



Computer & Literatur Verlag GmbH

DIE KUNST DES VERDECKENS

von Dr. Rolf Freitag

mit inhaltlichen Ergänzungen von
Jörg Braun, Rosa Riebl und Dr. Stefan Ritter

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 2011

© 2011 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 978-3-936546-65-1

INHALT

Vorwort	11
----------------------	-----------

Kapitel 1	
Diebstahlsicherung.....	15

1.1	Physikalische Zugangssicherung	16
1.1.1	Eingangsschlösser.....	17
1.1.2	Computersicherungen	18
1.1.3	Eingabeschutz.....	22
1.1.4	Biometrie.....	22
1.2	Paßwortschutz	24
1.2.1	Sichere Paßwörter.....	24
1.2.2	Unsichere Paßwörter.....	27
1.2.3	Paßwort-Speicherung.....	28
	Paßwort-Weitergabe.....	30
	Paßwort-Aufbewahrung	31
	Paßwort-Tresore	46
1.2.4	Laufendes System schützen	49
	Timeout	50
	Dienste und Schnittstellen: Firewire	53
	Computer ausschalten.....	54
1.3	Daten verschlüsseln.....	56
1.3.1	Risiken der Verschlüsselung.....	56
	Daten- und Paßwortverlust.....	56
	Rechtliche Probleme: Abstreitbarkeit.....	57
	Gefahren beim Einstieg	59
	Windows 64 und Gerätetreiber.....	63

1.3.2	Encrypting File System (EFS)	64
1.3.3	BitLocker	67
1.3.4	TrueCrypt	73
	TrueCrypt unter Windows	73
	TrueCrypt-Containerdateien	76
	TrueCrypt-Dateien	77
	Versteckte TrueCrypt-Container	84
	TrueCrypt-Partitionen und -Datenträger	90
	Vollverschlüsselung	94
	TrueCrypt unter Linux	100
1.3.5	Diskcryptor	106
	Laufwerks-Verschlüsselung	108
	CD-ISO-Dateien verschlüsseln	110
	Verschlüsseln des Systemlaufwerks	111
1.3.6	Linux-Standardverschlüsselung	112
	Loop-AES und Cryptoloop	112
	DM-Crypt und LUKS	113
1.3.7	FreeOTFE	124
1.4	Anti-Forensik	133
1.4.1	Aktive Bomben	133
1.4.2	Passive Bomben	134

Kapitel 2

Abhörsichere Kommunikation 137

2.1	Computernetzwerke.....	137
2.1.1	Kabelnetze	138
2.1.2	Funknetze (WLANs).....	139
	WPA unter Windows	142
	WPA unter Linux	145
2.2	Abhörsicher Telefonieren	146
2.2.1	Analoges Festnetz	147
2.2.2	Digitales Festnetz (ISDN)	147
2.2.3	DECT-Telefone	147
2.2.4	GSM.....	148
2.2.5	UMTS	149
2.2.6	IP-Telefonie	149

2.3	Verschlüsselte Serververbindungen	152
2.3.1	Internetserver.....	152
2.3.2	Suchmaschinen.....	157
	Scroogle	157
	Encrypted Google	158
2.3.3	Rechner-zu-Rechner-Verbindung	159
2.3.4	Virtual Private Networks	159
2.4	E-Mails verschlüsseln.....	159
2.4.1	Verschlüsseln mit GPG/PGP	160
2.4.2	Verschlüsseln in Thunderbird.....	165
2.4.3	Webmail verschlüsseln.....	170
	Mit GPG4win	171
	Dateien verschlüsseln mit Linux und KDE.....	175
	Dateien verschlüsseln auf der Kommandozeile	176
2.5	Abhörsicherer Chat mit OTR	183

Kapitel 3

Anonyme Kommunikation..... 191

3.1	Anonymer Netzwerkzugang.....	191
3.2	Anonym im Web	194
3.2.1	Tor	195
	Vidalia-Bundle unter Windows	196
	Tor und Linux/Unix.....	199
	Tor mit Browsern ohne Torbutton	207
	Das Vidalia-Kontroll-Panel.....	211
	Langzeittests.....	212
	Anonymer Onion-Server.....	213
3.2.2	Web-Proxies	214
3.2.3	Opera Turbo	216
3.2.4	Kommerzielle Anonymisierungsnetze	218
	ArmorSurf	218
	CyberGhost VPN	221
3.2.5	Geotargeting umgehen	222

3.3	Anonyme Tauschbörsen	224
3.3.1	Rechtliches.....	225
3.3.2	Technik.....	227
3.3.3	I2P (Invisible Internet Project).....	228
3.4	Anonymer Chat.....	234
3.5	Anonymes E-Mail	235
3.5.1	Anonymer E-Mail-Account.....	237
3.5.2	Webmail.....	238
3.5.3	Anonymer E-Mail-Versand	239
3.5.4	Anonymizer	240
3.5.5	Anonymer E-Mail-Empfang	240
3.6	Anonyme Identität	242
3.7	Anonyme Telefonie	244
3.7.1	Geheime Telefonnummer	244
3.7.2	Anonyme Mobiltelefonie	245
3.7.3	Rufnummernunterdrückung	246
3.7.4	Anonyme IP-Telefonie	248
3.7.5	Anonyme Faxübertragung.....	248

Kapitel 4

Spuren am PC

4.1	Spuren im Windows-System löschen.....	249
4.1.1	Die Auslagerungsdateien	251
4.1.2	Die Datei für den Schlafmodus.....	254
4.1.3	Temporäre Dateien	255
4.1.4	Überflüssige Programme und Daten	257
	Piriform CCleaner	258
	Wise Disk Cleaner Free und Wise Registry Cleaner.....	264
	Eraser	266
	Secure Eraser	266
	SecureWipeDelete	268
4.1.5	»Dokumente und Einstellungen« und »Benutzer«	268
4.1.6	Logdateien	269
4.2	Spuren im Linux-System löschen	269

4.3	Spuren im Benutzerkonto vermeiden	274
4.3.1	Doppeltes Benutzerverzeichnis unter Linux.....	278
4.3.2	Doppeltes Benutzerverzeichnis unter Windows.....	279
4.3.3	Benutzerdaten vollständig löschen.....	280
4.3.4	Vorzeigekonto	280
4.3.5	Vorzeigebetriebssystem.....	281
4.4	Spuren im Webbrowser löschen.....	281
4.4.1	Internet Explorer	284
4.4.2	Chrome.....	286
4.4.3	Opera	287
4.4.4	Mozilla Firefox	287
	History löschen.....	288
	Cookies löschen.....	290
	Privater Modus	291
	Browser-Addons.....	292
	AdBlock Plus.....	293
	Torbutton	296
	CS Lite	296
	Perspectives.....	298
	Ghostery	300
	Targeted Advertising Cookie Opt-Out (TACO)	301
	NoScript.....	302
4.4.5	Portable Webbrowser unter Windows.....	305
4.5	Spuren im E-Mail-Client löschen.....	307
4.5.1	Postfächer.....	308
4.5.2	E-Mails löschen.....	309
4.6	Spuren in Dokumenten löschen	310
4.6.1	In Office-Dokumenten	311
4.6.2	In Bildern.....	312
4.7	Spuren auf dem PC völlig vermeiden	313
4.7.1	Booten von Live-CD.....	315
4.7.2	Betriebssystem von USB-Stick	316

Kapitel 5

Daten sicher löschen323

5.1	Datenträgeraufbau.....	323
5.1.1	Festplatten.....	324
5.1.2	Wechseldatenträger.....	327
5.1.3	CD-R und DVD±R.....	327
5.2	Dateilöschverfahren.....	328
5.2.1	Einfaches Löschen.....	328
5.2.2	Sicheres Löschen.....	332
5.3	Einzelne Dateien sicher löschen.....	337
5.3.1	Löschen unter Windows.....	339
5.3.2	Löschen unter Linux.....	339
5.4	Kompletten Rechner sicher löschen.....	343
5.5	Festplatten sicher löschen.....	347
5.5.1	Löschen unter Windows.....	347
5.5.2	Löschen unter Linux.....	349
5.6	Partitionen sicher löschen.....	351
5.7	Tarnnetz.....	352

Adressen357

Stichwortverzeichnis359

VORWORT

Es gibt einige Selbstverständlichkeiten im Alltag. Beispielsweise würde niemand, der bei klarem Verstand ist, sich ein Schild mit seinem Namen, Geburtsdatum, Einkommen und Adresse nebst Aufbewahrungsort des Haustürschlüssels bei einem Gang durch die Fußgängerzone um den Hals hängen. Alle würden darin übereinstimmen, daß diese Angaben vertraulich sind und Fremde nichts angehen. Außerdem würde sich niemand ein Auto kaufen, bei dem der Hersteller die Türverriegelung wegrationalisiert hat. Weil er für dieses Fahrzeug in Deutschland aber ohnehin keine Typzulassung bekäme – über den Grund wäre man sich auch wieder einig –, stellt sich das Problem gar nicht.

Mit elektronischen Daten wird ganz anders und oft sehr sorglos umgegangen. Dabei spielt es keine Rolle, ob es die eigenen oder Daten über andere sind. Zu wenige Anwender machen sich Gedanken darüber, wer Zugang zu einem Computer hat, auf dem sie geheime Daten ablegen oder wer ihnen eigentlich gegenübersteht, wenn sie im Internet eigentlich vertrauliche Informationen ausplaudern. Die in einem Forum nur nebenbei erwähnte anstehende Urlaubsreise ist eine Einladung auf dem Silbertablett für kriminelle Existenzen; die Breitenwirkung ist die gleiche wie bei einer Anzeige in der Tageszeitung. Ebenso kann ein in der Mittagspause verwaister, nicht abgeschalteter PC geradezu eine Aufforderung sein, sich mal in aller Ruhe anzuschauen, welches neue Projekt denn da gerade in Arbeit ist.

In diesem Buch erkläre ich Windows- und Linux-Anwendern, wie sie auf dem Computer das Mitprotokollieren über ihr Tun abschalten und wie die auf dem Computer gespeicherten Daten geschützt werden müssen, damit kein Angreifer Erkenntnisse aus ihnen ziehen und zum Schaden des Opfers ausnutzen kann.

Angreifer im Sinne dieses Buchs sind neugierige Kollegen und Familienmitglieder, Diebe, Spione, Forensiker und Erpresser. Eine Person kann auch gleichzeitig mehrere dieser Funktionen ausfüllen.

Für die Wahrung der eigenen Privatsphäre gibt es ein paar wenige Regeln, die beherzigt werden müssen:

Informationen über sich selbst darf man nur herausgeben, wenn man sicher ist, daß der andere damit kein Schindluder treibt. Er darf nur das an Daten erhalten, was er unbedingt benötigt und nicht das, was er gern hätte. Es spricht auch nichts dagegen, im bestimmten Situationen ganz anonym zu bleiben und/oder mit erfundenen persönlichen Angaben zu operieren. Das Persönlichkeitsrecht ist das wichtigste Gut in unserer Staatsform und muß unter allen Umständen gewahrt werden! Auch wenn Politiker immer wieder damit liebäugeln, die Privatsphäre einzuschränken, weil sie nur zu gerne alle Lebensbereiche der Bürger kontrollieren würden.

Dieser Grundsatz gilt sowohl für das reale als auch für das virtuelle Leben. Insbesondere im Internet ist größte Vorsicht geboten. Nicht nur, daß man sich selbst an die Kandare nehmen muß, sondern man muß auch damit rechnen, daß unerlaubt Daten vom PC abfließen. Insbesondere soziale Netze wie Facebook gehen nicht zimperlich mit den auf dem Computer der Mitglieder gespeicherten Adressen um. Sie ziehen sie, unvorsichtig eingestellt, ungefragt aus dem Windows-Adreßbuch, um »Freunde« zu finden. Die Sekretärin, die in der Mittagspause auf ihrem Bürocomputer ihre sozialen Kontakte pflegt, riskiert also Geschäftsgeheimnisse. Weil aber Internet-Verbote bekanntermaßen ignoriert werden und die Vollsperrung auf Dauer auch nichts nützt, bleibt nur die Möglichkeit, unbelehrbaren Facebook-Anwendern Wegwerf-Benutzerkonten einzurichten, die keinen Zugriff auf die Geschäftsdaten haben. Wie das geht, steht natürlich in diesem Buch.

Hand in Hand mit der Datensparsamkeit geht das Vermeiden von Spuren. Auf dem Computer ist das nicht ganz einfach, denn alle Betriebssysteme sammeln eifrig alle Informationen über Benutzeraktivitäten und speichern sie in Logs oder der Registry. Wie Spuren durch das Installieren alternativer Anwendungsprogramme und das nachträgliche Bearbeiten von Metadaten vermieden beziehungsweise gelöscht werden, beschreibe ich ausführlich.

Auf einem Computer befindliche Daten müssen genauso gut geschützt werden wie solche auf Papier:

- Geheime Informationen gehören nicht ungesichert auf der Festplatte gespeichert; seine Scheckkartennummer läßt auch niemand offen auf dem Schreibtisch liegen.
- Geschäftspartnern dürfen Nachrichten nicht quasi ohne Briefumschlag über das Internet gesandt werden – niemand käme auf die Idee, ein Angebot auf einer Postkarte zu verschicken.
- Fremden muß der Weg in den Computer und in das eigene Netzwerk versperrt sein, ganz so wie man den Hausschlüssel auch nicht neben die Haustür hängt.

- Nicht mehr benötigte Daten müssen so gelöscht werden, daß sie nicht wiederhergestellt werden können. In einem Büro wandern alle vertraulichen Papiere ja auch in den Aktenvernichter.

Die Einhaltung dieser Prinzipien ist überhaupt nicht schwer, denn es gibt eine große Zahl meist sogar kostenfreier Softwarepakete, die dem Anwender und Administrator bei diesen Aufgaben helfen. Man findet die Programme meist auch auf einschlägigen Sammelseiten, speziell auch von Zeitschriften, die damit Kunden auf ihre Online-Portale locken wollen. Hierbei gilt aber: Finger weg! Sicherheitsrelevante Programme dürfen nur von den Originalseiten heruntergeladen werden, damit garantiert ist, daß man die aktuelle Version erhält. Ein an anderer Stelle gefundenes älteres Programm kann nicht nur Schadcode enthalten, sondern insbesondere auch Sicherheitslücken, die in der aktuellen Version längst geschlossen wurden.

Weil nicht alle Daten gleichermaßen geschützt werden müssen, werden in diesem Buch verschiedene komplexe Sicherheitsstufen definiert. Welche ein Leser benötigt, muß er selbst einschätzen.

Ist mit ungeschulten Angreifern zu rechnen, reicht eine niedrige Schutzebene. Das sind unter anderem Systemzugangs-Paßwörter, verschlüsselte Anwendungsdateien und sicheres Löschen von Dateien. Diese Schutzmaßnahmen schrecken zwar durchschnittliche PC-Anwender ab, halten aber einem professionellen Angreifer teilweise nicht lange stand.

Sind die auf dem PC gespeicherten Daten extrem wichtig und vertraulich und ist damit zu rechnen, daß ein geschulter Angreifer den Computer oder die Datenträger in seine Gewalt bringt, muß die höchste Sicherheitsstufe angewandt werden: die Vollverschlüsselung des ganzen Computers mit einem sehr guten Paßwort. Jeder Angreifer wird sich daran die Zähne ausbeißen! Paradoxerweise ist die höchste Sicherheitsstufe am leichtesten zu realisieren und der Anwender wird davon bei der täglichen Arbeit am wenigsten mitbekommen. Man muß sich aber im Klaren sein, daß je höher die Sicherheitsstufe ist, desto größer die Gefahr des Datenverlusts bei Hardware-Ausfall ist, denn selbst Restaurierungsprofis kommen nicht mehr an vollverschlüsselte Daten (was ja das eigentliche Ziel der Vollverschlüsselung ist). Um so wichtiger sind dann regelmäßige Backups, am besten verschlüsselte, falls der Angreifer auch sie in seine Gewalt bringt.

Um solche Angreifer abzuwehren, die sich in das Netzwerk einhängen, muß die über das Internet laufende Kommunikation verschlüsselt werden. Dieser Schutz ist äußerst wirksam.

Nicht im Buch weiter thematisiert ist das Sichern des Computers durch die Installation einer Firewall und eines Virens scanners. Die beiden Maßnahmen sind heute Pflicht, damit man nicht in die Situation kommt, daß man Hackern dadurch unwillentlich Vorschub leistet, daß sie in den eigenen PC eindringen und ihn gar als Ausgangspunkt für das Kompromittieren der ganzen Firma mißbrauchen können. Ich möchte allen Lesern aber diesbezüglich

trotzdem ein paar Gedanken zur Wahrung der Privatsphäre und des Datenschutzes mit auf den Weg geben.

Unbestritten ist, daß eine gut eingestellte Firewall Angriffe aus dem Internet verhindert. Auch Virens Scanner sind als Schutz vor Trojanern wichtig. Man muß sich aber gleichzeitig gut überlegen, wie und was man alles mit ihnen sichern will. Zu bedenken ist, daß ein Virens Scanner ungehindert auf dem Computer herumschnüffeln darf und daß er sich ständig mit dem Heimatserver verbindet und Daten dorthin melden kann, ohne daß man etwas dagegen tun kann. Unter diesem Gesichtspunkt sind alle Virens Scanner kritisch zu betrachten und eigentlich als potentielle Malware einzustufen, die man ja mit dem Virens Scanner zu vermeiden sucht. Antivirensoftware blind zu vertrauen ist leichtsinnig. Mit einer Ausnahme sind es alles proprietäre Programme ohne Überwachung von außen. Was die Hersteller der Antivirensoftware einbauen, wissen nur sie.

Welchen Virens Scanner man installieren will und welche Rechte man ihm geben möchte, muß jeder selbst entscheiden. Aber wie immer gilt, daß einheimischen Programmen eher als ausländischen vertraut werden kann, allein schon wegen der Haftung vor Gericht. Die nächste Frage, die sich stellt, ist, ob man wirklich Sicherheitssoftware installieren darf, die genau aus den Ländern stammt, vor denen die Landesämter für Verfassungsschutz warnen und vor denen wir uns schützen müssen. Sie sollen hier ruhig genannt werden: erstens China, zweitens Indien, drittens Rußland und viertens USA. Bei Antivirensoftware ist damit das Gros der Anbieter fast schon disqualifiziert. Kann man unter solchen Gesichtspunkten wirklich einem »Rising Antivirus« aus China seinen PC anvertrauen, auch wenn er ein deutsches TÜV-Zertifikat verliehen bekommen hat? Generell rate ich bei Virens Scannern und Firewalls deswegen immer zu Open Source, auch wenn diese Programme oft weniger komfortabel zu bedienen sind als kommerzielle. Die Entwickler verfolgen keine wirtschaftlichen Interessen und wissentlich eingebaute Backdoors würden im Quelltext binnen kurzer Zeit entdeckt. Sehen Sie sich auch als Windows-Anwender ruhig einmal ClamAV an.

Zum Schluß wünsche ich Ihnen eine spannende Lektüre und hoffe natürlich, daß Sie nie Ziel eines Angriffs werden!

Ihr Rolf Freitag

KAPITEL 1

DIEBSTAHL- SICHERUNG

Bewegliche Gegenstände unterliegen grundsätzlich einem erhöhten Diebstahlrisiko. Daß kleine, bewegliche Net- oder Notebooks oder gar scheckkartengroße Speicherkarten gestohlen werden, kann man sich leicht vorstellen, allerdings wechseln oft auch ganze Server und einzelne Hardwarekomponenten wie Festplatten unfreiwillig den Besitzer. Tatgeschehen sind teils Wohnungs- oder Büroeinbrüche, teils werden die Geräte aus geparkten Autos entwendet oder ihrem Besitzer nicht mehr zurückgegeben, wenn er seinen tragbaren Computer irgendwo vergißt.

Warum Computer gestohlen werden, hat verschiedene Gründe: Entweder geht es dem Dieb um die Hardware an sich, die er irgendwo zum Kauf anbietet, um sich schnell Bargeld zu verschaffen, oder er möchte an die auf dem Computer gespeicherten Daten gelangen, um einen geschäftlichen oder ideellen Vorteil zu erlangen, der Wert der Hardware ist in diesem Fall unerheblich.

Wird ein ganzer Computer entwendet, muß man damit rechnen, das Gerät nie wiederzubekommen. Ist ein großer Server oder ein mit besonders aufwendigen Komponenten zusammengestellter PC diebstahlversichert, wird man vom Versicherungsunternehmen finanziellen Schadenersatz nur zum Buchwert des Geräts erhalten. Ist es bereits abgeschrieben, geht man leer aus. Das kann natürlich sehr ärgerlich sein, denn ein Computer nicht von der Stange ist ganz schön teuer.

Viel ärgerlicher, ja sogar existenzgefährdend kann es aber sein, wenn der Dieb Zugriff auf die auf dem Computer gespeicherten Daten erlangt. Der Ingenieur, der zu Hause ungestört weiter an seinem neuen Patent tüfteln möchte und seinen Notebook mit allen relevanten Daten auf dem Weg von der Arbeitsstelle zerstreut in der U-Bahn liegenläßt, verschafft dem Dieb

wertvolle Informationen, die dieser an ein Konkurrenzunternehmen verkaufen kann, ganz zu schweigen vom Patent, das er nie anmelden wird können. Die Vorstandssekretärin, die den Notebook mit der angefangenen Berechnung der Vorstandsprovisionen auf den Rücksitz des vor der Bäckerei geparkten, offenen Cabrios liegenläßt, um nur mal schnell auf dem Weg in das Büro ein Brötchen zu kaufen, spielt der Presse unfreiwillig vertrauliche Gehaltsdaten in die Hände, die weidlich für Schlagzeilen genutzt werden können.

Hat man vertrauliche Daten zu verwalten, muß der Computer also besonders gut geschützt werden. Am besten zweistufig: Erstens ist die Hardware durch eine gute physikalische Zugangssperre zu schützen, zweitens sind die darauf gespeicherten Daten so aufzubereiten, daß sie kein Unberechtigter auslesen kann, der sich des Computers bemächtigt.

Dieses Kapitel lehnt sich bei der Beschreibung der physikalischen Zugangssicherung an den Maßnahmenkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) an, das empfiehlt, die Räume, in denen diebstahl- und spionagegefährdete Computer aufgestellt sind, einbruchssicher abzusperrern und die Computer selbst abzuschließen.

Bei der diebstahlssicheren Aufbereitung der Daten wird die sicherste Methode überhaupt vorgestellt: das Verschlüsseln der Festplatte. Kein Angreifer – egal ob unbedarft oder gut geschult – kann eine mit einer guten Software gegen ein gutes Paßwort verschlüsselte Festplatte auslesen.

1.1 PHYSIKALISCHE ZUGANGSSICHERUNG

In Firmen gelten normalerweise im Rahmen der IT-Sicherheitsleitlinien Vorschriften für das Betreten, Verlassen, Reinigen und Abschließen der internen Büros. Voraussetzung für deren Einhaltung ist wie immer, daß das Personal geschult und sensibilisiert wird.

In jedem sicherheitsbewußten Unternehmen wird nur den Personen Zutritt zum Firmengelände gewährt, die sich sicher ausweisen können. Im Hause selbst sind manchmal an stark frequentierten Stellen Personenvereinzler installiert, so daß keine Gruppen gewaltsam in die Räumlichkeiten eindringen können.

Am Home- beziehungsweise Telearbeitsplatz sind Sicherheitsmaßnahmen genauso nötig, allerdings in anderen Dimensionen. Eine gute Zugangssicherung ist mehrstufig und besteht aus beispielsweise einer sicheren und verschlossenen Eingangstür, einer verschließbaren Zimmer-/Bürotür und gegebenenfalls Schranktür oder einem abschließbaren Computergehäuse beziehungsweise einem gegen Diebstahl angeketteten Notebook.

Keinesfalls darf man Freunden oder Familienmitgliedern unkontrollierten Zugang zum Computer gewähren. Es ist schon vorgekommen, daß der fünfzehnjährige Sohn eines Berufsfotografen den Computer des Vaters während dessen Abwesenheit an einem Wochenende inklusive bearbeiteten und unbearbeiteten Aufträgen, den Scanner und den farbtreuen, teuren Monitor

verhökerte, um der Freundin kostbare Geschenke machen zu können. Als »Beweis« für einen Fremdeinbruch ließ er sich von den Freunden zusammenschlagen. Nachdem sich der Vater eine neue Ausrüstung anschaffte, ein neues Schloß in die Bürotür einbaute und dem Sohn den Schlüssel zu treuen Händen übergab, als er wieder über ein Wochenende verreisen mußte, verkaufte der Sohn zum zweiten Mal die PC-Ausrüstung des Vaters.



Bild 1.1: Notebook-Sicherung per Stahlkabel und Zahlenschloß von Kensington (Bildquelle: ACCO Europe)

Natürlich ist nicht immer kriminelle Energie im Spiel. Die kleine Tochter, die die vielen Knöpfe auf Papas Tastatur lustig findet und auch mal drücken möchte, wenn er nicht im Zimmer ist, kann unwissentlich wichtige Daten löschen. Oder eine Reinigungskraft zieht das Stromkabel, während das CAD-Programm gerade den mühevoll zusammengestellten Plan berechnet, damit sie besser mit dem Staubsauger in die Ecken kommt. Und das einen Tag vor der Abgabe, von der das weitere Überleben des Architekturbüros abhängt.

1.1.1 Eingangsschlösser

Zugangssicherungen sind in den meisten Fällen Türen mit einem Schloß. Die Stärke der Zugangssicherung hängt daher entscheidend von der Sicherheit dieses Schlosses und natürlich der Stabilität der Tür ab. Sichere Schlösser müssen mehrere Kriterien erfüllen:

- Sie sind technisch sicher,
- nur wenige und absolut vertrauenswürdige Personen besitzen einen Schlüssel und
- die Schlüssel dürfen nicht ohne weitere Umstände nachgemacht werden können.

Speziell in Mehrfamilienhäusern gibt es Generalschlüssel, durch die weitere Personen wie Verwalter einen zum Schließzylinder passenden Schlüssel haben. In diesem Fall empfiehlt es sich, möglichst bald nach der Schlüsselübergabe das Wohnungsschloß (den Schließzylinder) auszutauschen und

zwar gegen ein technisch sicheres Modell (siehe Tabelle 1.1). Das ursprüngliche Schloß muß man als Mieter natürlich aufheben und kurz vor der Übergabe beim Auszug wieder einbauen, denn es gehört zur Wohnung.

Schließzylinder	Hersteller	Zirka-Preis
Ikon SK 6	IKON	bis 90 Euro
CES 810RE 5	CES-Gruppe	zirka 80 Euro
DOM 333 ix 10 KG	DOM Sicherheitstechnik	ab 100 Euro
DOM ix Saturn	DOM Sicherheitstechnik	ab 115 Euro
BKS Serie 45 Janus	BKS GmbH	ab 70 Euro
Evva 3KS	Evva Sicherheitstechnik GmbH (Österreich)	ab 65 Euro

Tabelle 1.1: Beispiele für Sicherheits-Schließzylinder

Weitere Informationen zum Thema sichere Schließzylinder und Zugangssicherung/Einbruchschutz findet man in entsprechenden Berichten der Stiftung Warentest und den kriminalpolizeilichen Beratungsstellen, die in den meisten Städten kostenlos Auskunft geben.

Bei den Türen ist ein sicherer Schließzylinder auch im Versicherungsfall wichtig, denn ohne deutliche Einbruchsspuren zahlen Versicherungen generell keine Einbruchsschäden. Auch deshalb sollte man sich zumindest notieren, wem man wann welchen Zweitschlüssel gab. Wichtig zu wissen ist, daß laut deutschem Mietrecht bei einer vermieteten Wohnung der Eigentümer kein Recht auf einen Zweitschlüssel hat, außerdem muß er – mit Ausnahme eines echten Notfalls wie einem Wohnungsbrand – dem Mieter eine geplante Begehung der Wohnung rechtzeitig vorher ankündigen. Er darf generell maximal nur einmal pro Monat die Wohnung betreten und zwar zu den üblichen Zeiten, bei den meisten Arbeitnehmern also zwischen 18 und 20 Uhr. Auf der sicheren Seite ist man als Mieter, wenn man den Austausch des Schlosses in den Mietvertrag aufnimmt. Dann wälzt man bei Einbruchsschäden durch die Feuerwehr oder einen Handwerker das Risiko auf den Vermieter ab.

1.1.2 Computersicherungen

Über fünfzig Prozent aller heute verkauften Computer sind mobile Geräte. Diese unterliegen einer besonderen Diebstahlsgefährdung, weil sie leicht sind und unauffällig transportiert werden können. Die Gefahr besteht sowohl unterwegs als auch dann, wenn mit einem Notebook ausschließlich an einem fest installierten Schreibtisch gearbeitet wird.

Darüber hinaus sind mobile Geräte leicht zu entwenden, weil es oft vorkommt, daß Notebooks oder Handhelds unabsichtlich irgendwo liegengelassen werden. Oder der Besitzer trägt es in einer Tasche oder unter den Arm geklemmt mit sich am Körper, von wo es unschwer weggerissen werden kann.

Im stationären Betrieb empfiehlt es sich, das Notebook über ein Hartstahlkabel mit Schließkopf mit einem fest installierten Gegenstand zu verbinden (siehe auch Bild 1.1). Fast jedes Notebookgehäuse besitzt hinten oder auf der Seite eine mit einem Schloß-Symbol gekennzeichnete Buchse, die für solche Notebook-Schlösser vorgesehen ist. Ein bekannter Hersteller solcher Sicherheitstechnik ist Kensington (www.eu.kensington.com) aus der amerikanischen ACCO-Gruppe. Kensington bietet mehrere unterschiedliche professionelle Ausführungen von Notebook-Schlössern an, die sich preislich ab zirka 60 Euro bewegen. Billiglösungen sind nicht empfehlenswert. Sehr viel günstiger als die hochpreisigen Profi-Lösungen von Kensington selbst sind Kabel von Belkin (ab zirka 12 Euro), Logilink (bei Amazon ab etwa 6 Euro) oder Hama (ab 4 Euro), von Billiglösungen mit einfachen Schlössern darf man aber keine echte Sicherheit erwarten. Beim Produktvergleich muß auch immer darauf geachtet werden, daß das *Kensington Notebook Schloß* auch in den Produkten anderen Herstellern eingebaut ist, weil diese Art der Sperre mittlerweile als Standard gilt.

Die Probleme bei Desktop-Computern sind andere als bei Notebooks. Die Gefahr, daß sie beim Transport gestohlen werden, ist gering, Einbruchsdiebstähle aber natürlich nicht auszuschließen. Es gibt mehrere Ansätze gegen das einfache Entwenden der Hardware. Kensington bietet für den moderaten Preis von knapp 22 Euro ein System für Desktop-Computer an, mit denen drei beliebige Teile miteinander verbunden werden (siehe Bild 1.2). Wer den PC und den Monitor mitnehmen will, muß dann beispielsweise auch den Schreibtisch stehen, was natürlich nicht mehr so einfach ist.



Bild 1.2: Einzelgeräteschutz mit dem Kensington Desktop Microsaver
(Bildquelle: ACCO Europe)

Nur in Firmenumgebungen und hier auch eher für den Abteilungsserver, der nicht unbedingt im zentralen Serverraum stehen muß, sind abschließbare Schränke von Herstellern wie Rittal und Knürr sinnvoll, allerdings werden solche Schränke meist mit dem gleichen Standardschloß ausgestattet. Für höheren Sicherheitsbedarf gibt es Tresore mit integrierter Kühlanlage und speziellen Kabeldurchführungen. Allerdings kosten sie einen fünf- bis sechsstelligen Betrag, die Klimaanlage verbraucht zusätzlich Strom und solche Tresore wiegen zirka eine Tonne. Für besonders schützenswerte Daten sollte die Anschaffung solcher Sicherheitssysteme aber ins Kalkül gezogen werden. Selbstverständlich hilft das alles nur, wenn die Türen abgeschlossen sind.

Die beste Diebstahlsicherung ist immer, daß ein Gegenstand so versteckt oder weggeschlossen wird, daß er gar nicht gefunden wird oder wenigstens nicht gleich ins Auge fällt. Dieser Grundsatz gilt natürlich auch für Computer und Datenträger. Dazu gehört in erster Linie, daß PCs immer sicher aufbewahrt werden müssen und beim Transport im Auto niemals sichtbar liegengelassen werden dürfen. Der Kofferraum ist aber kein sicherer Aufbewahrungsort! Autoschlösser sind niemals sicher und in Sekundenschnelle aufgebrochen. Fahrzeuge mit komfortabler Funkzentralverriegelung, die mit fremden Signalen übertölpelt werden kann, sind besonders gefährdet.

Grundsätzlich gilt jedoch bei PCs, daß externe Sicherungsmaßnahmen fragwürdig sind, wenn es um den Schutz der gespeicherten Daten geht. Den Dieb, der nicht hinter der Hardware selbst her ist, sondern Interesse an den darauf gespeicherten Informationen hat, stört es nicht, daß der PC auf dem Schreibtisch festgeschraubt ist, wenn er die Festplatte entnehmen kann. Bei Desktop-Gehäusen hindern ihn daran maximal zehn Kreuzschlitzschrauben und zwei Kabel, die zu entfernen sind.

Das Verstecken von Hardware ist deshalb durchaus eine sinnvolle, zusätzliche Schutzmaßnahme. Ein Versteck schützt nach dem Prinzip »Wo nichts zu finden ist, kann auch nichts gestohlen werden«. Als Vorschläge für größere Hardware liest man manchmal Vorschläge wie Tarnnetze und gar Strategien wie das Vergraben, Einmauern oder als etwas anderes ausgeben, die meisten davon sind aber wenig praktikabel.

Für Kleinteile wie USB-Speichersticks gibt es aber viele unauffällige Versteckmöglichkeiten, mit denen die enthaltenen Daten eventuell sicher sind.

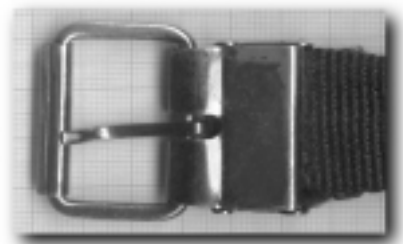


Bild 1.3: Ein unauffälliges Gürtelende mit einigen Gebrauchsspuren

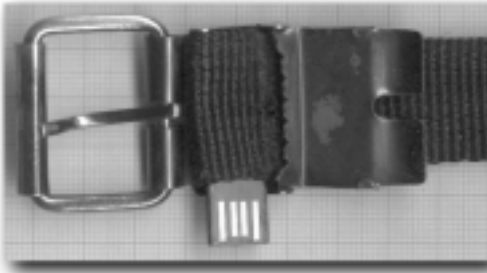


Bild 1.4: Nach dem Aufklappen und Herausziehen zeigt sich ein kleiner USB-Speicherstick. Nach schwarz anstreichen der Kontakte sähe er wie ein Stück Plastik zum Fixieren des Gürtelendes aus

Wie man in Bild 1.3 und Bild 1.4 am Beispiel eines Transcend Jetflash T3 mit einer Kapazität von 4 GByte sieht, paßt er problemlos in die Gürtelschlaufe im Inneren einer Gürtelschnalle. Weil die Gürtelschnalle aus magnetischem Stahl hergestellt ist, schützt sie den Stick mechanisch, schirmt ihn magnetisch ab und als Faradayscher Käfig schirmt sie ihn auch elektrisch ab. Die meisten Gürtel haben zwar nicht genau so einen Hohlraum aus Stahl, aber einen ähnlichen Aufbau und meistens Platz für einen kleinen Stick. Neben Transcend gibt es eine ganze Reihe bekannter Hersteller wie beispielsweise Verbatim, die Miniatur-USB-Sticks mit unterschiedlichen Kapazitäten für sehr angemessene Preise anbieten.

Für nasse und feuchte Verstecke wie Aquarien, Blumenerde und Salbentiegel eignen sich wasserdichte Sticks wie der Super Talent Pico-C. Die 8-GByte-Version kostet bei Amazon.de zirka 13 Euro.



Bild 1.5: Pico-C: Ein wasserdichter kleiner USB-Stick des Herstellers Supertalent (Bildquelle: amazon.de)

Noch kleinere Datenträger sind die Micro SD-Karten, die auch in eine hohle Münze passen, wie man sie bei <http://spy-coins.com> für um die 40 Euro erhält (siehe Bild 1.6).

Es gibt viele weitere Versteckmöglichkeiten, von denen man einige auf eBay mit der Suche nach »Geheimversteck« findet. Aber klar ist, daß dann auch Angreifer diese Verstecke kennen!

Ein anderer Ansatz ist, die vorhandene Umgebung nach Versteckmöglichkeiten durchzusehen und die Gegebenheiten zu nutzen. Gut geeignet sind Verstecke, die sich ohne Werkzeug nicht öffnen lassen, beispielsweise Hohlräume in Geräten, die man auf- und zuschrauben kann, ohne daß dies nachher leicht erkennbar ist. Dazu gehört aber auch eine sichere Befestigung oder

zumindest Polsterung der versteckten Inhalte, damit ein Schütteln das Versteck nicht verrät.



Bild 1.6: Hohle Münzen als Versteck für eine Micro-SD-Karte

1.1.3 Eingabeschutz

Um die Anzeige mobiler Rechner wie Notebooks und Handhelds vor fremden Blicken zu verstecken, wurden Blickschutzfilterfolien entwickelt. Sie werden auf den Monitor geklebt und grenzen den Sichtbereich, in dem die dargestellten Zeichen gut ablesbar sind, auf 15 bis 30 Grad ein. Damit hat man eine optische Zugangssicherung, die gegenüber seitlichen Sitznachbarn ausreicht. Nicht geeignet ist der Schutz gegen hintere Sitznachbarn, insbesondere, wenn sie über die Schulter des Benutzers auf den Monitor blicken können. Der Blickschutz hat den Nachteil, daß man als legaler Anwender ein deutlich dunkleres Bild in Kauf nehmen muß.

Der Preis eines Blickschutz-Filters von 3M, inmac oder Vikuiti liegt für 13-Zoll-Monitore bei etwa 55 Euro. Angeboten werden sie beispielsweise auf *ebay.de* und <http://www.privacyfilter24.com>. Aber auch die für ihre Notebook-Sicherungen bekannte Firma Kensington bietet professionellen Eingabeschutz, der je nach Bildschirmdiagonale von 54 Euro (14,1 Zoll) bis 70 Euro (17 Zoll) kostet und auch für stationäre LCD-Anzeigen mit einer Diagonale von 22 Zoll für den Preis von 95 Euro angeboten wird (siehe <http://eu.kensington.com/kensington/de/de/s/1173/laptopprivacyscreens.aspx>).

1.1.4 Biometrie

Ein einfaches Mittel, um sicherzustellen, daß niemand anders als man selbst sich an einem Computer einloggt, ist diesen mit einer biometrischen Analysehardware auszustatten. Biometrie heißt, daß ein persönliches, individuelles Merkmal zur Erkennung einer Zugangsberechtigung genutzt wird. Bekannte biometrische Merkmale sind Fingerabdrücke und Retinamuster. Angeboten werden Fingerabdruckscanner in verschiedenen Ausführungen, beispielsweise von Lenovo (vormals IBM) unter dem Begriff *Thinkoantage Client Security* für mobile Thinkpads und für Thinkcentre-Desktops. Dabei wird mit markigen Sprüchen behauptet, daß der PC auf diese Weise zum Datentresor wird und daß diese Lösung, mit einem TPM (Trusted Platform Module) er-

gänzt, absolute Sicherheit bringt (siehe <http://www.pc.ibm.com/europe/think/de/security.html?europe&cc=europe>). Wenn man allein auf Softwarelösungen von Microsoft und deren BitLocker-Verschlüsselung (siehe Kapitel 1.3.3 ab Seite 67) vertraut, ist der Grad der Sicherheit aber tatsächlich auch sehr hoch. Natürlich muß dann auch eine Windows-Version installiert werden, die überhaupt bitlockerfähig ist, sonst nutzen die Sicherheitsfunktionen überhaupt nichts.



Bild 1.7: Cherry FingerTIP ID Board G83-14400 mit Fingerabdruck-Scanner
(Bildquelle: Cherry AG)

Biometrie kann man aber problemlos nachrüsten, der bekannte Peripherie-Hersteller Cherry AG aus Auerbach/Opf. bietet mit seiner Serie FingerTIP ID sowohl Mäuse als auch Tastaturen an, in die ein Fingerabdruck-Scanner eingebaut ist. Es gilt dabei aber, daß die Hardware nur dann Sinn macht, wenn auch die entsprechenden Software-Treiber installiert sind und anstelle des Paßworts beim Systemstart immer der Fingerabdruck geprüft wird.



Bild 1.8: Platzsparend und wenig auffällig: Fingerabdruck-Scanner auf der Cherry FingerTIP ID Mouse M-4200
(Bildquelle: Cherry AG)

Der Kauf eines Fingerabdruck-Scanners allein reicht nicht, es wird immer die entsprechende Erkennungssoftware benötigt, die es nicht allein für Windows, sondern auch für Linux und BSD-Unix gibt¹. Es muß außerdem beachtet werden, daß es bessere und schlechtere Scanner gibt, denn wenn anstelle des echten Daumens auch eine Fotokopie reicht, nutzt er nichts. Wer außerdem zu einem potentiell gefährdeten Personenkreis gehört und nicht nur Angst vor Diebstahl haben muß, sollte ernsthaft daran denken, daß für den Fingerabdruck nur der Daumen und nicht die ganze Hand oder Person benötigt wird. Außerdem ist es für einen Erpresser erheblich einfacher, mit Gewalt einen Fingerabdruck zu erzwingen als das Paßwort eines abstreitbaren, versteckten Containers mit den gesuchten Daten.

Weiterhin nutzt die Biometrie dann nichts, wenn der Datenträger mit den gesuchten Informationen nicht verschlüsselt ist, da man nur das aktive Betriebssystem durch den Fingerabdruck schützt. Biometrische Absicherung ist immer dann sinnvoll, wenn Diebstahlsgefahr besteht und wenn sie mit anderen Sicherheitsmaßnahmen kombiniert wird.

1.2 PASSWORTSCHUTZ

Paßwörter sind der softwaretechnische Zugangsschutz für Benutzerkonten, E-Mail-Accounts und verschlüsselte Daten.

Beim Anlegen eines Anwenderkontos, oft auch Account genannt, wird der Anwender nach einem Paßwort gefragt. Er muß sich eines ausdenken, das Paßwort in ein vorgegebenes Feld eintragen und zur Sicherheit die Eingabe noch einmal bestätigen. Damit niemand, der vielleicht bei der Eingabe über die Schulter schaut, das Paßwort mitlesen kann, werden im Eingabefeld für jedes eingegebene Zeichen entweder ein oder mehrere Sternchen oder auch gar nichts angezeigt.

1.2.1 Sichere Paßwörter

Egal was man mit einem Paßwort schützt: Entscheidend für die Sicherheit ist, ein gutes Paßwort zu wählen.

Für ein sicheres Paßwort gelten bestimmte Mindestanforderungen:

- Es sollte wenigstens acht Zeichen lang sein.
- Es enthält mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen (wie beispielsweise ein Leerzeichen, ein +, - oder einen Unterstrich).
- Es ist kein Name.
- Es ist kein Begriff aus dem Wörterbuch.
- Es ist keine triviale Tastaturzeichenfolge.
- Es gilt für nur ein Konto.

¹ Siehe dazu auch: *Jürgen Dankoweit: Der authentifizierte Daumen. freeX 5/2010, S. 36-31.*

STICHWORTVERZEICHNIS

O	
0900-Nummer, Sperre	247
A	
Abstreitbarkeit	57
Access Point	139
ACPI-Betriebsstufen	270
ACPI-BIOS	254
ACPI-Steuerung (Linux)	270
ActiveSync	127
AdBlock Plus	293
Adhoc-Netz (WLAN)	139
Administrationsrechte holen (Linux)	104
Administrator-Konto (Windows)	275
Advertising-Netze	301
Analog-Modem	195
Analogtelefonie	146
– verschlüsseln	147
AnonBox	240
Anonym mobil telefonieren	245
Anonyme IP-Telefonie	248
Anonyme Tauschbörse	224
Anonyme Telefonie	244
Anonymer Chat	234
Anonymer Proxy 193	
Anonymes E-Mail	235
Anonymes Fax	248
Anonymes Filesharing	227
Anonymisierung	191
Anonymisierungsnetze	218
Anonymizer	193
anonymous-User	282
Anrufdienst, anonym	247
Anwendungsdatei, verschlüsselte	39
Arbeits-/Grafikspeicher auf HD auslagern	254
Arbeitsspeicher (Linux)	269
Arbeitsspeicher, Paßwort in	54
Arbeitsspeicherdatei	251
Archivformate, nicht verschlüsselbare	42
ArmorSurf	218
ATA-geschützter Bereich	327
Auslagerungsdatei (Windows)	251
Auslagerungsdatei löschen	251
Auslagerungsdatei verschlüsseln (Linux)	123
Auslagerungspartition	269
Auslagerungspartition (Linux)	112
Autologin	28
B	
badblocks	332, 354
–, Optionen	351
BartPE	107
Benutzerdaten vollständig löschen	280
benutzerdefinierte Daten (Win.), Ablageort	268
Benutzerkonto anlegen/löschen (Windows)	268, 274 f.
Benutzerkonto anlegen/löschen (Linux)	277
Benutzerkonto auf USB-Stick	278
Benutzerkonto, geheimes	280
Benutzerkonto, paralleles	274
Benutzerkonto, verstecktes (Linux)	278
Benutzer-Paßwort ermitteln	28
Benutzer-Paßwort umgehen	31
Benutzer-Paßwörter, Windows	28
Benutzer-Verzeichnis	275
Benutzerverzeichnis einhängen (Windows)	279
Benutzerverzeichnis, doppeltes (Win./Linux)	278 f.
Betriebssystem von USB-Stick booten	316
Bilder, GPS-Daten	312
Bilder, Metadaten	312
Bildschirmschoner-Einstellungen	50
Biometrie	22
BIOS, wechseln in	313
BIOS-Paßwort umgehen	31
BitLocker	67
– ohne Sicherheitshardware	68
– To Go	68
–, Laufwerk automatisch entsperren	72
–, Partitionen verschlüsseln	67
–, Paßwort	70
BitTorrent	224
Blickschutzfilterfolien	22
Bombe, aktive	133
Bombe, logische	134

Bombe, passive	134
Bootlaufwerk verschlüsseln	74
Bootloader-Paßwort.....	117
Bootmanager	317
Boot-Partition, verschlüsselte (Linux).....	120
Bootreihenfolge umstellen.....	313
Bootsektor	325
–, Endeckennung	326
Bootskript (Linux).....	271
Browser, portable Version.....	211
Browser, privater Modus	291
Browser-Addons	292
Browser-Chronik	288
Brute Force.....	25

C

CAcert-Root-Zertifikat	241
CCleaner	258
CD-ISO-Datei verschlüsseln.....	110
CD-RW/DVD ±RW löschen	328
Chat, Sitzungsschlüssel.....	184
Chat, Tor-Server.....	235
Chat-Verschlüsselung.....	183
Chrome, Inkognito-Fenster	286
Chrome, Sicherheits-Erweiterungen.....	287
Chrome/Chromium, Proxyeinstellungen	207
CHS-Verfahren	324
Claws-Mail.....	170
Computer ausschalten	54
Container	76
– verstecken.....	85, 131
–, portablen verschlüsseln	124
Cookies löschen	290 f.
Cookies nachträglich akzeptieren/verwerfen	297
Cookies von Drittservern.....	296
cryptoloop.....	112
Crypto-Mobiltelefon.....	148
Crypto-Stick.....	46
cryptsetup-luks	122
CS Lite	296
CyberGhost.....	221

D

Darik's Boot and Nuke/DBAN	346
Datei entschlüsseln	182
Datei entschlüsseln (asymmetrisch)	175
Datei sicher löschen.....	337
Datei verschlüsseln.....	34, 129
Datei verschlüsseln (asymmetrisch)	173
Datei/Verzeichnisse verschlüsseln m. EFS.....	64
Dateien löschen	328
Dateiinformationen	310
Datei-Metadaten	331
Dateisysteme, fremde lesen (Windows)	105
Datei-Wiederherstellungswerkzeuge.....	329

Datenbank packen.....	310
Datenblöcke	323
Datenträger automatisch löschen.....	134
Datenträger direkt bearbeiten.....	324
Datenträger mit Zufallszahlen füllen	352
Datenträger sicher löschen.....	346
Datenträger unter Linux/Unix.....	324
Datenträger verschlüsseln m. BitLocker	67
Datenträger, log./physikal. Adressen	333
Datenträger, magnetooptische	328
Datenträger, optische	327
Datenträgeranschlußverfahren, Datendurchsatz	317
Datenträgeraufbau.....	323
Datumseinträge.....	250
dd.....	324
DECT-Telefon, Verschlüsselung.....	147
Default-Gateway.....	228
Defragmentierung.....	264
De-Mail	160
Desktop-Computer abschließen.....	19
Device Configuration Overlay/DCO	327
Disk Cleaner	264
Diskcryptor.....	106
–, Bootlaufwerk verschlüsseln.....	107
–, CD verschlüsseln.....	108
–, CD-ISO-Dateien verschlüsseln	110
–, Laufwerks-Verschlüsselung	108
–, Systemlaufwerk verschlüsseln	111
DMA, Direct Memory Access.....	53
DM-Crypt	113
DNS.....	193
DNS-Server, frei zugängliche	193
DNS-Server, zensierte	193
Dokument, letzter Bearbeiter	311
Dokument, Zeitinformationen.....	311
Dokumentversionen.....	311
Domainnamen analysieren	303
DSL-Modem	195
DSL-Router.....	139
DuckDuckGo.....	214
DVD-RAM.....	328
Dynamisch wachsende Datei	82

E

EASUS Partition Master.....	99, 352
Eepsite	233
EFS, Benutzerpaßwort	67
EFS, Encrypting File System	64
EFS, Zertifikat	65
Einbindepunkte (Linux)	101
Eingangsschlösser.....	17
E-Mail umleiten.....	236
E-Mail unterschreiben.....	160, 164
E-Mail verschlüsseln.....	159
E-Mail, Abfallerimer	309

STICHWORTVERZEICHNIS

E-Mail-Account, anonym	237
E-Mail-Anhang verschlüsseln	160
E-Mail-Anonymizer	240
E-Mail-Client, portabel	308
E-Mail-Client, Spuren	307
E-Mail-Empfang, anonym	240
E-Mail-Header	235
E-Mail-Header fälschen	236
E-Mails komprimieren	310
E-Mails löschen	309
E-Mails, Speicherformat	309
E-Mail-Versand, anonym	239
.eml-Datei	308
Encrypted Google	158
Ende-zu-Ende-Verschlüsselung	160, 227
Enigma	165
Eraser	266, 339
EXIF-Daten löschen	312
ExifTool	312
ext2/3/4 verschlüsseln	103
Ext2Fsd	106
ext2-Treiber f. Win	105
Externen Datenträger booten	313
Externes Betriebssystem booten	313

F

Fake-ID-Generator	243
Falsche Adresse	242
FAT verschlüsseln	64, 81
FAT, maximale Dateigröße	82
Fedora verschlüsselt installieren	114
Fedora, Kompletterschlüsselung	115
Festplatte komplett verschlüsseln	95
Festplatte, leeren Platz löschen	96
Festplatte löschen	262
Festplatte sicher löschen (Linux)	349
Festplatte sicher löschen (Windows)	347
Festplatte, Reservespeicher	335
Festplattenbereich überschreiben	328
Festplattenwerte auslesen	336
Festplatten-Wiper	262
Filesharing	225
–, anonymes Protokoll	228
–, Default-Gateway	228
Fingerabdruck-Scanner	24
Fingerprint	162
Firefox, Chronik-Datenbank	288
Firefox, Cookies löschen	290
Firefox, History löschen	288
Firefox, portabel	306
Firefox, privater Modus	291
Firefox, Tor-Projekt	196
Firewall	138
Firewire-Schnittstelle	53
Flash-Cookies	301

Flashspeicher überschreiben	333
Flashspeicher, Reservespeicher	334
foremost	329
Freemailer	238
–, ausländischer	238
FreeOTFE	124
–, abstreitbare Container	131
–, äußerer/innerer Container	132
–, Dateigröße verschleiern	130
–, Paßwort	130
–, verschl. Linux-Partition einbinden	132
–, versteckte Container	131
Freien Platz auf HD überschreiben	266
Freien Speicher sicher löschen	262
Freien Speicher überschreiben (Linux)	272
Funknetz	139
Funkpeilung e. PCs	194
Funksignale verstärken	140

G

Gateways	192
Geheime Telefonnummer	244
Geheim Schlüssel verschlüsseln	172
Gelöschte E-Mails packen	310
Geo-IP aushebeln	195
Geo-IP aussuchen	224
Geo-Targeting aushebeln	215, 222
Gerätstatus ermitteln (Linux)	350
Ghostery	300
GnuPG installieren	165
GnuPG/GPG, Datei verschlüsseln	34
gnupg2	176
Google, verschlüsselte Suche	155, 158
.gpg	181
GPG/PGP	60, 160
– auf Kommandozeile	176
gpg2	176
GPG4Win	165, 171
GPG-Befehle	182
GPT/GUID Partition Table	325
GSM, Verschlüsselung	148

H

Hard/Softlinks überschreiben	337
Hardwareverschlüsselung	57, 67
Hauptspeicher auslesen	53
Headerdaten austauschen	192
Heimatverzeichnis	275
Herkunftsland verschleiern	196
hiberfil.sys (Windows)	251, 254
Homepage, roboterfestes Impressum	244
Host Protected Area verschlüsseln	95
Host Protected Area/HPA	327
https-Verbindungen	153, 298
HTTPS Everywhere	154

I

I2P	228
I2PSnark	229, 231
Identität, anonyme	242
IEEE 1394	53
IFS-Treiber	105
IMSI-Catcher	148
Infrastruktur-Netzwerk	139
In-place-Verschlüsselung	92
Instant-Messenger-Clients, OTR	183
Internet Explorer, Registry-Einträge löschen	284
Internet Explorer, InPrivate-Browsen	285
Internet Explorer, Konfiguration	285
Internet Explorer, Proxy-Einstellungen	209
Internet Explorer, Sicherheits-Erweiterungen	286
Internet Explorer, Spuren	284
Internet-Café	249
Internet-Provider, Adreßspeicherung	193
IP-Absenderadresse	192
IP-Adresse	192
– wechseln	192
– zurückverfolgen	193
–, aktuelle herausfinden	192
–, rückverfolgbar	195
IP-Adressen, Einwahl bestimmter verhindern	222
IP-Adreßpool	193
IP-Header, Bestandteile	192
IP-Paket, Zwischenstellen	194
IP-Telefonie	146
–, Verschlüsselung	149
IP-Zieladresse	192
ISDN	146
– verschlüsseln	147
ISDN-Modem	195

J

Jetico BCWipe Total WipeOut	347
Junction Point	279, 338

K

Kabelnetzwerk	138
Kartentelefon	247
KDE, Datei asymmetrisch verschlüsseln	175
KDE-Paßworttresor	48
kdepim	176
KeePass Password Safe	47
Kensington Notebook-Schloß	19
Kleopatra	170
KNOPPIX	315
Komplettverschlüss. e. Datenpartition	74
Kwallet	48

L

Länderkennung ändern	224
last.fm überall nutzen	223

Laufendes System schützen	49
Laufwerk verstecken	74
Laufwerk, verschlüsseltes ein-/aushängen (Lin.)	123
Laufwerk verschlüsseln	67, 108, 129
Laufwerksbuchstaben ändern	92
LBA-Verfahren	324
linkd	279
Linux auf bootbaren USB-Stick übertragen	344
Linux auf USB-Device installieren	317
Linux nachträglich verschlüsseln	122
Linux, automat. Verschlüsselung	114
Linux-Containerformate auf Windows	125
Linux-Device-Mapper (Definition)	113
Linux-Standardverschlüsselung	112
Linux-USB-Vorinstallationen	319
Live-CD booten	315
Local Shared Objects	301
Logdateien	192
Logdateien (Linux)	273
Logdateien löschen (Windows)	269
Logical Volume Manager, LVM	113
Logische Laufwerke	113
loop-Mountpunkt	123
Loop-AES	112
Loop-Device	112
Löschen protokollieren	351
Löschen, einfaches	331
Löschen, sicheres	261, 332
Löschprogramme, Ausführungsgeschw. (Linux)	343
Löschverfahren	332
LSO-Cookies	301
LUKS	113
LUKS-Partition, Anfangsbereich	113
LVM, verschlüsseltes	118

M

MAC-Adresse	141
MACChanger	141
Maildatei e. Benutzers (Linux)	277
Master Boot Record	95, 324
–, Endung	326
–, gelöscht	326
Master-Paßwort	34
MBOX-Postfach	308
Metadaten	310
– löschen	311
–, Office-Dokumente	311
Mobil telefonieren	245
Mobilfunkgespräch mitschneiden	148
Mobiltelefon, Standortermittlung unterdrücken	246
Mobiltelefon, Verbindungsdaten	246
Mobiltelefonie	146
Mülleimer löschen	328
Multi-Session-CD	328
Münzfernsprecher, gesperrte Nummer	247

STICHWORTVERZEICHNIS

N	
Namenszuordnung	193
NAT	195
NAT-Router	193
Netzwerk über Stromnetz	139
Netzwerkdurchsatz	138
Netzwerke verbinden	192
Netzwerkeinwahl bestimmter PCs definieren	141
Netzwerkkarten, IP-Adresse	192
Netzwerkkommunikation	137
Netzwerklaufwerk, Daten löschen	258
Newsgroup, E-Mail	243
NoScript	302
Not-Aus	55
Notebook, Schlafmodus	254
Notebook-Deckel zuklappen	254
Notebook-Schloß	19
Notebook-Sicherung	17
NTFS unter Linux	81
NTFS verschlüsseln	81
NTFS-Dateisystem, Erweiterung	64
NTFS-Filerestorer	330
NTFSLink	279, 338
Null-Byte, Muster	324
O	
Offenes WLAN	194
Öffentlichen Schlüssel herunterladen	172
Öffentlichen Schlüssel zurückziehen	179
Öffentlicher Münzfernsprecher	247
Öffentlicher Schlüssel	163
Öffentlicher Schlüssel, kompromittierter	164
Office-Datei (MS/00.o) verschlüsseln	40
.onion	213
Onion-Router	195
Onion-Server	213
Online-Benutzerkonto	281
OpenPGP	160
OpenPGP Card	45, 162
Opera Turbo	216
Opera, Proxy-Einstellungen	208
Opera, Sicherheits-Widgets	287
Ophcrack	28
OTR	183
OTR-Proxy	183
outguess	38
-, Parameter	39
Outlook, E-Mail-Speicherung	309
Outlook, GnuPG	165
Outlook, Mailverschlüsselung	170
P	
P2P, anonyme Teilnehmer	227
P2P-Netzwerk	225
pagefile.sys (Windows)	251
Papierkorb löschen	258
Partition	324
- überschreiben	352
-, erweiterte	325
-, verschlüsselte einbinden	279
- sicher löschen	351
- verschlüsseln	67, 129
Partitionierungstools	99
Partitionskennungen	326
Partitionstabelle, Aufbau	325
Partitionstabelle, Größe	325
Password Unlocker	41
Paßwort	24
- einer Partition ändern	113
- im Arbeitsspeicher	54, 70, 251
- in anderer Datei verstecken	37
- notieren	32
- verschlüsseln	33
-, leeres	28
-, unsicheres	27
Paßwortabfrage umgehen	28
Paßwort-Änderungen	25
Paßwortdatei verschlüsseln	34
Paßworterzeugungs-Programme	26
Paßwort-Formeln	26
Paßwortlänge	24
Paßwort-Manager, Mozilla	29
Paßwort-Speicherung	28
Paßwort-Tresor	46
Paßwortverlust	56
PDF, Metadaten	312
PGP	36, 160
Phishing	298
Pidgin, OTR	186
Pocket-PC-Emulator	126
Pocket-PC-Emulator, Shared Folder	127
Polipo	196
Port, Quell-/Absende-	192
Pre-Boot-Authentication	95
Prepaid-SIM-Karte	245
Privater Modus, Browser	291
Privater Schlüssel	163
Programme löschen	257
Proxy	192, 196
- für Localhost	208
Proxy-Einstellungen anpassen	207
Proxy-Netzwerk	195
Pseudo-Toplevel-Domain	213
Pseudozufallszahlengenerator	343
PuTTY	159
R	
Randomisieren, Anzahl	353
Randomisierung	334
RAR-Archiv verschlüsseln	44

Rechner sicher löschen.....343
 Registrierungseditor aufrufen251
 Registry Cleaner264
 Registry, Paßwort-Speicherung28
 Reserveblöcke auslesen.....335
 Router.....138, 192
 Router mit WLAN-Funktionalität.....139
 rsyslog.conf (Linux)273
 Rufnummernunterdrückung.....246

S

S/MIME.....160
 Schlafmodus deaktivieren (Linux)270
 Schlafmodusdatei löschen (Windows)254
 Schließzylinder17
 Schlüssel paßwortverschlüsseln167
 Schlüsselexport.....163
 Schlüssel-Fingerabdruck162
 Schlüssel-ID162
 Schlüssellänge162
 Schlüsselpaar.....161
 – erzeugen167
 Schlüsselserver.....163
 Schnittstellen deaktivieren53
 Schreib-/Lesetest.....349
 –, randomisierender.....354
 Schwarzes Brett243
 Scroogle157
 SD-Karte verschlüsseln90
 Seamonkey, Proxy-Einstellungen210
 Secure Eraser266
 SecureWipeDelete.....268, 348
 Sektor325
 Serververbindungen, verschlüsselte.....152
 Server-Zertifikat298
 Session-Cookie283, 291
 sftp153
 Shell terminieren52
 Shellerweiterungen63
 Shell-Konfigurationsdatei.....52
 shred, Optionen.....340
 Shutdown-Skript (Linux).....271
 Sicherungsdateien, automatisch löschen258
 SIM-Karte anonym kaufen.....245
 SIM-Karte registrieren.....242
 SIW.....336
 Skriptausführung verbieten302
 Skype.....149
 SMS-Pings.....246
 SOCKS-v5-Proxy195
 Spare Area.....334
 Sparse-Dateien/Images.....63, 80, 341
 Speicherblöcke, defekte auslesen335
 Speicherkarten, Dateien wiederherstellen333
 Speichersicherungsdatei.....251

Speicherzugriff, direkter.....53
 Spuren auf Windows249
 srm, Optionen.....340
 SRWare Iron, Proxy-Einstellungen207
 SSH159
 Standard-SMTP240
 Standby-Modus50, 254
 Standby-Modus (Linux)270
 Steganographie37
 Steghide.....37
 Stickware.....306
 Stromzufuhr unterbrechen55
 Suchmaschine, anonyme.....158, 214
 Suchmaschinen, verschlüsselnde157
 Surf-Verhalten analysieren.....300
 Swapdatei251
 Swapdatei, Größe einstellen.....251
 Swap-Partition, verschlüsselte120
 Switch (Netzwerk)138
 Sysinternal-Tools266
 Systemdateien (Windows) ändern250
 Systemdateien, versteckte anzeigen251
 Systemlaufwerk verschlüsseln111
 System-Logger (Linux)273
 Systempartition verschlüsseln.....107
 Systempartitionen, versteckte.....98

T

TACO.....301
 Tarnname erzeugen243
 TCP/IP, Antwortpakete192
 TCP/IP, Grundlagen.....191
 Telefonieren, abhörsicher146
 Telefonnummer, Auskunftssperre244
 Telefonnummer, Inverssuche.....244
 Temporärdateien löschen (Win.).....255
 Temporärdateien löschen (Linux).....271
 Temporärdateien verschlüsseln271
 Thunderbird, Absendedatum237
 Thunderbird, E-Mail verschlüsseln165
 Thunderbird, Speicherformat309
 Timeout50
 – auf Konsole/Shell einstellen.....51
 – einstellen.....50
 TMP/TEMP-Variablen (Windows)255
 T-Online, E-Mail-Speicherung.....309
 Tor Browser Bundle.....206
 Tor installieren.....195
 Torbutton.....196, 207, 296
 Tor-Netzwerk (The Onion Router)193f.
 Tor-Projekt, Bandbreitengraph212
 Tor-Projekt, Debian.....204
 Tor-Projekt, Download-Rate.....213
 Tor-Projekt, Fedora.....205
 Tor-Projekt, Firefox.....196

STICHWORTVERZEICHNIS

Tor-Projekt, Linux/Unix.....	199
Tor-Proxy.....	195
.torrent-Datei.....	224
Tor-Router anhalten.....	211
Tracker-Cookies.....	293, 302
TrueCrypt.....	73
– unter Linux.....	100
–, Abstreitbarkeit.....	73
–, äußerer/innerer Container.....	85
–, Fingerabdruck.....	80
–, Hash-Algorithmus.....	80
–, Ködersystem.....	94
–, Laufwerksbuchstaben ändern.....	92
–, Partit./Datenträger einbinden.....	93
–, portabler Modus.....	74
–, Rettungs-CD.....	94
–, Schlüsseldatei.....	81
–, Slot.....	101
–, USB-Stick/Karte verschlüsseln.....	90
–, Verschlüsselungsverfahren.....	78
–, versteckte Systempartitionen.....	98
TrueCrypt-Bootlader, spezieller.....	95
TrueCrypt-Bootmanager.....	77
TrueCrypt-Container.....	59
TrueCrypt-Container, versteckter.....	84
TrueCrypt-Containerdateien.....	76
TrueCrypt-Partitionen.....	90
TrueCrypt-Volumen.....	75
TrueCrypt-Dateien.....	77
Trust Center.....	161
Trusted Platform Module.....	22, 67
TweakUI.....	28, 50

U

Überflüssige Daten löschen.....	258
Überschreiben mit Null.....	332
Überschreibend löschen.....	332
Ubuntu verschlüsselt installieren.....	117
UMTS, Verschlüsselung.....	149
UMTS-Stick.....	195
Undelete Plus.....	330
UNetbootin.....	344
Universal-USB-Installer.....	318, 345
Urheberrecht.....	225
URL, typed (in Registry).....	284
USB-Distribution.....	319
USB-Geräte (Linux).....	317
USB-Stick formatieren.....	306
USB-Stick nicht automat. mounten.....	278
USB-Stick sicher löschen.....	343
USB-Stick verschlüsseln.....	74, 90
USB-Stick verstecken.....	20
USB-Stick, Betriebssystem auf.....	316
USB-Stick, booten von.....	345
USB-Stick, Dateisysteme.....	306

USB-Stick, Linux auf.....	344
USB-Treiber.....	317
USB-Versionen, Datenübertragungsgeschwindigkeit.....	317
useradd, userdel (Linux).....	277
UTC, Mailabsendedatum umrechnen in.....	237

V

Verschlüsseln.....	56
–, Datenverlust.....	164
Verschlüsselnde Filesharing-Netzwerke.....	227
Verschlüsselte Containerdatei.....	77
Verschlüsselte Datei, Header.....	58
Verschlüsselte Partition.....	77
Verschlüsselung, abstreitbare.....	57
Verschlüsselung, asymmetrische.....	161
Verschlüsselung, Risiken.....	56
Verschlüsselung, symmetrische.....	161
Vidalia-Bundle.....	196
Vidalia-Kontroll-Panel.....	211
Virenprüfprogramm.....	138
Virtual PC.....	126
Virtual Private Network.....	159
Virtualisierungslösungen.....	61
Virtuelle Maschine, CD brennen.....	96
Virtuelles verschlüsseltes Laufwerk.....	74
VoIP über VPN.....	248
Vollverschlüsselung (Definition).....	95
Vollverschlüsselung, Risiken.....	94
Volumen (Definition).....	75
Vorratsdatenspeicherung.....	137
Vorzeigebetriebssystem.....	281
Vorzeigekonto.....	280
VPN.....	221

W

Wear Leveling.....	333
– abschalten.....	334
Webadresse, Aufbau.....	302
Webbrowser, portabler.....	305
Webbrowser, Spuren.....	281
Web-Bugs.....	300, 302
Webmail.....	238
– verschlüsseln.....	170
Web-Proxy.....	193, 214
–, Opera.....	216
Webseiten-Filter.....	294
Webserver, vertrauenswürdiger/n. vertr.....	302
Wechseldatenträger, Aufteilung.....	327
Wechseldatenträger, Daten löschen.....	258
Wegwerf-Account.....	281
Wegwerf-E-Mail-Adresse.....	238
WEP-Verschlüsselung.....	140
Widerrufszertifikat.....	180
WinBuilder.....	107
Windows 64, Gerätetreiber.....	63

Windows Automated Installation Kit.....	107	WORM beschreiben	327
Windows installieren, Freischaltung.....	59	Wörterbuch-Attacke	25
Windows Mail, Speicherformat.....	309	WPA unter Linux	145
Windows virtualisieren, Lizenz.....	61	WPA unter Windows.....	142
Windows, Live-Rettungs-CD	107	WPA/WPA2-Verschlüsselung mit Pre-Shared Key..	140
Windows-Mobile-Emulator.....	126	WPA-Enterprise.....	140
Windows-Startpartition verschlüsseln.....	95	wpasupplicant	145
wipe	278, 339		
wipe, Optionen.....	343	Z	
Wise Registry Cleaner	264	Zertifikatsmanager GPA.....	170
WLAN.....	139	Zip-Archiv, verschlüsseltes.....	30, 41
–, Einbruch in.....	140	Zip-Bombe	134
–, Einwahl in offenes.....	194	Zufallszahlengenerator, überschreiben mit.....	272
WLAN-Basisstation.....	139	Zugangssicherung, physikal.	16
WLAN-Router	139, 194	Zwischendateien, Speicherort	255
WLAN-Verschlüsselung	140		