Robert Gödl

Anonym & sicher im Internet mit Linux

Der Praxiseinstieg für mehr Sicherheit und Datenschutz

mitp

Inhaltsverzeichnis

Einleitung 11

1 Anonym und sicher im Internet mit Linux 13
1.1 Warum sind Ihre Daten nicht sicher? 13
1.2 Wie und warum werden Daten gesammelt und Schadsoftware verbreitet? 13
1.2.1 Warum werden Daten im Internet gesammelt? 13
1.2.2 Wie werden Daten gesammelt? 15
1.2.3 Auswirkungen und Verwendung gesammelter Daten 17
1.2.4 Schadsoftware im Internet 17
1.3 Kann man sich anonym und sicher im Internet bewegen? 18
1.4 Linux als Betriebssystem und dessen Nutzung 18

Teil I Linux-Grundlagen 19

2 Linux Mint ausprobieren und installieren 21
2.1 Linux Mint herunterladen 21
2.2 Startmedium erstellen 22
2.2.1 ISOburn – bootfähige DVDs brennen 22
2.2.2 Etcher – bootfähige USB-Sticks erstellen 23
2.3 Den Computer vom Startmedium starten 23
2.4 Linux Mint ausprobieren 25
2.5 Linux Mint installieren 28
2.5.1 Partitionierung der Festplatte 30
2.5.2 Standort und Zeitzone 35
2.5.3 Benutzer anlegen und Installation abschließen 35

3 Linux Mint nutzen 37
3.1 Cinnamon – den Desktop kennenlernen 38
3.1.1 Erweiterte Desktop-Einstellungen unter Cinnamon 41
3.1.2 Nemo – der Dateimanager 44
3.1.3 Virtuelle Arbeitsflächen unter Cinnamon 45
3.2 Mate – der ressourcenschonende Desktop 46
3.2.1 Erweiterte Desktop-Einstellungen unter Mate 48
3.2.2 Caja – der Dateimanager unter Mate 50
3.2.3 Virtuelle Arbeitsflächen unter Mate 50

3.3 XFCE – ressourcenschonend und schnell 51
3.3.1 Erweiterte Desktop-Einstellungen unter XFCE 53
3.3.2 Thunar – der Dateimanager unter XFCE 54
3.3.3 Virtuelle Arbeitsflächen unter XFCE. 56
3.4 Andere Desktop-Umgebungen 57

4 Das System 59
4.1 Die Verzeichnis-Hierarchie – wo ist was zu finden?. 59
4.1.1 Das Home-Verzeichnis 62
4.1.2 Rechte an Ihren Daten – Gruppen 64
4.2 sudo – der Administrator unter Linux Mint 66
4.3 Das Terminal – die Kommandozeile 67
4.3.1 Der Aufbau des Terminals und Grundlagen 68
4.3.2 Ordner-Inhalte anzeigen und in der Verzeichnis-Hierarchie navigieren. 69
4.3.3 Welche Befehle für welche Aufgaben? – Hilfe am Terminal und Optionen 70
4.3.4 Arbeiten mit Dateien und Ordnern am Terminal 71
4.3.5 Kopieren und Einfügen am Terminal. 74
4.4 Drucker- und Scannertreiber 74

5 Software unter Linux Mint verwalten 77
5.1 Linux Mint aktuell halten 77
5.2 Software installieren und aktualisieren 79
5.2.1 Der Linux-Mint-Standard – Debian-Pakete (die Paket-Verwaltung) 79
5.2.2 Flatpak – noch mehr Software. 84
5.2.3 AppImages – ausführbare Dateien 85
5.2.4 PPAs – Software von Ubuntu- und Linux-Mint-Benutzern 85
5.2.5 Snap – der Ubuntu-Standard. 86
5.3 Wichtige Treiber installieren 89
5.4 Weitere Schriften installieren 90

6 Häufig genutzte Software und Alternativen zu Windows-Software 91
6.1 Dateimanager 91
6.1.1 Dolphin – der KDE-Dateimanager 92
6.1.2 Krusader – Funktionen ohne Ende 92
6.1.3 GNOME Commander – das Gegenstück zu Krusader 93
6.1.4 Midnight Commander (MC) – Dateimanager für das Terminal 94

6.2 Webbrowser 95
6.2.1 Firefox – der bekannte Webbrowser 95
6.2.2 Waterfox – ressourcenschonender Firefox 96
6.2.3 Vivaldi – der Nachfolger von Opera 96
6.2.4 Google Chrome 97
6.2.5 Microsoft Edge 98
6.3 Office 99
6.3.1 LibreOffice – der Standard unter Linux 99
6.3.2 FreeOffice und Softmaker Office 100
6.3.3 Onlyoffice – perfekt kompatibel 101
6.4 Bildbearbeitung 102
6.4.1 Gimp – die professionelle Bildbearbeitung 102
6.4.2 Darktable – RAW-Bildbearbeitung 104
6.4.3 digiKam – Bilder sammeln und organisieren 105
6.5 PDF-Editor 106

Teil II Anonym und sicher surfen mit Linux 107

7 Anonym im Internet 109
7.1 Anonyme Webbrowser 109
7.1.1 Den passenden Browser finden 109
7.1.2 Konqueror – der anonyme Webbrowser 111
7.2 Cookies – kleine Datenspeicher 116
7.2.1 Cookies von Drittanbietern unterbinden 118
7.2.2 Nervige Cookie-Meldungen blockieren 119
7.3 Zählpixel – unsichtbare Links 120
7.3.1 Zählpixel blocken 120
7.4 Skripte – Software zur Datensammlung 121
7.4.1 NoScript – Skripte auf Websites blockieren 121
7.5 AdBlocker / Werbeblocker – Blockieren von Werbung und Datensammlung 122
7.6 Tor Browser – viel Anonymität mit wenig Aufwand 123
7.7 OnionShare – anonym Dateien über das Internet teilen und chatten 126
7.8 Anonym chatten mit Jami 128
7.9 Rclone – verschlüsselte Backups in der Cloud 131
7.9.1 Unverschlüsselte Backups mit Rclone 131
7.9.2 Verschlüsselte Backups mit Rclone 134
7.9.3 Backups mit Rclone erstellen und aus der Cloud herunterladen 135
7.9.4 Bestehende Cloud-Zugänge mit Rclone bearbeiten, löschen und neue hinzufügen 138
7.10 Joplin – anonyme Notizen auf allen Geräten 139

8 Erweiterte Möglichkeiten für Anonymität im Internet 143
8.1 DNS-Server ändern 143
8.1.1 DNS-Server unter Linux ändern 144
8.1.2 DNS-Server am Router ändern 146
8.2 Firefox und die Telemetrie 146
8.3 Proxys zum Anonymisieren nutzen 148
8.4 Das Tor-Netzwerk für das komplette Betriebssystem nutzen 150
8.4.1 Tor als Client nutzen 151
8.4.2 SelekTor – den Tor-Endknoten wählen 152
8.5 Anonym im Internet suchen 155
8.5.1 YaCy installieren 156
8.5.2 YaCy nutzen 156
8.6 Virtuelle Maschinen 160
8.6.1 VirtualBox – einfach zu benutzen 160
8.6.2 Virt-Manager – schnell und performant 168

9 Daten verschlüsseln 179
9.1 Daten auf dem Computer verschlüsseln – verschlüsselte Container 179
9.1.1 zuluCrypt – für alle Desktop-Umgebungen und USB-Sticks/externe Festplatten 179
9.1.2 Plasma Vault – verschlüsselte Container unter KDE 183
9.2 Linux-Distribution verschlüsseln 184
9.2.1 Warum verschlüsselt man ein komplettes Betriebssystem? 184
9.2.2 Auf verschlüsselte Linux-Distributionen zugreifen 185
9.2.3 Verschlüsseltes Linux automatisch per TPM-Chip entschlüsseln 188
9.3 E-Mails verschlüsseln und signieren 191
9.3.1 Wie funktionieren GPG und PGP? 192
9.3.2 GPG-Schlüssel unter Linux erstellen 193
9.3.3 E-Mails verschlüsseln 197
9.3.4 E-Mails signieren 202
9.4 Steghide und Stegosuite – Dateien in anderen Dateien verstecken 203
9.4.1 Steghide installieren und nutzen 203
9.4.2 Stegosuite installieren und nutzen 206

10 Die anonyme Cloud mit Nextcloud 207
10.1 Was wird für Nextcloud benötigt? 207
10.2 Eine statische IP-Adresse für Ihren Router 207
10.2.1 Wie funktioniert dynamisches DNS? 208
10.2.2 DynDNS einrichten 208

10.3 Nextcloud installieren 210
10.3.1 Nextcloud via Docker oder Podman installieren 210
10.3.2 Nextcloud direkt installieren 211
10.4 Einführung in Nextcloud 214

11 Sicherheit allgemein 217
11.1 Grundlagen zur Sicherheit 217
11.1.1 Nutzen Sie nur Software aus sicheren Quellen 217
11.1.2 Prüfen Sie Terminal-Befehle und Skripts 218
11.1.3 Vorsicht vor gefälschten Systemmeldungen 219
11.2 Passwort- und Account-Sicherheit 219
11.2.1 Sichere Passwörter erstellen 219
11.2.2 Passwort-Manager / Passwort-Safes 221
11.2.3 Zwei-Faktor-Authentifizierung unter Linux. 226
11.3 Mehr Zeit ohne Spam – mehr Sicherheit ohne Phishing 227
11.3.1 Spamassassin in Thunderbird integrieren. 229
11.3.2 Spamassassin in Evolution integrieren. 230
11.3.3 Spamassassin in Kmail integrieren 231
11.4 Lynis – die Sicherheit von Linux prüfen 233
11.5 Sicherheitslücken von jedem Betriebssystem, jeder Software und jeder Hardware finden. 235
11.6 VPN – Virtual Private Network. 238
11.6.1 Die Funktionsweise von VPN 239
11.6.2 VPN einrichten 240

12 Firewall und Virenscanner 245
12.1 Die Firewall 245
12.1.1 GUFW – die grafische und einfach zu nutzende Firewall 248
12.1.2 Konfiguration der Firewall mit UFW am Terminal. 251
12.1.3 Firewalld – die Firewall unter Fedora und anderen Linux-Distributionen 254
12.1.4 OpenSnitch – die softwarebasierte Firewall unter Linux . . . 257
12.1.5 Portmaster – »nach Hause telefonieren« unter Linux unterbinden 259
12.2 Virenscanner unter Linux. 262
12.2.1 ClamAV auf dem Terminal nutzen. 263
12.2.2 ClamTK – Suche nach Schadsoftware mit grafischer Oberfläche. 265
12.2.3 Andere Virenscanner für Linux. 266
12.3 Firejail – Software unter Linux in die Sandbox sperren 267
12.3.1 Firejail nutzen. 268

12.3.2 Firetools nutzen 272
12.4 AppArmor –Berechtigungen für Software vergeben 274
12.4.1 Voraussetzungen schaffen 274
12.4.2 AppArmor anpassen 276
12.4.3 Eigene Profile für AppArmor erstellen 278

13 Tails – Das anonyme und sichere Betriebssystem 283
13.1 Vor- und Nachteile der Arten der Installation 283
13.2 Installation auf USB-Stick 284
13.3 Brennen auf DVD 286
13.3.1 Unter KDE Plasma 286
13.3.2 Unter Cinnamon und GNOME 287
13.3.3 Unter XFCE 288
13.4 Tails starten und nutzen 290

Weiterführende Webseiten 295

Stichwortverzeichnis 297

Einleitung

Das Internet ist heute nicht mehr nur ein Medium, in dem Sie Informationen finden, mit anderen kommunizieren können und das Ihnen Unterhaltung bietet, sondern auch ein Medium, mit dem Daten über Sie gesammelt werden.

Mit Ihren Daten verdienen Unternehmen Geld – aber nicht nur Unternehmen, sondern auch Betrüger und Datendiebe. Glauben Sie mir, Aussagen wie »ich habe nichts zu verbergen« sollten Sie sich zweimal überlegen.

Manche meinen, auf ein wenig Anonymität zu achten, sei umständlich, zeitaufwendig und vielleicht auch schwierig. Dies ist aber eigentlich gar nicht der Fall – es kommt nur darauf an, wie weit Sie gehen wollen. Manche Gegenmaßnahmen erfordern gerade einmal ein paar Mausklicks wie etwa die Nutzung anonymisierender Webbrowser-Erweiterungen (diese haben unter jedem Betriebssystem einen Nutzen). Etwas weiter gehen Sie schon mit der Nutzung von Linux, denn dieses Betriebssystem sendet keine Daten an seine Hersteller und erschwert es auch sonstigen Datensammlern, an Ihre Daten zu kommen. Ebenfalls ist Malware unter Linux noch immer kein Thema, über das man wirklich sprechen muss – solche gibt es einfach nicht (auch, wenn manche das Gegenteil behaupten).

Es gibt natürlich auch etwas tiefer gehende Themen, mit denen Sie Ihre Daten schützen können – solche erfordern zwar meist zu Beginn etwas an Einarbeitung, vielleicht auch an Konfiguration von Software, anschließend genügt aber meist ein Mausklick, um mehr Anonymität zu erzielen und natürlich auch höhere Sicherheit zu haben.

Dieses Buch bietet Ihnen folgende Themen:

- **Linux Mint installieren und nutzen** – Linux bietet Ihnen schon von Grund auf ein gewisses Maß an Anonymität. In diesem Buch wird die Installation von Linux Mint einfach und detailliert beschrieben. Linux Mint wurde gewählt, weil es sich hierbei um eine sehr einfach zu installierende und zu nutzende Linux-Distribution handelt. Mit dieser Anleitung lassen sich aber auch viele andere Linux-Distributionen installieren wie etwa Ubuntu, Kubuntu, Linux MX, Manjaro und viele mehr.
- **Linux-Grundlagen** – Sie lesen in diesem Buch, wie Sie Linux nutzen – also etwa, welche grafischen Oberflächen (Desktop-Umgebungen) es gibt, deren Unterschiede und welche Software Sie nutzen, um Ihre Dateien zu verwalten,

und wie Sie weitere Software installieren und das System aktuell halten. Auch hier lassen sich viele Dinge auf andere Distributionen problemlos übertragen.

- **Einfache Wege zur Anonymität** – Sie lesen mehr über einfache Mittel, um mehr Anonymität im Internet zu erlangen. Oft genügen hier ein paar Mausklicks und Sie benötigen keine speziellen Kenntnisse.
- **Erweiterte Wege zur Anonymität** – Mehr Anonymität bekommen Sie natürlich, indem Sie weiteres Wissen ansammeln, entsprechende Software nutzen und diese anpassen. Dieses Buch bietet Ihnen alles, was Sie dafür brauchen.
- **E-Mails verschlüsseln** – Sie lesen hier, wie die Verschlüsselung von E-Mails funktioniert. Es gibt noch immer Benutzer, die meinen, E-Mails zu verschlüsseln wäre schwierig und umständlich, dabei genügen wenige Mausklicks.
- **Die private Cloud** – Mit einer Software wie Nextcloud benötigen Sie keine Cloud-Anbieter wie Google, Amazon oder Microsoft mehr. Damit können Sie selbst kleine Communities mit Bekannten aufbauen sowie Bilder und vieles mehr mit diesen teilen.
- **Sicherheit** – Neben der Anonymität bietet Ihnen dieses Buch auch einen Einstieg in die Sicherheit. Linux ist zwar schon von Grund auf sicherer als etwa Windows – gerade auf einem Laptop, mit denen Sie etwa auch öffentliche Netzwerke nutzen –, Sie sollten jedoch etwa die Firewall aktivieren. Ebenso können Sie unter Linux Virenscanner und ähnliche Software nutzen.
- **Tails** – Tails bietet Ihnen Anonymität und Sicherheit ohne Vorwissen. Es handelt sich hierbei um ein Betriebssystem, das jede Kommunikation über das Internet anonymisiert und als Live-System und durch weitere Technologien im Hintergrund natürlich auch Sicherheit bietet.
- **Weiteres** – Darüber hinaus finden Sie in diesem Buch zusätzlich viele weitere Tipps rund um die Anonymität und Sicherheit im Internet.

Das Buch ist so konzipiert, dass Sie es von vorne bis hinten durcharbeiten können, um einen umfassenden Einstieg in Linux als Betriebssystem und die möglichen Maßnahmen für mehr Anonymität und Sicherheit im Internet zu erhalten. Das detaillierte Inhaltsverzeichnis sowie das Stichwortverzeichnis am Ende des Buches ermöglichen es Ihnen darüber hinaus, die Themen, die Sie besonders interessieren, gezielt anzuspringen oder später erneut nachzuschlagen.

Nach der Lektüre sind Sie nicht nur darüber informiert, in welchen Situationen Sie besonders auf die Sicherheit Ihrer Daten achten sollten, sondern können auch einfache und fortgeschrittene Methoden für mehr Anonymität und Sicherheit praktisch umsetzen.

Kapitel 1

Anonym und sicher im Internet mit Linux

1.1 Warum sind Ihre Daten nicht sicher?

Während der Entstehung des Internets (etwa 1981 bis 1983) und dem anschließenden Aufbau dieses weltweiten Netzwerks stand vor allem der Austausch von Informationen im Vordergrund. So wurden etwa Daten vom Kernforschungszentrum CERN in der Schweiz an die Wissenschaftler rund um die Welt verteilt.

Später (ca. ab 1990) wurden auch immer mehr private Webseiten im Internet veröffentlicht. Meist teilte man so seine Hobbys oder Vereine verbreiteten damit ihre Termine für Treffen und andere Informationen. Langsam haben auch erste Unternehmen damit begonnen, sich über kleinere Webseiten zu bewerben. Auch erste Suchmaschinen traten zu dieser Zeit im Internet auf, um Benutzern das Durchsuchen des wachsenden Inhalts des Internets zu ermöglichen.

Als immer mehr Benutzer Zugang zum Internet bekamen (etwa um das Jahr 2000 herum), sind auch die kommerziellen Interessen um dieses Netzwerk gewachsen. Soziale Medien verbreiteten sich und immer mehr Unternehmen erkannten, mit dem Internet lässt sich auch Geschäft machen – etwa, indem man seine Waren darin zum Verkauf anbietet, oder mit Werbung. Heute stehen auch die Daten der Benutzer des Internets im kommerziellen Interesse. Was man mit diesen Daten so anfangen kann, ist nicht ohne.

Über diesen ganzen Zeitraum bis heute ist nicht nur das kommerzielle Interesse an Daten der Benutzer gewachsen, sondern auch daran, mit illegalen Methoden an diese zu gelangen – so hat sich auch die Entwicklung von Schadsoftware geändert. Zu Beginn ging es den Entwicklern darum, zu zeigen, was sie können oder einfach nur Schaden anzurichten. Heute geht es bei der Entwicklung solcher Software auch um kommerzielle Interessen.

1.2 Wie und warum werden Daten gesammelt und Schadsoftware verbreitet?

1.2.1 Warum werden Daten im Internet gesammelt?

Ich betreibe selbst eine kleine Webseite (mehr dazu am Ende des Buches) rund um Linux und freie Software – ich gebe es gleich zu, auch ich sammle Daten. Ich

sammle Daten über die Leser meiner Webseite, weil mich interessiert, welche Beiträge gerne gelesen werden und welche wiederum nicht. Verstehe ich, welche Themen meine Besucher interessieren, weiß ich auch, über welche Themen ich mehr schreiben kann. Kommerzielles Interesse habe ich beim Sammeln der Daten nicht, ich will Benutzern Linux zeigen, es ihnen schmackhaft machen und erklären, wie man damit arbeitet.

Aber die meisten Webseiten (es gibt natürlich Ausnahmen), die Sie im Internet finden, bieten Ihnen Informationen nicht an, weil sie so großzügig sind. Einfach ausgedrückt steckt kommerzielles Interesse dahinter. Nur selten will jemand kostenlos Informationen anbieten.

Um dies näher zu erklären, nehme ich jetzt wieder meine Webseite rund um Linux als Beispiel. Ich sammle folgende Daten:

- **Welche Artikel werden gelesen und wie häufig?**
- **Welches Betriebssystem wird genutzt?**
- **Welcher Webbrowser wird genutzt und welche Version der Software?**
- **Aus welchem Land kommt der Leser, aus welcher Region und aus welcher Stadt?**
- **Kommt der Leser wieder?**
- **Auf welche Links auf der Webseite klickt der Leser?**
- **Von welcher Webseite kommt der Leser oder welche Suchmaschine hat er genutzt?**

Mit diesen Daten könnte man mit kommerziellem Interesse schon etwas anfangen. Würde ich Werbung machen, könnte ich etwa einem Software-Hersteller anbieten, Werbung für eine Software zu machen, wenn darüber auf meiner Webseite viel gelesen wird. Würde Werbung angezeigt, die meine Leser überhaupt nicht interessiert, würden sie schnell darüber hinwegscrollen, Werbung hingegen, für deren Produkt man sich interessiert, wird natürlich eher angeklickt. Dies ist aber sehr vereinfacht ausgedrückt.

Nehmen wir einmal diverse Online-Medien – ganz egal ob es sich um Nachrichten-Portale handelt, um Webseiten, die Wissen anbieten, oder um soziale Medien. Die meisten Webseiten sammeln Daten nicht einmal selbst, sondern deren Betreiber bieten anderen (etwa Werbetreibenden oder Datensammlern, die Daten an andere weiterverkaufen) an, Daten über ihre Leser zu sammeln. Auf einer Webseite können sich so oft mehrere Datensammler versammeln, die auf eigene Interessen aus sind.

Je mehr Daten über einen Internet-Benutzer gesammelt werden, desto mehr lässt sich daraus über dessen Interessen herausfinden, und je mehr man über einen Benutzer weiß, desto mehr Geld lässt sich mit diesen Daten verdienen. Die meisten Datensammler interessieren sich nicht einmal selbst für die gesammelten Daten, sondern verkaufen diese wieder an andere Unternehmen.

1.2.2 Wie werden Daten gesammelt?

Die Möglichkeiten zum Sammeln von Daten sind schier unendlich – so gibt es etwa Software, die im Hintergrund einer Webseite arbeitet, ohne dass Sie etwas davon mitbekommen. Eine solche Software wäre etwa Matomo (kostenlose *Webseiten-Analyse*). Ist diese Software auf einem Webserver installiert und Sie rufen eine überwachte Webseite auf, zeigt diese folgende Daten (nur ein kurzer Auszug):

- Ihr genutztes Betriebssystem und dessen Version
- Ihren genutzten Webbrowser und dessen Version, im Webbrowser installierte Erweiterungen (Add-ons)
- Welchen Computer Sie benutzen
- Welche Webseite Sie sich ansehen und wie lange, welche Bilder Sie angeklickt haben
- Auf welche Links Sie klicken, von welcher Webseite Sie kommen (etwa, wenn Sie auf einen Link geklickt haben, um auf die Webseite zu kommen)
- Welche Suchmaschine Sie genutzt haben, um die Webseite zu finden, mit welchen Begriffen Sie gesucht haben
- Ihre aktuelle IP-Adresse, diese zeigt auch, in welchem Land, in welcher Region und in welcher Stadt Sie gerade sind
- Wie oft Sie wiederkommen

Wie schon beschrieben – dies war nur ein kurzer Auszug. In der Abbildung sehen Sie die Übersichtsseite dieser Software:

Matomo ist nicht die einzige Software dieser Art, es gibt viele.

Neben Webseiten-Analyse-Software gibt es zahlreiche Möglichkeiten, Ihre Daten zu sammeln:

- **Cookies:** Hierbei handelt es sich um kleine Textdateien, die auf Ihrem Computer gespeichert werden. Vor zwei Jahrzehnten hatten diese Cookies nur eine sinnvolle Funktion: Besuchten Sie eine Webseite, meldeten sich dort an und nahmen Einstellungen vor, haben diese Cookies diese Einstellungen gespeichert. Heute dienen sie dazu, Ihren Weg durch das Internet zu verfolgen – haben Sie etwa einen Account bei Facebook (Google, Yahoo ...) und Sie besuchen eine Webseite, die entsprechend angepasst wurde, weiß Facebook, Sie sind gerade auf dieser Webseite.
- Von anderen Webseiten **verlinkte Bilder:** Nicht immer sind die Bilder einer Webseite auf demselben Webserver gespeichert wie die eigentliche Webseite, die Sie gerade ansehen. Öffnen Sie eine Webseite mit einem solchen verlinkten Bild, bekommt auch der Server, auf dem das Bild eigentlich gespeichert ist, alle Daten.

- **Zähl-Pixel** sind nicht sichtbar. Hierbei handelt es sich um kleine Grafiken, meist ein Pixel groß. Diese können in den Hintergrund der Webseite eingearbeitet sein, ohne dass Sie sie sehen können, und wirken so wie die im letzten Absatz beschriebenen verlinkten Bilder.
- Ihr **Internet-Anbieter** sieht alles, was Sie im Internet tun. Über dessen System läuft Ihre komplette Kommunikation im Internet. Jeden Klick, den Sie auf einer Webseite vornehmen – Ihr Internet-Anbieter bekommt es mit.
- **E-Mails** sind reiner Text. Eine E-Mail läuft über mehrere sogenannte Mail-Server, bevor sie beim Empfänger ankommt. Jeder, der zu einem solchen Mail-Server Zugang hat, kann Ihre E-Mails lesen und sie, wenn er es möchte, auch verändern, ohne dass der Empfänger der E-Mail etwas davon mitbekommt.

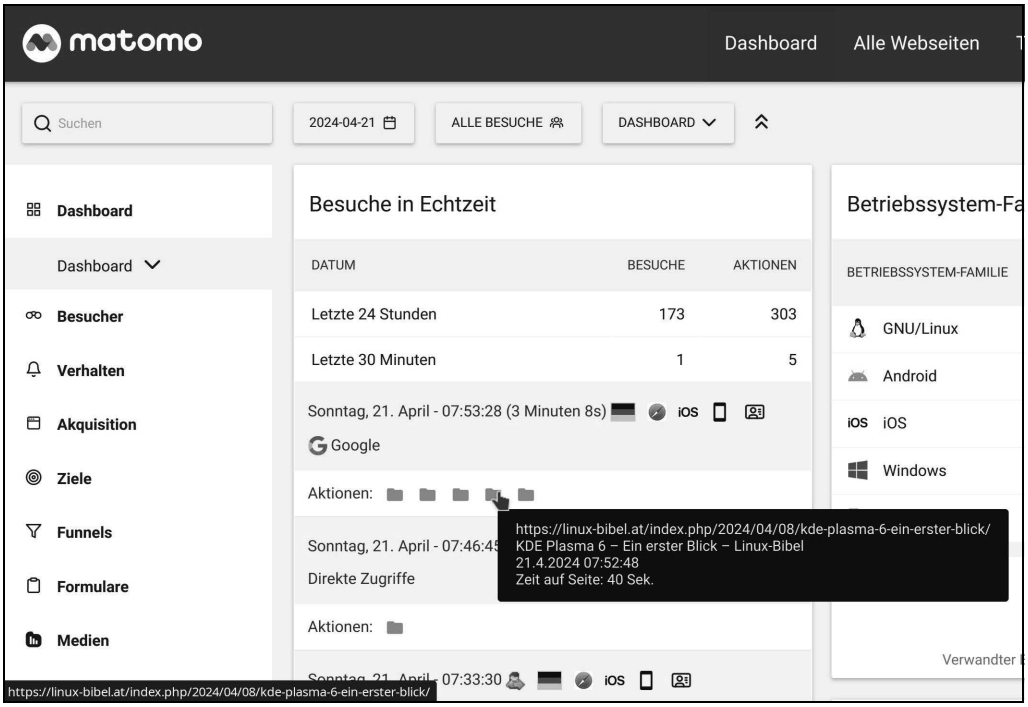

Abb. 1.1: Matomo – Webseiten-Analyse

- **Messenger** sind heute so gut wie auf jedem Computer installiert. Facebook-Messenger, WhatsApp ... Es gibt Messenger ohne Ende. So manche sammeln auch Daten über Sie.
- Ihr genutztes **Betriebssystem** – bis auf Linux sammeln die meisten Betriebssysteme Daten über Sie. Das Betriebssystem ist Ihnen sehr nahe und kommt so natürlich am einfachsten an Daten über Sie.

- Ihr genutzter **Webbrowser** ist natürlich der einfachste Weg, um an Daten über Ihre Aktivitäten im Internet zu kommen.

1.2.3 Auswirkungen und Verwendung gesammelter Daten

Die meisten gesammelten Daten dienen vor allem den kommerziellen Interessen von Unternehmen. Meist geht es darum, aus den gesammelten Daten Profile für einzelne Benutzer zu erstellen, und aus den gesammelten Daten lassen sich ausgezeichnete Profile erstellen. Was gefällt einem Benutzer, was braucht er, was will er? Im besten Fall wird Ihnen entsprechende Werbung auf Webseiten geliefert, beim Suchen über Suchmaschinen oder per E-Mail, SMS oder diverse Messenger.

Aber natürlich sammelt auch der Staat Daten über die Internet-Benutzer. Im schlechtesten Fall könnte man unverschuldet in unangenehme Situationen kommen. Nur ein paar sehr einfache Beispiele: Sie suchen nach einer Software und landen auf einer Webseite, die solche illegal anbietet. Sie suchen nach Informationen und landen auf einer Webseite, die solche ebenfalls illegal anbietet oder von Extremisten (welcher Art auch immer) gerne besucht wird. Hierdurch könnten Sie schneller mit dem Gesetz in Konflikt geraten, als Ihnen lieb ist.

Immer wieder lese ich bei entsprechenden Diskussionen den Satz: »Ich habe nichts zu verbergen.« Mit solchen Aussagen sollte man vorsichtig sein. Achten Sie auf ein wenig Anonymität im Internet, ist im einfachsten Fall zumindest der E-Mail-Account nicht mit Werbung vollgespammt und Ihre Internet-Besuche mit weniger nerviger Werbung belastet.

1.2.4 Schadsoftware im Internet

Vor etwa zwei bis drei Jahrzehnten diente Schadsoftware vor allem dem Zweck, Daten zu vernichten. Böswillige Menschen wollten zeigen, was sie können. In dieser Zeit reichte oft ein Backup, um Betriebssystem und Daten wiederherzustellen.

Heute dient Schadsoftware meist demselben Zweck wie das Sammeln von Daten – dem kommerziellen Interesse. Man will Daten von anderen entwenden, um sich daran zu bereichern –, oder man nimmt dem eigentlichen Besitzer von Daten den Zugang dazu. Etwa, indem man dem Besitzer eine Schadsoftware (Ransomware) unterjubelt, die die Daten verschlüsselt, und erst nach der Bezahlung bekommt er wieder die Möglichkeit, an die Daten zu kommen (oder auch nicht).

An solche Schadsoftware gelangt man heute über verschiedene Wege, auch unter Linux, insbesondere indem man über unsichere Quellen Software bezieht oder auch sonst zu unvorsichtig ist. In diesem Buch lesen Sie unter anderem, wie Sie solche Situationen vermeiden.

1.3 Kann man sich anonym und sicher im Internet bewegen?

Grundsätzlich: ja und nein. Vor zwei Jahrzehnten war es einfacher, heute muss man sich schon etwas informieren und auch reagieren.

Die Methoden, wie Unternehmen an Ihre Daten kommen und Menschen mit böswilligen Absichten Ihnen Schadsoftware unterjubeln, werden immer ausgefeilter. Gegen manche Dinge kann man sich recht einfach wehren, bei anderen muss man sich etwas mehr anstrengen und auch etwas Zeit investieren.

In diesem Buch werden Sie lesen, mit welchen Methoden man an Ihre Daten kommen will und auch warum, aber natürlich auch, wie Sie dagegen vorgehen können. Ebenso werden Sie erfahren, was Sie gegen die immer weiter wachsende Gefahr durch Schadsoftware unternehmen können.

1.4 Linux als Betriebssystem und dessen Nutzung

Linux ist nicht nur gegen Schadsoftware resistenter als Windows, sondern auch gegen das Sammeln von Daten über das Internet. Linux ist heute sehr einfach zu installieren, zu konfigurieren und zu nutzen. Viel der bekannten Software, die Sie unter Windows oder macOS nutzen, lässt sich auch unter Linux verwenden – meist ohne Einschränkungen.

Linux Mint ist gerade für Linux-Einsteiger ohne große Computer-Kenntnisse sehr interessant – aus diesem Grund wird diese Linux-Distribution in diesem Buch genutzt (die meisten Beschreibungen werden sich jedoch auch auf anderen Linux-Distributionen problemlos umsetzen lassen).

Sie werden lesen, wie Sie Linux Mint installieren, an Ihre Bedürfnisse anpassen und nutzen, und natürlich auch, wie Sie damit, so gut es geht, sicher und anonym im Internet unterwegs sind. Nach der Installation von Linux Mint wird das Thema »anonym und sicher im Internet« vor allem unter auf Debian basierenden Linux-Distributionen, also auch unter Linux Mint, Ubuntu, Kubuntu und vielen Distributionen mehr beschrieben.

Kapitel 2

Linux Mint ausprobieren und installieren

In diesem Kapitel lesen Sie, wie Sie ein startfähiges Medium (DVD oder USB-Stick) erstellen, um Linux Mint auf Ihrem Computer auszuprobieren oder auch zu installieren. Auch lernen Sie die verschiedenen Varianten von Linux Mint kennen: mit anderen grafischen Oberflächen oder anderer vorinstallierter Software. Sie erfahren, welche Möglichkeiten Sie im sogenannten *Live-System* haben und natürlich, wie Sie Linux Mint installieren.

2.1 Linux Mint herunterladen

In diesem Buch wird Linux Mint als Betriebssystem genutzt. Es ist vor allem unter Linux-Einsteigern sehr beliebt, da diese Linux-Distribution sehr einfach zu installieren und zu nutzen ist. Linux Mint basiert auf Ubuntu und Ubuntu wiederum auf Debian – Sie können also alle Tipps in diesem Buch unter allen auf Debian basierenden Linux-Distributionen direkt übernehmen (Debian, Ubuntu, Mint, Pop!_OS, Linux MX, Zorin und viele mehr). Unter anderen Linux-Distributionen können Software-Pakete, die Sie direkt über die Paket-Verwaltung installieren, geringfügig anders heißen.

Sie finden Linux Mint unter `https://www.linuxmint.com/download.php` kostenlos zum Download in folgenden Konfigurationen (die Unterschiede liegen nur in der Benutzeroberfläche bzw. der grafischen Desktop-Umgebung. Im Gegensatz zu Windows gibt es für Linux unterschiedliche Desktops):

- **Cinnamon Edition** – Der Standard-Desktop unter Linux Mint, sehr modern und für Umsteiger von Windows sehr einfach zu bedienen. Mindestens 4 GB RAM, besser aber 8 GB RAM sollten im Computer eingebaut sein.
- **Cinnamon Edition – Edge ISO** – Dasselbe wie die zuvor beschriebe Version, jedoch mit aktuellerem Kernel – sollte auch mit gerade im Handel erschienenen (also sehr aktuellen Computern) zurechtkommen.
- **XFCE Edition** – Für ältere Computer gedacht, kommt also auch mit schwächerer Hardware problemlos klar. Mindestens 4 GB RAM sollten im Computer eingebaut sein. Ebenso sehr einfach zu nutzen, Umsteiger von Windows sollten problemlos damit umgehen können. Auch bietet XFCE sehr viele Einstellungen, mit denen man sich den Desktop an seine Bedürfnisse anpassen kann.

- **Mate Edition** – Für alte Computer gedacht, mindestens 2 GB RAM sollten in Computer eingebaut sein, besser natürlich 4 GB. Dieser Desktop ist ohne große Umstellung von Umsteigern einfach zu benutzen, auch wenn die grafische Oberfläche zunächst etwas ungewohnt erscheinen mag.

2.2 Startmedium erstellen

Linux Mint lässt sich nicht so einfach unter Microsoft Windows oder macOS installieren, da es sich dabei nicht um eine gewöhnliche Software, sondern um ein Betriebssystem handelt. Sie erhalten beim Download eine sogenannte »ISO-Datei« – diese brennen Sie etwa bootfähig auf eine DVD oder kopieren sie bootfähig auf einen USB-Stick und starten in beiden Fällen den Rechner von diesem erstellten Medium aus.Bootfähig bedeutet, der Computer muss davon starten können, das heißt, er muss die nötigen Dateien an bestimmten Orten vorfinden. Sie können die Datei also nicht einfach wie ein Video auf eine DVD brennen oder die Datei nicht einfach auf den USB-Stick verschieben. Hierfür ist eine Software nötig, die dies passend erledigt.

2.2.1 ISOburn – bootfähige DVDs brennen

ISOburn ist eine kostenlose Software für Microsoft Windows – damit lassen sich ISO-Images schnell und einfach bootfähig auf DVDs brennen. Sie finden diese Software unter `https://isoburn.org/` zum Download (siehe Abbildung 2.1).

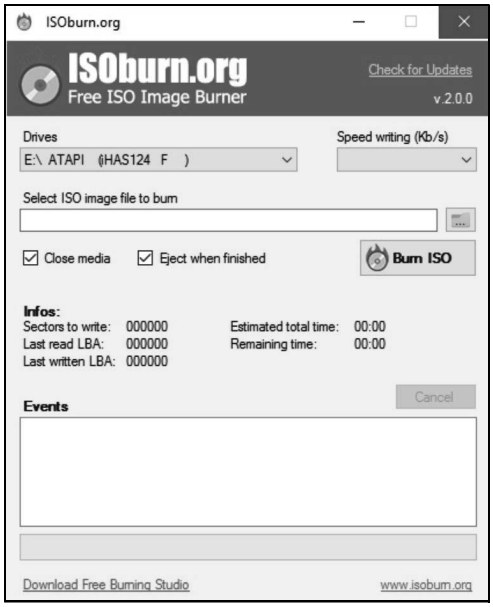

Abb. 2.1: ISOburn – ISO-Images bootfähig auf DVDs brennen

Mit dem Schalter DRIVES geben Sie das Laufwerk an, mit dem Sie die DVD brennen wollen, und mit SELECT ISO IMAGE FILE TO BURN wählen Sie die zu brennende ISO-Datei. Alle anderen Einstellungen können Sie belassen, wie sie sind – anschließend klicken Sie auf den Schalter BURN ISO.

2.2.2 Etcher – bootfähige USB-Sticks erstellen

Mit der Software Etcher lassen sich per Mausklick bootfähige USB-Sticks erstellen. Sie finden diese kostenlose Software unter `https://www.balena.io/etcher/` für Windows, macOS und Linux zum Download (Abbildung 2.2).

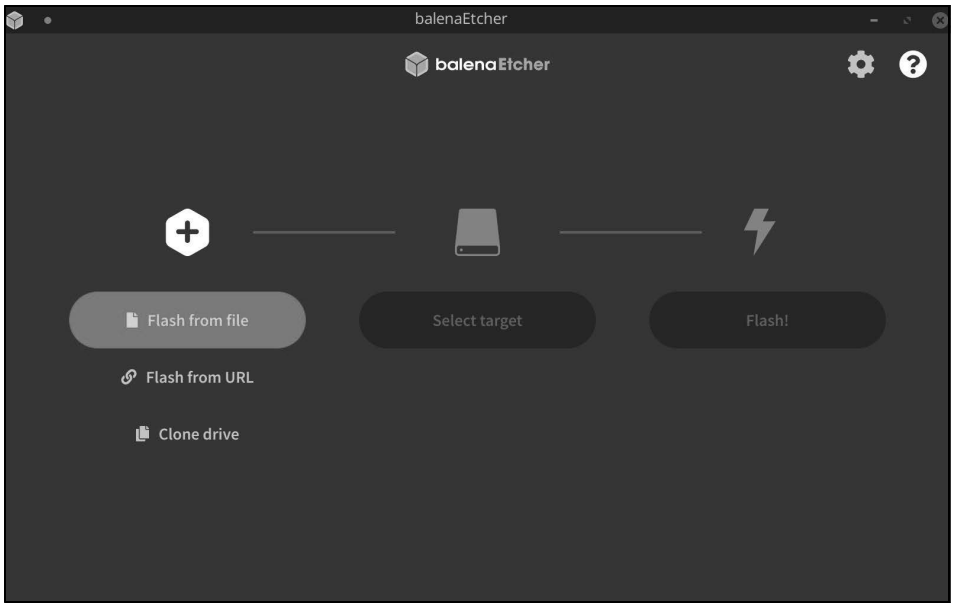

Abb. 2.2: Etcher – bootfähige USB-Sticks erstellen

Mit dem Schalter FLASH FROM FILE wählen Sie die heruntergeladene ISO-Datei aus, dann geben Sie mit SELECT TARGET den angeschlossenen USB-Stick an und starten den Vorgang mit FLASH!.

2.3 Den Computer vom Startmedium starten

Bei Linux Mint handelt es sich um ein installierbares Live-System. Dies bedeutet, Sie müssen Linux Mint nicht installieren, sondern können es vor der Installation auch nur ausprobieren. Solange Sie es nicht installieren, wird am Computer nichts geändert.

In der Grundkonfiguration startet meist auch mit eingelegter Linux-Mint-DVD oder angeschlossenem Linux-Mint-USB-Stick trotzdem das bereits installierte Windows. Dies können Sie auf älteren Computern im BIOS und auf aktuelleren Computern im UEFI ändern. Hierbei handelt es sich um die grundlegende Firmware des Computers. In diese gelangen Sie je nach Computer-Hersteller mit einer der folgenden Tasten: F2, F10, F12 oder Entf – in der Beschreibung des Herstellers finden Sie nähere Informationen. Die passende Taste drücken Sie bei Start des Computers mehrmals schnell hintereinander, bis Sie das Fenster der Firmware sehen. In Abbildung 2.3 sehen Sie eine mögliche BIOS-Variante.

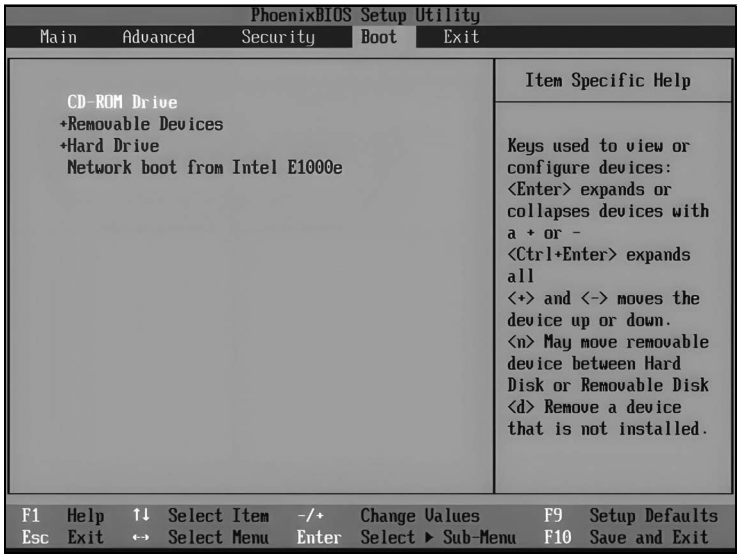

Abb. 2.3: BIOS – das Bootmenü

Im BIOS nutzen Sie die Pfeiltasten zur Navigation, mit den Pfeiltasten links und rechts wechseln Sie zwischen den Menüeinträgen. Zur Auswahl einer Funktion nutzen Sie die Pfeiltasten auf und ab. Sie benötigen zur Auswahl des Datenträgers für den Start mit Ubuntu das Menü BOOT. Als Erstes markieren Sie mit den Pfeiltasten den DVD- oder USB-Eintrag – mit den Tasten F5 und F6, je nach Hersteller auch + und -, verschieben Sie den Eintrag ganz nach oben (Informationen zu den Tasten finden Sie ganz rechts).

Das UEFI ist meist etwas moderner aufgebaut (siehe Abbildung 2.4).

Nicht immer, aber im UEFI der meisten Hersteller können Sie die Maus statt der Tasten nutzen. Ist dies nicht so, nutzen Sie wie im BIOS die Pfeiltasten. Wie im BIOS finden Sie auch im UEFI einen Menüeintrag namens BOOT. Öffnen Sie diesen und setzen Sie das Startmenü an die oberste Stelle.

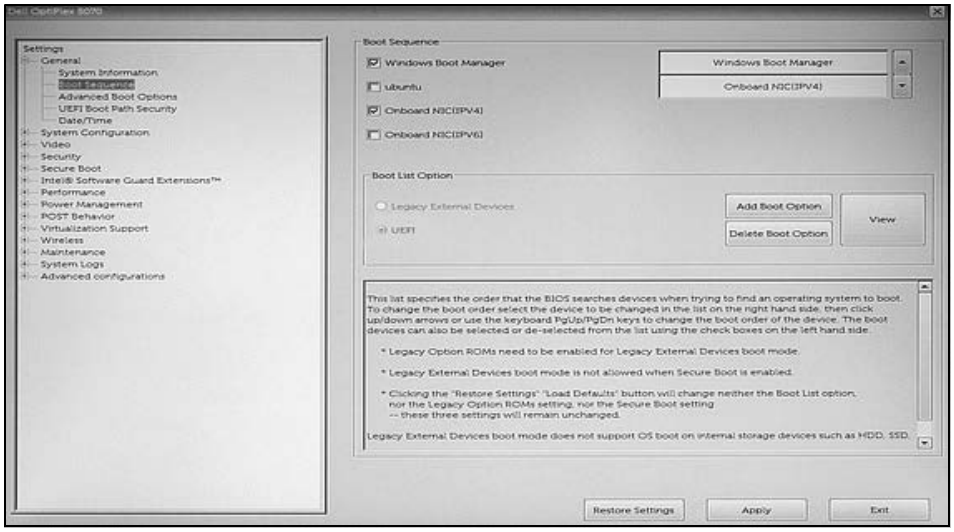

Abb. 2.4: UEFI

Egal, ob im BIOS oder im UEFI – Sie sollten die Option FAST BOOT suchen und deaktivieren. Je nach Hersteller findet sich die Option in einem anderen Menü. SECURE BOOT zu deaktivieren, ist in den meisten Fällen heute nicht mehr nötig – dies tun Sie nur, wenn sich Ubuntu nicht starten lässt.

Zuletzt übernehmen Sie die Einstellungen mit einem Klick auf den Schalter APPLY oder SAVE AND EXIT – im BIOS dient dazu meist die Taste F10. Der Computer startet neu vom ausgewählten Startmedium.

2.4 Linux Mint ausprobieren

Wie zuvor schon kurz angeschnitten, handelt es sich bei Linux Mint um ein Live-System. Es läuft komplett im Arbeitsspeicher des Computers. Sie können das System und die vorinstallierte Software ausprobieren, Einstellungen vornehmen, Dateien erstellen oder im Internet surfen. Auch die eingebaute und angeschlossene Hardware lässt sich testen. Bevor Sie das System installieren, wird am bereits installierten System nichts geändert. Starten Sie den Rechner ohne das Linux Mint-Startmedium neu, startet wieder das installierte Windows oder macOS.

Startet Linux Mint, sehen Sie zu Beginn das Logo der Distribution. Das System startet normalerweise ohne Meldungen. Von einem USB-Stick sollte das System innerhalb einer Minute starten, mit DVD dauert es etwas länger. Ändert sich mehrere Minuten nichts, wird wahrscheinlich ein Problem mit der Grafik vorliegen. Sie sollten dann das System mit Strg+Alt+Entf neu starten und, sobald Sie das Logo von Linux Mint sehen, die Esc-Taste drücken. Damit gelangen Sie in das Bootmenü (siehe Abbildung 2.5).

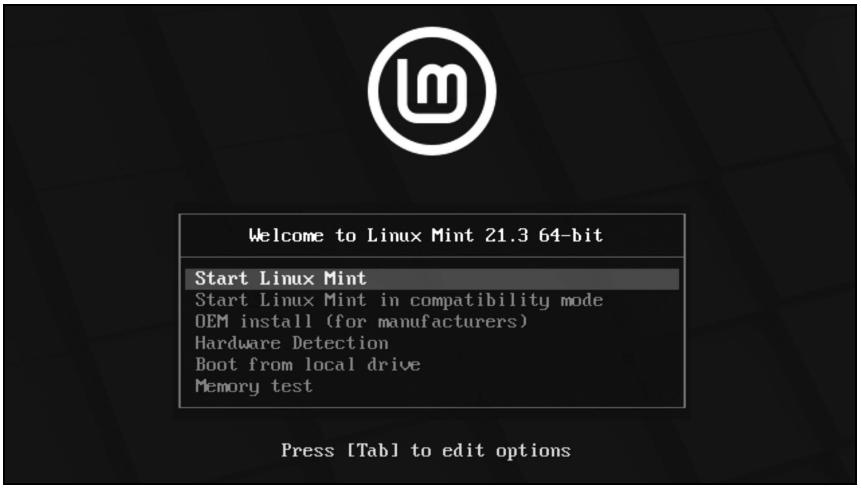

Abb. 2.5: Das Linux-Mint-Bootmenü

Hier nutzen Sie die Pfeiltasten (auf und ab) zur Navigation. Wechseln Sie auf den Eintrag START LINUX MINT IN COMPATIBILITY MODE und bestätigen mit Eingabe.

Es sollte dann nur wenige Sekunden dauern, bis das Linux-Mint-Logo wieder erscheint (von DVD gestartet, dauert dies wieder etwas länger, da optische Medien langsamer arbeiten). Anschließend erscheint der Desktop von Linux Mint (siehe Abbildung 2.6).

Abb. 2.6: Linux Mint ausprobieren oder installieren

Wir werden uns hier das Live-System kurz ansehen und gleich danach die Installation starten. Die übrigen Funktionen des Desktops werden wir uns in Kapitel 3 näher ansehen.

Sie finden am unteren Bildschirmrand das Panel – oder auch ganz einfach *Leiste* genannt. Diese stellt unter Linux Mint das Pendant zur Taskleiste unter Windows dar.

Links in diesem Panel finden Sie das Anwendungsmenü, in der Mitte den Bereich, der die offenen Fenster anzeigt und rechts den Systembereich mit der Uhr. Neben der Uhr finden Sie auch den Network-Manager, dieser zeigt Ihnen die verfügbaren WLAN-Netzwerke. Über den Network-Manager bzw. Netzwerk-Manager (je nach Desktop-Umgebung wird Ihnen dieser unter deutscher oder englischer Bezeichnung unterkommen – im Buch selbst werden Sie meist die englische Bezeichnung vorfinden) und dessen Einstellungen kommen Sie auch via UMTS-Stick ins Internet. In Abbildung 2.7 sehen Sie das geöffnete Anwendungsmenü.

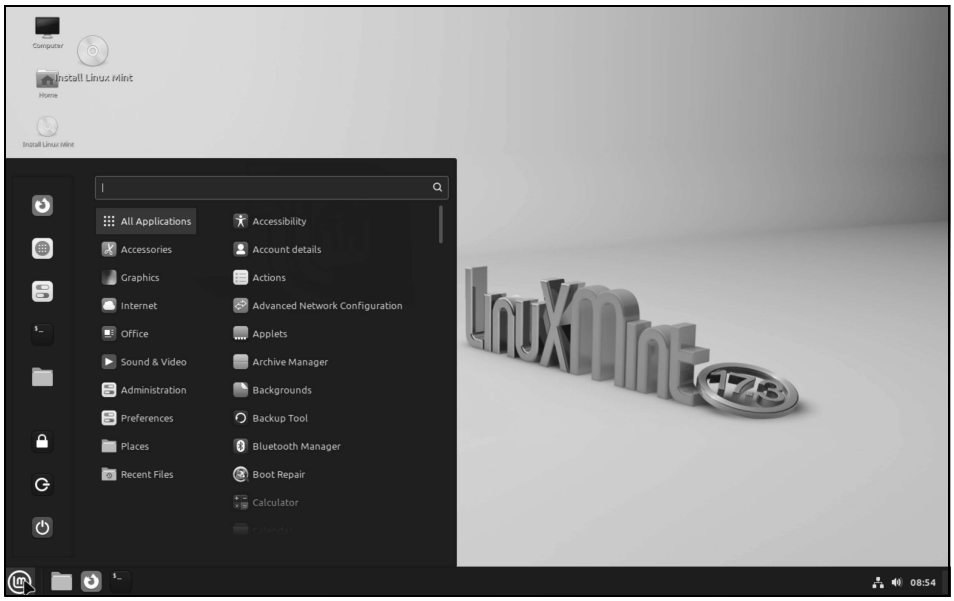

Abb. 2.7: Das geöffnete Anwendungsmenü unter Linux Mint mit Cinnamon als Desktop

Das Anwendungsmenü zeigt ganz links oft genutzte Software, wie etwa den Webbrowser (Firefox), den Dateimanager, das Terminal (siehe auch Abschnitt 4.3) und die Einstellungen. Rechts daneben finden Sie das eigentliche Anwendungsmenü – dieses zeigt links die Liste der Kategorien. Fahren Sie mit dem Mauszeiger über eine Kategorie, zeigt sich der Inhalt, also die installierte Software.

Sie können das Menü auch durchsuchen, indem Sie einfach drauflos tippen, ohne in das Suchfeld oben zu klicken.

2.5 Linux Mint installieren

Haben Sie sich dafür entschieden, Linux Mint zu installieren, gelingt dies schnell und einfach ohne Vorwissen. Linux Mint wurde so geschaffen, dass es für jeden einfach zu installieren und zu nutzen ist.

Tipp

Zur Installation von Linux Mint ist eine Internetverbindung nicht absolut notwendig, aber vorteilhaft. Vor allem geht es darum, dass Linux Mint nicht alle Treiber gleich mit dabei hat – insbesondere die Treiber für WLAN. Funktioniert die WLAN-Verbindung im Live-System nicht, sollten Sie den Computer per Netzwerkkabel mit dem Router verbinden, um an die entsprechenden Treiber zu kommen.

Es gibt verschiedene Arten, Linux Mint zu installieren:

- **Linux Mint alleine auf dem Computer** – Sie ersetzen dabei das bisher installierte Betriebssystem durch Linux Mint.
- **Linux Mint neben Windows oder einem anderen Linux** – Linux Mint wird auf einem freien Platz auf der Festplatte neben Windows oder einem anderen Linux installiert. Beim Start des Rechners wählen Sie aus, welches Betriebssystem gestartet werden soll.
- **Linux Mint auf einer externen Festplatte oder auf einem USB-Stick** – Sie installieren Linux Mint auf einem externen Speicher. Wenn Sie diesen anschließen, starten Sie Linux Mint. Allerdings ist ein USB-Stick auf Dauer nicht empfehlenswert – er wird nicht lange halten und schnell kaputtgehen.

Den entsprechenden Schalter für die Installation finden Sie als Icon am Desktop links oben – es ist bezeichnet durch INSTALL LINUX MINT.

Die Einstellungen zur Installation beginnen mit der Auswahl der Sprache (siehe Abbildung 2.8).

Sie wählen zu Beginn die Sprache – also Deutsch. In dieser Sprache ist anschließend auch das installierte Linux Mint. Nach jeder Einstellung klicken Sie unten rechts auf den Schalter WEITER.

Weiter geht es mit der Tastaturbelegung – diese ist bereits an die ausgewählte Sprache angepasst. Wenn gewünscht, können Sie diese hier aber natürlich anpassen. Sind Sie kein Entwickler, werden Sie aber keine Anpassungen brauchen. Prüfen Sie im Feld unten vor allem die Sonderzeichen (siehe Abbildung 2.9).

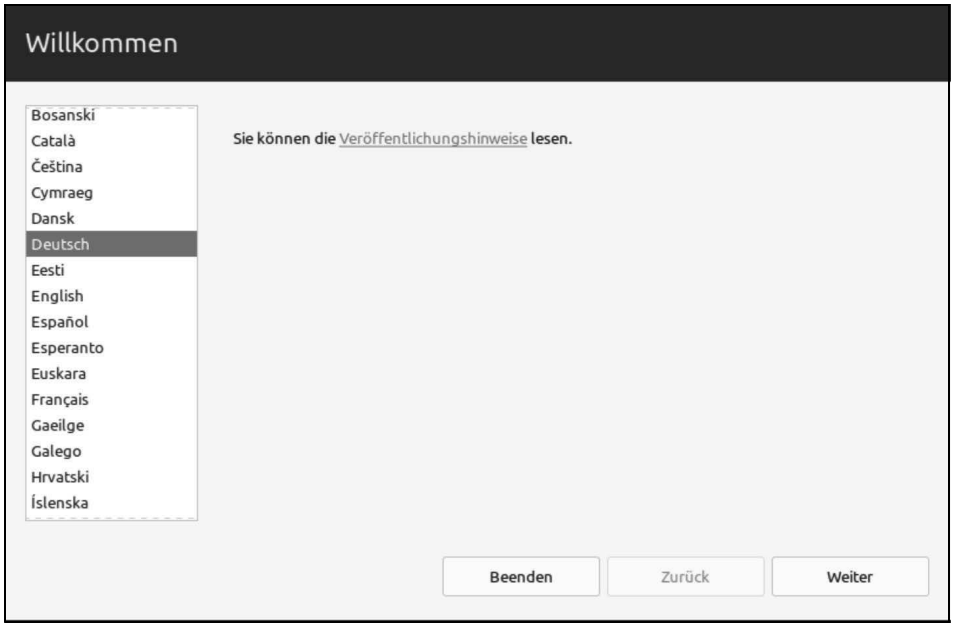

Abb. 2.8: Start der Installation – Auswahl der Sprache

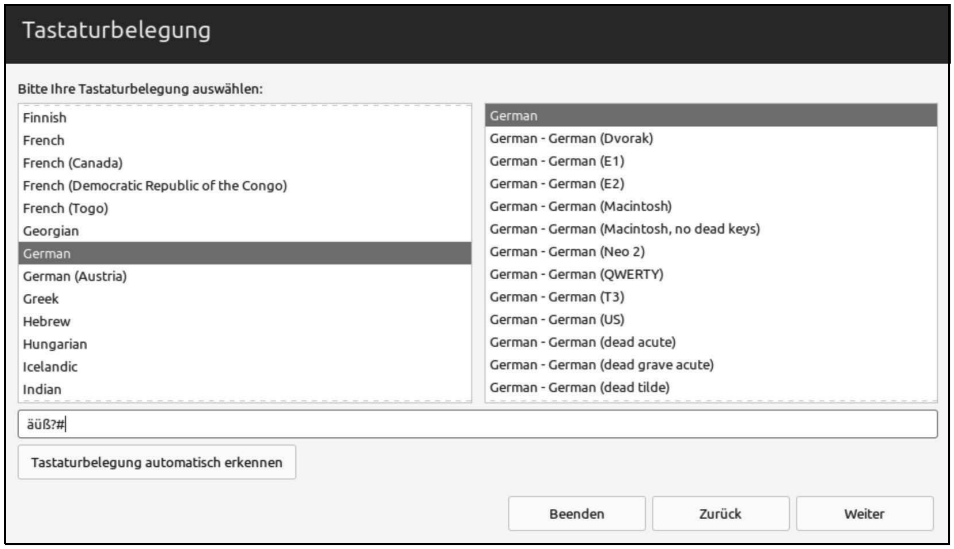

Abb. 2.9: Installation – Auswahl des Tastaturlayouts

Es folgt die Möglichkeit der automatischen Installation von Multimedia-Codecs – aktivieren Sie die Checkbox, werden Codecs installiert, mit denen sich die bekanntesten Videos und Audio-Dateien abspielen lassen (auch im Webbrowser).

Stichwortverzeichnis

A

Abhängigkeit 87
AdBlocker 122
Administrator 61, 66
  erstellen 67
Adobe Acrobat 106
Aktive Ecken 42
Aktualisierungsverwaltung 77
  Download zu langsam 79
Anonym chatten 126
  Jami 128
Anonym Dateien teilen 126
Anonyme Notizen 139
Anonyme Suchmaschine 155
Anwendung
  Einstellungen 64
Anwendungsaktualisierung 78
Anwendungsmenü 38, 46, 52
AppArmor 274
  automatisch starten 275
  Konfiguration 275
  Modi 276
  Profile 276
  Profile aktivieren 278
  Profile erstellen 278
  Rechte 281
AppImage 85
Applets 42, 49
Application Firewall 257
apropos 70
Arbeitsfläche
  virtuelle 45
Arbeitsflächenumschalter 51, 56
Archiv 45
Ausstiegsknoten 150
Authenticator 226
Automatisch entschlüsseln 188
Avast 267

B

Backup
  automatisch 136
  verschlüsselt 131
Bash-Bombe 219
Benutzer
  erstellen 44
  Gruppe 64
  Rechte 64
Berechtigung 64, 274
Besitzer 64
Betriebssystem
  Verschlüsselung 184
Bildbearbeitung 102
Bilder
  verlinkte 15
Bildschirmauflösung 43
BIOS 24
Bootfähig 22
Bootloader 33
Bootmenü 25
Brasero 287
Brave 111
btrfs 33

C

Caja 50
cd 69
Chatten
  anonym 126, 128
China 110
Chrome 97, 109
Chromium 111
Cinnamon 21, 38
  Anwendungsmenü 38
ClamAV 262, 263
  Dateien und Verzeichnisse durchsuchen 264
  grafische Oberfläche 265
  Viren-Datenbank aktualisieren 263
Cloud 131, 207
Container 179, 183
  öffnen 182
  verschlüsselter 179
Cookie AutoDelete 119
Cookie-Banner 119
Cookie Manager 119
Cookies 15, 112, 116
  Ausnahmen 114
  löschen 114
  Meldungen 119
  von Drittanbietern 118
cp 73

D

Darktable 104
Datei
  anonym teilen 126
  löschen 71

mehrere gleichzeitig umbenennen 54
öffnen mit 45
persönliche 62
standardmäßig öffnen mit 43
temporäre 62
versteckte 61, 63
Dateimanager 91
Caja 50
Konqueror 112
Nemo 44
Thunar 54
Dateisystem 32, 59, 181
virtuelles 60
Daten
retten 185
Datenbank 212
Debian 77
Debian-Paket 79
installieren über das Terminal 82
Status 81
Desklets 42
Desktop 37
mehrere gleichzeitig 37
virtueller 45
digiKam 105
DNS-Server 143
ändern 144
Router 146
Docker 210
Dokument 62
Dolphin 92
Drucker 74
DuckDuckGo 155
Duden 101
DynDNS
Dienst 207
Router 208

E

Edge 98, 110
EFI-Partition 32
Einstellung
Anwendungen 64
Einstiegsknoten 150
E-Mail
entschlüsseln 198
mit Kmail verschlüsseln 200
mit Thunderbird verschlüsseln 198
Schlüssel 192
signieren 191, 202
Spam 228
verschlüsseln 191, 197
Verschlüsselung 192
Endknoten
wählen 152
Entschlüsseln
automatisch 188
E-Mails 198
Etcher 23
Evolution 228
Spamfilter 230
Explainshell 218
Exploit 237
Explorer 59
ext4 33

F

Fast Boot 25
Fedora
Firewall 254
Festplatte
Partitionierung 30
verschlüsseln 179
Firefox 95, 110
Erweiterungen 96, 119
Telemetrie 146
Tor 151
Firejail 267
grafische Oberfläche 272
Profile 268
Firetools 272
Firewall 245
Fedora 254
IP/TCP 245
softwarebasierte 257
Firewalld 254
Applet 257
Permanent 255
Port 255
Runtime 255
Sicherheitszonen 255
Firmware 61
Flathub 218
Flatpak 77, 84, 217
Formatierung 33
FreeOffice 100
Fritz!Box 208, 241
DynDNS-Anbieter 208

G

Geoblocking 238, 244
Ghostery 120
Gimp 102
Erweiterungen 102
Pinsel 104
Plugins 102, 103
Skripte 103
GNOME 57
GNOME Commander 93
Gnome Disks 284
GNOME-Panel 292
Google 109
Google Chrome 97
Datenschutz 97
GPG 191
GPG-Schlüssel 192
am Terminal erstellen 196
erstellen 193

KDE Plasma 194
Seahorse 195
Thunderbird 193
GRUB 33
Gruppe 64
erstellen 65
GUFW 248
Ausnahmen 249
Profile 249

H

Hintergrundbild 48, 53
ändern 40
home 61
Homeoffice 239
Home-Verzeichnis 60, 62, 68
Host 143

I

I DON'T CARE ABOUT COOKIES 120
Installation 28
IP/TCP 245
IP-Adresse 143, 245
statische 207
verschleiern 148
Iptables 251, 262
IPv4 143
IPv6 143
ISOburn 22, 286

J

Jami 128
Joplin 139

K

K3b 286
KDE 111
Kdeconnect 249
Ports 252
KDE Plasma 57
GPG-Schlüssel 194
verschlüsselte Container 183
KeePassXC 221
Gruppen 223
Passwort anzeigen 225
Passwort-Editor 223
Passwort-Generator 223
Webbrowser-Erweiterung 225
KGpg 194
Kmail 228
E-Mails verschlüsseln 200
Kommandozeile 67
Konfiguration 61
Konqueror 111
Einstellungen 112
Kontextmenü 50
Krusader 92
Kubuntu
Firewall 254

L

Ländersperre 152
Leiste 27, 38, 52
LibreOffice 99
Lightroom 104
Linux-Distribution
verschlüsselte 185
Linux Mint
Anwendungsmenü 27
Download 21
Live-System 23, 25, 184
ls 71
Lynis 233

M

Mailserver 191
Manpage 70
MariaDB 211
Maschine
virtuelle 160
Master PDF Editor 106
Mate 22
Anwendungsmenü 46
Applets 49
Dateimanager 50
Thema installieren 49
virtuelle Arbeitsfläche 50
Mate Tweak 49
Matomo 15
Metasploit 235
Module 237
Microsoft 110
Microsoft Edge 98
Datenschutz 98
Microsoft Office 99
Midnight Commander 94
mkdir 72
Mullvad 110
mv 73

N

Nemo 44
Netfilter 245, 248, 251
Network-Manager 27
Netzwerk
vertrauenswürdiges 240
Netzwerk-Protokoll 93
Netzwerk-Verzeichnis 61
Nextcloud 207
Administrator 214
Dateien freigeben 216
installieren 210
Port 209
NoScript 121
Notizen
anonyme 139

O

Öffentlicher Schlüssel
suchen 200
Office 99

OnionShare 126
Onlyoffice 101
OpenSnitch 257
OpenVPN 240
Opera 96, 110
  Datenschutz 98
Ordner 59
  markieren 45
  navigieren am Terminal 69
  Zugriffsrechte 64, 65
Orte 45

P

Paket 246
Paket-Verwaltung 79
Panel 27
Partition
  verschlüsselte 186
Partition / 31
Partitionierung 30
Passwort 219
  Abfrage abschalten 36
  gehackt 219
  Generator 220
Passwort-Manager 221
Passwort-Safes 221
PDF 106
PGP 191
PGP-Schlüssel 192
Phishing 226, 228
Photoshop 102
Plasma Vault 183
Podman 210, 250
Port 246
Portmaster 259
PPA 85
  deinstallieren 86
  installieren 85
  Probleme 86
Profil 17, 121
Proxy 148
  HTTPS 149
  Liste 149

Q

Qemu 168

R

Ransomware 17
  virtuelles Betriebssystem 166
RAW-Bildbearbeitung 104
Rclone 131
  Optionen 132
  Verschlüsselung 134
Recht 64
rm 72
root 61, 66
Router 146
  DynDNS 208
  IP-Adresse 243
Ruhezustand 32

S

Samba 255
Sandbox 267
Scanner 74
Schadsoftware 17
Schlüssel 181
  öffentlicher 192
  privater 192
Schlüssellänge 197
Schnellstarter 39
  Mate 47
Schrift 90
  installieren 90
Schriftgröße 42
Seahorse 195
  GPG-Schlüssel 195
Secure Boot 25
SelekTor 152
SelekTor Proxy Reset 154
Services 250
Sicherheitsaktualisierung 78
Sicherheitsgrundlagen 217
Sicherheitslücke 235
Signieren 191
Skripte 121
Snap 77, 87, 218
Snap-Paket
  aktualisieren 89
  deinstallieren 89
  installieren 88
Softmaker Office 100
Software
  Rechte 274
  suchen (Terminal) 83
  verifizierte 217
Spam 17, 227
Spamassassin 228
  in Evolution 230
  in Kmail 231
  in Thunderbird 229
Startmedium 22
Startmenü 24
Startprogramme 43
Steganografie 180, 203
Steghide 203
  installieren 203
Stegosuite 203, 206
Suche 39, 46, 52
Suchmaschine 155
sudo 66
Suspend to disk 32
SWAP-Partition 32
Synaptic 79, 80
System
  verschlüsseln 30
Systemd 258
Systemdatei 72
Systemverzeichnis 60

T

Tails 151, 283
  Installation 283, 284
  klassisches Anwendungsmenü 292
  Software installieren 292
  USB-Stick 284
TCP 241
Teams 99
Telemetrie 260
Telemetrie-Daten 146
Temporäre Datei 62
Terminal 67, 68
  automatische Vervollständigung 68
  Datei kopieren 73
  Datei löschen 71
  Datei umbenennen 73
  Datei verschieben 73
  GPG-Schlüssel erstellen 196
  Hilfe 70
  kopieren und einfügen 74
  Navigation 69
  Optionen 71
  Ordner erstellen 72
  Ordner löschen 72
  Platzhalter 72
  Software suchen 83
  Textdateien bearbeiten 73
Texteditor 73
Thema 42, 49
  installieren 54
Thunar 54
Thunderbird 193, 228
  E-Mails verschlüsseln 198
  GPG-Schlüssel 193
  Spamfilter 229
Tor
  Client 151
  Endknoten 152
  Firefox 151
  Geschwindigkeit 151
  Tails 283
Tor als Client 151
Tor Browser 123, 151, 293
Tor mit Knoten-Wahl 151
Tor-Netzwerk 150
TP-Link 146, 208, 241
TPM-Chip 188
Trackingpixel 120
Treiber 74, 89
  aktualisieren 89
Tunnel 240

U

uBlock Origin 123
UDP-Protokoll 246
UEFI 24
UFW 251
  Logging 253
  Regeln 252
USB-Stick
  bootfähiger 23
  verschlüsseln 179

V

Verlinkte Bilder 15
Verschlüsselte Linux-Distribution 185
  Daten retten 185
Verschlüsselung 179
  Betriebssystem 31, 184
  E-Mails 192
Versteckte Datei 61, 63
Verzeichnis-Hierarchie 59
Virenscanner 262
  automatisieren 266
  grafische Oberfläche 265
Virt-Manager 168
  Dateien teilen 175
  Festplatte 172
  Grafikkarte 174
  Ressourcen 172
  Vollbildmodus 174
VirtualBox 160
Virtuelle Arbeitsfläche 45
  Mate 50
  XFCE 56
Virtuelle Maschine 160
  Festplatte 162
  Gemeinsame Ordner 166
  Größe der Festplatte 162
  RAM 162
  Ransomware 166
Virtuelles Dateisystem 60
Vivaldi 96, 110
VM 161
VPN 238
  Server 240
  Tunnel 240
  Zertifikat 242

W

Waterfox 96, 110
Webbrowser 17, 95
  anonyme 109
Webseiten-Analyse 16
Werbeblocker 122
Werbung 17
WLAN 28
Wurzelverzeichnis 59

X

XFburn 288
XFCE 21, 51
  Anwendungsmenü 52
  Favoriten 52
  virtuelle Arbeitsfläche 56
xfs 33

Y

YaCy 155, 156
Yandex 110
YubiKey 181

Z

Zählpixel 120
Zertifikat 240
ZIP 45
Zombie-Prozess 233
zuluCrypt 179
Zwei-Faktor-Authentifizierung 226