Alternativen zu kommerzieller, nicht-freier Software

und zu den „privaten Geheimdiensten“

(Update vom 31. Mai 2017)

1. Computer-Betriebssysteme

Die Auswahl an alternativen, freien Betriebssystemen ist riesig und für den Neuling kaum zu überblicken. Abseits der Windows- und Mac OS X-Monokulturen herrscht eine bunte, beeindruckende =>Vielfalt.

Für Ein- und Umsteiger besonders geeignet ist Linux Mint. Hierbei wiederum eignet sich die Variante mit dem MATE-Desktop vor allem für all jene Umsteiger besonders, die zuvor mit Windows arbeiteten.

- Download Linux Mint 18.1 „Serena“- MATE => hier (sicherer Download von heise.de)

Die recht einfache Installation wird im =>offziellen deutschsprachigen Handbuch beschrieben.

Hilfe zu Linux Mint bekommt man u.a. in der deutschen Online-Community von Linux Mint, der Webseite =>linuxmintuser.de. Da Linux Mint ein Ubuntu-Derivat ist, also quasi „unter der Haube“ ein Ubuntu steckt, bietet auch das =>Wiki der Seite ubuntuusers.de umfangreiche Hilfe, Beschreibungen und Anleitungen, welche fast alle genau so für Linux Mint gelten.

Anmerkung: Auf neueren Rechnern, die statt BIOS mit UEFI und SecureBoot starten (ab Windows 8) wird ein Start von Linux Mint verhindert, weil dessen Startdatei (Bootloader) nicht von Microsoft signiert ist. Das ist natürlich eine ziemliche Frechheit und richtet sich vor allem gegen die Konkurrenz durch freie Software (=>Hintergründe). Um Linux Mint dennoch starten zu können, muss man im UEFI/in Windows das sogenannte SecureBoot abschalten („=>wie =>geht =>das?“).

Hinweis: Die Computerzeitschrift c't aus dem Heise-Verlag hat jüngst ein =>Sonderheft „Umstieg auf Linux“ herausgegeben. Dort wird u.a. ausführlich und verständlich beschrieben, wie man auf Linux umsteigen kann, was dabei zu beachten ist und wie man dabei seine Daten verlustfrei mit nimmt.

2. Mail-Verschlüsselung

Für alle Betriebssysteme eignet sich das =>GnuPG-Verfahren hervorragend. Selbst Supercomputer bräuchten viele Jahre, um eine damit verschlüsselte Mail zu knacken. Aber vor allem ist GnuPG freie Software, welche nicht so ohne Weiteres und unbemerkt durch Konzerne und Geheimdienste korrumpiert werden kann. GnuPG kombiniert man am besten mit dem für alle Desktop-Betriebssysteme verwendbaren (und freien) Email-Programm =>Thunderbird und dem dafür vorgesehenen Addon =>Enigmail. =>Hier wird ausführlich erklärt, wie man mit Enigmail und Thunderbird Mail-Verschlüsselung einrichtet und benutzt. Es gibt auch unzählige =>Video-Tutorien im Netz, die das =>noch einmal anschaulich erklären.

Eine weitere, sehr unkomplizierte Möglichkeit, seine Mails zu verschlüsseln, ist der Email-Dienst =>Tutanota. Tutanota befolgt zwar nicht die sprichwörtliche „reine Lehre“, insbesondere bezüglich der Schlüsselerzeugung und deren Verwaltung nicht, aber ist besser als gar nichts. Ein Vorteil von Tutanota ist, dass man =>auch jemandem mailen kann, der selbst nicht verschlüsselt. Tutanota eignet sich auch gut für Smartphones und Tablets. =>Ausführliche (Selbst)Beschreibung des Dienstes.

3. Email-Konto

Wer einen Euro im Monat übrig hat, sollte sich ein Konto bei dem kleinen, aber feinen Berliner Email-Provider =>Posteo zulegen. Posteo arbeitet werbefrei, transparent und weitestgehend anonym. Und ist gegenüber staatlichen Zugriffen äußerst skeptisch =>eingestellt. Dass der Email-Account bei Posteo einen Euro pro Monat kostet und nicht wie bei anderen, großen Anbietern kostenlos ist, sollte nicht darüber hinwegtäuschen, dass man bei den „Kostenlosen“ selbstverständlich bezahlt – mit seinen persönlichen Daten (ein Nutzerprofil solcher Kostenlos-Angebote, zusammengestellt aus den persönlichen Daten des Nutzers, kann einige Euro wert sein; es wird damit gehandelt.).

Genau so empfehlenswert, fast noch ein bisschen besser als Posteo, ist der gleichfalls in Berlin ansässige Email-Provider =>mailbox.org. Auch hier berappt man einen Euro pro Monat für das Konto. mailbox.org glänzt gegenüber Posteo mit einer Reihe von Feineinstellungen für diejenigen, die das wollen und können. So ist es u.a. möglich, =>Mails so zu markieren – z.B. solche an Onlineshops, dass diese nicht unbemerkt die eigene Emailadresse weiter vermarkten können. Darüber hinaus bekommt man bei mailbox.org sehr sicheren Onlinespeicher ab dem kleinsten Email-Tarif (1 €) mit dazu.

4. Sicherer Surfen

Um beim alltäglichen Surfen im Internet ein wenig anonymer zu bleiben, empfiehlt es sich, zusätzlich zum verwendeten Haupt-Browser das =>Tor-Browser-Bundle zu installieren und zu nutzen. Zu beachten dabei ist, dass man den Tor-Browser n i c h t dazu verwenden sollte, um sich bei Onlinediensten, Foren, Email-Postfächern oder etwa seiner Hausbank zum Online-Banking anzumelden, bzw., alle Dinge damit unterlässt, bei denen Passwörter u. Ä. abgefragt werden („=>warum?“)! Nutzen sollte man den Tor-Browser also für alltägliches Surfen, Stöbern, Lesen und Videoanschauen im Internet. Achten sollte man unbedingt auch darauf, immer die aktuellste Version des Tor-Browsers zu verwenden. (Mehr Hintergründe und Erläuterungen finden sich in diesem 3-teiligen, leicht verständlichen und kompetenten =>Blogbeitrag des freien IT-Sicherheitsspezialisten Mike Kuketz aus Karlsruhe.)

Wie man seinen Haupt-Browser daneben und zusätzlich mit entsprechenden Erweiterungen =>gegen Datenkraken absichern kann, wird auf der sehr interessanten, kompakten und auch anderweitig hochinformativen Seite =>PRISM-Break erläutert.
Wer ein VPN nutzt, bewegt sich noch sicherer durch's Internet und schlägt dem Freundeskreis Vorratsdatenspeicherung zusätzlich ein Schnippchen. Empfehlenswert für Linux-Nutzer ist hier u.a. die Software Bitmask und darin die Nutzung der Server von Calyx und/oder Riseup.net.

5. Suchmaschinen

Wer mit Google sucht, wird von Google heimgesucht – ungefragt und meist ohne das zunächst selbst zu bemerken. Aus diesem Grund empfehlen sich alternative Suchmaschinen. Eine sehr gute Alternative ist die Suchmaschine =>Startpage. Aber auch =>DuckDuckGo oder die Metasuchmaschine =>Ixquick (selber Betreiber wie Startpage) sind großartige Alternativen.

6. Sogenannte soziale Netzwerke

Ein Leben ohne Facebook, Twitter & Co. ist möglich und alles andere als sinnlos! Wenn man aber ohne nicht auskommt (oder das glaubt), sollte man Alternativen nutzen, bei denen man nicht die

Kontrolle über seine persönlichen Daten abgibt oder verliert. =>Diaspora bietet sich hier an, oder auch =>GNU Social und =>Mastodon.

7. Videotelefonie

So wie es für die Internetsuche inzwischen den Begriff „Googeln“ gibt, gibt es für das Videochatten den Begriff „Skypen“. Skype gehört schon seit einiger Zeit zu Microsoft. Skype-Gespräche sind verschlüsselt - aber leider nur so lange, bis sie auf den konzerneigenen MS-Servern einlaufen. Dort werden alle Inhalte wieder entschlüsselt. In so einem Fall von Verschlüsselung überhaupt zu reden, ist natürlich lächerlich und eigentlich absurd. Noch absurder ist dies angesichts der Enthüllungen von Edward Snowden, der u.a. die Zusammenarbeit der Konzerne mit der NSA offenlegte. Wer also – neben einer sehr guten Funktionalität – wert auf echte Ende-zu-Ende-Verschlüsselung beim „Skypen“ legt, sollte sich die Open-Source-Software =>Jitsi einmal ansehen. Und nutzen (mehr dazu u.a. =>hier und hier).

8. Smartphone und Tablet (Android)

Wer ein Smartphone oder Tablet mit dem Google-Betriebssystem Android verwendet, sollte unbedingt ernsthaft darüber nachdenken, dieses Betriebssystem gegen =>LineageOS oder gegen =>Replicant auszutauschen. Auch lohnt ein Blick auf =>F-Droid als Alternative zu Google Play.

9. Die eierlegende Apfelwelt - Apple, iOS, OS X

Die Geräte von Apple (iPhone, iPad, iMac usw.) und deren eigens für diese bereitgestellten Softwares (iOS, OS X) und Dienste (iTunes, iCloud etc. pp.) sehen besonders gut aus und bieten eine hervorragende Funktionalität. Was man dabei leicht übersehen kann, ist, dass diese Geräte, deren Softwares und die damit verbundenen exklusiven Dienste aus mehreren Gründen ganz besonders an- und auffällig sind, was die permanente Ausspähung durch Apple selbst aber somit eben auch durch staatliche Geheimdienste betrifft (siehe u.a. =>hier, =>hier und =>hier). Apple-Geräte sind zudem das, was man sprichwörtlich als „goldenen Käfig“ bezeichnen würde. Aufgrund dieser Eigenschaften =>empfiehlt die Seite PRISM-Break sogar, solche Geräte – insbesondere jene mit dem Betriebssystem iOS – überhaupt nicht mehr zu benutzen und auszutauschen, da das Risiko für den Einzelnen, die Kontrolle über seine persönlichen Daten vollständig zu verlieren, viel zu hoch sei.

10. WhatsApp?

Finger weg! Einer der =>perfidesten Datenkraken überhaupt (gehört zu =>Facebook). Nutzen Sie statt dessen =>Surespot oder =>Signal. Oder wenigstens =>Threema. Überzeugen Sie Ihre Freunde von den Alternativen.

Weiterführende Links zum Themenkomplex

Wer Genaueres wissen möchte, kann im inzwischen über 400 Seiten umfassenden und ständig aktualisierten =>Privacy-Handbuch nachlesen.
Brandaktuelle Infos zu kritischen IT-Sicherheitslücken gibt jederzeit bei =>heise Security.