You shall not pass!

Wie wir neugierigen Leuten, die an unsere Daten wollen,
das Leben schwerer machen.

Für Einsteiger*

* Also für dich und mich und Mutti und Vati und Onkel und Tante

22. April 2017
Uwe Kremmin
Starring openSUSE
Guest Star: LibreOffice

Über mich

Erst gläubiger Windows-Anhänger

2006, mit Vista, mochte ich nicht mehr

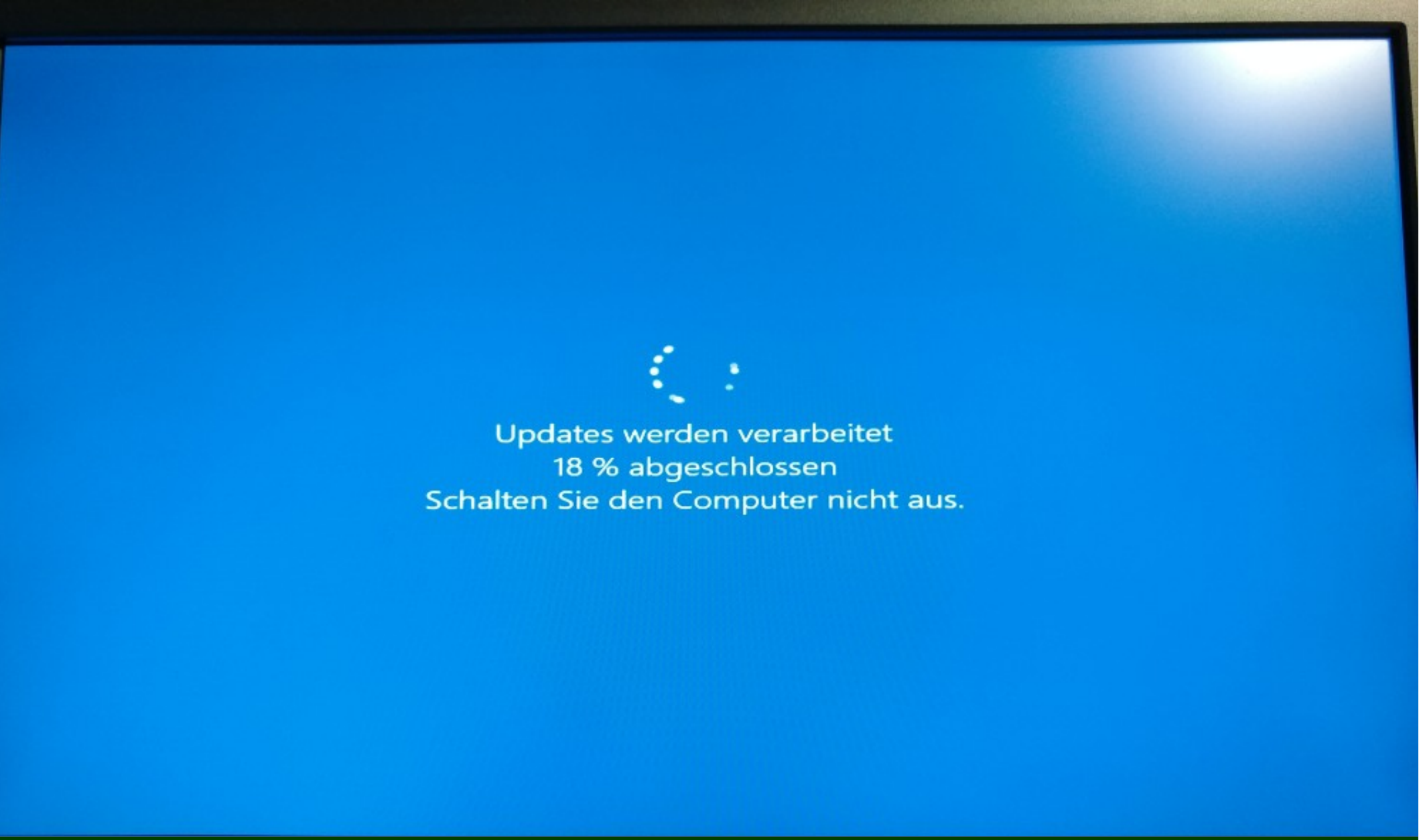
Diverse (GNU-)Linuxe probiert

Heute openSUSE, manchmal Ubuntu, Mint, Puppy, Knoppix, libreELEC, Raspbian

Meine PCs tun, was ich will

Ich freue mich jedesmal, wenn ich mit ihnen arbeite

E-Technik studiert, diverse Halbleiterfirmen, heute Marketing



Das bleibt mir erspart.

IT-Sicherheit?

Angriffe über

Software (Betriebssystem, Anwendungen, Browser, …)

Schlamperei in Organisationen (Siehe z. B. SSL-Zertifikate, weiter hinten)

Obskure Hardware (“BadUSB”, Keylogger, ...)

Seltsame WLAN-Signale https://thehackernews.com/2016/11/hack-wifi-password.html

Töne https://www.schneier.com/blog/archives/2013/12/acoustic_crypta.html

Social Engineering (“Chef” braucht Passwort, “verlorener” USB-Stick, …)

...

Was wir heute erreichen wollen

Jemand, der unseren PC in die Finger bekommt, soll nicht an unsere Daten kommen.

Laptop in der Raststätte liegen gelassen.

Wir erschweren Angriffe über den Browser.

Wir machen den Leuten, die an der Leitung lauschen, das Leben schwer.

Wir besuchen die Schmuddelecken des Internet ohne Sorgen.

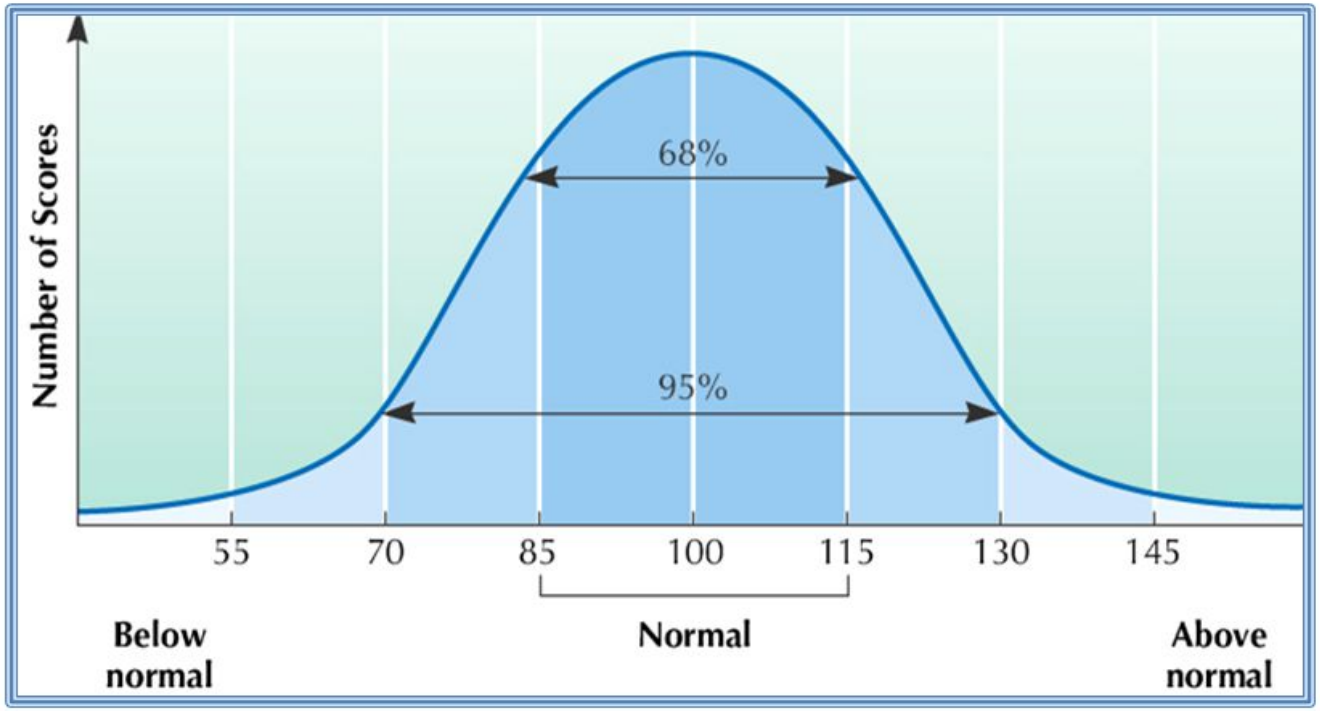
“Warum denn???”

1. **Weil wir es können**
2. **Weil wir es dürfen**
3. **Weil wir es müssen**
4. **Weil wir es auch in Zukunft dürfen wollen**

“Your right to vote: Use it or lose it.”

“Aber das interessiert doch keinen!”

Measuring Intelligence—The Normal Distribution of IQ Scores



Von: http://slideplayer.com/slide/1597494/

Jemand, der unseren PC in die Finger bekommt, soll nicht an unsere Daten kommen.

Dazu müssen wir die Daten (auf der Festplatte) verschlüsseln.

Windows kann das. Der “BitLocker” hat aber eine “Backdoor”.

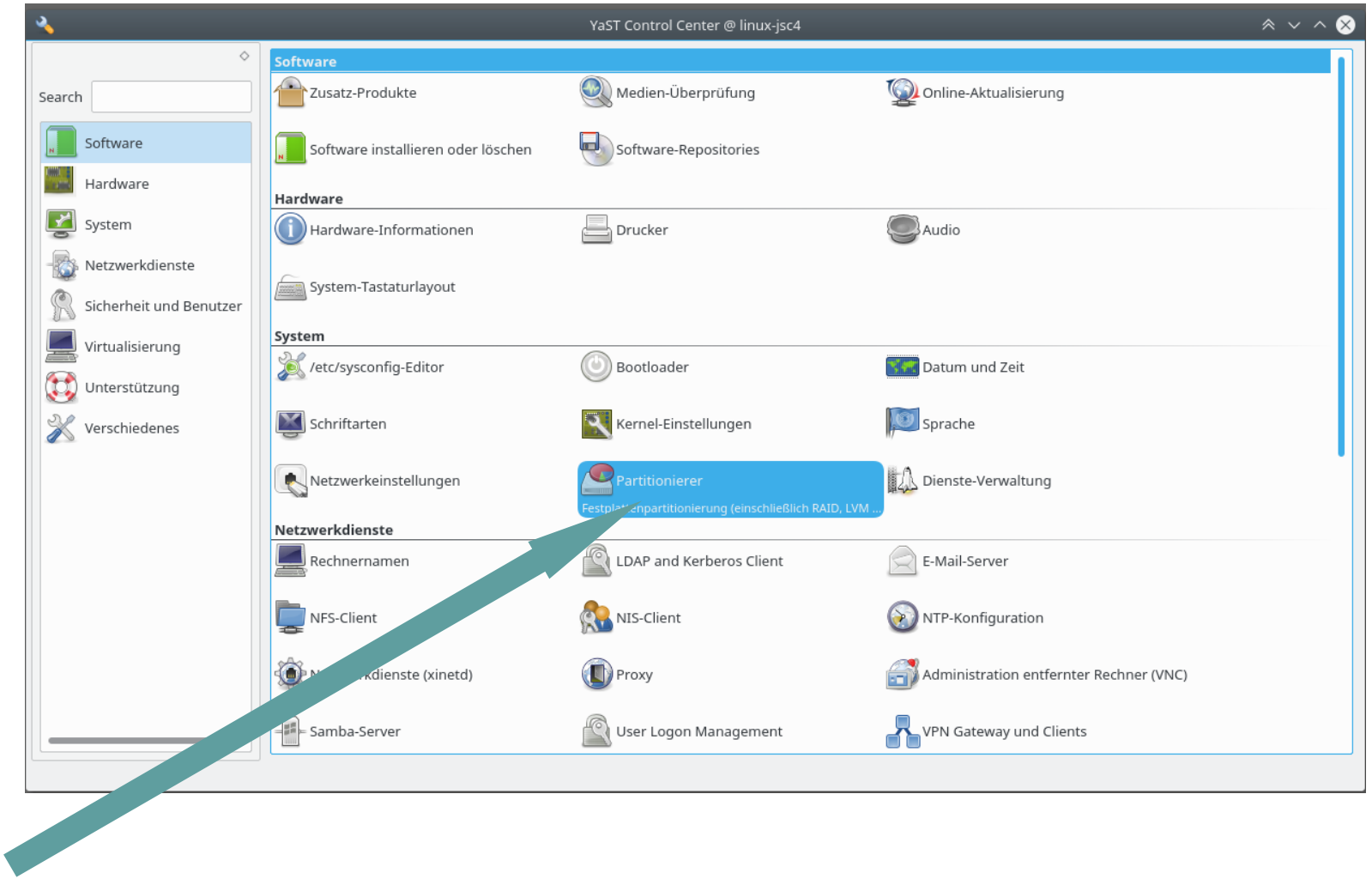
“Eine groteske Sicherheitslücke [...] gewährt Angreifern vollen Zugriff auf verschlüsselte Windows-Laufwerke.”

https://www.heise.de/newsticker/meldung/Windows-10-Laufwerksverschluesselung-laesst-sich-waehrend-Versions-Upgrades-umgehen-3549348.html

Linux kann auch – und besser - verschlüsseln.
Und hat keine Backdoor.

Laufwerk verschlüsseln unter openSUSE

YaST ist dein Freund



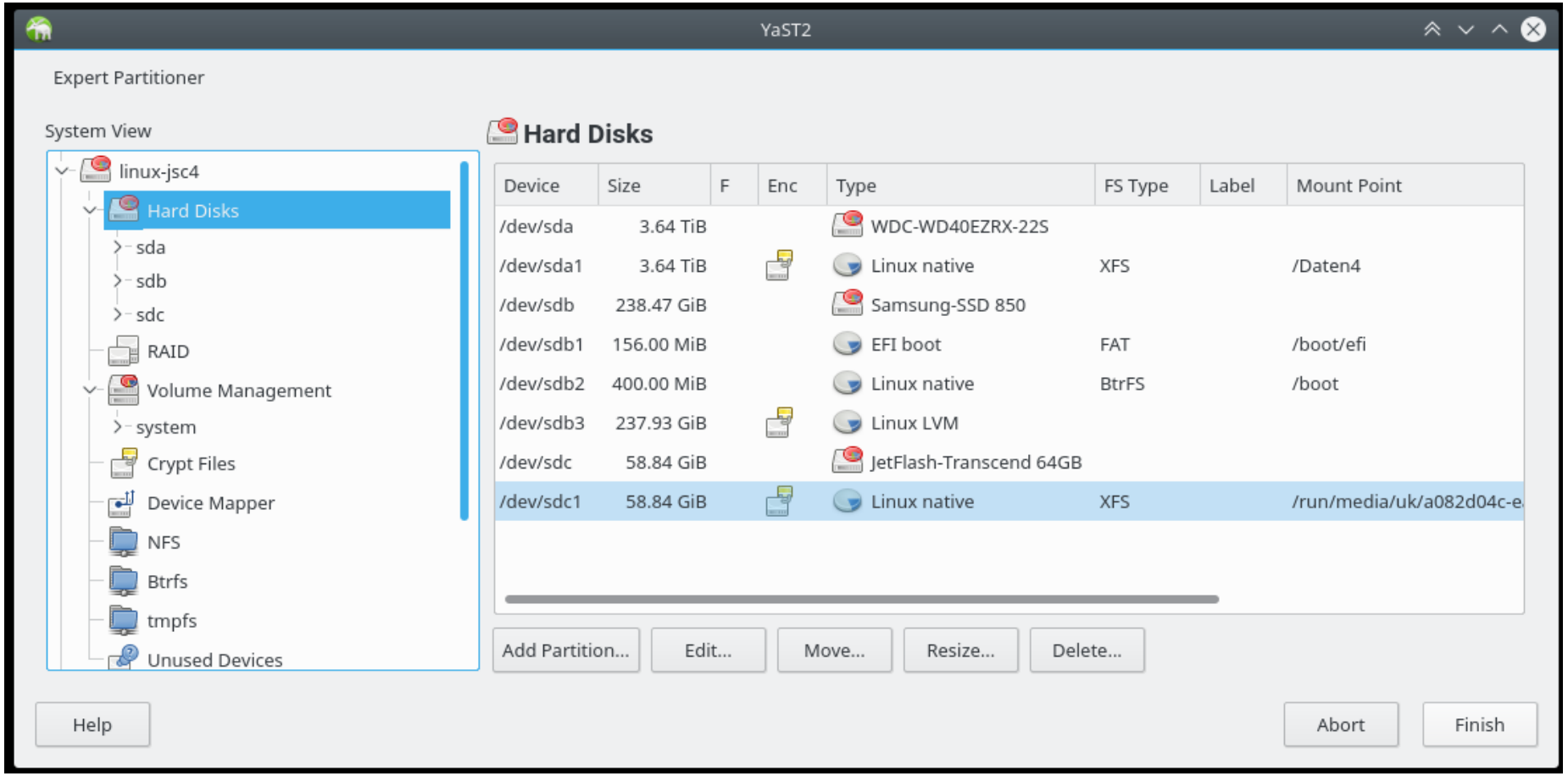
Wir brauchen den Partitionierer

Hier legt man fest, wie das System seine Festplatten benutzt.

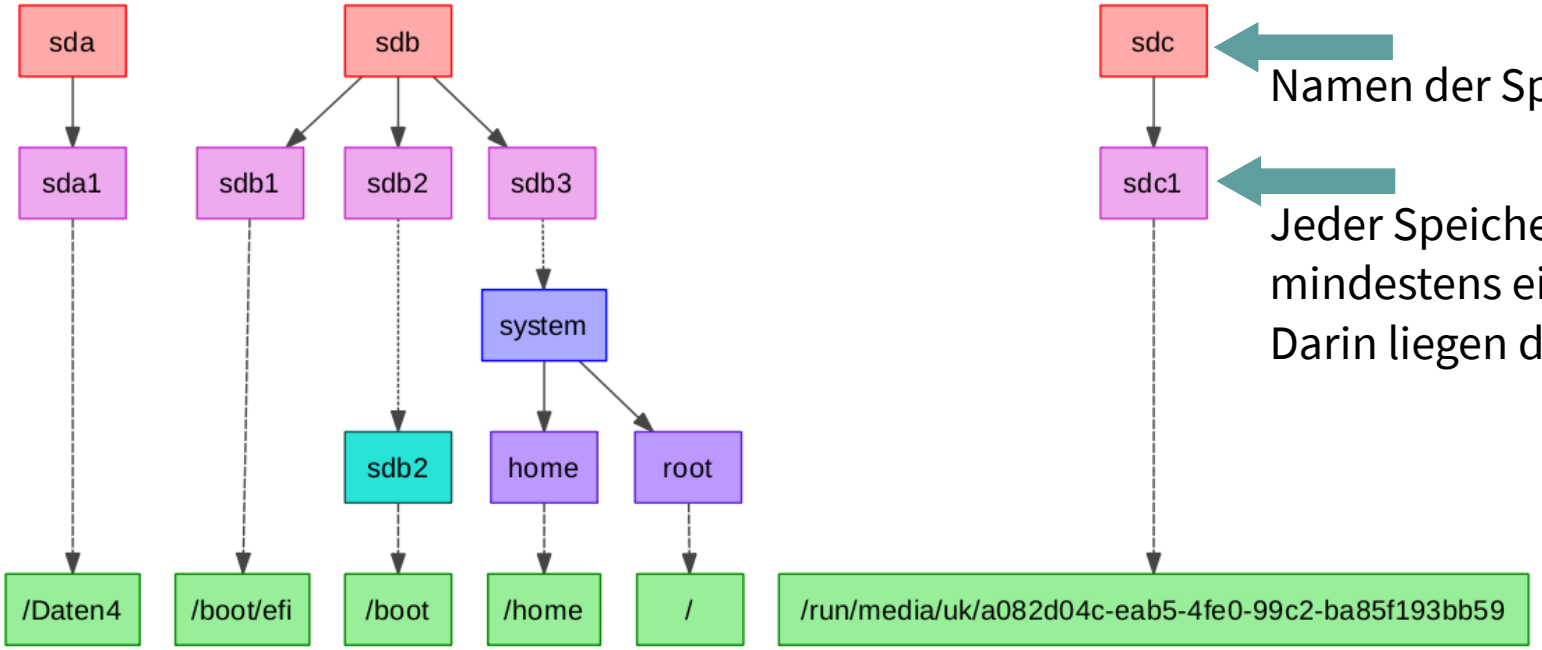
(Hier muss man wissen, was man tut.)

(Sonst ist alles aus!)

Der zeigt uns die eingebauten Festplatten



Andere Darstellung



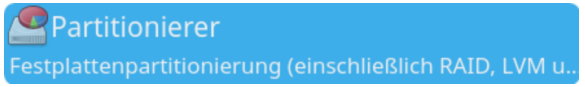
Namen der Speicher.

Jeder Speicher besitzt mindestens eine “Partition”. Darin liegen die Daten.

Unter diesen Adressen findet man die Partitionen.

Und so verschlüsselt man einen USB-Speicher (1)

1. YaST starten und Partitionierer auswählen.
Liste der angezeigten Festplatten ansehen.



2. Stick einstecken. In YaST auf “Rescan Devices” (bzw. deutsche Entsprechung) klicken. Das baut die Liste der vorhandenen Speicher neu auf.
Der Speicher, der neu dazugekommen ist, ist der USB-Stick.

Achtung: Stick verliert beim Verschlüsseln alle darauf gespeicherten Daten.

Kapazität des Speichers

So heißt der Stick.

Die Partition ist mit diesen Dateisystem formatiert.

So heißt die Partition darauf.

Auf dem Stick ist nur diese eine Partition.
Sie nimmt den gesamten Platz ein.

Unter dieser Adresse ist der Speicher in das Dateisystem eingebunden (“mount point”).

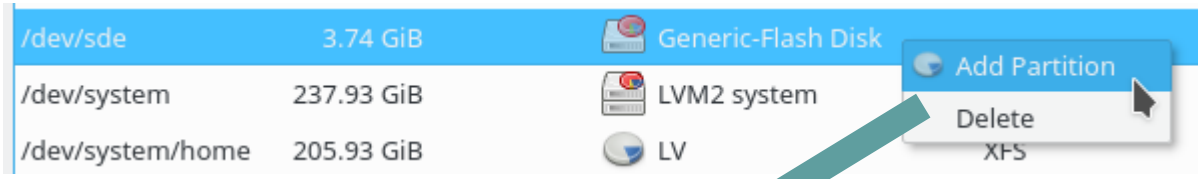
Und so verschlüsselt man einen USB-Speicher (2)

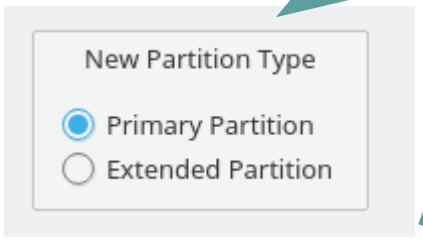
3. Existierende Partition löschen
   (hier: /dev/sde1) mit
   rechtem Mausklick darauf.

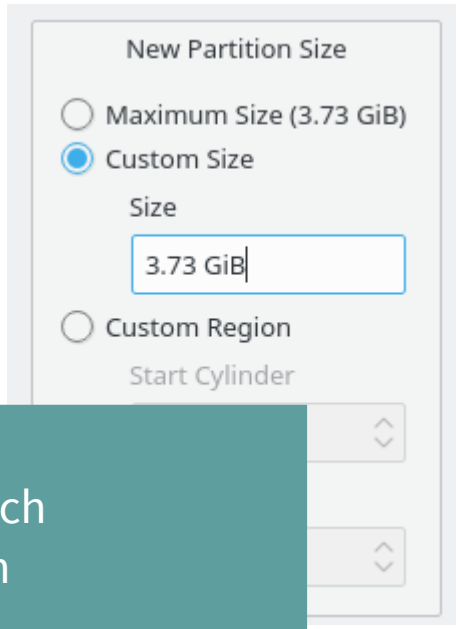
4. Dann neue Partition anlegen (“Add Partition”).
   Dazu rechter Mausklick auf Speicher (hier: /dev/sde).

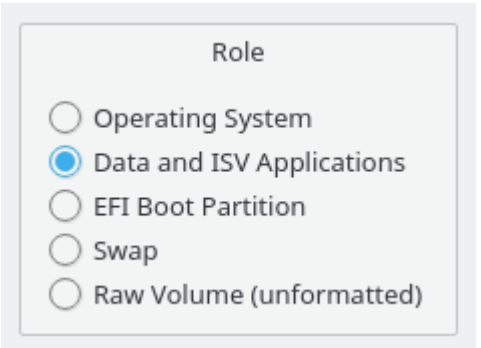
/dev/sde	3.74 GiB	Generic-Flash Disk		
/dev/sde1	3.73 GiB	Linux native	Ext4	/run/media/uk/ceaacc10-2527-4edb-957b-fa3f0462fd0c

Und so verschlüsselt man einen USB-Speicher (3)







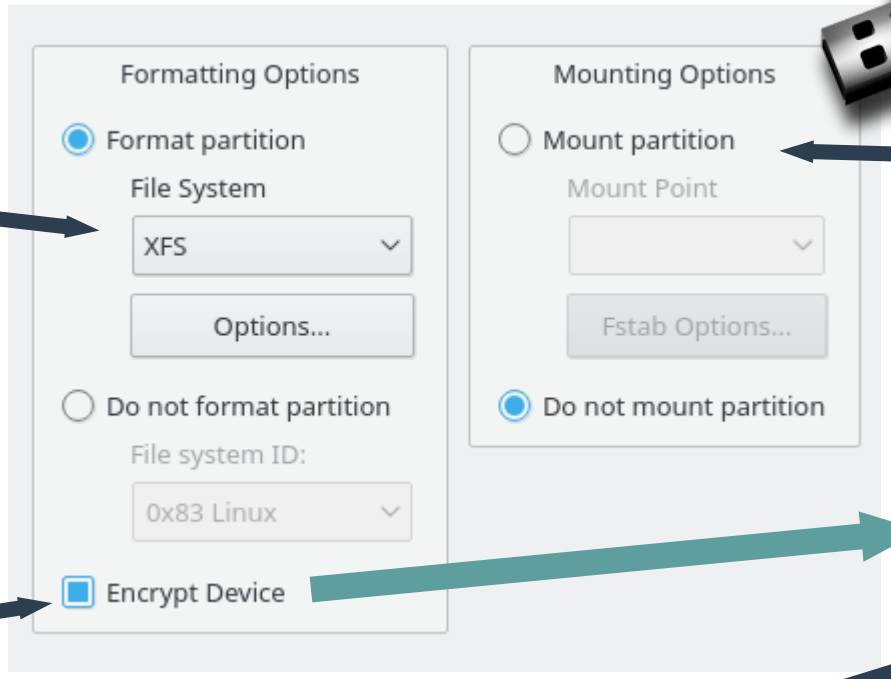


Jedesmal einfach
weiter klicken

Und so verschlüsselt man einen USB-Speicher (4)

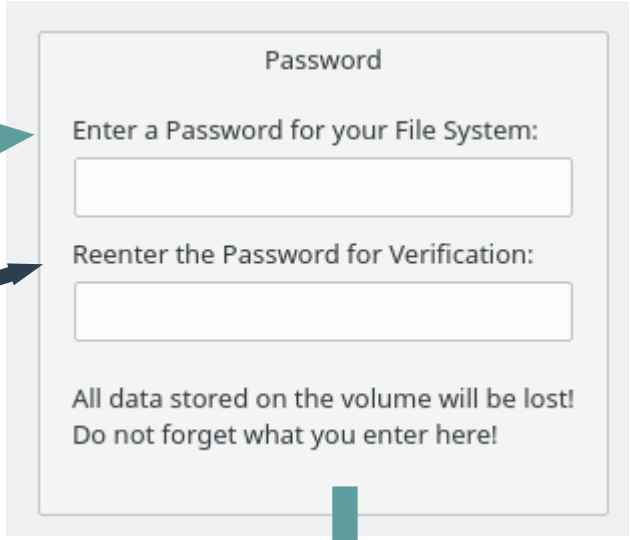
Gewünschtes Dateiformat auswählen (XFS ist OK).

Das braucht man, falls der Speicher fest eingebaut wird, z. B. bei einer Festplatte.



Hier klicken!

Passwort eingeben.



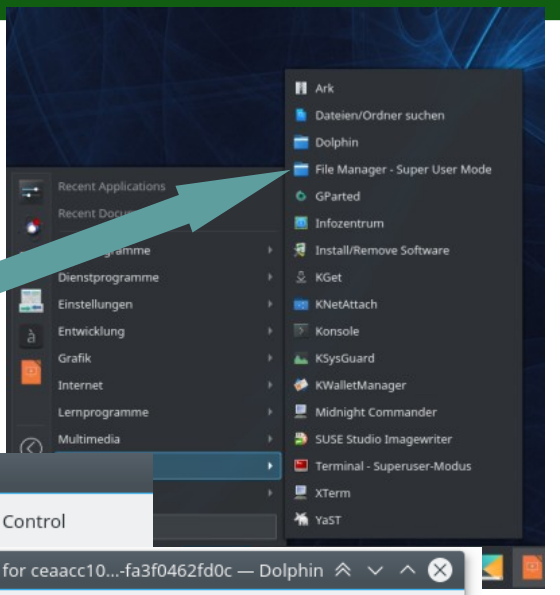
Fast fertig

Und so verschlüsselt man einen USB-Speicher (5)

Der Stick ist jetzt verschlüsselt und durch den Administrator (root) beschreibbar.

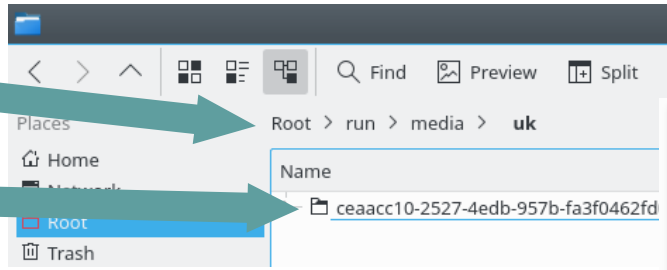
Damit ihn alle beschreiben können, tun wir das:

Dateimanager im “Super User Mode” starten



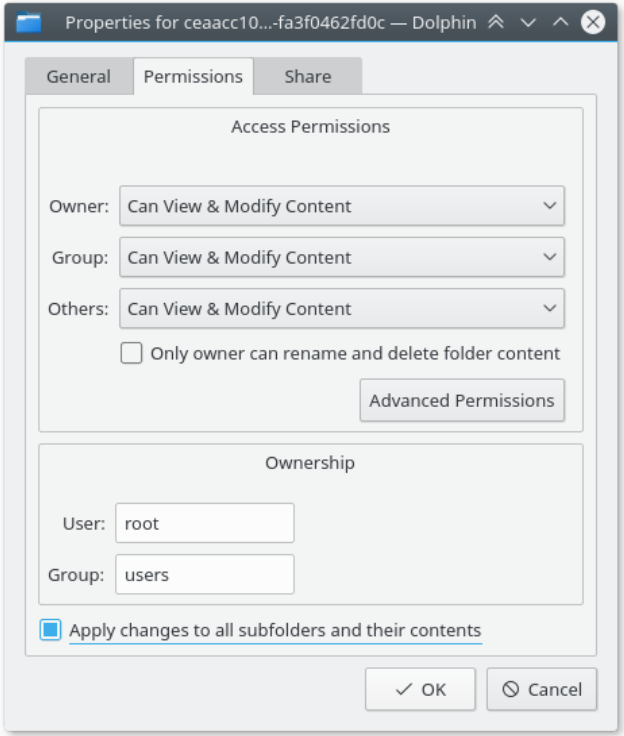
Dahin gehen

Das ist der Speicher



Rechte Maustaste darauf klicken: “Eigenschaften”

Berechtigungen für diesen Speicher so einstellen:



Fertig!

Das Verschlüsseln dauert insgesamt max. 2 Minuten.

Festplatten verschlüsseln

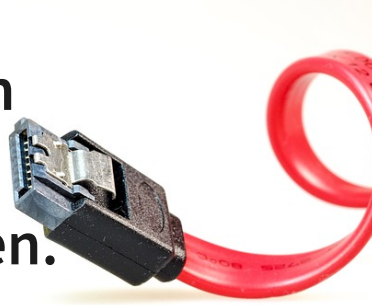
Für eingebaute Festplatten geht das fast genau so.

Dabei mount point festlegen. Also einen Ort, wo der Speicher erscheinen soll.
Beispiel: /MeineDaten

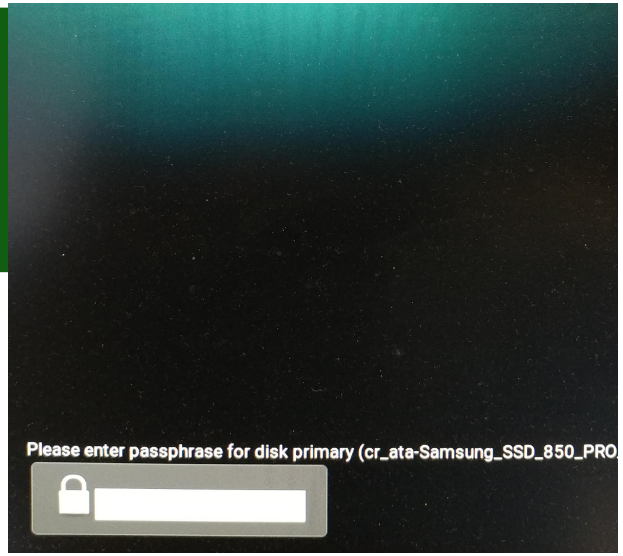
Am besten macht man das, wenn man das System neu installiert.

Der Installer von openSUSE ist hervorragend!

**Sie machen es zum ersten Mal? Dann installieren Sie zum Üben openSUSE auf einem USB Speicher. Tipp:
Datenkabel von den internen Festplatten dafür vorher abziehen.**



Weiterführende Ideen



System komplett verschlüsseln (YaST kann das).

Statt Passwort eine Entschlüssel-Datei verwenden, die auf einem USB-Speicher ist, den Sie immer bei sich haben.

Am Besten:
(Unverschlüsselten) Boot-Bereich nicht auf interner Festplatte, sondern auf USB-Speicher unterbringen, den Sie immer bei sich haben.

Siehe auch hier:
http://thesimplecomputer.info/full-disk-encryption-with-ubuntu
https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html
https://wiki.archlinux.org/index.php/Dm-crypt/Encrypting_an_entire_system#Encrypted_boot_partition_.28GRUB.29

Wir erschweren Angriffe über den Browser

Der Browser: Das Einfallstor für Probleme

Windows-Nutzer glauben an Antivirensoftware

Die macht das System aber nur unsicherer (…für erfahrene Anwender. Laien brauchen so etwas aber - unter Windows.)

Mehr Infos dazu:

https://www.golem.de/news/antivirensoftware-die-schlangenoel-branche-1612-125148.html

http://www.silicon.de/41639873/pro-und-contra-av-software-deinstallieren

https://www.theregister.co.uk/2017/01/27/gag_free_ex_mozilla_dev_joins_antivirus_roasting_chorus_its_poison/

https://www.heise.de/newsticker/meldung/US-CERT-warnt-vor-HTTPS-Inspektion-3660610.html?wt_mc=rss.ho.beitrag.atom

Schauen wir uns an, was wir statt dessen tun können

FOCUS ONLINE

Suche

Politik Finanzen Wi… Gesundheit Kultur Panorama Sport Digital Reisen Auto Immobilien Video Local

EILMELDUNG + + + Nach Giftgas-Angriff: U… hen mit Alleingang in Syrien, falls UN nicht handelt + + +

24-Stunden-Newsticker

alle Ne…

+++ US-Politik im News-Ticker +++: Trump verbannt seinen Chefstrategen Steve Ban...
Nach Giftgas-Angriff: USA drohen mit Alleingang in Syrien, falls die UN nicht ha...
Sprachaufzeichnung und Bild von Verdächtigem: "Eine Sensation": Freund der Böger...

The Weather Channel

Ausland Aktualisiert vor 27 Minuten 7742

Nach Giftgas-Angriff

USA drohen mit Alleingang in Syrien, falls die UN nicht handelt

Irak, Syrien, Libyen – in diesen Ländern wütet die Terrormiliz „Islamischer Staat" besonders brutal. Nach den Anschlägen von Paris hat die Anti-IS-Koalition ihre Angriffe gegen die islamistische Terrormiliz intensiviert. Auch Deutschland beteiligt sich mit Aufklärungsflugzeugen und Soldaten. »

Gesundheit vor 47 Minuten 1

Dramatische Missstände an Kliniken

Intensivkrankenschwester erzählt: „Ärzte ignorieren oft simpelste Hygieneregeln"

Überlastete Pflegekräfte, vernachlässigte Patienten, multiresistente Keime, mangelnde Hygiene – das sind nur einige derzeit diskutierte Schlagworte. Was läuft schief in Deutschlands Krankenhäusern? FOCUS Online hat mit einer Intensivkrankenschwester gesprochen. »

Deutschland 13:01 Uhr 24

Bundeskabinett beschließt Gesetzentwurf

Kulturelle und religiöse Motive gelten nicht: Warum Verbot von Kinderehen richtig ist

Keine Frage: Der nun vom Bundeskabinett beschlossene Gesetzentwurf zum Verbot von Kinderehen ist richtig. Das gilt auch, obwohl die bisherige Regelung, wonach Jugendliche ab 16 Jahren heiraten konnten, wenn die Eltern zustimmten, so gut wie nicht mehr nachgefragt wird. *Von FOCUS-Online-Korrespondentin Martina Fietz* »

Krebs kann sich durch zahllose Hinweise zeigen. Doch viele Menschen nehmen potenzielle Warnsignale nicht ernst. Symptome für Krebs lassen nämlich auch oft auf harmlosere Krankheitsbilder schließen. Einige Anzeichen sollten Sie mit einem Arzt

Eigentlich wollten Sie doch nur zu focus.de

Aber diese ungebetenen Gäste wollen auch Programme auf Ihrem PC ausführen.

Einstellungen...
Informationsleiste anzeigen, wenn Skripte blockiert werden
Am unteren Rand anzeigen
Klang ausgeben, wenn Skripte blockiert werden
Permanent "Allow" commands in private windows
Skripte allgemein erlauben (nicht empfohlen)
Temporäre Berechtigungen aufheben
Alle Beschränkungen für diese Seite aufheben
Temporär alle Beschränkungen für diese Seite aufheben
Berechtigungen dieser Seite speichern
Kürzlich blockierte Websites
Nicht vertrauenswürdig
googletagmanager.com verbieten
ioam.de erlauben
ioam.de temporär erlauben
bf-ad.net erlauben
bf-ad.net temporär erlauben
gstatic.com erlauben
gstatic.com temporär erlauben
outbrain.com erlauben
outbrain.com temporär erlauben
lp4.io erlauben
lp4.io temporär erlauben
lotto24.de erlauben
lotto24.de temporär erlauben
focus.de erlauben
focus.de temporär erlauben

Skripte sind momentan verboten
Mittelklick oder Umschalt+Klick, um die Seiteninformationen aufzurufen...

| <SCRIPT>: 130 | <OBJECT>: 0

“JavaScript allows website creators to run any code they want when a user visits their website.”

Siehe hier:
https://www.datenschutzbeauftragter-info.de/skriptsprachen-und-javascript-einfach-erklaert/
https://heimdalsecurity.com/blog/javascript-malware-explained/

NoScript ist dein Freund!

Das ist eine Erweiterung für Firefox.

"... blockiert JavaScript, Java-Applets, Adobe Flash, Microsoft Silverlight und andere Web-Techniken."

Eine Freigabe von Seiten erfolgt über eine Positivliste oder nur temporär bis zum Schließen des Browsers.

https://noscript.net/
https://de.wikipedia.org/wiki/NoScript
https://en.wikipedia.org/wiki/NoScript

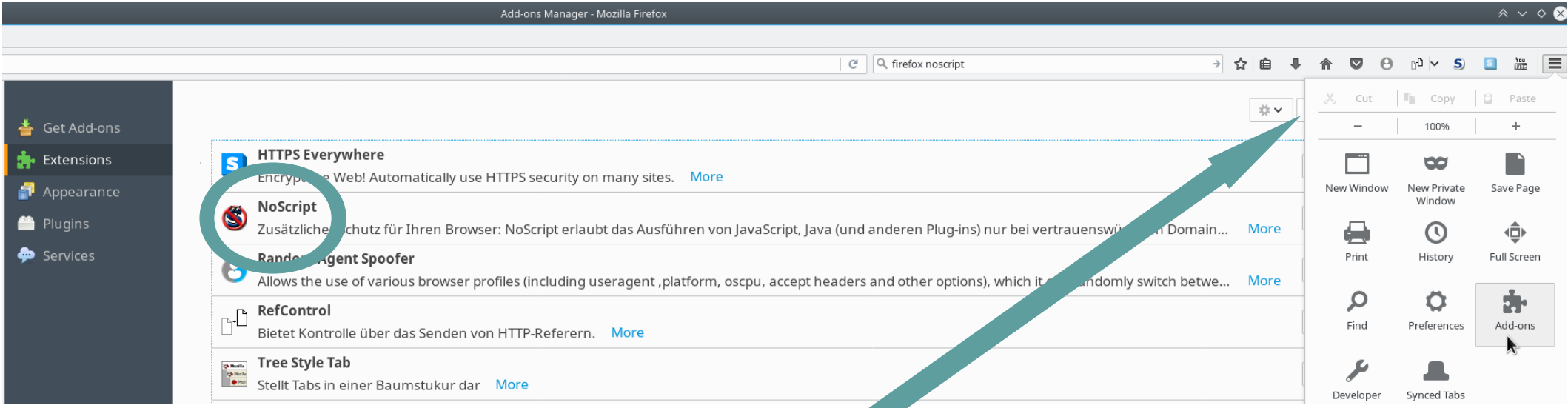
Nützlich: Panopticlick.eff.org

(Das ist ein klickbarer Link)

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	3.01	8.04	no javascript
Hash of canvas fingerprint	3.01	8.04	no javascript
Screen Size and Color Depth	3.01	8.04	no javascript
Browser Plugin Details	3.01	8.04	no javascript
Time Zone	3.0	8.02	no javascript
DNT Header Enabled?	0.74	1.67	True
HTTP_ACCEPT Headers	4.54	23.26	text/html,application/xhtml+xml,application /xml;q=0.9,*/*;q=0.8 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	3.01	8.04	no javascript
Language	2.98	7.9	no javascript
System Fonts	3.01	8.04	no javascript
Platform	2.99	7.94	no javascript
User Agent	6.63	98.9	Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Touch Support	3.01	8.04	no javascript
Are Cookies Enabled?	0.18	1.13	Yes

Ohne JavaScript kann eine (angreifende) Webseite nicht viel ausrichten.

NoScript installieren



Darunter ist ein Suchfeld.
-Nach NoScript suchen.
-NoScript installieren.

Ohne JavaScript geht einiges nicht

Shopping, Flüge buchen, Youtube, ….

Scripte dafür also temporär oder permanent erlauben.

Aber nur die nötigen!

Meine Browser (in dieser Priorität)

Firefox

- Für's übliche Browsen
- Mit NoScript, HTTPS Everywhere, RefControl

(und Tree Style Tab und browser.sessionstore.interval = 600000)

- Allow pages to choose their own fonts, instead of my selections above = Nein

Chromium

- Für Webdesign mit Wordpress. Alle Settings möglichst restriktiv

Chrome

-So gut wie alles aktiviert. Für Notfälle, falls eine (vertrauenswürdige) Seite auf keinem der anderen Browser läuft

Wir machen den Leuten, die an der Leitung lauschen, das Leben schwer

Zwei Probleme:

Jede unverschlüsselte Datenübertragung im Internet kann jeder Server mitlesen, an dem sie vorbei kommt.

Über Ihre IP-Adresse findet man Sie.

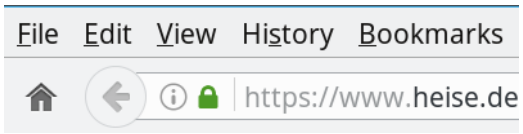
Lösung: HTTPS und ggf. ein VPN (Virtual Private Network)

So verschlüsseln wir unsere Datenübertragung

Verwenden Sie https:// statt http://, falls der Server (die Webseite), den Sie besuchen wollen, HTTPS kann.

Installieren Sie die Erweiterung “HTTPS Everywhere” im Firefox, Chromium und Chrome.
Die wählt automatisch HTTPS aus, falls der Server HTTPS unterstützt.
(Weniger tippen müssen.)

Achten Sie auf diese Anzeige:



Aber Vorsicht!

HTTPS ist SSL (bzw. TLS). Das ist zwar besser als nichts, hat aber Schwächen.

Mehr Infos hier:
http://www.hackerfactor.com/blog/index.php?/archives/752-SSL-Fingerprinting-and-Hijacking.html

SSL braucht “Zertifikate”. Bei deren Verwaltung wird manchmal geschlampt.

Mehr Infos hier:
https://www.heise.de/security/meldung/Chrome-soll-ab-sofort-Zertifikate-von-Symantec-herabstufen-3663517.html
https://www.golem.de/news/chrome-google-plant-drastische-massnahmen-gegen-symantec-1703-126916.html
https://www.engadget.com/2017/03/31/when-the-s-in-https-also-stands-for-shady/
(bei Letzterem sind auch die Comments interessant)

https: Probleme

Antivirensoftware kann SSL kaputt machen

Relevant:
https://www.heise.de/newsticker/meldung/US-CERT-warnt-vor-HTTPS-Inspektion-3660610.html?wt_mc=rss.ho.beitrag.atom

Siehe auch hier:
https://eric-diehl.com/does-https-prevent-man-in-the-middle-attacks/

Letztere zeigt auch, wie man MITM feststellen kann

Sollten Sie tun.

https://www.ceilers-news.de/serendipity/207-Man-in-the-Middle-Angriffe-auf-HTTPS.html

Manche Webseite liefern auch HTTP-Inhalte auf HTTPS-Seiten aus...

So verbergen wir unsere IP-Adresse

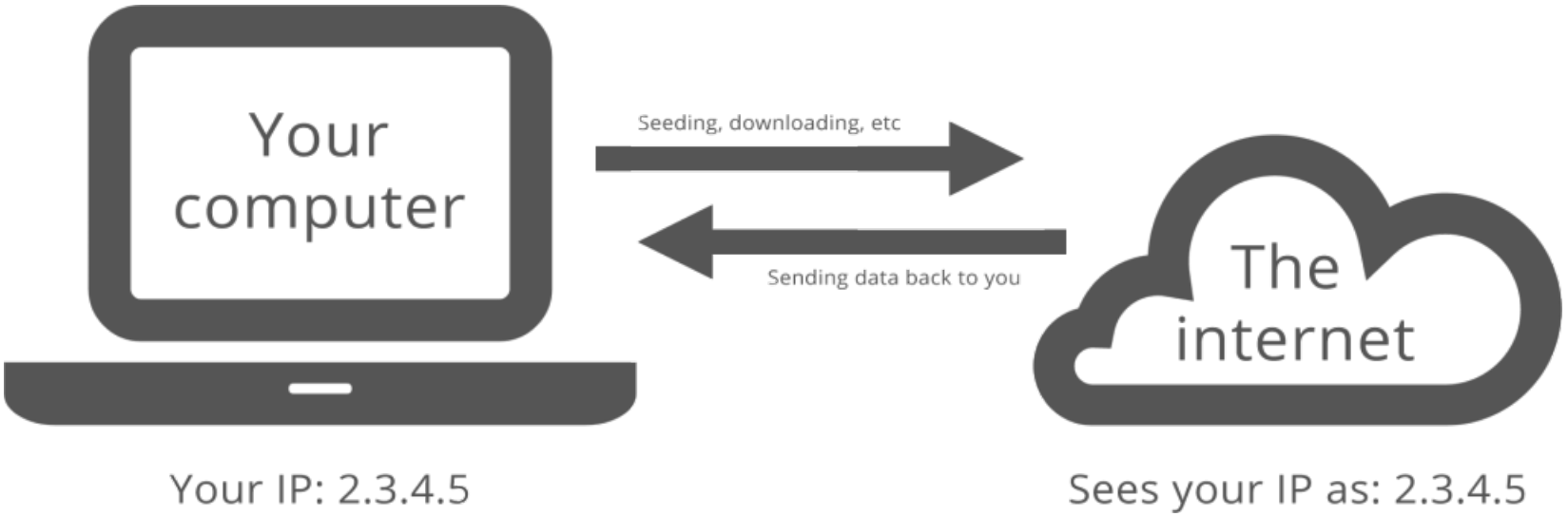
Wir benutzen ein VPN (Virtual Private Network)

Es gibt dafür kommerzielle Anbieter oder Tor

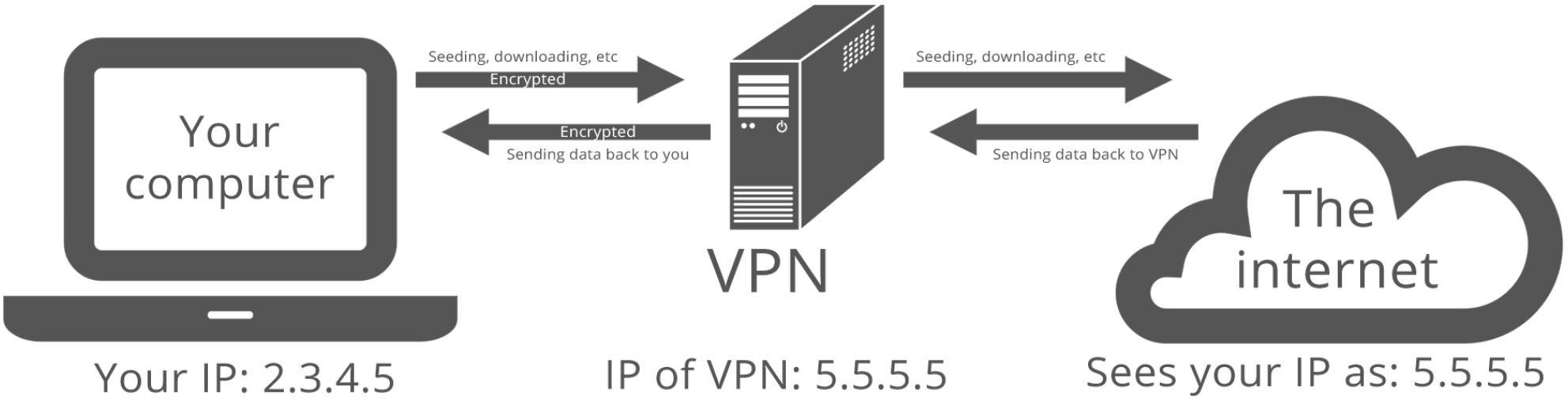
Unterschiedliche Stärken/Schwächen

Beide werden übrigens manchmal geblockt

Ohne VPN: Ihre IP-Adresse ist sichtbar



Mit VPN: Ihre IP-Adresse ist nicht sichtbar

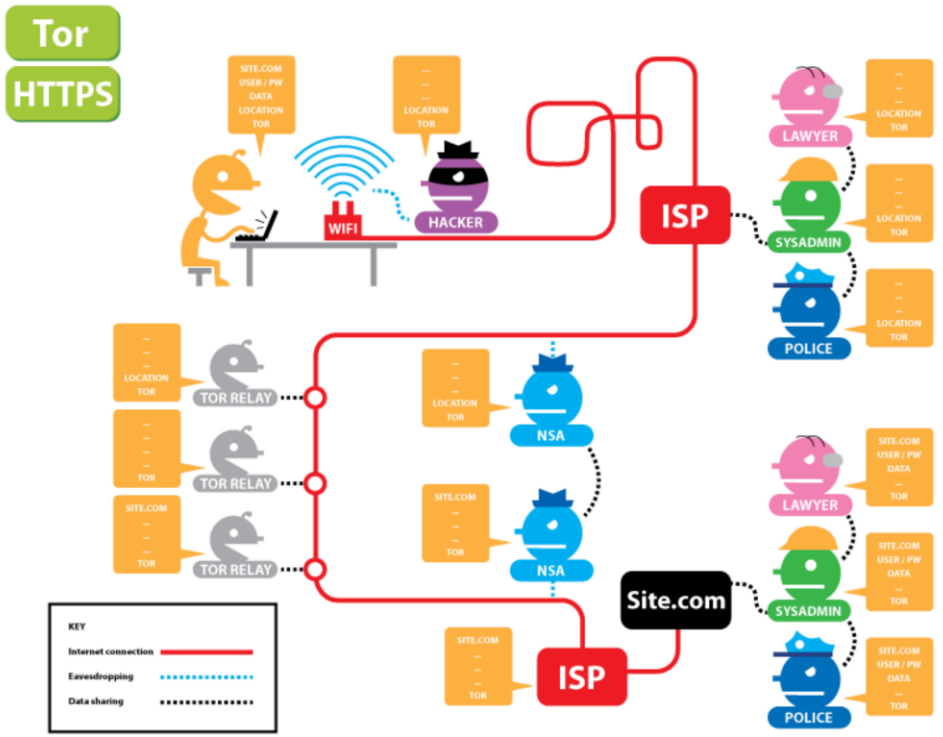


Bei Tor haben Sie mehrere dieser “Nodes” hintereinander.

Bilder von seedboxgui.de

Demo

Eine nützliche Demo der Electronic Frontier Foundation die zeigt, was ein Lauscher sieht, wenn Sie Tor und/oder HTTPS ein- oder ausgeschaltet haben.



https://www.eff.org/pages/tor-and-https

Tor oder kommerzielles VPN?

Tor:

Man muß niemandem vertrauen

Eher Langsam

Kostenlos

Exit-Node problematisch: Besser keine persönlichen Daten angeben.

“Even with HTTPS, TOR offers no protection since SSL certificates can be faked and can change with each HTTPS request.”

… und hier?

Kommerzieller Anbieter:

Anbieter sieht alle meine Daten (bis auf https)

Schnell(er)

Kostet ein paar Euro im Monat

Siehe auch:
https://www.hackerfactor.com/blog/index.php?/archives/721-TOR-and-Trust.html

Tor bequem benutzen

Installieren Sie einfach diesen Browser:

https://www.torproject.org/projects/torbrowser.html.en

Noch besser: Booten Sie eine spezielle Linux-Distribution:

Tails https://tails.boum.org

Whonix https://www.whonix.org

Siehe dazu nächstes Kapitel.

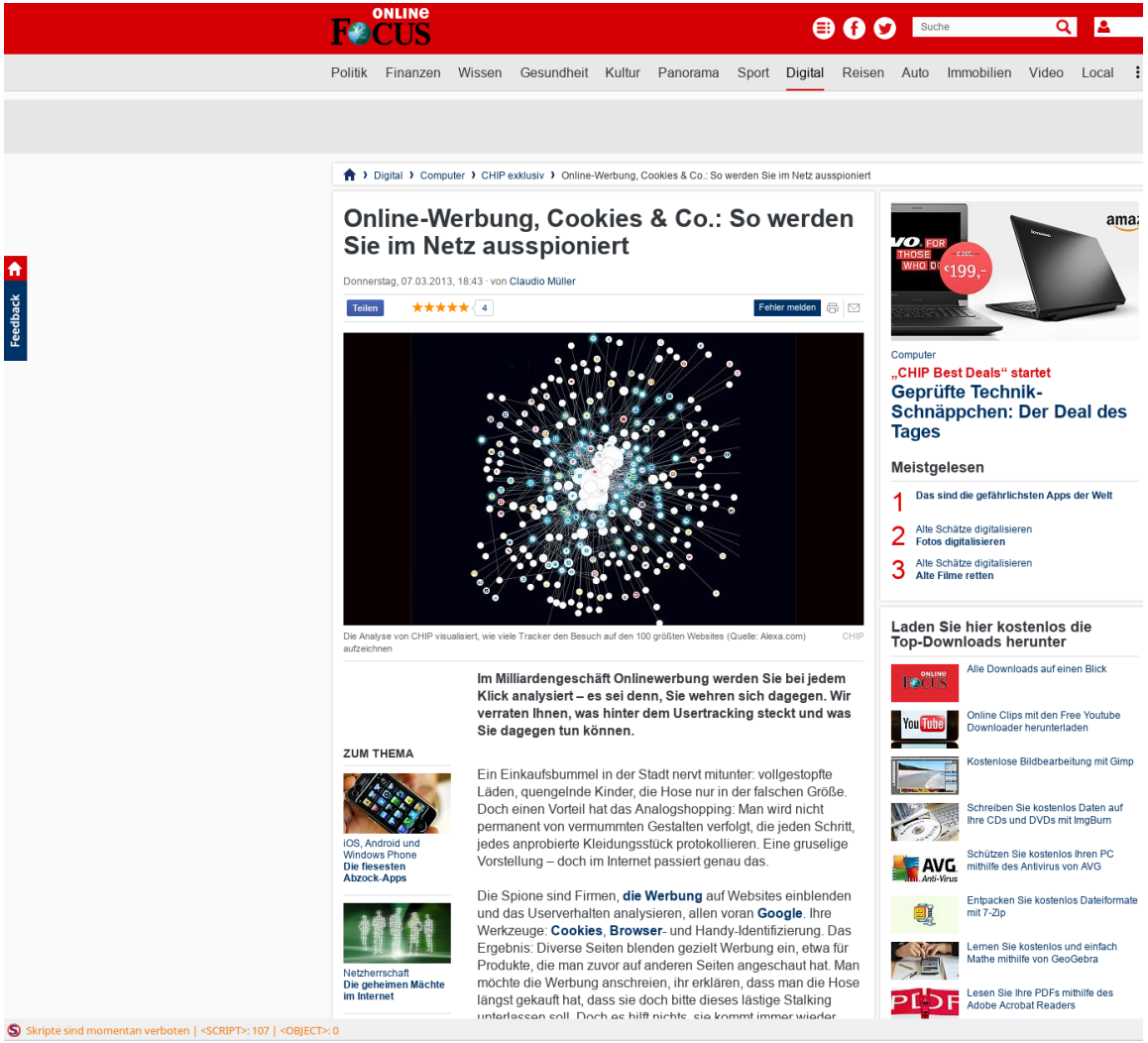
Senden Sie keinen persönlichen Daten ~~über eine nicht-verschlüsselte Verbindung~~: Der Exit-Node liest mit.

Wir besuchen die Schmuddelecken des Internet ohne Sorgen

Typische Schmuddelecken:

- Spiegel.de
- Bild.de
- Stern.de
- ARD.de
- Focus.de
- …

107 Scripte ???



Wir besuchen die Schmuddelecken des Internet ohne Sorgen

Was tun, wenn wir
diese Seiten mit eingeschaltetem
JavaScript brauchen?

Verschiendene Betriebssysteme einsetzen

Linux vom USB-Stick booten

(… aber Festplatten bleiben eingeschaltet? Gefährlich! Diese vorher verschlüsseln.)

Qubes OS einsetzen

Cool, kann ich bei mir aber nicht installieren (Grafik-Treiber…)

https://www.qubes-os.org/

Lösung: Festplattenumschalter

Mehrere Festplatten einbauen, aber nur die jeweils benötigte einschalten
(bevor Sie den PC starten).
Die anderen können nicht manipuliert werden (weil ausgeschaltet).

Festplattenumschalter? Aber wie???

Zum Beispiel so:

Sie bauen mehrere SATA-Festplatten/SSDs in Ihren PC ein

Für verschiedene Anwendungen

Zum Beispiel:

Eine mit OpenSUSE (Haupt-Betriebssystem. Restriktive Browser.)

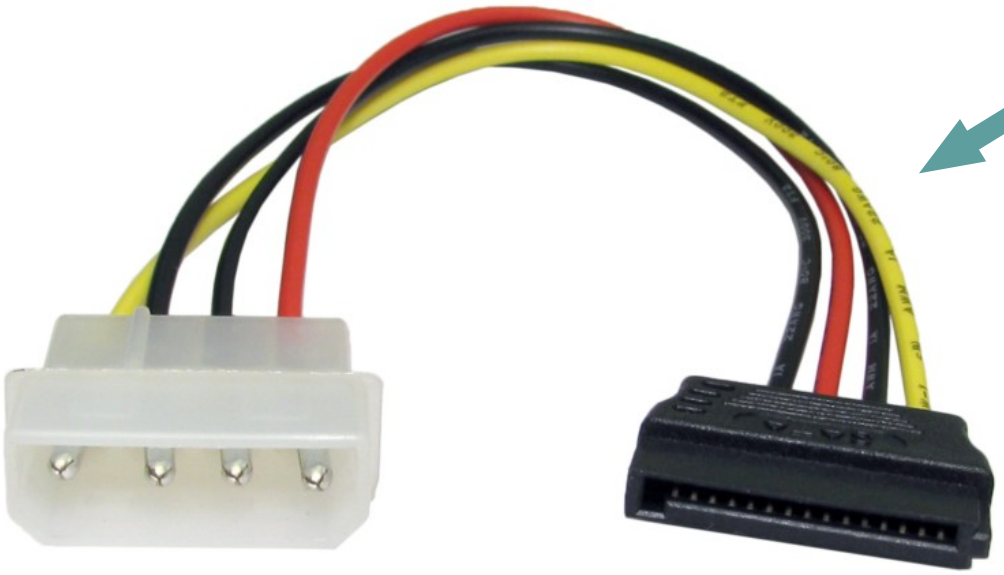
Eine mit PC-BSD (Spielwiese, um zu sehen, was es noch so gibt)

Eine mit Windows (Falls man mal ein Windows-Program braucht)

Eine mit Ubuntu (Alles erlaubt: Mit Chrome-Browser und aktivieren Scripten, Flash, Cookies etc. um Focus.de zu besuchen, verdächtige .zip-Dateien aus SPAM-Emails zu öffnen, u.s.w.)

Zu faul dazu? Wegwerf-Betriebssystem in virtueller Maschine ist besser als nichts.

Und so wählen Sie die jeweilige Festplatte aus



Hier schaltet man den Strom ab!

Z. B. durch Umschalter, der die 5V-Leitung (rot) umschaltet.

Oder mit einer kleinen Relais-Schaltung.

(Das ist ein Stromversorgungskabel für Festplatten.)

Umschalter kann man kaufen

Oder selber bauen

Laufwerk-Umschalter*

* Atuelle Version ohne Windows

(Ich weiss, ich weiss… Überdimensionierte Relais
in einem zur Dauerlösung gewordenen Probeaufbau.)

Zusammenfassung

Nutzen Sie Ihre Rechte

Verwenden Sie so viele dieser Tipps wie möglich

Halten Sie Ihre Software aktuell

Machen Sie Backups

Stärken Sie die Alternativen: Statt Microsoft/Intel besser Linux/AMD

Holen Sie keinen Hund vom Züchter, sondern vom Tierheim