| C.4 Das Programm bruteExample | 578 |
| C.5 Webmin-Exploit | 584 |
| C.6 Debian SSH Key Tester | 586 |
| C.7 Linux vmsplICE Local Root Exploit | 588 |

Glossar
Seite 595

Stichwortverzeichnis
Seite 599

VORWORT

Spätestens seit dem Sommer 2008 kann kein Computersystem mehr als unverwundbar bezeichnet werden. Zu diesem Zeitpunkt schaffte der Trojaner W32.Gammima.AG über infizierte Speicherkarten den Weg ins All und befahl die Computer der internationalen Raumstation IIS.

Beispiele gibt es genug für erfolgreiche Angriffe auf Computersysteme. Ob das Entwenden einer Million Datensätze von der Online-Jobbörse Monster.com, der Diebstahl von über 17 Millionen Kundendatensätzen bei T-Mobile oder Spionage über das Internet – die Bedrohung der IT-Systeme ist sehr real. Kein Computersystem ist unverwundbar, professionelle Hacker können in jedes anvisierte Computersystem einbrechen. Dabei sind private PCs, die ja meist unter Microsoft Windows laufen, sogar sicherer als Firmen-PCs, denn der Privatanwender läßt meist regelmäßig und zeitnah die automatischen Sicherheitsupdates des Betriebssystems über das Internet ausführen, in Firmen, wo eine solche Eigeninitiative der Mitarbeiter untersagt ist, werden die Sicherheitspatches auf den PCs oft so spät eingespielt, so daß die Computer mit den Sicherheitslücken in der Zwischenzeit leicht angegriffen werden können. Für ein betroffenes Unternehmen kann die Konsequenz vom kräftigen Image- bis hin zum wirtschaftlichen Totalschaden reichen, weshalb es unerlässlich ist, vorbeugende Maßnahmen zu ergreifen.

Bei Unternehmen kristallisieren sich meist die Internet-Angebote als Schwachstelle der IT-Sicherheit heraus. Cyberkriminelle verteilen über gehackte Webseiten Schadsoftware an Besucher der Seite oder erhalten über Lücken Zugriff auf die angeschlossene Datenbank und die dort gelagerten Kundendaten. Steht

der Webserver im Firmennetzwerk, kann der Angreifer auf diesem Weg sogar Zugriff auf das interne Netzwerk eines Unternehmens erhalten, weil viele Internet-Anwendungen nur unzureichend geschützt sind. Über die Hälfte der in 2008 gefundenen Schwachstellen hatten mit Webanwendungen zu tun, immer mehr als beliebtes Angriffsziel offenbaren sich dabei die AJAX-Anwendungen, die im Zuge des sogenannten Web 2.0 Popularität erlangten. Sie benötigen JavaScript, nutzen XML-Dateien zum Datenaustausch und kommunizieren über dynamische Serverseiten (PHP oder ASP) mit einem Datenbanksystem. Aufgrund ihrer Komplexität enthalten sie naturgemäß öfter und schwerere Fehler als einfache Webauftritte. Findet ein Angreifer eine Lücke in einer Anwendung, über die er eigenen JavaScript-Code in die Seite einbetten kann, ist er in der Lage, die Anwendung zu manipulieren. Schafft er es dann, die XML-Dateien abzufangen, kann er die oft unverschlüsselten Daten mitlesen. Eine SQL-Injection-Schwachstelle im PHP- oder ASP-Code sorgt eventuell für den Zugriff auf die Datenbank und die darin enthaltenen Daten.

Oft stellen die über verschiedene Wege im Internet gehackten Server gar nicht das eigentliche Ziel dar – das sind die Endanwender und ihre Client-Computer. Über diese Server werden schadhafte Inhalte in eigentlich vertrauenswürdige Webseiten eingeschleust. Der bösartige Code greift dann über JavaScript aktive Inhalte wie Flash oder ActiveX oder auch Fehler im Browser, mit dem die Seite besucht wird, den Computer des Besuchers an. Schafft es der Angreifer, auf diesem Weg eigenen Programmcode auf dem Rechner des Anwenders auszuführen, erlangt er meist auch die Kontrolle über ihn. Der Computer wird dann Teil eines großen Netzes von infizierten Computern unter der Kontrolle des Angreifers. Solche Netze werden Bot-Netze genannt, ihre Aufgaben sind unter anderem das Versenden von Spam-E-Mails und verteilte Angriffe auf populäre Webseiten mit dem Ziel, diese vorübergehend lahmzulegen. Bot-Netze sind ein lukratives Geschäft für Kriminelle, die durch die Vermietung der Netze an Spammer oder andere zwielichtige Personen viel Geld verdienen.

Natürlich sind auch Standardlösungen verwundbar. Im Internet kursieren detaillierte Auflistungen bekannter Schwachstellen und wie sie ausgenutzt werden können. Baukästen zur Erzeugung von schadhaften PDF- oder Word-Dokumenten, Flash-Filmen und Webseiten liegen gleich bei. Auch sind die Zeiten, in denen nur ausführbare Dateien eine Gefahr enthalten, vorbei, heutzutage kann jede Datei – egal ob Dokument, Bild oder Film – einen Computer verseuchen. Damit sind auch weniger begabte Kriminelle in der Lage, ein System erfolgreich anzugreifen und Malware zu verbreiten.

Zum Verhindern von Angriffen gibt es verschiedene Sicherheitsmodelle, die einen unterschiedlich starken Schutz bieten. Bei der Wahl des Sicherheitsmodells kann man auf bewährte Sicherheitsarchitekturen zurückgreifen oder

ein eigenes Sicherheitsmodell implementieren, das auf den Maßnahmen des IT-Grundschutz-Katalogs des Bundesamts für Sicherheit in der Informationstechnik (BSI) basiert. Es bietet eine Art Kochrezept für ein normales Schutzniveau an, wobei auch Eintrittswahrscheinlichkeiten, potentielle Schadenshöhen und Kosten für die Umsetzung der Absicherung berücksichtigt werden. Das Grundschutzhandbuch ermöglicht den Verzicht auf eine von Experten zusammengestellte Sicherheitsanalyse, da es pauschalisierte Gefährdungen voraussetzt. So sind auch Nicht-Experten in der Lage, die notwendigen Maßnahmen herauszufinden und zusammen mit Fachleuten umzusetzen. Das Open-Source-Programm *Verinice* von <http://verinice.org/> kann den Sicherheitsbeauftragten bei der Umsetzung des Katalogs unterstützen. Die erfolgreiche Implementierung des Grundschutzes läßt sich vom BSI mit einem Grundschutz-Zertifikat bestätigen.

Sicherheit darf aber nicht auf Kosten der Produktivität gehen. Das sicherste System nützt wenig, wenn niemand damit arbeiten kann!

Das Sicherheitsmodell *Security by Obscurity* (Sicherheit durch Geheimhaltung) verfolgt den Ansatz, ein System sei so lange sicher, wie niemand von ihm weiß. Dies bezieht sich auf die Existenz, den Inhalt, Sicherheitsvorkehrungen und weitere sicherheitsrelevante Informationen. Allerdings gibt es gerade im Internet viele Möglichkeiten, Informationen über ein Ziel zu erhalten und Ziele zu finden. Daher sollte dieses Modell niemals als einziger Schutz Anwendung finden. Bei einer *Host Security* (individuelle Sicherung der Computer) wird jeder PC eigenständig bestmöglich abgesichert, was die Sicherheit eines Servers sowie eines normalen PCs gewährleistet. Dieser Ansatz ist jedoch in einem Unternehmen mit vielen Clients und Servern nicht mehr haltbar, dort koexistiert eine Vielzahl an unterschiedlicher Hard- und Software, deren individuelle Wartung einen nicht zu bewältigenden Aufwand erfordern würde.

Beim Konzept der *Network Security* (Sicherung der IT-Umgebung im Ganzen) wird die IT-Struktur durch die Kontrolle des Netzwerkzugriffs der einzelnen Computer und ihrer angebotenen Dienste abgesichert, wobei anhand von Firewalls die internen Systeme geschützt werden, kombiniert mit sicheren Authentifizierungsmaßnahmen und der verschlüsselten Übertragung von Daten im Netzwerk. Dieses Modell ist gut erweiterbar und kann eine hohe Anzahl an Computern mit vertretbarem Aufwand schützen. Je nach Größe und Aufteilung der IT-Struktur hat auch dieses Modell seine Grenzen und es sollte besser ein mehrschichtiger Ansatz gewählt werden.

Dieses Modell in Kombination mit Host Security für wichtige interne Server, Server im Internet und zur Absicherung gegen Angriffe aus dem Intranet bietet einen entsprechend hohen Schutz gegen die vorgestellten Gefahren und ist die architektonische Grundlage der in diesem Buch vorgestellten Schutz-

maßnahmen. Man sollte sich jedoch bewußt sein, daß kein Sicherheitsmodell einen unüberwindbaren Schutz bieten kann. Ein schlecht gelaunter Zeitgenosse mit (scheinbar) erlaubtem Zugang zu Daten und Informationen kann immer noch »berechtigt« großen Schaden anrichten. Ein Sicherheitsmodell kann keinen perfekten Schutz bieten; das Ziel ist es, Einbrüche selten, begrenzt und kostenneutral zu halten und damit Schaden vom Unternehmen abzuhalten.

Die Verteidigung gegen Angriffe und Schadsoftware ist also eine wahrliche Kunst. Ich habe dieses Buch für die vielen Systemadministratoren und Informatiker geschrieben, die wie ich in kleineren und mittleren Firmen für »die EDV-Technik« zuständig sind. Wir können programmieren, installieren PCs, sind oft die wandelnde Hotline für die Anwender und administrieren das Netzwerk, weil es sich nicht lohnt, eine extra Kraft mit dieser Aufgabe zu betrauen. Natürlich würde ich mich auch freuen, wenn der eine oder andere Geschäftsführer, der sonst wenig mit Computern zu tun hat, das Buch zumindest überfliegen würde. Ihm möchte ich auch zeigen, wie gefährlich es ist, wenn er die Wichtigkeit der Sicherheit seiner IT unterschätzt.

Aufgeteilt habe ich das Buch in die Bereiche Gefahrenabwehr, Angriffserkennung, Schwachstellenanalyse und Forensik. Damit decke ich alle Facetten der IT-Sicherheit ab. Zuerst zeige ich, wie Angriffe von außen und innen auf Clients, Server und Netzwerke durch den richtigen Aufbau des Netzwerks, eine sichere Art der Datenübertragung und durchdachte Softwareinstallationen auf den PCs verhindert werden.

Um rechtzeitig mitzubekommen, ob das eigene Netz nicht doch zum Objekt der Begierde durch Kriminelle oder Scripting-Kiddies wurde, beschreibe ich, wie Intrusion-Detection-Systeme installiert werden, die versuchte (und erfolgreiche) Einbrüche mitprotokollieren. Steht die ganze Sicherheitsstruktur, muß sie natürlich auch getestet werden. Das Mittel zum Zweck sind Penetration Tests, die die (Nicht-)Durchlässigkeit des Systems unter Beweis stellen. Tritt doch der Ernstfall ein und ein Angreifer konnte Zugriff erlangen, muß das geschädigte System analysiert werden. Die dabei unter anderem vorgestellte Technik des Reverse Engineering setzt Grundkenntnisse im Disassemblieren voraus, ein Crashkurs hilft beim Auffrischen. Außerdem zeige ich noch, wie ein Exploit entwickelt werden könnte. Dies ist ein probates Mittel, die Sicherheit einer Software auf die Probe zu stellen.

Zum Schluß dieses Vorworts möchte ich noch denen danken, die zum Entstehen und Gelingen dieses Werks beigetragen haben.

Zuerst danke ich meiner Frau Nadine für ihre Geduld und ihr Verständnis in dieser Zeit. Ganz besonders dafür, daß sie in mein Leben getreten ist und es seither mit Freude und Liebe bereichert. Meinen Eltern Wilfried und Marina Werth gebührt Dank, da sie mit meinem ersten Computer meinen »IT-Stein« überhaupt erst ins Rollen gebracht haben.

Ebenso danke ich meinen Freunden und Kollegen für ihre Unterstützung über die gesamte Zeit, insbesondere Nadine und Marina Werth, Mike Garrecht, Nicole Vortmann, Volker Fischer und Dominik Janisch für das aufopferungswillige Korrekturlesen von Texten aus einer anderen Welt.

Auch danke ich allen referenzierten Autoren für ihr spannendes und informatives Material sowie die entwickelten Tools und Programme. Natürlich bin ich auch all den unbekanntem Autoren für ihr Material dankbar, auf das ich bei Internet-Recherchen gestoßen bin und es keinen gekennzeichneten Autor gab oder ich längst vergessen habe, wo ich die Informationen gefunden hatte. Vielen Dank an meine Lektorin und Verlegerin Frau Riebl für eine wunderbare Zusammenarbeit und die Verwirklichung dieses Buchs, außerdem Marc Ruef, der es vor Drucklegung gelesen und als gut bewertet hat.

Ebenso möchte ich Volker Fischer danken, weil er mich immer ohne zu zögern unterstützt, wenn ich mal Hilfe brauche. Dann noch Thomas Biege, der mir die IT-Security überhaupt erst schmackhaft gemacht hat und mir beim Einstieg in die Materie oft geholfen hat.

Viel Spaß beim Lesen und Nachvollziehen wünscht Ihnen

Thomas Werth

Die Quelltexte, die im Anhang dieses Buchs abgedruckt sind, können von der Verlagswebseite unter www.CuL.de heruntergeladen werden.

GELEITWORT

Auch wenn es gerne vergessen wird, so wurde doch der Computer ursprünglich aus zwei Gründen entwickelt: Zum einen sollte er sehr große Datenmengen aufnehmen und verarbeiten können, zum anderen sollte er mit der Durchführung dieser repetitiven Aufgabe dem Menschen die Zeit erschließen, sich mit wichtigeren und komplexeren Dingen auseinandersetzen zu können. Wir leben nun dank des Computers im Informationszeitalter, in dem der Besitz, die Verarbeitung und die direkte Weitergabe von Daten und Datenstrukturen zu einem wichtigen Maßstab unseres täglichen Lebens geworden sind.

Informationen lassen sich aber mißbrauchen.

Thomas Werth zeigt in diesem Buch die bestehenden und drohenden Gefahren des Informationszeitalters in der Praxis. Didaktisch geschickt bespricht er im ersten Teil die grundlegenden Gefahren moderner Computersysteme, im zweiten Teil macht er sich gemeinsam mit dem Leser daran, mit technischen Hilfsmitteln potentielle Schwachstellen und vorhandene Sicherheitslücken im Rahmen unterschiedlicher Tests auszumachen. Und im dritten Teil widmet er sich dem Thema Computerforensik, das er anhand der Analyse erfolgreicher Attacken erklärt. Dabei zeigt der Autor dem Leser bei jeder Station grundlegende Mechanismen auf, die er nach und nach durch seinen Erfahrungsschatz bereichert. Auf diese Weise können auch Einsteiger im Bereich der Computersicherheit Fuß fassen und bekommen mit dem Buch eine solide Basis für das detaillierte Selbststudium an die Hand. Es eignet sich deshalb als Lehrbuch mindestens so gut wie als Nachschlagewerk, das während der Phasen der Prävention (Hardening/Auditing) und der Analyse (Forensik) immer wieder eine sehr gute Stütze liefern wird.

In diesem Sinne bleibt mir nichts anderes übrig, als dem interessierten und aufmerksamen Leser viel Spaß mit dem vorliegenden Buch zu wünschen. Der Bereich der Computersicherheit ist seit jeher ein spannendes Thema, das besonders in einer geschickten Verknüpfung mit praktischen Anwendungsbeispielen an Nervenkitzel nur schwer zu überbieten ist!

Marc Ruef

Security Consultant

KAPITEL 1

BEDROHUNGEN UND RISIKEN

Um verstehen zu können, warum ein Schutz der IT-Systeme so wichtig ist, muß erst einmal gezeigt werden, welche Gefahren überhaupt bestehen. Aus diesem Grund widmet sich dieser erste Teil des Buchs den möglichen Gefahrenquellen und Angriffsflächen und es wird aufgezeigt, welche Güter verwundbar sind, welcher Schaden für ein Unternehmen entstehen kann und welche Sicherungsstrategien für den Schutz der IT-Systeme möglich sind.

Beim Schutz ihrer IT-Systeme befinden sich Firmen nicht in einem rechtsfreien Raum. So sind Unternehmen mit dem Firmenstandort Deutschland sogar indirekt durch gesetzliche Vorgaben verpflichtet, sich mit der Thematik der IT-Sicherheit auseinanderzusetzen. Insbesondere das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG §91 Abs. 2 Aktiengesetz) macht hier Vorgaben und stellt Forderungen bezüglich des Risikomanagements an Kapitalgesellschaften. Die Gesetzesbegründung besagt, daß im Rahmen des Risikomanagements Elemente wie ein Frühwarnsystem, ein internes Überwachungssystem einschließlich einer Revision und ein Controlling vorhanden sein müssen.

Das Handelsgesetzbuch (HGB) schreibt dem Kaufmann in §238 Abs. 1 vor, wie seine Bücher zu führen sind. Im 4. Abschnitt folgen Vorschriften zum Internen Kontrollsystem (IKS) eines Unternehmens, die hohe Anforderungen an die Datensicherheit in Unternehmen stellen. Diese gesetzlichen Vorgaben können durch ein IT-Sicherheitskonzept realisiert werden.

Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang von öffentlichen und nicht-öffentlichen Stellen mit personenbezogenen Daten und stellt in der Anlage zum Gesetzestext Anforderungen bezüglich Zutritts-, Zugangs-,

Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle. Ebenso verweist das Gesetz auf Möglichkeiten zur Überprüfung der Sicherheitsmaßnahmen anhand eines Datenschutzaudits.

Unternehmen, deren Mitarbeiter ihren Telefonanschluß oder Internetzugang am Arbeitsplatz auch zu privaten Zwecken nutzen, zählen als Erbringer von Telekommunikationsdiensten und fallen somit in den Anwendungsbereich des Telekommunikationsgesetzes (TKG). Ziel des TKG ist unter anderem die Wahrung des Fernmeldegeheimnisses im Bereich der Telekommunikation, betroffene Unternehmen müssen den Anforderungen dieses Gesetzes genügen.

Da der Gesetzgeber unterschiedliche gesetzliche Vorgaben an Unternehmen stellt und IT-Sicherheitsvorfälle einen enormen wirtschaftlichen Schaden verursachen können, sollte die individuelle geltende Rechtslage für ein Unternehmen deshalb im Zweifelsfall immer von einem Experten geprüft werden.

1.1 SCHÜTZENSWERTE GÜTER UND BEDROHUNGSARTEN

Jede Firma besitzt drei wesentliche Güter, die geschützt werden müssen: ihre Daten, ihre Ressourcen (CPU, Festplattenspeicher und ähnliches) und ihr Ruf. Diese Punkte befinden sich in unterschiedlichen Gefährdungslagen.

Die Sicherheit, Integrität und Verfügbarkeit der Daten muß gewährleistet sein. Das heißt, Dritte sollten weder in der Lage sein, die Daten einzusehen, noch sie zu ändern. Maßnahmen, um dies zu gewährleisten, verhindern Datendiebstahl, Manipulation und Wirtschaftsspionage. Die Daten müssen aber jederzeit den berechtigten Benutzern zur Verfügung stehen, weil andernfalls ein Produktionsausfall drohen kann.

Erlangt jemand unbefugte Kontrolle über die Ressourcen, kann er die Server und Arbeitsstationen einer Firma fremdsteuern und sie auch für weitere kriminelle Machenschaften mißbrauchen. In jedem Fall werden dem Produktionsbetrieb dabei Ressourcen entzogen.

Die Reputation entspricht dem Vertrauen und Ansehen der Firma, was eine wichtige Rolle im Kampf um Aufträge auf dem freien Markt spielt. Ein Angreifer kann diese ideellen Werte beschädigen, wenn er sich im Internet mit der Identität der angegriffenen Firma bewegen kann. Seine Aktionen erwecken dann den Anschein, als ob sie von der betroffenen Firma kommen würden. Eine andere Form der Rufschädigung ist die Veröffentlichung von Kundendaten, die durch Datendiebstahl verlorengegangen sind.

Ein erfolgreicher Angriff hat im allgemeinen erhebliche Kosten für ein Unternehmen zur Folge. Ein Teil dieser Kosten ist kalkulierbar, zum Beispiel der, der für die Wiederherstellung verlorener Daten aufgewendet werden muß. Es gibt aber auch monetär kaum meßbare Kosten, die beispielsweise durch den Vertrauensverlust entstehen, den man bei Benutzern, Kunden, Investoren und Mitarbeitern erleidet, ganz zu schweigen vom Imageschaden.

Die oben beschriebenen Güter sind ständig unterschiedlichen Bedrohungen ausgesetzt, wobei die Bandbreite der Risiken von Defekten bis hin zu professionellen Angriffen reicht. Hardwareausfälle sind selten das Werk böswilliger Zeitgenossen, Defekte lassen sich nun mal bei technischen Geräten nicht ausschließen. Man denke hier nur an das liebe Auto.

Angriffe hingegen entstehen oft aus einer zugrundeliegenden Motivation heraus – sei es aus Geltungsdrang, Rache oder als Ausführung eines bezahlten Auftrags. Mögliche Folgen solcher Attacks sind dann unter anderem Einbruch, Verfügbarkeitsausfall oder Informationsdiebstahl. Auch Unachtsamkeiten der Mitarbeiter können zu Verfügbarkeitsausfällen führen, etwa wenn versehentlich die Daten der aktuellen Forschungszeige gelöscht wurden.

Für ein Unternehmen gilt es, diese Risiken zu minimieren. Dabei hilft die Beantwortung der drei folgenden Fragen:

- Was ist zu schützen?
- Wer oder was bedroht diese schützenswerten Güter?
- Wie wahrscheinlich ist der Eintritt eines Schadenfalls und welcher Schaden kann tatsächlich entstehen?

Um die erste Frage »Was ist zu schützen?« zu beantworten, müssen die Systeme und Daten einer Firma bewertet werden. Es muß also geklärt werden, was wie wertvoll ist. Durch Detailfragen läßt sich der Wert jedes IT-Objekts abschätzen:

- Welchen Wert besitzen die auf einem System abgelegten Daten? Welche Folgen hat deren unwiderrufliche Löschung oder ihre uneingeschränkte Weitergabe?
- Wie lange darf das System maximal ausfallen? Welche Ausfälle sind akzeptabel und nicht geschäftskritisch? Welche Art von Ausfall hat ernste Folgen für das Unternehmen?
- Wie schnell nach einem Schadensfall muß ein System wieder einsatzbereit sein? Wie hoch darf der Aufwand sein, um das Problem angemessen zu beheben?

Die Abarbeitung der obigen Detailfragen ergibt die gesuchte Liste der zu schützenden Systeme und Daten einer Firma.

1.1.1 Potentielle Angreifer

Nun zur Frage, wer oder was die schützenswerten Güter bedroht.

Potentielle Angreifer lassen sich in vier Kategorien einstufen:

- Normale Endanwender

Von allen Angreifertypen besitzt der normale Endanwender den geringsten Wissensstand. Er benutzt den Computer als Arbeitsmittel und hat kein tieferes Wissen über ihn. Qualitativ sind seine Angriffe eher minderwertig. Dennoch geht von ihm Gefahr aus, die sich jedoch eher aus unbe-

absichtlichen oder fahrlässigen Handlungen ergibt. Beispielangriffe für diese Kategorie sind das absichtliche Löschen von Daten oder das bewußte Deaktivieren von Computersystemen. Normale Schutzmaßnahmen können Angriffe von Endanwendern bereits abwehren, dennoch ist ein wichtiger Faktor deren verhältnismäßig hohe Anzahl in einem Unternehmen. In einer Firma mit 450 Mitarbeitern sind oft nicht mehr als 15 Mitarbeiter in der IT-Fachabteilung beschäftigt, die restlichen Mitarbeiter fallen also in die Kategorie normaler Endanwender. Das bedeutet, daß von über 95 Prozent der Angestellten ein geringes aber immerhin erkennbares Risiko ausgeht.

— Skript-Kiddies

Anwender, die ihre ersten Schritte im Bereich der Computersicherheit unternehmen, werden von erfahrenen Hackern als Skript-Kiddies bezeichnet. Sie besitzen ein oberflächliches Wissen über Computersicherheit, das aber dazu ausreicht, vorgefertigte Angriffstools und Anleitungen aus dem Internet zu besorgen und anzuwenden. Angetrieben werden sie meist von Neugierde oder Geltungsdrang. Die häufigsten Angriffstypen sind entsprechend Angriffe mit dem Ziel, ein System zum Ausfall zu bringen (Denial of Service) oder die Verunstaltung von Webseiten (Defacements). Ihre Angriffe schlagen meist fehl, wenn das heruntergeladene Programm nicht wie beschrieben arbeitet oder die Anleitung nicht exakt zum angepeilten Zielsystem paßt. Die Ziele werden in der Regel zufällig oder nach Popularität ausgewählt. Computersysteme, die einer gewissen Härtung unterzogen wurden und regelmäßig aktualisiert werden, sind gegen Angriffe von Skript-Kiddies ausreichend geschützt. Skript-Kiddies sind im Internet häufig vertreten.

— Semiprofessionelle Angreifer

Der semiprofessionelle Angreifer hat sich intensiv in das Thema Computer eingearbeitet. Er verfügt über viel Wissen aus einem Spezialgebiet, typischerweise handelt es sich bei dieser Gruppe um Linux- und Windows-Administratoren. Bekannte Schwachstellen werden teilweise verstanden und können ausgenutzt werden. Einfache Sicherheitsvorkehrungen, die Endanwender und Skript-Kiddies stoppen, halten diesen Angreifer nicht auf. Hier sind Sicherheitseinstellungen, die auch alternative Angriffswege blockieren, gefragt. Gerät der semiprofessionelle Angreifer an ein System außerhalb seines Fachgebietes, verfügt er nur noch über den Wissensstand eines Skript-Kiddies. Bei der Motivation spielen Neugierde und Geltungsdrang eine geringere Rolle als noch bei den Skript-Kiddies, es kommen jedoch persönliche Interessen wie Rache oder Bereicherung hinzu. Aufgrund der weiten Verbreitung von Spezialisten im IT-Sektor ist auch die Anzahl der semiprofessionellen Angreifer als hoch anzusehen.

— Professionelle Angreifer

Sie stellen die größte Bedrohung dar, denn ihr Wissen ist umfassend und ihre Angriffe besitzen eine hohe Qualität. Professionelle Angreifer besitzen viel Erfahrung auf dem Gebiet der Computersicherheit. Teilweise stammt diese Erfahrung aus der Arbeit als Penetration Tester oder auch aus nachrichtendienstlichen Aktivitäten. Daher kann die Motivation solcher Angreifer auch militärisch oder politisch bedingt sein. Ein professioneller Angreifer verfügt über ein breites Wissen und schließt schnell Wissenslücken. Damit ist er in der Lage, auch bisher unbekannte Hindernisse bei genügend Zeit und mit ausreichenden Ressourcen zu überwinden, womit er sich von allen anderen Angreifer-Kategorien absetzt. Nur starke und mehrschichtig angelegte Schutzmaßnahmen, die gegen alle erdenklichen Angriffe gerüstet sind, können das Risiko eines professionellen Angriffs senken. Hier muß ein Unternehmen den für sich geeigneten Schutz bestimmen und ständig weiterentwickeln, wobei verschiedene Schutztypen kombiniert werden können. So kann der benötigte Zeitaufwand, um ein System zu knacken, erhöht werden, bis der Angriff unrentabel wird. Damit wird erreicht, daß Informationen zumindest eine Zeitlang sicher sind. Ist es dem Angreifer möglich, danach Zugriff auf die Information zu erhalten und diese Information verliert jedoch nach dem Zeitraum an Bedeutung, kann die Information als sicher angesehen werden.

Ein anderer Ansatz ist die Reduzierung des Schadeneinflusses. Durch eine redundante Systemauslegung kann die Auswirkung eines Denial-of-Service-Angriffs egalisiert werden, da binnen Sekunden das Alternativsystem die Arbeit des ausgefallenen Systems übernimmt.

Oder es wird die Durchführung schädlicher Aktionen durch physikalische Maßnahmen zu verhindern versucht. Muß beispielsweise beim Aktualisieren des Firewall-Regelsatzes der Weg über einen USB-Stick gegangen werden, ist es einem Angreifer aus der Ferne unmöglich, einzugreifen. Er ist nicht in der Lage, den USB-Stick entsprechend zu beschreiben und in das Gerät einzustecken. Die Firewall ist damit sicher gegen unbefugte Änderungen von außen.

Dieser Angreifertyp stellt zahlenmäßig den geringsten Anteil der vier Kategorien. Seine Motivation ist in den meisten Fällen beruflich verankert oder entstammt wirtschaftlichen Interessen.

Die letzte Frage, wie wahrscheinlich der Eintritt eines Schadenfalls mit welchem Schaden ist, hängt mit der Qualität der zu erwartenden Angreifer zusammen. Aus der Motivation kann abgeleitet werden, welcher Angreifer aus den vier genannten Kategorien zu erwarten ist. Mit dem Wissen um die Qualität der Angriffe kann sowohl der zu erwartende Schaden wie auch die Wahrscheinlichkeit vorhergesagt werden.

Die Ausgangslage der Risikoeinschätzung ist die Marktposition des eigenen Unternehmens. Sie ergibt sich aus der Bekanntheit und dem Operationsradius der Firma. Ein lokaler Elektroinstallateur, der seine Abrechnungen auf einem PC schreibt, gibt ein ganz anderes Angriffsziel ab als ein weltweit agierender Konzern, der in seinen Datenbanken geheimes Forschungswissen lagert. Je bekannter ein Unternehmen, desto beliebter ist es als Angriffsziel bei Skript-Kiddies und das Risiko steigt entsprechend. Jedes Skript-Kiddie träumt sicherlich davon, die Startseite von Google mit dem eigenen Namen zu verschönern. Dennoch sind Skript-Kiddies nicht wählerisch bei der Auswahl ihrer Ziele, weshalb jedes Computersystem zufallsbedingt Opfer eines Skript-Kiddie-Angriffs werden kann. Der Schaden durch Skript-Kiddies reicht von der Verunstaltung des Internetauftritts bis zum Verlust oder der Verteilung der Daten, die sich hinter dem Webauftritt befinden.

Handelt ein Unternehmen auf dem Weltmarkt und exportiert seine selbstentwickelten Produkte in fremde Länder, ist mit Wirtschaftsspionage zu rechnen. Dies ruft den professionellen Angreifer auf den Plan. Die Wahrscheinlichkeit eines Angriffs ist nicht zu unterschätzen, fremde Nachrichtendienste sind auf diesem Bereich sehr aktiv. Nur durchdachte und gepflegte Sicherheitsmaßnahmen können das Risiko solcher Angriffe reduzieren. Andernfalls kann sich der Firmeneigentümer sicher sein, daß eigene Entwicklungen von fremden Firmen zum Patent eingereicht werden, noch bevor der eigene Patentantrag ausgefüllt ist.

1.1.2 Hardwareausfall

Zu den Gefahrenquellen, die keinen Angriff im eigentlichen Sinne darstellen, jedoch als ernste Bedrohungen zu werten sind, zählt der durch den Ausfall von Servern oder anderen Hardware-Komponenten verursachte Datenverlust. Der Schaden eines solchen Unfalls kann einen Angriff noch übertreffen. Verursacht ein Daten- oder Serverausfall einen Produktionsstillstand, wird dies mindestens wirtschaftliche Folgen nach sich ziehen. Die Folgen können mit entsprechenden Datensicherungen und redundanten Systemen meist abgefangen werden. Die folgenden Anleitungen sind als generelle Vorschläge und Ideensammlung zu verstehen, keinesfalls als Kochrezept, denn vor dem Implementieren eines geeigneten Backup- und Storage-Systems muß das zu sichernde Umfeld genau analysiert werden.

Ein akzeptabler Schutz vor Ausfällen läßt sich durch das Zusammenspiel von Datensicherungen und redundanten Systemen mit der Vorsorge und Pflege von Hardwarekomponenten erreichen. Wichtige Serverdaten könnten statt auf einzelnen, fehleranfälligen und alten Festplatten auf einem RAID-System gelagert werden. Der Ausfall einer einzelnen Festplatte führt dann aufgrund der relativ ausfallsicheren Architektur des Systems nicht unbedingt zu einem

Datenausfall. Es gilt aber immer, daß die Chance sehr groß ist, daß zwei gleiche Platten gleichen Alters beide zeitnah ausfallen können. Aus diesem Grund ersetzen RAID-Systeme keine Backups.

Genauso kann bei fehlenden Investitionsvolumen zu jedem Server eine virtuelle Kopie mittels einer virtuellen Maschine angelegt werden, statt teure Zweitgeräte vor Ort stehen zu haben. Die Daten werden auf einem RAID-System ausgelagert und sind somit unabhängig vom Server verfügbar. Fällt der Server aus, kann unvermittelt die virtuelle Kopie seinen Platz einnehmen und bis zur Reparatur des Servers seinen Dienst übernehmen.

Bei Geräten wie Backbone-Switches, die keine virtuelle Kopie zulassen, sind entsprechende Leerkapazitäten vorzusehen, so daß im Falle eines Ausfalls die restlichen Geräte den Ausfall kompensieren und zumindest das Kernnetzwerk aufrecht erhalten werden kann. Durch vertraglich zugesicherte Austauschzeiten durch den Lieferanten kann auch hier die Ausfallzeit kalkuliert werden. Ist die Supportzeit abgelaufen, sollte die Neuanschaffung der Hardware einem reparierten Gerät ohne Support vorgezogen werden.

Es empfiehlt sich, für solche Fälle vorab eine Notfallrichtlinie im Unternehmen verankert zu haben. Eine Anleitung für das Anlegen von Notfall- und Datensicherungsrichtlinien ist in Kapitel 2.1 ab Seite 85 nachzulesen.

Natürlich müssen auch Einwirkungen von außen in die Betrachtungen einbezogen werden, Elementarschäden durch Naturkatastrophen sollen an dieser Stelle aber vernachlässigt werden. Es ist sicherlich ratsam, einen Serverraum nicht im Keller einzurichten, wenn die Gegend von Hochwasser bedroht ist, ebenso sind auch die Gefahren ausgehend von einem Brand nicht zu unterschätzen. Zudem sollte eine Klimaanlage die Server vor Hitze und eine unterbrechungsfreie Stromversorgung vor Stromausfällen schützen.

1.2 ANGRIFFSARTEN

Ein Angriff kann viele Gesichter haben, die folgende Liste stellt die geläufigsten Arten vor, dabei wird zwischen Einbruch, Verfügbarkeitsausfall und Informationsdiebstahl unterschieden.

- Ein Einbruch versetzt den Angreifer in die Lage, einen Computer exakt so zu benutzen, wie es einem autorisierten User erlaubt ist.
- Ein Denial-of-Service-Angriff (Verfügbarkeitsausfall) verhindert, daß Computer und Netzwerke von den Anwendern genutzt werden können.
- Informationsdiebstahl bietet eine große Bandbreite an Arten und Zielen. Per Telefon können persönliche Informationen erschlichen oder auf elektronischem Wege kann geheimes Wissen entwendet werden.

1.2.1 Adware

Ein Adware-Programm blendet Werbung auf dem installierten Computer ein. Das ist nicht unbedingt etwas Böses, denn legitime Software kann über Werbung finanziert werden und so kostenlos dem Endanwender zur Verfügung gestellt werden. Problematisch ist die Situation dann, wenn Adware ohne die Einwilligung des Anwenders installiert wird. In solchen Fällen werden oft auch Daten über den Anwender gesammelt, dem Browser zusätzliche Werbe-Popups untergeschoben und eine Deinstallation stark erschwert.

1.2.2 Backdoor

Eine Backdoor (Hintertür) ist Software, die es dem Angreifer ermöglicht, bestimmte Computer über das Internet zu steuern. Ist die Hintertür einmal offen, nistet sie sich ins System ein und fügt ihm eine Autostart-Funktion hinzu. Bei jedem Systemstart wird diese dann aktiv und stellt über das Internet eine Verbindung zum Angreifer her, der den Computer somit vollständig kontrollieren kann.

1.2.3 Denial of Service

Ein Denial-of-Service-Angriff (DoS) verhindert den legitimen Zugriff auf einen Computer, eine Webseite oder andere Ressourcen. Erreicht wird dieser Zustand, indem ein Angreifer das System überlastet. Dies kann durch unzählige Anfragen an einen Webserver geschehen, der die Anfragen anderer Nutzer dann nicht mehr bearbeiten kann. Ebenso kann eine bekannte Lücke in einem Betriebssystem oder Programm ausgenutzt werden, das auf manipulierte Daten mit einem Absturz reagiert.

1.2.4 Distributed Denial of Service

Bei einem Distributed-Denial-of-Service-Angriff (DDoS) versucht ein Verbund aus Rechnern gemeinsam, ein Zielsystem durch gleichzeitige Anfragen zu überlasten. Ein solcher Verbund wird auch *Bot-Netz* genannt, denn das Netzwerk besteht aus Bots, die jeden übermittelten Befehl ihres »Meisters« ausführen. Ein solches Computernetzwerk wird meist mit Hilfe von Trojanern konstruiert. Die infizierten Computer befolgen die über den Trojaner übermittelten Befehle des Angreifers und werden so zu einer mächtigen Waffe.

1.2.5 Dialer

Dialer-Programme zielen vorwiegend auf Modem- und ISDN-Einwahlverbindungen ab. Dabei wird auf dem Computer des Anwenders ein Programm installiert, das die Nummer des Internetproviders automatisch durch eine teure Bezahlnummer ersetzt. Über diese neue Nummer wird dann der



Internetzugang hergestellt und es fallen immense Kosten für den Computerebetreiber an. In Zeiten der Breitbandanschlüsse ist die Gefahr durch Dialer zwar gesunken, jedoch ist sie nicht eliminiert.

1.2.6 Keylogger

Ein Keylogger protokolliert mit einem dem Computer untergeschobenen Programm alle Tastatureingaben des Anwenders und speichert sie in einer geheimen Datei ab. Der Angreifer kann diese Datei bei Bedarf einsehen und erhält so Zugriff auf vertrauliche Daten wie zum Beispiel Passwörter.

1.2.7 Pharming

Pharming leitet das Opfer von einer legitimen Webseite auf eine gefälschte Kopie um. Die Angriffstechnik basiert darauf, daß Computer andere Computer über eine eindeutige Zahl adressieren. Da Menschen sich Zahlen wie 192.168.0.1 nicht gut merken können, wurden die Domännennamen eingeführt. So läßt sich *www.meineBank.beispiel* leichter merken als 192.168.12.243. Der Computer setzt den eingegebenen Namen für den Anwender transparent (das heißt, ohne daß er es bemerkt) in die richtige Adresse um und stellt die Verbindung zum Ziel her. An dieser Stelle setzen die Angreifer an: Sie manipulieren den Computer so, daß er bestimmte Namen mit untergeschobenen Adressen auflöst. Auch kann ein Trojaner installiert werden, der den Anwender automatisch auf gefälschte Seiten umleitet. So landet er trotz korrekt eingegebener URL nicht auf der echten Bankseite und übermittelt seine Daten direkt dem Betrüger.

1.2.8 Phishing

Phishing zielt anhand gefälschter Informationen darauf ab, dem Benutzer Passwörter und persönliche Daten zu entlocken. Dazu erhält der Anwender oftmals eine E-Mail von einem bekannten Unternehmen oder einer Bank, in dem er aufgefordert wird, einem Link zu folgen, der auf eine scheinbar dem Unternehmen zugeordnete Seite führt. Alle Daten, die auf dieser Seite eingegeben werden, landen direkt beim Angreifer und er kann sich fortan im Namen seines Opfers bewegen. Besitzt ein Unternehmen eine Website, kann ein Angreifer auch direkt ein Opfer auf diese Seite schleusen. Es kann auch keinen Angriff erkennen, da es sich tatsächlich auf der Originalseite befindet. Dennoch kann der Angreifer aufgrund eventueller Programmierfehler auf der Webseite alle dort eingegebenen Informationen abfangen. Diese Art des Angriffs ist als *Cross-Site Scripting* bekannt.

Eine gezielte Form von Phishing ist das Spear-Phishing, bei dem gezielt ein Opfer attackiert wird. Gerade bei Angriffen auf Unternehmen wird auf diese Weise versucht, Mitarbeiter zur Herausgabe von Zugangsdaten zu bewegen.

1.2.9 Ransomware

Ransomware ist eine Software, die auf dem Zielsystem wichtige Daten und Dateien verschlüsselt und erst nach Zahlung eines »Lösegelds« wieder preisgibt. Einige Angriffe arbeiten auch mit psychologischen Druckmitteln und drohen etwa, alle dreißig Minuten eine Datei unwiederbringlich zu löschen, bis das Lösegeld beim Angreifer eingegangen ist.

1.2.10 Rootkit

Ein Rootkit ist eine Sammlung von Programmen, die den Betriebssystemkern des befallenen Computers manipulieren und Systemprogramme ändern. Sie können die Spuren, die diese Aktivitäten hinterlassen, sogar beseitigen und Dateien und Prozesse verstecken. Beispielsweise werden Systemprogramme (wie zum Auflisten von Dateien) vom Anwender unbemerkt durch solche ersetzt, die Schaden anrichten. Trojaner, Backdoors oder auch Internetwürmer machen gerne von dieser Technik Gebrauch, um die Infektion des Rechners zu verbergen. Rootkits zu erkennen ist sehr schwierig, denn sind sie einmal gestartet, kann auch ein Antiviren-Programm durch das Rootkit getäuscht werden und den Systembefall nicht erkennen.

1.2.11 Spam

Spam ist die elektronische Form von unaufgeforderter Werbepost, mit der sicherlich jeder Anwender mit E-Mailzugang schon in Berührung gekommen ist. Solche Werbe-E-Mails bieten schnelles Geld, günstige Medikamente, Glücksspiel oder ähnliches an. Neuere Generationen von Spam tarnen sich und sind nicht offensichtlich als Werbung zu erkennen. Spam ist immer noch ein lohnendes Geschäft, da der Absender oft auf infizierte Computersysteme zurückgreift und so keine eigenen Kosten hat. Eine geringe Quote an positiven Rückmeldungen reicht aus, um Gewinn zu machen.

1.2.12 Spoofing

Beim Spoofing wird die Quelle einer Kommunikation gefälscht, eine E-Mail scheint von einem anderen Absender zu stammen als vom tatsächlichen Sender. Beim Phishing wird gern auf diese Möglichkeit zurückgegriffen, um die Authentizität der Phishing-E-Mail zu steigern. Für den Anwender sieht es dann so aus, daß die E-Mail tatsächlich von seiner Bank stammt. Auch kann ein Mitarbeiter in einem Unternehmen getäuscht werden und eine gefälschte E-Mail von dem Systemadministrator mit der Aufforderung erhalten, sein Passwort herauszugeben. Spam hingegen nutzt gefälschte Absenderadressen, um seine Herkunft bewußt zu ändern. So erhält der Spamabsender weder nicht zustellbare Rückläufer noch Beschwerden über die Werbung. All dies landet bei dem echten Besitzer der gefälschten Absenderadresse.



1.2.13 Spyware

Spyware spioniert den Benutzer aus und meldet sein Verhalten an den Angreifer. Dabei werden alle Aktivitäten des Anwenders protokolliert und es kann ein Verhaltensmuster eruiert werden. Ob dies dann für Werbezwecke oder als Grundlage für einen Angriff dienen soll, liegt allein im Ermessen des Angreifers. Spyware verlangsamt den infizierten Computer und kann auch zu Abstürzen führen.

1.2.14 Trojaner

Ein Trojaner gibt vor, ein legitimes Programm zu sein, um den Anwender zur Installation zu verleiten, in Wahrheit verfügt der Trojaner jedoch über versteckte Schadfunktionen. Wird das Programm gestartet, führt es im Hintergrund für den Anwender unsichtbar ganz andere Funktionen als angepriesen aus. Dies kann zum Beispiel eine Backdoor inklusive Keylogger oder auch Spyware sein.

1.2.15 Viren

Viren beeinträchtigen die Sicherheit eines Computers. Sie können Daten stehlen oder löschen oder weitere Schadprogramme aus dieser Auflistung nachinstallieren. Viren benötigen immer ein Medium oder Programm, über das sie sich weiterverbreiten können; sie infizieren entweder andere Programme, nutzen ein E-Mailprogramm oder befallen einen USB-Stick.

Der Dateivirus ist eine der ältesten Virenformen. Hier wird vorzugsweise eine ausführbare Datei infiziert und der Programmcode des Virus ersetzt den Startcode der Anwendung. Beim Hochfahren der befallenen Anwendung wird zuerst der Virus aktiv und dann erst wird die Anwendung aufgerufen. Diese Viren befallen weitere Dateien im Zugriff und verbreiten sich über ihre Verteilung.

E-Mail-Viren verbreiten sich automatisch per E-Mail; zur Infektion klickt der Anwender auf einen an eine E-Mail angehängten (getarnten) Virus oder ein verseuchtes Dokument. Jeder Anhang an eine E-Mail kann einen Virus enthalten, wird dieser Anhang aufgerufen, kann der Computer infiziert werden. Wird ein Fehler im E-Mailprogramm ausgenutzt, kann sogar das einfache Lesen einer E-Mail zum Befall durch den Virus führen. Über das Adreßbuch des E-Mail-Clients verbreiten sich die Viren weiter.

Makroviren verstecken sich in Dokumenten und Dateien und nutzen für ihre Schadfunktionen die Makrosprache eines Programms aus. Ein populäres Beispiel für die Umgebung von Makroviren ist Microsoft Office, insbesondere Word und Excel sind betroffen. Mit dem Öffnen eines infizierten Dokuments wird der Virus aktiv und befällt das Computersystem.

Selbst Mobiltelefone sind inzwischen nicht mehr sicher vor Viren, über die Bluetooth-Schnittstelle oder Kurznachrichten können sich die Viren verbei-

ten. Die Schadfunktionen unterscheiden sich nicht sonderlich von denen auf einem echten Computer, sind jedoch auf die Möglichkeiten des jeweiligen Mobilgerätes beschränkt.

Auch PDAs sind nicht vor Viren geschützt. Gerade hier ist eine Zunahme an Viren in Zukunft zu erwarten, da immer mehr PDAs genutzt werden. Auch als Infektionsquelle kommen PDAs in Betracht, da sie von Zeit zu Zeit immer wieder mit einem PC verbunden werden.

1.2.16 Würmer

Würmer unterscheiden sich in der Verbreitungsart von Viren, sie suchen selbständig nach neuen Opfern, die sie angreifen. Dabei nutzen sie Sicherheitslücken in Betriebssystemen aus. Ist ein Angriff erfolgreich, installiert sich der Wurm, lädt weitere Schadprogramme nach und sucht erneut nach weiteren Opfern im Internet. Ein Wurm kann ernsthaften Schaden verursachen, die nachgeladenen Programme können Backdoors enthalten, die Daten auf dem befallenen System verschlüsseln oder den Computer als Waffe in einen Verbund aus Rechnern integrieren. Hinzu kommt noch, daß oft mit einem großen Wurmausbruch die Geschwindigkeit im Internet spürbar nachläßt. Dies liegt an dem enormen Datenaufkommen, das durch den Wurmausbruch generiert wird.

1.3 ANGRIFFSVEKTOREN

Die oben aufgeführten Angriffsarten finden auf den unterschiedlichsten Wegen statt. Generell gilt aber, daß ein System anschließend mit großer Wahrscheinlichkeit kompromittiert ist, wenn ein Angreifer erst einmal in der Lage ist, eigenen Code auszuführen, den er über eine Sicherheitslücke eingeschleust hat.

Möglichkeiten zur Fernsteuerung gibt es in den meisten Fällen, sobald der PC in irgendeiner Form Kontakt zum Internet hat:

- Bei Servern, die selbst im Internet stehen, kann eine bestehende Verbindung über die angebotenen Dienste getarnt werden.
- Bei Computern im inneren Netzwerk einer Firma kann meist über einen HTTP-Tunnel die Firewall des Unternehmens überwunden werden. Dabei wird das Hypertext Transfer Protocol (für die Übermittlung von Webseiten) zweckentfremdet, wobei in dieses Protokoll die zu übermittelnden Daten des Angreifers zur Steuerung der Computer eingebettet werden. Setzt der Cyberkriminelle zudem noch auf das erweiterte Hypertext Transfer Protocol *HTTps* – das zusätzliche »s« steht für »secure« und gibt an, daß die Daten verschlüsselt übertragen werden –, kann der Netzverkehr nicht mehr von einem Einbruchserkennungssystem ausgewertet werden. Wenn eine Firewall auf diese Art durchbohrt wird, ist das also

sehr schwer zu entdecken. Eine Proxy-Firewall, die in der Lage ist, dieses Protokoll zu analysieren, kann ermächtigt werden, HTTPS-Verbindungen aufzubrechen, um in den Datentransfer Einsicht zu erhalten. Nur so kann ein solcher Tunnel aufgespürt werden.

Man sollte sich also darüber bewußt sein, daß ein Computer mit Zugang zum Internet auch von einem Cracker aus der Ferne gesteuert werden kann, wobei er jeden möglichen Angriffsvektor ausprobieren wird, um die Kontrolle über den angegriffenen Computer mittels Trojanern, Backdoors, Rootkits oder ähnlicher Schadsoftware zu erreichen. Der Cracker wird auch gern Umwege beschreiten, wenn er sein Ziel erreichen kann. Bei den nachfolgend vorgestellten Angriffsvektoren wird er auch die im Internet veröffentlichten Listen mit Sicherheitslücken und den dazu passenden Angriffswegen konsultieren. Die Mailingliste *Full Disclosure* wie auch das Archiv auf *www.Mil-worm.com* bieten einem Cracker alles, was er für einen erfolgreichen Angriff benötigt.

Kommunikation über TCP/IP

Damit ein Angreifer überhaupt aus der Ferne auf fremde Computer zugreifen kann, müssen die Computer miteinander kommunizieren können. Ein Protokoll regelt den Datenaustausch zwischen miteinander verbundenen Systemen. Jedes netzwerkfähige Betriebssystem besitzt eine Implementation solcher Protokolle zum Datenaustausch. Das verbreitetste Protokoll im Internet heißt TCP/IP, es ist in mehrere Schichten unterteilt. Die unterste Schicht ist die Netzzugangsschicht, deren Aufgabe es ist, die einzelnen Bits über ein physikalisches Medium zum Zielsystem zu übertragen. Darauf setzt die Vermittlungsschicht auf, die über das Internet-Protokoll Daten versendet und empfängt. Zur Adressierung der einzelnen Systeme erhalten diese eindeutige IP-Adressen, was in etwa einer Hausnummer in der Straße »Netzwerk« entspricht.

Als nächstes kommt die Transportschicht. Sie stellt sicher, daß die durch die vorherigen Schichten beförderten Daten an die richtigen Ports gesendet werden.

Die Anwendungsschicht bildet die oberste Ebene und stellt die Verbindung zu den Netzwerkanwendungen her. Die Programme bieten einen Dienst auf einem Port an und können über diese Layer senden und empfangen. Dabei benötigen sie meist ein weiteres, spezielles Protokoll für den angebotenen Dienst. Die bekanntesten Protokolle in diesem Zusammenhang sind HTTP (Webseiten), FTP (Dateitransfer), SMTP und POP3 (E-Mail).

TCP/IP funktioniert verbindungsorientiert. Das bedeutet, daß das Protokoll garantiert, daß die Daten am Zielsystem in der Reihenfolge ankommen, wie sie vom Quellsystem versendet werden. Zudem wird sichergestellt, daß keine Daten unterwegs verlorengehen. Die Daten werden dabei paketweise übertragen, die zu übermittelnden Daten werden in kleinere Pakete zerlegt, die dann übermittelt wer-

den. Ein zentrales Element bei der Paketübertragung sind die TCP-Flags, die die Kommunikation steuern. Im einzelnen sind dies:

- SYN (S): Synchronisiert die Verbindung.
- FIN (F): Leitet das Ende einer Verbindung ein.
- RST (R): Unverzügliche Beendigung einer Verbindung.
- PLC (-): Platzhalter, kein Flag wird genutzt.
- ACK (ACK): Bestätigt den Empfang eines Pakets.

Diese Flags, mit denen wir später bei verschiedenen Analyseprogrammen noch in Berührung kommen werden, sollen an dem für TCP/IP typischen 3-Wege-Handshake erläutert werden. Ein Verbindungsaufbau in TCP/IP läuft in drei Schritten ab (daher auch der Name »3-Wege-Handshake«):

Zuerst (1) sendet der Client ein Paket an den Zielport des Servers mit gesetztem SYN-Flag. Bei einem geöffneten Port auf dem Zielsystem erhält der Client ein Paket mit gesetztem SYN- und ACK-Flag als Antwort (2). Diese bestätigt der Client wiederum mit dem Senden eines Pakets, bei dem das ACK-Flag aktiviert ist (3). Damit ist der Verbindungsaufbau abgeschlossen und die eigentliche Datenübertragung kann beginnen.

Durch die Adressierung über IP-Adressen und Nutzung der im Internet verfügbaren Protokolle kann ein Angreifer Kontakt zu fremden Systemen aufnehmen und mit ihnen Daten austauschen. Über den Datenaustausch ist er dann in der Lage, diese Rechner zu steuern.

— Externe Angriffe

Ein Angriff über die externe Netzwerkanbindung auf exponierte Server liegt jederzeit im Bereich des Möglichen und Machbaren, sobald ein Unternehmen an das Internet angebunden ist. Solche Angriffe, bei denen der Angreifer oder Wurm über die Datenleitung Schadsoftware wie zum Beispiel Backdoors, Trojaner, Rootkits oder Keylogger installieren kann, können auf unterschiedlichen Wegen eingeleitet werden. Am häufigsten ist das Versenden von Malware an E-Mailadressen der Firma oder Angriffe auf Server mit Internetverbindung. Ziel ist es in den meisten Fällen, Zugriff und Kontrolle über Computer und ihre Daten von außen zu bekommen und auf diese Weise die Computer steuern zu können. Mit dieser Möglichkeit kann der Rechner in ein Bot-Netz aufgenommen werden und für DDoS-Angriffe, zum Spam-Versand oder für das Hosten von Phishing-Seiten genutzt werden.

— Indirekte externe Angriffe

Ein Angriff auf das Intranet mittels E-Mail kann bereits zum Erfolg führen, wenn ein unausgeschlafener und unaufmerksamer Mitarbeiter versehentlich den E-Mail-Anhang ausführt, der Trojaner oder Viren mit dem Ziel,

den Computer zu infizieren, enthält. Durch Sicherheitslücken in Anwendungsprogrammen wie PDF-Viewer oder Grafiksoftware ergeben sich noch weitere Wege, um einen Computer hinter einer Firewall im Intranet zu infizieren, denn manipulierte Dokumente, Bilder oder Archive lassen sich durch E-Mail oder auf Webseiten verteilen. Werden diese betrachtet, nutzt die Datei eine eventuelle Sicherheitslücke im Anzeigeprogramm aus und führt den Angriff durch.

Bei der Wahl schwacher Passwörter können die Server im Internet einem Brute-force-Angriff zum Opfer fallen. Bei einem solchen Angriff werden verschiedene Passwörter durchprobiert, bis eines paßt und den Zugang zum System gewährt. Ebenso kann eine unbekannte Sicherheitslücke in einem Dienst (Mail, HTTP, SSH) von einem Cracker ausgenutzt werden, um das System unter seine Kontrolle zu bekommen. Hat ein Angreifer einen exponierten Server so weit, kann er ihn für Angriffe auf das Intranet mißbrauchen. Er lädt dann Angriffsprogramme auf den Server nach, die es ihm erlauben, das Intranet zu untersuchen und potentielle Ziele zu identifizieren. Nachdem die Ziele ermittelt sind, werden sie von diesem Server aus angegriffen. Meistens wird nicht mit einem solchen Angriff von einem eigenen Server gerechnet und es fehlen natürlich Verteidigungsmaßnahmen dagegen. So steht dem Angreifer das Tor zum Intranet offen und er kommt an Daten und Computersysteme, die eigentlich über das Internet nicht zu erreichen sein sollten.

— **Interne Angriffe**

Interne Angriffe von Mitarbeitern oder Personal mit Zugang zum Intranet bergen ein hohes Risikopotential. Verfügt jemand bereits über den Zugriff auf einen PC im inneren Netzwerk, stehen ihm eine Vielzahl von Angriffsmöglichkeiten zur Verfügung. Die Ursachen eines solchen Angriffs können vielfältig sein – Frustration, Unvermögen, Social Engineering oder Bestechung. Das Ausmaß hängt von den Fähigkeiten des Verursachers ab, das Spektrum reicht von Datendiebstahl oder Verschaffen von höheren Benutzerberechtigungen bis hin zum Ausfall der IT. Verschafft er sich administrative Kontrolle über seinen PC (Boot-CD), kann er eigenständig das interne Netz und alle damit verbundenen Computer angreifen sowie die Daten im Netzwerk erfassen. Das Ergebnis seines Feldzugs ist direkt ersichtlich aus dem Vergleich seines Könnens multipliziert mit seiner Motivation für das Überwinden der angewandten Schutzmaßnahmen des Firmennetzwerks zur Abwehr von Angriffen aus dem Inneren.

— **Physikalische Angriffe**

Eine physikalische Zugangskontrolle sollte gewährleisten, daß nur berechtigte Personen Zugang zu den Servern erhalten, was schon im Vor-

feld verhindert, daß ein Angreifer lokalen Zugang zu einem Server erhält. Denn besitzt er erst einmal lokalen Zugang, kann er schnell Vollzugriff auf den Server erhalten.

Beispielsweise kann bei einem Linux-/Unix-Server am Bootprompt mit der Bootoption `init=/bin/sh` in den Bootmanagern LILO und Grub das System mit einer Rootshell gestartet werden, die dem Anwender Vollzugriff auf den Server gewährt. Der vollständige Bootprompt sieht wie folgt aus:

```
vmlinuz root=/dev/sda1 init=/bin/sh
```

Sitzt ein Angreifer vor diesem Prompt, kann er uneingeschränkt Programme installieren und ausführen sowie die Konfiguration des Servers ändern. Er ist in der Lage, auf alle verfügbaren Daten des Servers zuzugreifen, kann sie kopieren, ändern oder löschen. Zur Lösung dieses Problems kann Grub mit einem Passwort versehen werden¹.

Jeder der folgenden Abschnitte beschreibt ein Szenario, in dem in unterschiedlichen Situationen Zugriff auf Computersysteme oder Daten erlangt wird. Dabei wird veranschaulicht, wie sich fehlende Schutzmaßnahmen auswirken und wo die Grenzen von Schutzmaßnahmen liegen. Die Szenarien decken die häufigsten Einsatzgebiete und Angriffspunkte moderner IT-Umgebungen ab. Somit bietet das Kapitel einen Überblick über die normalerweise unsichtbaren Gefahren im Bereich der Informationstechnik.

1.3.1 Windows-Client fernsteuern

Es klingt eigentlich unglaublich: Jemand ist in der Lage, das Firmen-Netzwerk aus dem Internet zu kontrollieren. Daß das aber tatsächlich möglich ist, zeigt die folgende Schritt-für-Schritt-Analyse von Sicherheitsvorkehrungen. Dabei wird erläutert, wie sie ein Angreifer überwinden kann.

Als erstes Beispielszenario sei ein Netzwerk angenommen, das durch einen Proxyserver, über den die Client-PCs Zugriff auf das Internet (WWW) erhalten, geschützt ist. Im Vorgriff auf das nächste Kapitel seien kurz die Sicherheitsmaßnahmen erläutert: Eine Firewall, die unerwünschten Datenverkehr blockiert, schottet die Client-PCs gegen Zugriffe aus dem Internet ab. Es ist nur HTTP/HTTPs-Verkehr für das Surfen im Web zugelassen, jeder andere Datenverkehr ist ausgeschaltet. Außerdem wacht ein Intrusion Detection System (IDS) über den Datenverkehr. Es soll Angriffe auf die Computersysteme im internen Netzwerk erkennen und gegebenenfalls den Administrator alar-

¹ Wie Grub von USB-Stick, Diskette oder CD gebootet wird und dadurch der Passwortschutz dieses Bootloaders umgangen werden kann, ist bei K. Zürnstein: Reparaturwerkstatt. freeX 2'2009, Seite 8ff. nachzulesen.



STICHWORTVERZEICHNIS

3

3-Wege-Handshake30

A

Absenderinform. fälschen60
 Access Point.....40
 Access Point Impersonation-Angriff.....44
 Access Point simulieren.....44
 Access-Point, MAC-Adresse anzeigen333
 Account übernehmen.....374
 ACK-Flag.....30
 ACLs103
 ActionScript.....180
 ActiveX-Komponenten180
 Adblock Plus189
 Address Space Layout Randomization (ALSR).....296
 Address Space Layout Randomization überwinden 302
 Administrative Rechte auf mobilen Endgeräten38
 Administrative Rechte erlangen.....51
 Adreß-Index.....511
 ADSL sichern.....97
 Adware24
 AES.....40
 AES, Sicherheit.....223
 Aircrack-NG.....41, 333
 Aircrack-NG aktualisieren44
 AJAX.....180
 ALSR-Schutz überwinden297
 Alternate Data Streams (ADS).....35
 Amap.....352
 Anfragender, Antwort senden an seine IP-Adresse..118
 Angreifer, (semi-)professioneller20
 Angreiferarten19
 Angriff, physikalischer.....31
 Angriffe, interne.....31
 Angriffsarten23
 Angriffskennung109
 Angriffsprogramm.....323
 Angriffspuffer.....311
 Angriffsvektoren28
 Angriffswege, Listen mit29
 Antidebugging.....522
 Antiviren-Programm34, 595
 Anwenderschulung204
 Apache.....148
 Apache-Exploits.....386
 API-Aufrufe v. Anwendungen protokollieren521
 Apple, freigegebene Anwendg. von.....221
 Application Level Gateway98
 Archivierungsrichtlinie.....89
 ARP.....121
 ARP-Anfragen beantworten115
 arpd.....115
 ARP-Pakete42
 ARP-Poisoning54
 ARP-Spoofing121
 ARP-Tabelle automat. füllen.....122
 ARP-Tabellen, dynamische umstellen.....122

ARP-Tabellen, statische122
 Arpwatch123
 Array v. Registern511
 Assembler507
 Assembler, Adressierung512
 Assembler, Anweisungen512
 Assembler, call-Befehl513
 Assembler, Daten im Speicher halten511
 Assembler, Funktionsumfang507
 Assembler, Intel-Syntax507
 Assembler, Operanden512
 Assembler, Register509
 Assembler, ret-Befehl.....513
 Assembler, Signaturen.....518
 Assembler, Unterprogramme.....513
 Auslagerungsdatei analysieren (Win)479
 Authentifizierung umgehen400
 Authentisierung.....92, 595
 Authentisierungsserver.....43
 Autonome Systeme79
 Autopsy.....445, 446
 Autoruns.....455
 Autostart deaktivieren.....203
 Autostart untersuchen (Linux)466
 Autostart-Prüfung455, 458

B

Backdoor.....24, 595
 Backtrack44, 339
 Backtrack installieren.....340
 Backtrack konfigurieren343
 Backtracking.....468
 Backup.....595
 Backupstrategie.....226
 Banner Grabbing352
 BASE konfigurieren111
 Basepointer.....514
 Befehlszeiger513
 Benutzerauthentisierung.....95
 Benutzereingabe, Steuerzeichen in289
 Benutzereingaben reduzieren535
 Beweisaufnahme, Dokumentation.....481
 Beweisaufnahme, Protokoll.....474
 Beweise, juristische Verwertbarkeit480
 Beweissicherung.....481
 Beweissicherung, To-do-Liste483
 Beweiszettel482
 Bilddatei-Exploit.....211
 Binary-Audit535
 bind-Payloads323
 Bind-Shell aufrufen254
 Bitlocker.....202
 BMP-/JPG-/WMF-Sicherheitslücken211
 Boot and Root-Angriff.....201
 Border Gateway Protocol79
 Bot-Netz30
 Boundary-Tag.....278
 Breakpoints plazieren519
 Browser Helper Objects.....231
 Browser sichern.....179

| | |
|--|----------|
| Browser, Ausführungsrechte..... | 183 |
| Browser, Malware verschmelzen mit..... | 35 |
| Browser-Plugins..... | 179 |
| Brute-force-Angriff..... | 31 |
| Brute-force-Angriff starten/durchführen..... | 62, 371 |
| Brute-force-Angriffe, Tool für..... | 327 |
| BSI Grundschutz-Handbuch..... | 90 |
| BSS Buffer-Overflow..... | 267 |
| BSS-Segment, schwachstelle ausnutzen..... | 267 |
| Buffer-Overflow..... | 241, 537 |
| Bytecode-Verifier..... | 538 |

C

| | |
|--------------------------------------|----------|
| C#,..... | 537 |
| C/C++..... | 536 |
| Cain..... | 52, 332 |
| CDP-Pakete belauschen..... | 77 |
| Chaosreader..... | 329 |
| Chckrootkit..... | 462 |
| chkporc..... | 465 |
| Chunk, Verwaltungsinformationen..... | 278 |
| Chunks..... | 276 |
| Clickjacking..... | 75 |
| Clientseitige Sicherheit..... | 490 |
| Clientsicherheit..... | 175 |
| Cloud Computing..... | 40 |
| Codeblock-Entschlüsselung..... | 527 |
| Codehooks suchen..... | 457 |
| convert..... | 573 |
| Cookie-Daten ändern..... | 404 |
| Cookies, permanente/Session-..... | 183 |
| Cookie-Verschlüsselung..... | 148 |
| CPU-Register überwachen..... | 520 |
| Cracker..... | 595 |
| Chrome (Webbrowser)..... | 183, 194 |
| Cydia..... | 222 |

D

| | |
|--|---------------|
| Damn Vulnerable Linux..... | 338, 395, 414 |
| Darkspy..... | 457 |
| Data-Bereich..... | 241 |
| Datei verschlüsseln..... | 224 |
| Dateianalyse (Linux)..... | 459 |
| Dateianalyse (Win.)..... | 451 |
| Dateiausführung verhindern, Windows..... | 200 |
| Dateiausführungsverhinderung..... | 296 |
| Dateien remote sichern..... | 227 |
| Dateien verstecken..... | 26 |
| Dateien wiederherstellen..... | 444, 448 |
| Dateischutz (Win) aushebeln..... | 552 |
| Dateisignaturen lesen..... | 449 |
| Dateisignaturen, vordefinierte..... | 449 |
| Dateispeicherort, ursprünglicher..... | 476 |
| Dateisystem-Schutzflag..... | 533 |
| Dateiwiederherstellung..... | 448 |
| Dateizugriff möglich?..... | 357 |
| Daten im Puffer manipulieren..... | 243 |
| Daten im Speicher ändern..... | 274 |
| Daten retten..... | 444 |
| Daten sichern..... | 226 |
| Daten verschlüsseln..... | 201 |
| Daten verschlüsselt ablegen..... | 223 |
| Datenausführungsverhinderung..... | 200 |
| Datenbank SQL-Befehle übergeben..... | 397 |
| Datenbank-Backdoor..... | 397 |

| | |
|--|-------------|
| Datendiebstahl..... | 18 |
| Datenintegrität prüfen (Linux)..... | 461 |
| Datensicherheit..... | 596 |
| Datensicherung..... | 596 |
| Datensicherungsrichtlinie..... | 88 |
| Datenstrom des Zielnetzwerkes belauschen..... | 42 |
| Datenträger, VM erzeugen aus..... | 449 |
| Datenträger-Duplikation..... | 480 |
| Datenträger-Verschlüsselung..... | 201 |
| Datentypen, unterschiedlich große..... | 283 |
| Datenverkehr abfangen..... | 79 |
| Datenverkehr zu Angreifer umleiten..... | 54 |
| Datenwiederherstellung..... | 228 |
| dd..... | 444 |
| DDoS..... | 24 |
| Deauth-Angriff..... | 334 |
| Debugger-Flag..... | 522 |
| Denial of Service (DoS)..... | 23, 24, 596 |
| DES, Sicherheit..... | 223 |
| Desktop-Firewall..... | 176 |
| Desktop-Firewall, Funktionsweise..... | 147 |
| DHCP-Server einrichten..... | 45 |
| Dialer-Programm..... | 24 |
| Dienste finden..... | 373 |
| Dienste/Ressourcen eines Ziels finden..... | 352 |
| dig..... | 60 |
| digitaler Fingerabdruck..... | 95 |
| Disassemblat, DLLs..... | 516 |
| Disassemblat, Enums..... | 516 |
| Disassemblat, Structs..... | 515 |
| Disassemblat, Unterprogrammaufrufe..... | 516 |
| Disassemblat, verschlüsselter Code..... | 523 |
| Disassemblat, Zeichenfolge..... | 516 |
| Disassembler..... | 239, 507 |
| Distributed Denial of Service..... | 24 |
| DLL-Startprogramm..... | 519 |
| DMZ..... | 101, 596 |
| DMZ einrichten..... | 105 |
| DMZ, erreichbare Serverdienste..... | 105 |
| DNS-Einträge, lokale..... | 49 |
| DNS-Forward..... | 345 |
| dnsmap..... | 62 |
| dns-ptr..... | 351 |
| Domain, best. als Absender..... | 61 |
| Domain-Account angreifen..... | 52 |
| Domäneninformationen abfragen..... | 60 |
| Domänennamen..... | 25 |
| DoS..... | 24 |
| Doubling Strings, JavaScript..... | 181 |
| Drahtlose Netzwerke prüfen..... | 333 |
| Drahtlosen Netzwerkverkehr abhören..... | 38, 40 |
| Drahtloses Netzwerk (siehe auch bei WLAN)..... | 136 |
| Dynamische Analysen..... | 536 |

E

| | |
|---------------------------------------|-----|
| EAX-Register ausnutzen..... | 311 |
| EBP..... | 514 |
| Echtheit v. Daten..... | 95 |
| Einbruch..... | 23 |
| Eingeloggte User anzeigen..... | 461 |
| Eingeschränkte Ausführungsrechte..... | 201 |
| Einsprungsadresse verschleierte..... | 524 |
| EIP..... | 513 |
| ELF-Binary..... | 302 |
| ELF-Datei untersuchen..... | 416 |
| E-Mail mit Schadcode-Anhang..... | 33 |

| | |
|--|------------------------|
| E-Mail-Absender fälschen | 26 |
| E-Mailrelay installieren | 103 |
| E-Mails verschlüsseln | 225 |
| E-Mails z. int. Mailserver weiterleiten..... | 103 |
| E-Mails-Anhang verschlüsseln..... | 226 |
| Embedded Linux..... | 220 |
| encrypt_password..... | 569, 573 |
| Enigmail | 226 |
| Enterprise Security Manager..... | 198 |
| Epiphany (Webbrowser) | 190 |
| ESP | 512 |
| ESP, springen zu | 310 |
| Ethernet-Frames v. VLAN-Tags | 132 |
| Ettercap..... | 53, 238, 329 |
| Ettercap, allg. Optionen..... | 331 |
| Ettercap, Anzeigeeoptionen..... | 330 |
| Ettercap, Aufruf..... | 329 |
| Ettercap, Log-Optionen..... | 330 |
| Ettercap, Sniffing-/Angriffsoptionen..... | 330 |
| Ettercap, User-Interface-Typ..... | 330 |
| Exchange E-Mailserver einrichten..... | 160 |
| Exchange VSAPI 2.5..... | 160 |
| Exchange, Domänensicherheit..... | 162 |
| Exchange, E-Mail-Anhänge blockieren..... | 161 |
| Exploit | 36, 109, 239, 382, 596 |
| Exploit in Metasploit integrieren..... | 256 |
| Exploit testen..... | 256 |
| Exploit, Angriffsstring..... | 308 |
| Exploit-Techniken..... | 296 |
| Externe Netzwerkanbindung, Angriff auf..... | 30 |

F

| | |
|---|----------|
| F.I.R.E.-CD | 475 |
| Fake..... | 596 |
| Fake-Authentication-Angriff..... | 333 |
| Fallen aufstellen..... | 114 |
| Fault Injection..... | 536 |
| Fehlerbeh. in try/catch-Blöcken..... | 538 |
| Fernsteuerung | 28 |
| Festplatte verschlüsseln | 224 |
| file | 449 |
| File Inclusion..... | 148, 338 |
| find-Payloads | 323 |
| FIN-Flag..... | 30 |
| FinTS | 233 |
| Firefox, Sicherheitseinstellungen | 186 |
| Firefox-Addons | 187 |
| FireHol | 147 |
| Firewall..... | 596 |
| Firewall überwinden | 35 |
| Firewall umgehen..... | 28 |
| Firewall, Änderungen überwachen..... | 108 |
| Firewall, Kriterien..... | 177 |
| Firewall, Leak-Tests..... | 176 |
| Firewall, Ports öffnen | 107 |
| Firewall-Auswahl..... | 176 |
| Firewall-Konfiguration prüfen..... | 458 |
| Firewallregel, Aufbau | 107 |
| Firewallregeln ermitteln | 317 |
| Firewall-Regeln konfigurieren..... | 106 |
| Firewallsysteme..... | 494 |
| Flash blockieren..... | 189 |
| Flash, Schadsoftware in | 180 |
| Flash-Objekte, manipulierte..... | 179 |
| flawfinder..... | 536 |
| FLIRT-Tools..... | 518 |

| | |
|---|----------|
| Flock (Webbrowser) | 190 |
| Flüchtige Daten sichern | 475 |
| Flüchtige Daten sichern (Windows) | 476 |
| Flüchtige Daten sichern, Linux..... | 476 |
| Foremost..... | 448 |
| Forensic Analysis ToolKit, The..... | 476 |
| Forensische Analyse..... | 471 |
| Forensische Programme (Linux) | 477 |
| Forensische Programme (Windows)..... | 478 |
| Formatstring-Fehler | 538 |
| Formatstring-Overflow | 288 |
| FreeRadius | 139 |
| FreeRADIUS-WPE-Patch | 50 |
| Frox..... | 104 |
| FTP-Proxy installieren..... | 104 |
| FTP-Server..... | 104 |
| FTP-Verbindungen, Rückkanal..... | 104 |
| Funknetz..... | 137 |
| Fuzzer | 246, 536 |
| Fuzzing..... | 243 |

G

| | |
|---|----------|
| Galeon (Webbrowser) | 190 |
| Gateway | 596 |
| Gateway-Zugang von außen | 73 |
| gen_ethers.pl..... | 122 |
| Genehmigte Verbindungen, Angriffe über..... | 109 |
| Geräte sicherstellen | 482 |
| GET | 540 |
| gets..... | 537 |
| getwd..... | 537 |
| Glibc 2.3.x, Schwachstelle | 282 |
| Gnupg4Win..... | 225 |
| GnuPG-basierte Verschlüsselung mit Thunderbird..... | 225 |
| Google Chrome (Webbrowser)..... | 183, 194 |
| Google Hacking..... | 68 |
| Google, Datensammler | 183 |
| Google.com | 68 |
| Googledorks..... | 68 |
| Google-Suche..... | 346 |
| Grub, Passwort | 32 |
| Grundschutz-Handbuch | 90 |
| Gruppenrechte finden | 375 |
| Gruppenrichtlinien-Editor | 169 |

H

| | |
|--|---------|
| Hacker..... | 596 |
| Hackerparagraph..... | 314 |
| Handshake angreifen | 334 |
| Handshake erzwingen | 334 |
| Hardware.Firewall | 97 |
| Hardwareausfall | 22 |
| Hash | 95, 596 |
| Hauptspeicher..... | 511 |
| Hauptspeicher auslesen (Windows)..... | 479 |
| Hauptspeicheranalyse (Linux) | 476 |
| HBCI..... | 233 |
| Heap Buffer-Overflow | 274 |
| Heap, reservierte Speicherstellen | 276 |
| Heap-Speicherverwaltung..... | 276 |
| Heap-Verwaltung..... | 241 |
| Helios Lite..... | 457 |
| HIEW | 524 |
| Hintergrundübertragungsdienst von Microsoft..... | 36 |
| Höhere Rechte erlangen..... | 36, 170 |

| | |
|-------------------------------------|---------|
| Homepage manipulieren..... | 406 |
| Honeyd installieren..... | 115 |
| Honeyd, Alarmskript..... | 116 |
| Honeyd-Netzwerk..... | 414 |
| Honeyd-Ports..... | 114 |
| Hook in System..... | 456 |
| Hostfestplatte, Zugriff auf..... | 212 |
| Hping2..... | 316 |
| HTML-E-Mails..... | 197 |
| HTTP/FTP-Proxy..... | 99 |
| HTTP-Datenverkehr untersuchen..... | 404 |
| HTTP-Proxy..... | 102 |
| HTTPs..... | 201 |
| HTTPs-Verbindungen analysieren..... | 29 |
| HTTP-Tunnel..... | 99 |
| Hydra..... | 62, 327 |
| Hydra, Parameter..... | 328 |

I

| | |
|--|-------------------|
| I/O-Funktionen, gepufferte..... | 535 |
| Icesword..... | 457 |
| IDA..... | 239, 414 |
| IDA, Bibliotheken einbinden..... | 518 |
| IDA, Darstellungshilfen..... | 515 |
| idaPatcher..... | 522 |
| Identität vortauschen..... | 121 |
| Idle-Scan..... | 316 |
| IFS..... | 534 |
| IIS absichern..... | 158 |
| IIS, Logging einstellen..... | 159 |
| IIS, Remote-Zugang anlegen..... | 158 |
| IISLockdown..... | 158 |
| Image anlegen..... | 445 |
| Image untersuchen..... | 446 |
| Image-Dateien, VM erzeugen aus..... | 449 |
| Image-Erstellung..... | 444 |
| Infektion verbergen..... | 26 |
| Informationsbeschaffung..... | 345 |
| Informationsdiebstahl..... | 23 |
| Instruction-Tracing..... | 520 |
| Integer, Vorzeichenfehler..... | 285 |
| Integer, Wertabschnitts-Fehler..... | 283, 286 |
| Integer, Wertebereichprüfung..... | 282 |
| Integer-Overflow..... | 282, 283, 535 |
| Integer-Typen..... | 283 |
| Integrität..... | 108, 217, 461 |
| Integrität konfigurieren..... | 171 |
| Integrität..... | 18, 95, 597 |
| Internet Explorer erweitern..... | 231 |
| Internet Explorer, Sicherheitseinstellungen..... | 183 |
| Internet, Aufbau des..... | 79 |
| Internetanwendungen kapern..... | 71 |
| intitle-Modifikator..... | 68 |
| Intranet vom Internet abtrennen..... | 101 |
| Intrusion-Detection-System (IDS)..... | 97, 109, 497, 597 |
| Intrusion-Detection-System, Logserver..... | 109 |
| Intrusion Detection Systeme umgehen..... | 323 |
| IP-Adresse..... | 29 |
| IP-Adressen eines Ziels finden..... | 351 |
| IP-Adressen, Verwaltung..... | 79 |
| IP-Bekanntmachung versenden..... | 80 |
| IP-Bereich kidnappen..... | 80 |
| iPhone..... | 221 |
| iPhone, Jailbreak..... | 222 |
| iPhone, root-Rechte..... | 222 |
| IP-Tables..... | 49, 177 |

| | |
|--------------------------------|-----|
| IP-Tables-Frontend..... | 147 |
| IP-Telefon am PC-Anschluß..... | 77 |
| IP-Telefon angreifen..... | 77 |
| iTAN..... | 231 |
| iTAN/BEN..... | 232 |
| iTANplus..... | 232 |
| iTunes..... | 221 |

J

| | |
|-------------------------------------|---------------|
| Java..... | 182, 537, 538 |
| Java blockieren..... | 189 |
| JavaScript selektiv aktivieren..... | 187 |
| JavaScript, Rekursion..... | 181 |
| JavaScript, Routinen..... | 180 |
| JavaScript, Sandbox-Prinzip..... | 180 |
| Java-Session anzeigen..... | 400 |
| John the Ripper..... | 325 |

K

| | |
|--|------------|
| Karmetasplit..... | 44 |
| Keepass..... | 202 |
| Kerberos API Spy..... | 521 |
| Kernelfirewall e. Linux-Systems..... | 49 |
| Kernel-Firewall, Linux..... | 177 |
| Kernelspeicher sichern (Linux)..... | 476 |
| Keylogger..... | 25, 27, 36 |
| Klon-Angriffe..... | 539 |
| K-Meleon (Webbrowser)..... | 190 |
| Kodierung..... | 499 |
| Kollisionspasswörter..... | 433 |
| Kommunikation kontrollieren..... | 53 |
| Kommunikation verschlüsseln..... | 201 |
| Konfigurationsfehler finden..... | 361 |
| Konqueror, Sicherheitseinstellungen..... | 195 |
| Kryptoanalyse..... | 420 |
| Kryptographische Algorithmen, private..... | 498 |

L

| | |
|---|-----|
| Längenprüfung..... | 536 |
| Laufende Prozesse überprüfen (Linux)..... | 464 |
| Laufwerk, Autostart deaktivieren..... | 203 |
| Laufzeitanalyse..... | 519 |
| Laufzeitverhalten e. Prog. überwachen..... | 460 |
| LD_LIBRARY_PATH..... | 534 |
| LD_PRELOAD..... | 534 |
| Link umbiegen..... | 75 |
| Linux, Firewall..... | 177 |
| Linux-Firewall, anwendungsgesteuert..... | 177 |
| Linux-Kernel, verwundbare..... | 392 |
| Live View..... | 449 |
| Live-Systemanalyse (Linux)..... | 461 |
| Live-Systemanalyse (Windows)..... | 455 |
| Localhost, Kontrolle des Datenverkehrs auf..... | 210 |
| Logdateien prüfen (Linux)..... | 467 |
| Login angreifen..... | 400 |
| Logserver..... | 109 |
| Logserver, zentraler..... | 123 |
| Lokale Variablen, Größe..... | 517 |
| Lokaler Nutzer mit root-Rechten..... | 588 |

M

| | |
|-------------------------------|-----|
| MAC-Adresse anzeigen..... | 333 |
| MAC-Adresse manipulieren..... | 137 |

| | |
|---|-------------|
| MAC-Adresse, Filter für | 136 |
| Macchanger..... | 137 |
| Macintosh, Firewall..... | 177 |
| macof..... | 135 |
| Magicscrescue..... | 448 |
| Mailrelay-Dienst..... | 103 |
| malloc..... | 241 |
| Malware | 597 |
| Malware entwickeln..... | 36 |
| Man in the Middle | 121 |
| Man-in-the-Middle-Angriff..... | 53, 79, 238 |
| Mausklicks abfangen..... | 75 |
| MDB-Dateien | 73 |
| Metasploit Framework | 323 |
| Metasploit Framework, Payload | 323 |
| Metasploit-Konsole aufrufen | 324 |
| Meterpreter..... | 323 |
| Meterpreter Payload | 50 |
| Microsoft RemvalTool..... | 457 |
| Milw0rm | 386 |
| MIME-Typen..... | 161 |
| mlock..... | 535 |
| MMS, Sicherheitslücke | 38 |
| Mobile Endgeräte | 37 |
| Mobile Endgeräte, Kaufberatung..... | 218 |
| Mobiltelefon, Schadcode als Bild tarnen | 38 |
| Mobiltelefon-Wurm | 38 |
| MS Access, Sicherheitslücke..... | 73 |
| MSFGui..... | 323 |
| msfpayload | 254 |
| mTAN | 232 |
| MTU-Wert ändern..... | 46 |
| MX-Record..... | 597 |
| MySQL-Abfrage..... | 65 |

N

| | |
|---|----------|
| Nagios installieren..... | 127 |
| Nagios, Plugins | 127 |
| nano..... | 391 |
| Nessus..... | 315 |
| Netzverkehr erhöhen | 333 |
| Netzwerk in Segmente unterteilen..... | 129 |
| Netzwerk in Umgebung bekanntmachen | 136 |
| Netzwerkadapter zum Intranet..... | 102 |
| Netzwerkbrücke einrichten (Linux) | 92 |
| Netzwerkbrücke einrichten (Windows) | 91 |
| Netzwerkoperationen suchen..... | 452 |
| Netzwerkoperationen, Funktionsnamen..... | 452 |
| Netzwerksicherheit..... | 95 |
| Netzwerksniffer..... | 77, 329 |
| Netzwerksniffer für Windows..... | 332 |
| Netzwerküberwachungstool..... | 452 |
| Netzwerkverfügbarkeit überwachen..... | 127 |
| Netzwerkverkehr filtern..... | 333 |
| Netzwerkverkehr überwachen..... | 110 |
| Netzwerkverkehr untersuchen | 97 |
| Netzwerkzugriff steuern | 95 |
| new..... | 241 |
| NFS-Freigaben suchen..... | 57 |
| NFS-Server, Sicherheitslücke | 57 |
| Nikto..... | 63, 335 |
| Nikto, Parameter | 336, 337 |
| Nmap..... | 316 |
| Nmap Portangabe und Scanreihenfolge | 319 |
| Nmap, aggressiver Scan | 322 |
| Nmap, aktive Hosts prüfen..... | 322 |

| | |
|--|-----|
| Nmap, Aufrufparameter | 316 |
| Nmap, Ausgabe | 321 |
| Nmap, Betriebssystemerkennung | 319 |
| Nmap, Firewall-/IDS-Evasion | 320 |
| Nmap, Host-Discovery | 318 |
| Nmap, ohne ping prüfen..... | 322 |
| Nmap, Scantechniken..... | 318 |
| Nmap, Scriptscan | 319 |
| Nmap, Service-/Versionserkennung | 319 |
| Nmap, Spoofing..... | 320 |
| Nmap, Timing-Schalter | 352 |
| Nmap, Zielangaben..... | 318 |
| Non-executeable Stackschutz | 296 |
| NoScript..... | 187 |
| Notfallrichtlinien..... | 23 |
| Notfallvorsorgerichtlinie..... | 89 |
| nlookup | 469 |
| NTFS, Sicherheitslücke..... | 35 |

O

| | |
|---|---------|
| Obfuscator..... | 182 |
| Off-by-One Buffer-Overflow..... | 259 |
| Öffentliche Server angreifen | 62 |
| Oinkmaster..... | 111 |
| Oktett | 597 |
| One-Time-Pad, Sicherheit..... | 223 |
| Online-Banking..... | 229 |
| Opcodes..... | 251 |
| OpenPGP..... | 201 |
| Open-Source-Software | 597 |
| OpenSSL | 93, 174 |
| OpenSSL, Verschlüsselungsverfahren | 380 |
| OpenVPN | 91, 219 |
| OpenVPN, Bridging-Modus..... | 91 |
| OpenVPN, Routing-Modus | 91 |
| Opera, Sicherheitseinstellungen..... | 193 |
| Ophcrack | 52 |
| osCommanding-Plugins | 64 |
| OS-Detect Skript | 479 |
| Outlook 2000-2003, Sicherheitslücke | 34 |
| Outlook-Clients..... | 161 |
| Overflow, prüfen auf..... | 247 |

P

| | |
|--|-----|
| Package Scope | 539 |
| Packet-Injection | 45 |
| Pakete fremder WLANs mitlesen..... | 41 |
| Paketfilter zum Internet..... | 98 |
| Paketfilter zum Intranet..... | 98 |
| Paketfilter, Funktionsweise | 147 |
| paketweise Datenübertragung..... | 29 |
| Palm OS | 220 |
| Parent-Proxy | 103 |
| Partition mit nosuid mounten..... | 170 |
| Pascal-Konvention | 517 |
| Passphrase | 137 |
| passwd-Datei suchen | 70 |
| Passwort angreifen | 333 |
| Passwort ermitteln | 416 |
| Passwort wiederherstellen..... | 449 |
| Passwort wiederherstellen (Windows)..... | 332 |
| Passwort zurücksetzen..... | 449 |
| Passwort, falsches --> Systemzugang..... | 272 |
| Paßwort, Klartextübermittlung | 421 |
| Passwortänderungen suchen (Linux) | 466 |

| | |
|---|----------|
| Passwortaufbewahrung | 202 |
| Passwortdatei eines Webservers ausgeben | 65 |
| Passwortdatei, Zugriff auf | 394 |
| Passwortdateien | 325 |
| Passwörter | 202 |
| Passwörter sicher verwahren | 500 |
| Passwörter, verschlüsselte brechen | 332 |
| Passwort-Hash brechen | 55 |
| Passwortknacker | 325 |
| Passwortliste | 62 |
| Patchanalyse | 434 |
| Patchen | 521 |
| PATH | 534 |
| patternCreate | 249 |
| Payload | 250 |
| Payload erzeugen | 254 |
| PDA, Betriebssystem | 218 |
| PDA's | 37, 218 |
| PDF-Lesesoftware, Sicherheitslücke | 33 |
| Pe_Scripts | 516 |
| Penetration Testing | 314 |
| Penetrationstest | 597 |
| Penetration-Testsystem aufsetzen | 340 |
| PGP | 201 |
| Pharming | 25 |
| Phishing | 25 |
| Phishing-Angriff | 75 |
| PHP | 148, 540 |
| PHP patchen | 148 |
| PHP, Datenbankzugriffe | 544 |
| PHP, Datenübermittlung | 540 |
| PHP, Variablen-Verarbeitung | 540 |
| PHP-Funktionen, Ausführung unterbinden | 148 |
| PHPMyAdmin patchen | 156 |
| PHP-Optionen, unsichere | 150 |
| PHP-Seiten ohne Passwortschutz | 70 |
| PHP-Shell | 148 |
| PHP-Shell, eigene plazieren | 358 |
| PHPSyslog-NG | 125 |
| ping | 316 |
| Ping-Sweep | 351 |
| PIN-TAN-Verfahren | 231 |
| Pipes | 535 |
| PLC-Flag | 30 |
| PLScsi | 223 |
| Poison Null-Byte | 538 |
| Polymorphe Programme suchen | 459 |
| Poolfinder | 479 |
| pop | 512 |
| Popunder, Anzeige von | 182 |
| Popup, Anzeige von | 182 |
| Popup-Blocker | 183 |
| Port 8080 | 102 |
| Port-Anfragen weiterleiten | 105 |
| Ports prüfen | 353 |
| Ports, offene anzeigen | 455 |
| Portscan | 461 |
| Portscanner | 57 |
| POST | 540 |
| Post-Mortem-Analyse | 471, 479 |
| POST-Parameter | 405 |
| Prepared Statements | 544 |
| Pre-Shared Key | 40, 92 |
| printf-Aufrufe | 418 |
| printf-Familie | 538 |
| printf-Funktionen | 288 |
| Private VLAN | 133 |
| Privilegierte User finden | 375 |

| | |
|---|----------|
| Procedure Linkage Table | 302 |
| Process Dumper | 476 |
| Process Explorer | 452, 521 |
| Process Monitor | 452 |
| Programmablauf manipulieren | 302 |
| Programmdatei wiederherstellen | 476 |
| Programme, unbekannte isolieren | 451 |
| Programmfehler finden | 239 |
| Programmieren, sicheres | 531 |
| Programmumgebung | 533 |
| Programmverhalten-Monitor | 452 |
| Protokollanalysen | 98 |
| Protokolle, verschlüsselte | 147 |
| Proxy, Firewallserver hat Zugriff auf | 103 |
| Proxy, nicht-transparenter | 104 |
| Proxy-Einstellungen d. IE ermitteln | 559 |
| Proxy-Firewall | 29 |
| Proxyserver | 99 |
| Prozeßmonitor | 521 |
| Prozeßspeicher | 241 |
| Prozeßspeicher beobachten | 452 |
| PSH Toolkit | 52 |
| PSK | 40 |
| Ptfinder | 479 |
| Puffer | 241 |
| Pufferadresse ermitteln | 262 |
| Pufferinhalt, Disassemblat | 575 |
| push | 512 |
| pw-inspector | 334 |

Q

| | |
|---|-----|
| Qemu-img | 450 |
| Qualitätsprüfungen | 535 |
| Quelltext e. Programms rekonstruieren | 413 |

R

| | |
|--------------------------------|--------------------|
| Race-Conditions | 532 |
| RADIUS-Server | 44, 139 |
| RADIUS-Server einrichten | 140 |
| RAID-System | 23 |
| Rainbow-Tabellen | 52, 332 |
| Ransomware | 26 |
| ratle | 547 |
| RATS | 536 |
| Redundante Server | 228 |
| Regelsatz für Firewall | 98 |
| Register, flüchtige | 514 |
| Registryzugriffe | 453 |
| Remote Shell | 36 |
| Ressourcen überwachen | 127 |
| ret2eax | 311 |
| ret2esp | 310 |
| ret2Pop | 310 |
| ret2ret | 309 |
| Return-into-lib(c) | 296, 297 |
| Return-into-PLT | 296, 302 |
| Reverse Engineering | 240, 413, 507, 536 |
| Reverse Payloads | 323 |
| Reverse-DNS-Anfragen | 351 |
| Risikoeinschätzung | 22 |
| rkHunter | 463 |
| Root-Exploit | 36 |
| Rootkit | 26, 35 |
| Rootkit installiert? | 455 |
| Rootkit Revealer | 457 |

| | |
|---|----------|
| Rootkit Unhooker | 455 |
| Rootkits suchen | 455, 463 |
| root-Passwort | 370 |
| root-Passwort finden | 379 |
| root-Passwort setzen | 343 |
| root-Rechte auf Server erhalten | 383 |
| root-Shell öffnen | 368 |
| Rootshell, booten in | 51 |
| Rootshell, starten mit | 32 |
| Router mit Anbindung an RADIUS-Server | 139 |
| Router-Sicherungsmaßnahmen | 40 |
| Routing im Internet, Sicherheitslücke | 80 |
| RPM, Datenintegrität prüfen mit | 462 |
| RST-Flag | 30 |
| Rsync | 227 |

S

| | |
|--|---------|
| Safari, Sicherheitseinstellungen | 194 |
| SAM-/Systemdatei untersuchen (Win) | 449 |
| Samba-Freigaben suchen | 384 |
| Sandbox | 538 |
| SAP-Modell | 471 |
| scanf | 537 |
| Schadcode | 492 |
| Schadsoftware | 597 |
| Schlüssel | 222 |
| Schlüsselaustausch | 491 |
| Schützenswerte Güter | 18 |
| Schwachstellen, untersuchen auf | 59 |
| Schwachstellenerkennung | 237 |
| Schwachstellenscanner | 315 |
| Schwachstellentest, automatischer | 315 |
| Seamoney, Sicherheitseinstellungen | 190 |
| Secure Shell | 173 |
| Security Policy | 598 |
| Segmentation Fault | 300 |
| Sender Policy Framework | 60, 598 |
| Separator für Shell-Argumente | 534 |
| Server einer Domain finden | 62 |
| Server entfernt steuern | 173 |
| Server härten | 147 |
| Server in Domänen finden | 345 |
| Server in Netzblöcken finden | 351 |
| Server mit Inter- u. Intranetzugang | 98 |
| Server Side Includes manipulieren | 406 |
| Server übernehmen | 382 |
| Server, interner, Angriff von | 31 |
| Server, Vollzugriff auf | 32 |
| Server-Attrappe | 115 |
| Serverdienste | 147 |
| Serverintegrität überwachen | 170 |
| Serversicherheit | 147 |
| Server-Zertifikat anlegen | 142 |
| Serverzugriffe, unsichere erkennen | 237 |
| Session-Verschlüsselung | 148 |
| setuserid | 170 |
| shadow-Datei suchen | 70 |
| Shared Folders | 210 |
| Shared Library, Pfad zu | 534 |
| Shell öffnen | 303 |
| Shellcode disassemblieren | 524 |
| Shellcode-Zeiger ändern | 310 |
| Shellzugriff über Netzwerk | 560 |
| Sicherheit des eig. Systems bewerten | 37 |
| Sicherheitsanalyse | 315 |
| Sicherheitsanalyse, Methodik | 345 |

| | |
|--|------------------------|
| Sicherheitsleitlinie, Aufbau | 85 |
| Sicherheitsleitlinie, Verantwortliche | 485 |
| Sicherheitslücke, unbekannt | 31 |
| Sicherheitslücken, Listen mit | 29 |
| Sicherheitsupdates autom. einspielen | 148, 162 |
| Sicherheitsupdates, fehlerhafte finden | 434 |
| Sicherheitsupdates, Linux | 162 |
| Sicherheitsupdates, Windows | 162 |
| Sicherheitsupdates, Windows-Server | 163 |
| sigmake | 518 |
| signaturbasiert | 34 |
| Signaturdateien | 519 |
| Signaturerkennung | 493 |
| Kript-Kiddie | 20 |
| Sleuth Kit | 445 |
| Smart TAN | 232 |
| SMB-Protokoll angreifen | 332 |
| Snort | 97, 109 |
| Snort installieren | 110 |
| Snort, Funktionsweise | 110 |
| Snort-Rules aktualisieren | 111 |
| Social Engineering | 59 |
| Sophos | 199 |
| Sourcecode-Audit | 535 |
| Space-Sled | 304 |
| Spam | 26 |
| Spanning Tree Protocol manipulieren | 136 |
| Spear-Phishing | 25 |
| Speicher analysieren (Win) | 479 |
| Speicheradresse, Label | 512 |
| Speicheraufbau | 241 |
| Speicherbereich gezielt löschen | 535 |
| Speicherbereich, Code unterschieben | 243 |
| Speicherbereiche überschreiben | 536 |
| Speicherbereinigung | 539 |
| Speicherplatz reservieren | 512 |
| Speicherüberlauf | 241 |
| Speicherüberlauf ausnutzen | 244 |
| Speicherverwaltung | 241, 537 |
| Spiegelbild v. Daten anlegen | 444 |
| Spionagesoftware | 39 |
| Spoofing | 26 |
| sprintf | 537 |
| Spuren analysieren | 472 |
| Spuren sichern | 471 |
| Spyware | 27 |
| SQL, Hochkomma | 65 |
| SQL-Anweisung | 396 |
| SQL-Anweisung manipulieren | 65 |
| SQL-Injection | 64, 148, 338, 395, 544 |
| Sqlsyslogd | 125 |
| SQL-Truncation | 66 |
| Squid konfigurieren | 102 |
| Squid, Zugriffsbeschränkungen | 103 |
| SSH | 216 |
| SSH einrichten | 227 |
| SSH, root-Login unterbinden | 174 |
| SSH, Userauthentifizierung mit Schlüssel | 173 |
| SSH1-Verbindungen aufbrechen | 329 |
| SSH1-Verschlüsselung aushebeln | 53 |
| SSH2 | 237 |
| SSH2 einschalten | 173 |
| SSH2-Verbindungen -> SSH1 | 53 |
| SSH-Exploit | 389 |
| SSH-Keys, Schwachstelle | 586 |
| SSID unterdrücken | 136 |
| Stack Buffer-Overflow | 242 |
| Stack Juggling | 297, 309 |

| | |
|---|----------|
| Stack, ob. Element | 512 |
| Stack, Werte auslesen von | 289 |
| Stack, Zugriff auf | 512 |
| Stackbereinigung | 517 |
| Stackpointer | 512 |
| Stack-Segment | 241 |
| Stackspeicher, nicht ausführbar | 296 |
| Stackspeichergöße | 517 |
| Stak, nicht ausführbaren umgehen | 297 |
| Stammzertifizierungsstelle | 145 |
| Standardprogramme, Schwachstellen | 72 |
| Standardsoftware, Lücken in | 201 |
| Standardsoftware, Sicherheitslücken | 38 |
| Standleitung sichern | 97 |
| Starkes Passwort | 202 |
| Start-of-Authority-Informationen abfragen | 469 |
| Steuerzeichen in Benutzereingabe | 289 |
| strcat | 537 |
| strcpy | 311, 537 |
| Stringanalyse | 459 |
| strncpy-Aufruf | 435 |
| Stunnel | 93, 219 |
| Stunnel, Dienst anbieten | 93 |
| Suchmaschine | 68 |
| sudo | 368 |
| Suhosin | 148 |
| SUID-Angriffe | 170 |
| SUID-Bit suchen | 171 |
| SUID-Programme auflisten | 171 |
| SUSEFirewall2 | 147 |
| Switch, Angriff auf | 135 |
| Switch, VLAN-geeignet | 129 |
| Symbian OS | 219 |
| Synchronisation verteilter Datenbanken | 533 |
| SYN-Flag | 30 |
| SYN-Flag setzen | 316 |
| SYN-Portscan | 364 |
| Syslog-NG installieren | 123 |
| Syslog-NG, Datenbank | 125 |
| Syslog-NG, GUI f. DB-Zugriff | 125 |
| System kompromittieren | 28 |
| System-/Anwendungserkennung | 363 |
| system-Adresse finden | 299 |
| Systemanalyse | 444 |
| Systemänderungen suchen | 461 |
| Systembefehle ausführbar? | 355 |
| Systemdatei ersetzen | 555 |
| Systemdateien, Zeitstempel | 475 |
| Systeme identifizieren | 351 |
| system-Funktion | 298 |
| Systemfunktionen, umgeleitete suchen | 457 |
| Systemkonfigurationsdateien ändern | 368 |
| Systemmeldungen zentral sammeln | 123 |
| Systemplatte verschlüsseln | 224 |
| System-Shutdown | 484 |
| Systemspeicher sichern (Linux) | 476 |
| Systemzeit | 472 |

T

| | |
|-------------------------------------|-----|
| Tamper Data | 402 |
| Täter-Identifikation | 468 |
| TCP/IP | 29 |
| TCP-Flags | 30 |
| TCP-Proxy | 105 |
| Telefongespräche mitschneiden | 76 |
| TELNETs-Verbindung mitlesen | 237 |

| | |
|--|----------|
| Terminalzugriff auf Server | 173 |
| Text auf Bildschirm schreiben | 288 |
| Text-Segment | 241 |
| Threads zur Laufzeit e. Windows | 479 |
| Thunderbird | 225 |
| Tool | 598 |
| Traceroute | 82 |
| Tracing Register Flag | 523 |
| Tragbare Computer | 37 |
| Transparentes Routing | 49 |
| Tresor als zusätzliches Laufwerk | 202 |
| Tresor, digitaler | 202 |
| Trigger | 397 |
| Trinity Rescue Kit | 449 |
| Trojaner | 27 |
| Truecrypt | 202, 224 |
| Trunking-Ports, Angriff auf | 135 |
| TrustedCA.pem | 145 |
| Tshark | 77 |
| TTL-Wert v. Paketen manipulieren | 82 |
| Tunnel finden | 28 |
| Tunnel für Netzwerkanfragen | 91 |
| Twofish, Sicherheit | 223 |
| Typüberprüfung | 538 |

U

| | |
|---|-----|
| Überfluten mit MAC-Adressen | 135 |
| Umgebungsvariablen | 533 |
| Untersuchungsumgebung sicherstellen | 475 |
| URL manipulieren | 402 |
| URLScan | 158 |
| USB-Stick mit Fingerabdruck-Identifikation, Sicherheitslücke | 223 |
| USB-Sticks | 203 |
| User-/Systeminformationen ausgeben | 367 |

V

| | |
|---|----------|
| Verbindungen verfolgen | 329 |
| Verbindungen, aktive in passive konv. | 104 |
| Verbindungsdaten auflisten | 454 |
| Verbindungswege zw. Netzen autonom. Systeme | 79 |
| Verfügbarkeit von Daten | 18 |
| Verfügbarkeitsausfall | 23 |
| Vergleichsdatenbank zu System | 171 |
| Verschleierung | 502 |
| Verschlüsselte Verbindung zu bes. Dienst | 93 |
| Verschlüsselte Verbindung zw. entf. Geräten | 91 |
| Verschlüsselte Verbindungen prüfen | 98 |
| Verschlüsselung | 222, 499 |
| Verschlüsselung, asymmetr. Verfahren | 222 |
| Verschlüsselung, symmetr. Verfahren | 222 |
| Verschlüsselungsalgorithmus für WLANs | 40 |
| Verschlüsselungsroutine brechen | 578 |
| Verschlüsselungsverfahren, sicherstes | 223 |
| Versteckte Dateien suchen | 457 |
| Versteckte Prozesse suchen | 465 |
| Versteckte Prozesse suchen (Linux) | 463 |
| Vertraulichkeit | 95 |
| Verzeichnisse mit auszuführenden Prog. | 534 |
| vi, Befehlssatz | 96 |
| Viren | 27 |
| Viren, Mobiltelefone | 27 |
| Virenprüfung | 98 |
| VirtualBox-Images suchen | 450 |
| Virtualisierer, Produktüberblick | 206 |

| | |
|---|---------|
| Virtual-PC-Images suchen | 450 |
| Virtuelle Datenkopie | 23 |
| Virtuelle LANs | 129 |
| Virtuelle Maschine (siehe auch unter VM) | 205 |
| Virtuelle Umgeb./Masch., Gefahren | 209 |
| Virtuelles lokales Netz | 76 |
| Virtuelles privates Netzwerk (siehe auch bei VPN) | 91 |
| Virus, Wirt des | 27 |
| VLAN-Angriffe | 134 |
| VLANs mit Tagging | 130 |
| VM, Ausbruch aus | 210 |
| VM, Denial of Service | 213 |
| VMs finden | 449 |
| VMs konvertieren | 450 |
| VMs, Administrationszugang | 216 |
| VMs, Backdoor-Interface | 211 |
| VMs, BIOS | 217 |
| VMs, Bootvorgang | 217 |
| VMs, Datensicherungen | 218 |
| VMs, Datenverkehr and. VM einsehen | 213 |
| VMs, File Sharing | 215 |
| VMs, gemeinsame Zwischenablage | 209 |
| VMs, Host-Angriff | 210 |
| VMs, Möglichkeiten des Host | 213 |
| VMs, Patch-Management | 216 |
| VMs, Shared Folders | 210 |
| VMs, Tastatureingaben mitschneiden | 210 |
| VMs, Zeitabgleich | 215 |
| VMs, zentraler Logserver | 217 |
| VMs, Zugriff auf phys. Host-Laufwerke | 216 |
| VM-Server, Hintergrunddienste | 215 |
| VM-Server, Netzwerkebene | 214 |
| VM-Server, Remote-Zugang | 215 |
| VM-Server, Schutzmaßnahmen | 214 |
| VMware Converter | 450 |
| VMware, Backdoor-Befehle | 212 |
| VMware, Backdoor-Interface ansprechen | 211 |
| VMware, virtuelles BIOS | 140 |
| VMware-Format, Image konvertieren in | 450 |
| VMware-Images suchen | 449 |
| VNC (Virtual Network Computing) | 216 |
| VNC-Verbindungen mitlesen | 329 |
| Voice-VLAN | 76 |
| voiphopper | 78 |
| Vorzeichenfehler | 284 |
| VPN (Virtual Private Network) | 91, 598 |

W

| | |
|--|----------|
| W3AF | 338, 359 |
| W3af Framework | 63 |
| Wardriving | 136 |
| Web 2.0 | 179, 182 |
| Web Application Attack and Audit Framework | 338 |
| Web of Trust | 189 |
| Webanwendungen prüfen | 338 |
| Webanwendungen untersuchen | 395 |
| Webbrowser-Sicherheit | 179 |
| Webgoat | 395 |
| Webinhalte, aktive | 182 |
| Webmin-Exploit | 386, 584 |
| Webseite, Aussehen manipulieren | 407 |
| Webseite, Liste vertrauenswürdiger | 189 |
| Webseite, umleiten auf gefälschte Kopie | 25 |
| Websites, Prüfdatenbank | 189 |
| Websitesbesucher-Identifikation | 183 |
| Websites-Zugriff mit HTTP-Proxy | 102 |

| | |
|---|----------|
| Webserver auf Schwachstellen prüfen | 63 |
| Webserver härten | 148 |
| Webserver scannen | 335 |
| Webserver, Passwortdaten-Abfrage | 65 |
| Webservices | 40 |
| WEP | 40 |
| WEP-/WPA-Key auslesen | 50 |
| WEP-Cracking | 333 |
| WEP-ges. Netzwerk aufbrechen | 333 |
| WEP-Verschlüsselung brechen | 137 |
| Werblocker | 183 |
| Werbe-Popup | 24 |
| Werbung blockieren | 189 |
| Werbung einblenden | 24 |
| Whois-Abfragen | 345 |
| WHOIS-Datenbanken | 470 |
| Windows Mobile | 221 |
| Windows, Dateien mit Passwörtern auslesen | 51 |
| Windows, Domain-Accounts wiederherstellen | 52 |
| Windows, lok. Benutzerdat. wiederherstellen | 52 |
| Windows, Verbindungsdaten mitlesen | 54 |
| Windows, verschlüsselte Passwörter anzeigen | 52 |
| Windows-Client fernsteuern | 32 |
| Wireless Distribution System | 137 |
| Wireshark | 452, 460 |
| Wirtschaftsspionage | 18 |
| WLAN-Angriffe | 136 |
| WLAN-Karte, Monitormodus | 45 |
| WLAN-Reichweite erhöhen | 137 |
| WLAN-Router | 40 |
| WordPress 2.6.1, Schwachstelle | 66 |
| Wortliste | 43, 62 |
| Wortlisten generieren | 325 |
| WOT | 189 |
| WPA | 40 |
| WPA/WPA2-Verschlüsselung mit Pre-Shared Key | 137 |
| WPA-Cracking | 333 |
| WPA-Enterpr. gesch. Netz, Zugangsdaten | 50 |
| WPA-Enterprise-Verschlüsselung einrichten | 139 |
| WPA-PSK | 40 |
| WSUS, Verwaltungskonsole | 166 |
| WSUS-Dienst | 163 |
| Würmer | 28 |

X

| | |
|-------------------------|--------------|
| Xen-Images suchen | 450 |
| XHydra | 327 |
| Xprobe2 | 352 |
| XSS | 67, 180, 338 |

Z

| | |
|---------------------------------------|----------|
| Zeichenfolge erzeugen | 249 |
| Zeichenfolgen formtirt ausgeben | 288 |
| Zenmap | 323 |
| Zertifikat | 598 |
| Zertifikate f. Benutzerprüfung | 92 |
| Zertifikate, signierte | 147 |
| Zertifikate-Datei | 145 |
| Zertifizierungsstelle | 174, 598 |
| Zielanwendung kapern | 566 |
| Ziele scannen | 351 |
| Zonealarm | 177 |
| Zugangsdaten zum Netz finden | 327 |
| Zugangskontrolle | 95 |
| Zugangsstelle | 598 |