Erstellen eines sicheren PC´s / Laptop

Ersteller	Inhalt	Datum
	Initiale Erstellung	25.01.2019

Inhalt

Vorwort

Ein sicherer PC / Laptop kann eine weitreichendere Definition unterliegen. Insbesondere auf den Bezug der Nutzung. Der Ansatz dieses Tutorials ist es, einen PC aufzusetzen, der sich im Netz weitgehend unerkannt bewegen kann. Ferner wird auch das Thema der Verschlüsselung des Geräts behandelt.

Folgende Settings werden in diesem Tutorial beschrieben:

- Festplatten verschlüsseln
- Nutzung eines VPN
- Browser Konfiguration
- Ändern der Hardware ID
- Mikrofon und Kamera deaktivieren
- Einrichten einer Blue Screen Methodik für sofortiges Verschlüsseln
- Einrichten einer Virtuellen Maschine (VM-Ware)

Schritt 1: Festplatte verschlüsseln

Nachdem ihr ein Betriebssystem eurer Wahl aufgespielt habt, ist es unabdingbar, den Laptop zu verschlüsseln. Die Verschlüsslung ist die Lebensversicherung einer jeden Person. Sie erschwert dem Finder oder Dieb das Kompromittieren Eurer Daten, oder den Behörden eine Ermittlung gegen euch erheblich, bzw. macht es sogar im Optimalfall unmöglich.

Empfohlen wird ein Passwort mit einer Länge von 30 Zeichen, aber in der Regel kann man sagen, je länger es ist, desto schwieriger wird es eure Verschlüsselung zu knacken.

Oft wird diskutiert, mit welchem Tool man verschlüsseln soll. Da sich Veracrypt bewährt hat und dies noch sicher sein sollte, ist es ratsam auch dieses zu benutzen.

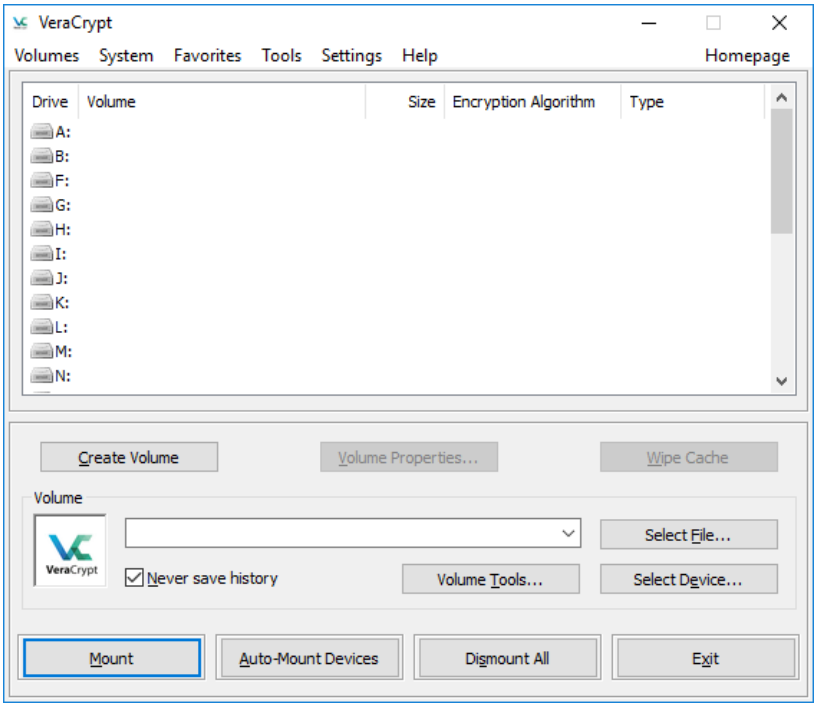
DOWNLOADLINK

Da wir unser komplettes System verschlüsseln wollen, ist eine Installation auf dem Betriebssystem unausweichlich.

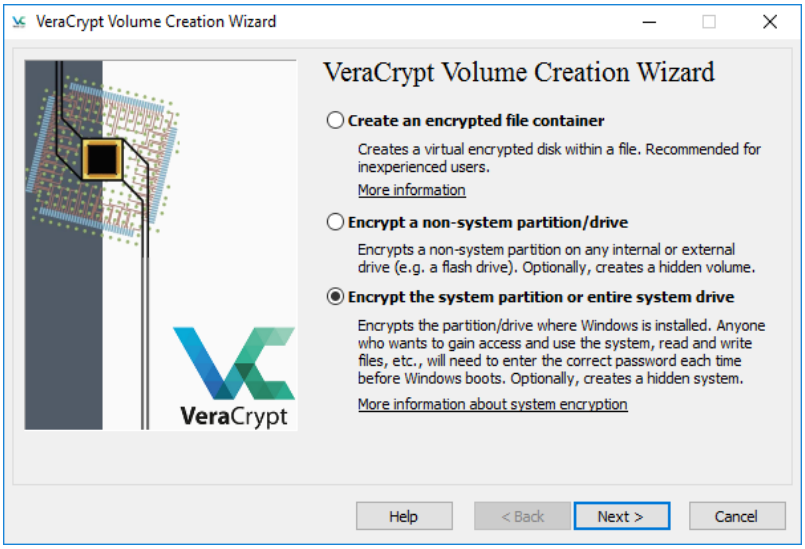
Ich erkläre nun die Installation und Einrichtung Schritt für Schritt:

Verschlüsselung einer Systempartition mit VeraCrypt
Die Anleitung führt durch die Systempartitionverschlüsselung mithilfe von VeraCrypt.
Anmerkung: Die nachfolgende Anleitung wurde auf einem Windows 10 angefertigt. Die Software ist allerdings auch für Mac und Linux vorhanden und funktioniert gleich - einzige Unterschiede sind Visualisierungen (der Fenster) und die Installation.
Container erstellen

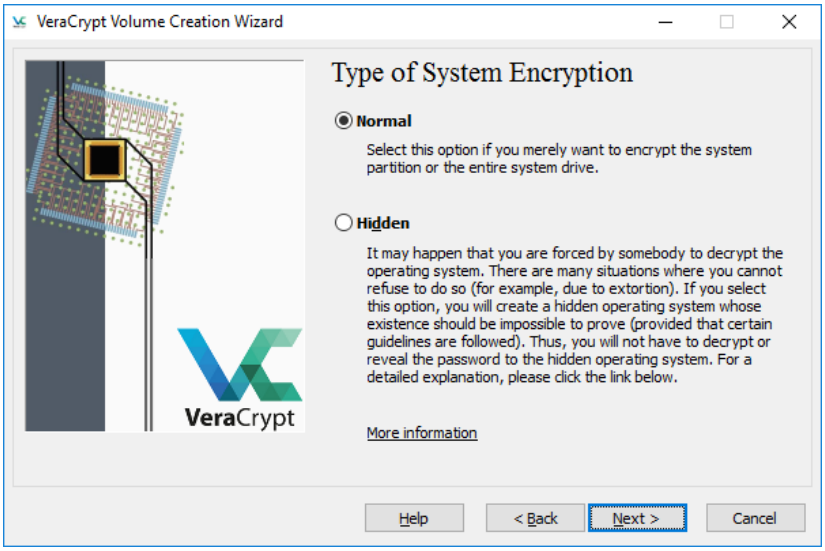
1. Klicken Sie auf “Create Volume ...“.



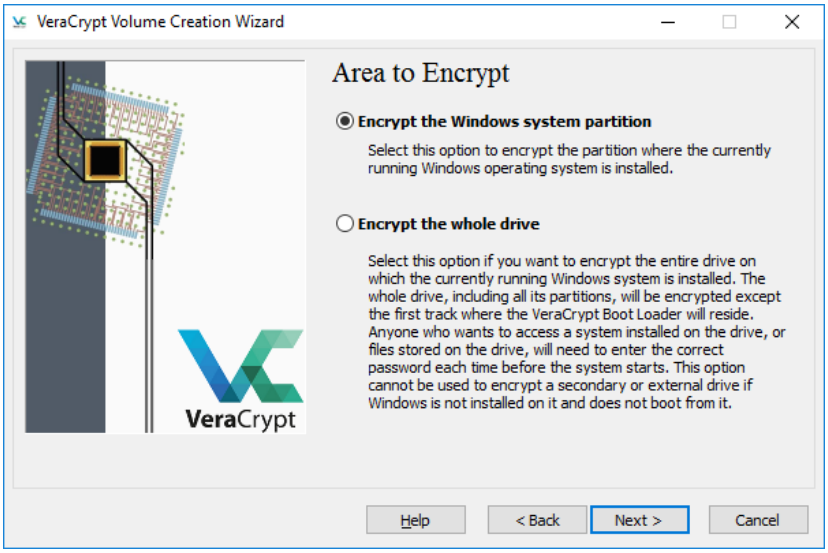
2. Wählen Sie "Encrypt the System Partition or entire System Drive" und klicken Sie auf "Next >".



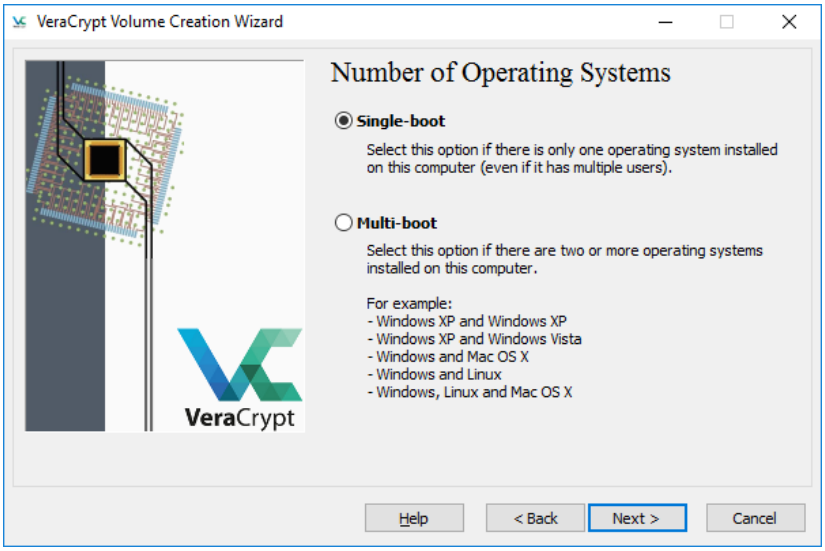
3. Wählen Sie "Normal" und klicken Sie auf "Next >"



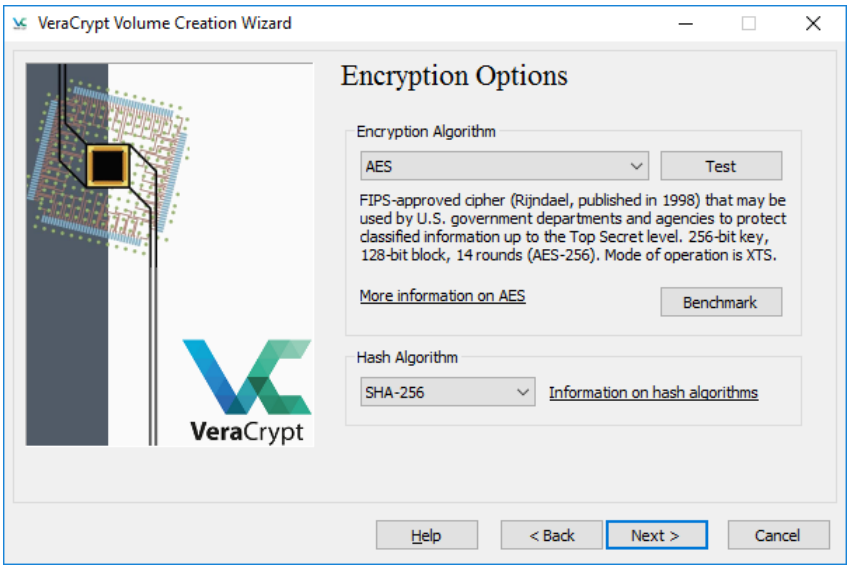
4. Wählen Sie den zu verschlüsselnden Bereich aus. "Encrypt the Windows System Partition" verschlüsselt nur die Partition auf der das Betriebssystem liegt (generell C:), während andere Partitionen auf derselben Festplatte unverschlüsselt bleiben. Letztere lassen sich jedoch auch nochmals extra verschlüsseln, was eine größere Sicherheit bietet, wenn unterschiedliche Passwörter gewählt werden.
Deshalb wird in dieser Anleitung nur die Systempartition verschlüsselt. Wählen Sie also "Encrypt the Windows System Partition" und klicken Sie anschließend auf "Next >".



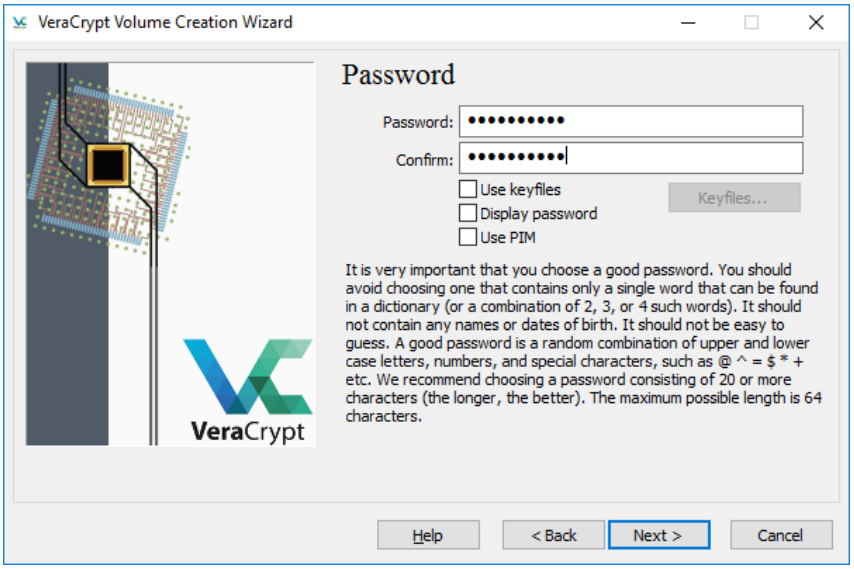
5. Anzahl der Betriebssysteme: Bei den meisten Nutzern wird auf dem Gerät nur ein Betriebssystem installiert sein. Deshalb wird diese Anleitung sich damit befassen. Wählen Sie also "Single-boot" und klicken Sie auf "Next >"
Anmerkung:
Sollten mehrere Betriebssysteme installiert sein (z.B. zwei verschiedene Windows Versionen, Windows+Linux etc.), wählen Sie "Multi-boot".



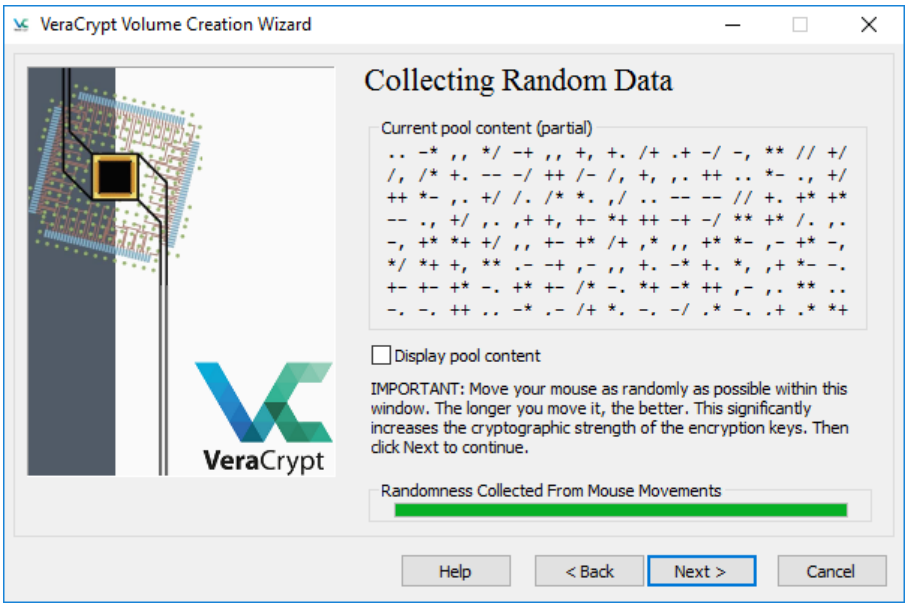
6. Wählen Sie danach einen Verschlüsselungsalgorithmus und einen Hash-Algorithmus aus. Klicken sie anschließend auf "Next >".



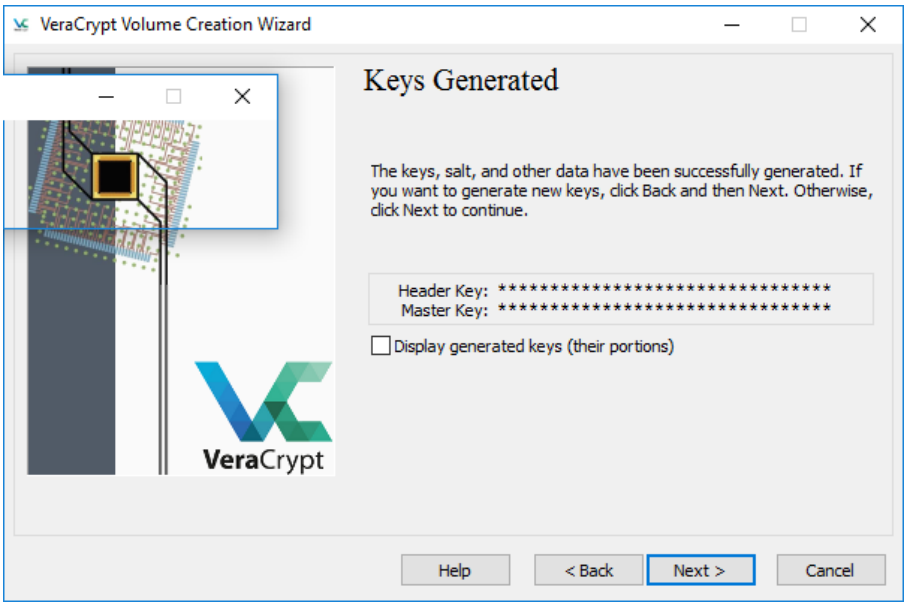
7. Wählen Sie danach ein Passwort aus und klicken Sie anschließend auf "Next >".



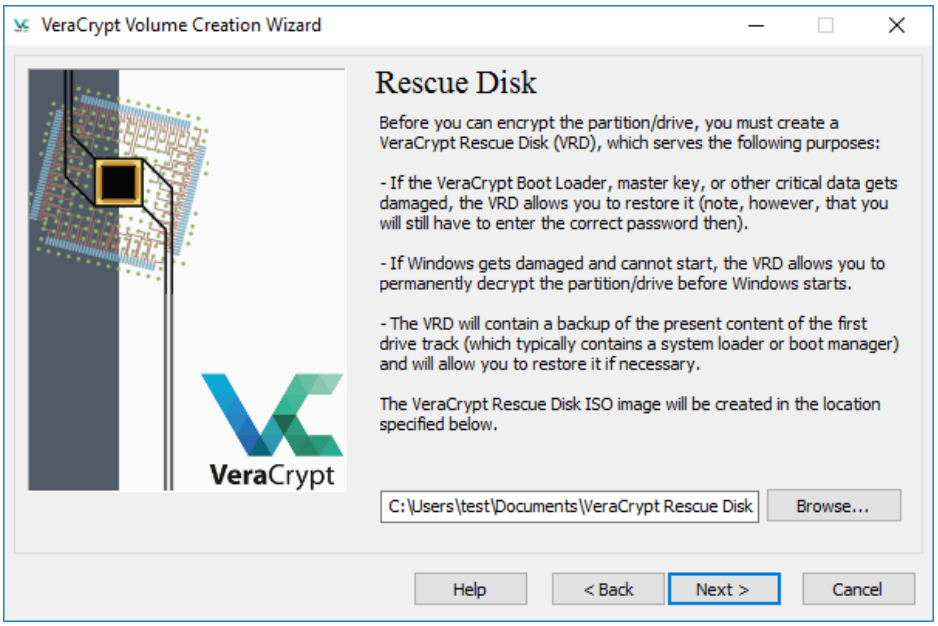
8. Im nachfolgenden Fenster werden Sie darum gebeten, Ihre Maus so zufällig wie möglich über das Fenster zu bewegen. Dies ist wichtig, damit die Verschlüsselung möglichst einzigartig ist. Es ist empfohlen, dies mindestens 30 Sekunden zu machen. Eine Leiste am unteren Teil des Fensters wird sich mit der Zeit füllen. Wenn sie voll ist, erhalten Sie die höchste Sicherheit. Klicken Sie danach auf "Next >".



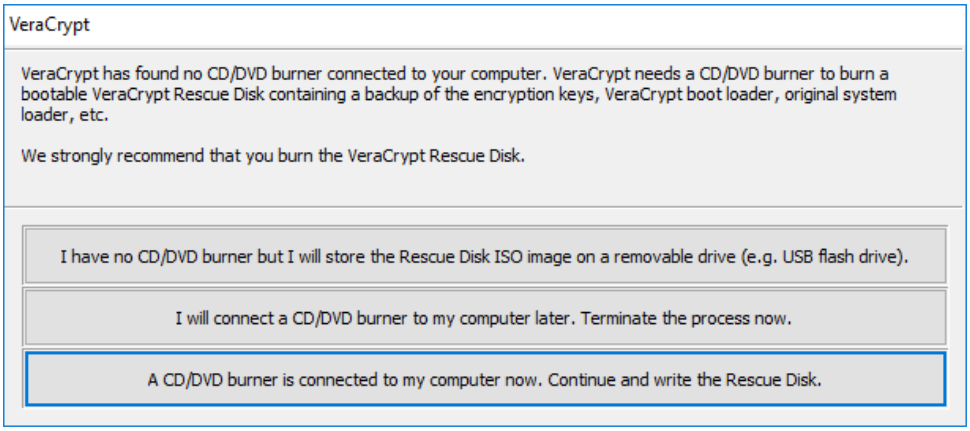
9. Im nächsten Fenster können Sie sich die generierten Schlüssel anzeigen lassen, wenn Sie möchten. Klicken Sie danach auf "Next >"



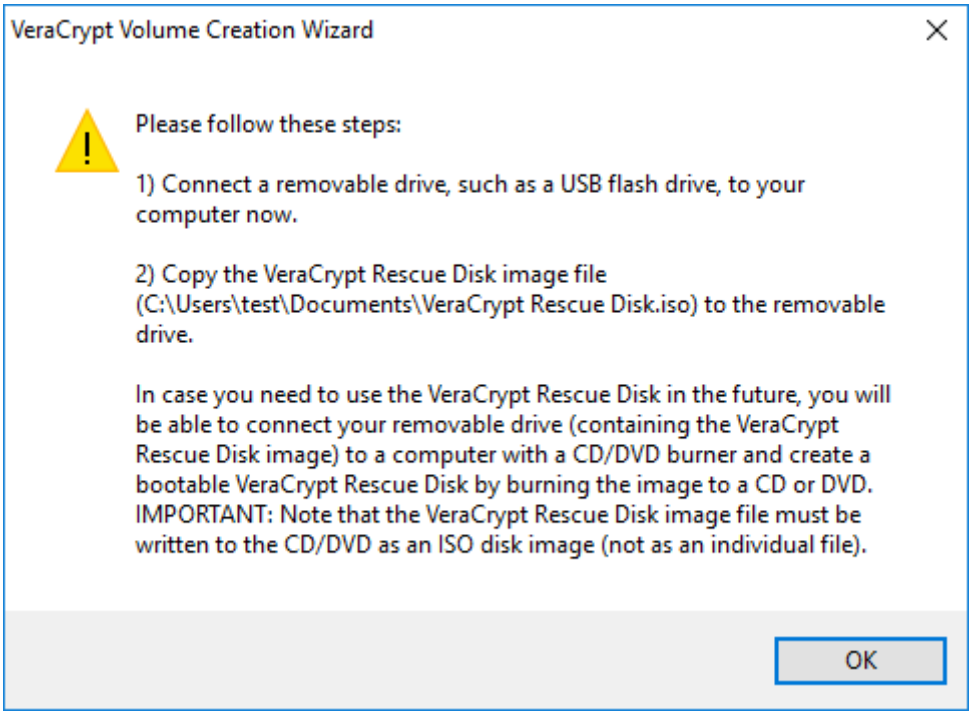
10. Nun müssen Sie eine sogenannte "Rescue Disk" erstellen. Diese ist nötig, falls das Dateisystem irgendwie beschädigt werden sollte (Stromausfall, Absturz etc.), um das System wiederherzustellen.
Wählen Sie einen Speicherort aus und klicken Sie auf "Next >".



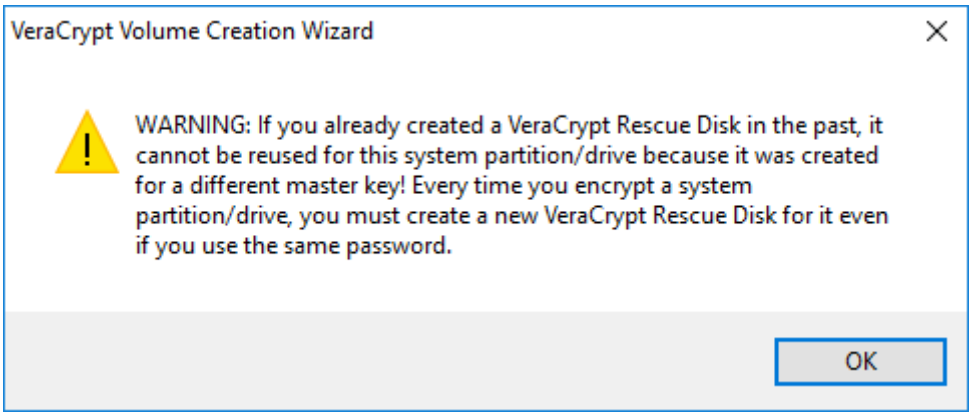
11. Sollte kein CD-Brenner an dem System angeschlossen sein warnt VeraCrypt davor die "Rescue Disk" unbedingt zu einem späteren Zeitpunkt entweder auf einen USB Stick oder eine CD zu brennen. Klicken Sie auf die erste Option um die Datei zu speichern und später manuell auf einen USB-Stick zu ziehen.



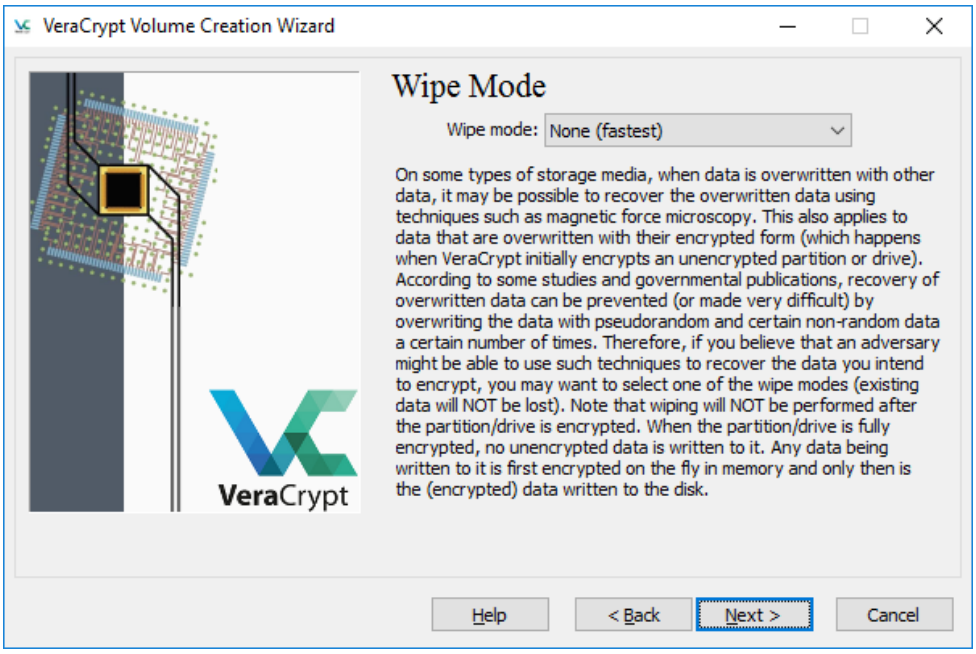
12. Nach der Auswahl der USB-Stick Option warnt VeraCrypt noch einmal die Datei unbedingt auf einen USB-Stick zu ziehen. Klicken Sie auf "OK".



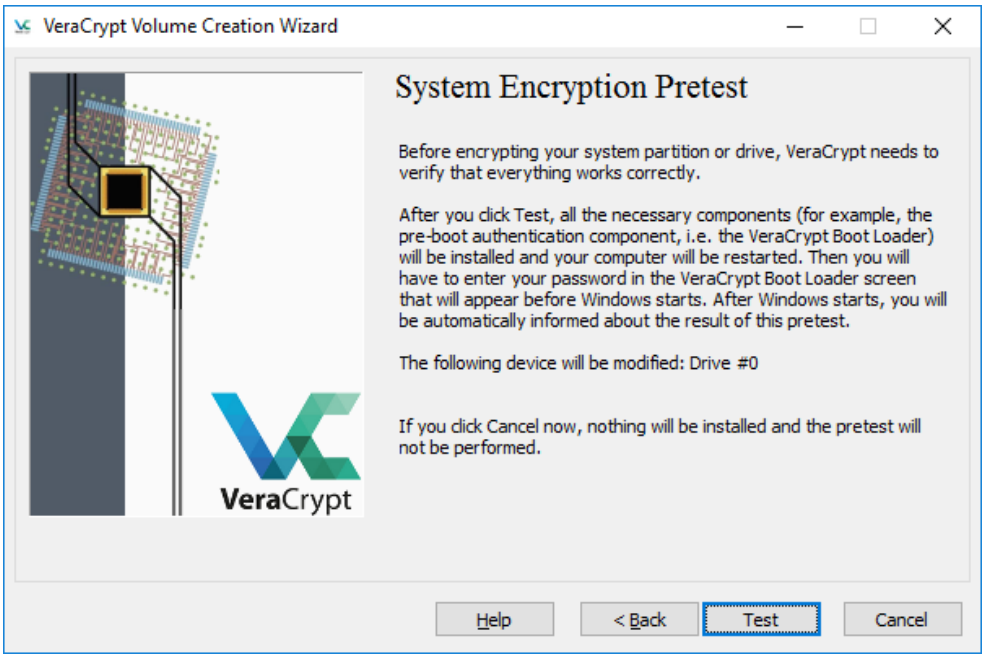
13. Falls Sie das System zuvor bereits verschlüsselt hatten und eine "Rescue Disk" erstellt hatten wird diese bei der neuen Verschlüsselung nicht funktionieren. Deshalb unbedingt die aktuelle "Rescue Disk" aufbewahren. Klicken Sie auf "OK"



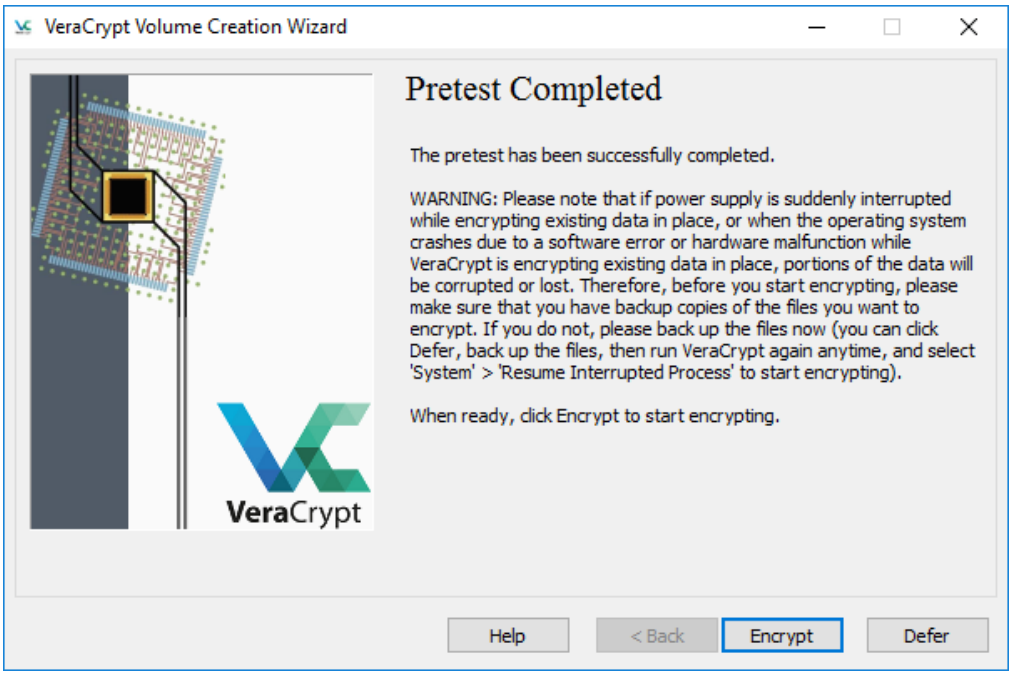
14. Wählen Sie den "Wipe Mode". Hierbei kann generell "None (fastest)" benutzt werden, außer Sie möchten verhindern, dass früher gelöschte Daten eventuell wiederhergestellt werden könnten.
Klicken Sie anschließend auf "Next >".



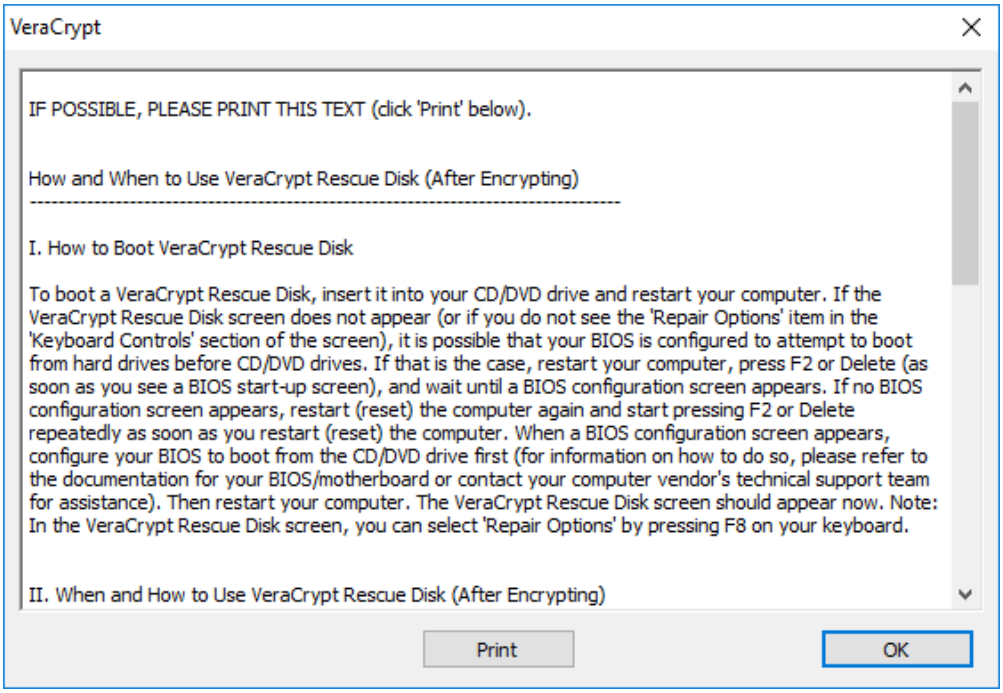
15. Bevor VeraCrypt die Systempartition verschlüsselt wird das Starten des Computers mit dem zuvor ausgewählten Passwort getestet. Bei einem Fehler kann das System weiterhin genutzt werden, was nach der Verschlüsselung nicht mehr möglich wäre. Klicken Sie auf "Test".



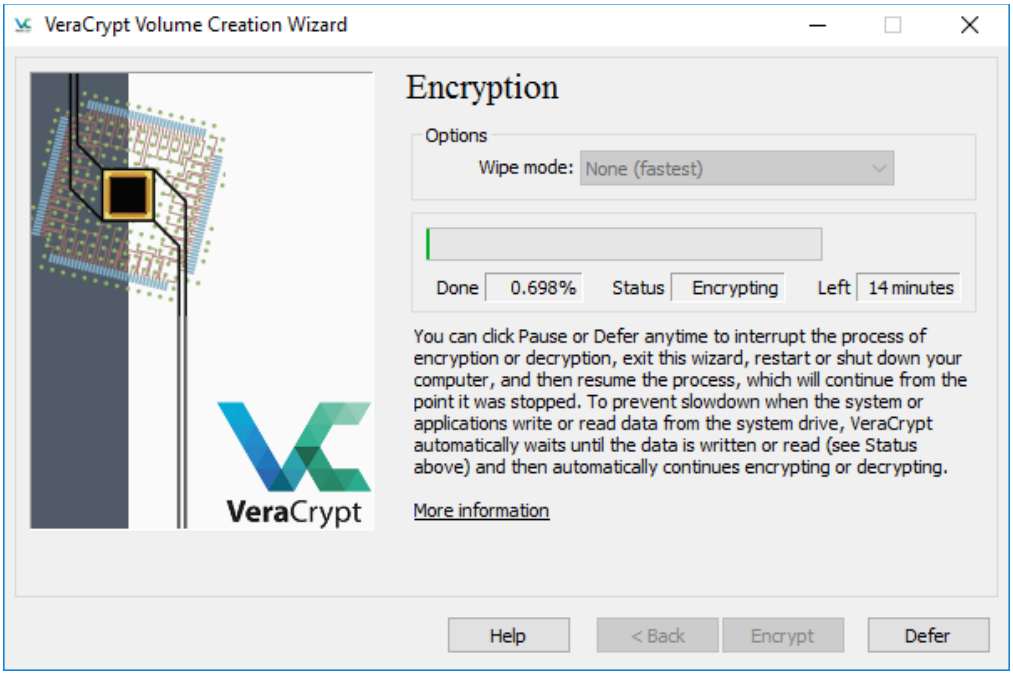
16. Nachdem der Computer neu gestartet hat und das Passwort korrekt eingegeben wurde, startet sich VeraCrypt automatisch um anzuzeigen, dass der Test erfolgreich war. Wenn Sie bereit sind das System zu verschlüsseln ("Rescue Disk" extern gespeichert und ein Backup der Daten gemacht", klicken Sie auf "Encrypt".



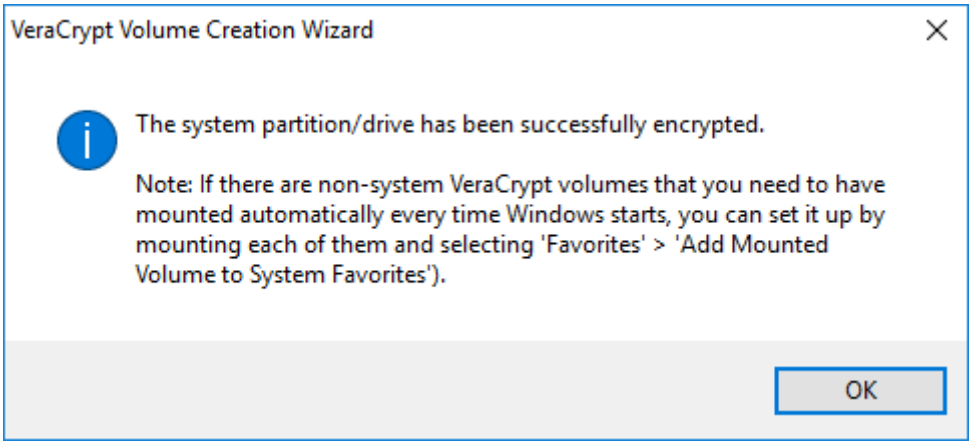
17. Bevor das System verschlüsselt wird erhalten Sie nochmals eine Anleitung zur Benutzung der "Rescue Disk". Lesen Sie sich diese aufmerksam durch und klicken Sie anschließend auf "OK".



18. Nun wird Ihr System verschlüsselt. Es wird eine ungefähre Laufzeit angegeben.



19. Sobald die Verschlüsselung fertig gestellt ist erhalten Sie eine Bestätigung.



Nutzung
Die Nutzung dieser Funktion erfolgt automatisch. Bei jedem Neustart des Betriebssystems erhalten Sie nun eine Aufforderung, ihr Passwort einzugeben. Ebenso kann es sein, dass Sie darum gebeten werden, Ihr PIM einzugeben. Sollten Sie bei der Einrichtung kein PIM vergeben haben, lassen Sie das Feld leer (drücken Sie einfach die Enter-Taste). Das Passwort wird nun verifiziert und kurz darauf fährt der Bootvorgang wie gewohnt fort.

Eine Anleitung für eine Vollverschlüsselung findet ihr hier:
https://www.kim.uni-konstanz.de/e-mail-und-internet/it-sicherheit-und-privatsphaere/sicheres-endgeraet/datenverschluesselung/verschluesselung-einer-systempartition-mit-veracrypt/

Nachdem ihr euer System verschlüsselt habt, empfiehlt es sich für Windows die Sicherheitsupdates zu installieren. Einfach für eure passende Windows-Version die Sicherheitsupdate Vollversion googeln.

Schritt 2: VPN-Anbieter Installieren

Grundvoraussetzungen um überhaupt sicher starten zu können, ist eine VPN Mitgliedschaft, bei einem der bekannten VPN Anbietern. Der monatliche Preis beträgt nun inzwischen nur noch knapp 12 Euro im Monat. Diese hat jeder irgendwie übrig. 12 Euro ist nicht die Welt, aber unsere Sicherheit schon! Die meisten schwören auf Perfekt Privacy (PP seit 2008) da dieser Provider laut eigenen Angaben nicht loggt. Dafür spricht, dass es bei PP noch keine bekannten Fälle eines Bustes gibt, der auf das Versagen des VPN Anbieters zurückzuführen ist. Was vielleicht auch noch ganz interessant ist: Bei PP laufen die Server über RAM-Disks und nicht über Festplatten. Insgesamt überzeugt PP auch durch ihre stets offene Kommunikation mit den Kunden im Website Internen Forum. Zu Seite von PP kommt ihr hier: perfect-privacy.com. Installiert den Client von Perfect Privacy auf eurem Rechner.

Habt ihr das gemacht, müsst ihr noch testen, ob der DNS Leakschutz von Perfect Privacy auch funktioniert. Das geht unter anderem direkt auf der Seite von Perfect Privacy oder aber hier:

DOWNLOADLINK

Schritt 3: Browser konfigurieren

Im nächsten Schritt installieren wir den Browser Firefox. Den Download gibt’s hier:

DOWNLOADLINK

Es ist meistens sinnvoll, direkt von der Seite des Herstellers zu downloaden und nicht über Portale wie Chip etc. Da kommt meistens eh nur Malware mit, wenn man nicht aufpasst. Außerdem geht ihr so sicher, die aktuellste Version zu installieren.

Nachdem ihr Firefox installiert habt, geht ihr nun in die Suchzeile oben und gebt "about:config" ein. Dort ändert ihr folgende Parameter. Hier gibt es die Anleitung mit Erklärung:

Möchte man mit dem Firefox-Browser sicher und Anonym surfen, sollte man etwas in der Config abändern. Um auch zu verstehen bzw. nachvollziehen zu können was man da macht, sollte man sich den ganzen Text durchlesen. Um die Config zu öffnen, bitte "about:config" eingeben und Enter drücken. Danach einfach nach den Befehlen suchen und abändern.

Geolocation API abschalten

Mit Hilfe der Geolocation API kann die geografische Position des Surfers relativ genau bestimmt werden. Zur Ortsbestimmung können je nach vorhandener Hardware im Rechner die WLANs in der Umgebung genutzt werden oder GPS-Hardware... Im ungünstigsten Fall kann der Standort nur anhand der IP-Adresse bestimmt werden. Die Nutzung der API erfolgt mit JavaScript. Aktuelle Firefox Versionen fragen nach, bevor der Zugriff auf die Geolocation API erlaubt wird. Trotzdem habe ich ein besseres Gefühl, wenn man es komplett deaktiviert. Dafür muss man unter "about:config" die folgende Variable setzen:

geo.enabled false
geo.wifi.uri (leerer String)
browser.search.geoip.timeout 1

Diese Einstellung ist wichtig, wenn man die eigene IP-Adresse mit Anonymisierungsdiensten oder VPNs versteckt.

WebGL deaktivieren

WebGL stellt eine JavaScript-API für das Rendering von 3D-Objekten bereit. Es kann für das Fingerprinting der Performance der Grafikhardware und OpenGL Implementierung genutzt werden, wie die Studie Perfect Pixel: Fingerprinting Canvas in HTML5 zeigt. Das Fingerprinting via WebGL kann mit folgenden Einstellungen verhindert werden:

webgl.disable-extensions true
webgl.min_capability_mode true
webgl.disable-fail-if-major-performance-caveat true

Außerdem ist WebGL ein (unnötiges) Sicherheitsrisiko, weil damit Angriffe auf das Betriebssystem möglich werden. Durch nachgeladene Schriften können Bugs in den Font Rendering Bibliotheken ausgenutzt werden, das gab es für Linux (CVE-2010-3855), Windows (ms11-087) oder OpenBSD (CVE-2013-6462). Die WebGL Shader Engines haben auch gelegentlich Bugs, wie z.B. MFSA 2016-53. Deshalb empfehlen wir, WebGL komplett zu deaktivieren, um das Risiko zu reduzieren:

webgl.disabled = true

WebRTC deaktivieren

WebRTC ist eine Technologie, die direkte Telefonie und Videochats zwischen Surfern im Browser ermöglichen soll. Derzeit gibt es wenig sinnvolle Anwendungen für diese Technologie und ich würde ein spezialisiertes Programm wie Jitsi bevorzugen. Wer es einmal ausprobieren möchte, kann sich Palava.tv oder browser meeting anschauen. Mit WebRTC kann die lokale IP Adresse des Rechners im LAN und die öffentliche IP Adresse ermittelt werden, wie eine Demonstration von D. Roesler zeigt. Auch VPN-Verbindungen können damit ausgetrickst werden. Außerdem kann das Vorhandensein von Kamera und Mikrofon als Feature im Browser Fingerprint genutzt werden.

Bei Firefox kann man WebRTC unter "about:config" deaktivieren:

media.peerconnection.enabled = false
loop.enabled = false
loop.facebook.enabled = false

Timing APIs deaktivieren
Die hochgenauen Timing APIs können von Webanwendungen zur Analyse des Ladens von Ressourcen oder des Nutzerverhaltens missbraucht werden (Timing Attacks on Web Privacy, PDF). Wenn man seinen Browser zum Lesen von Webseiten und nicht vorrangig für Games verwendet, sollte man die APIs deaktivieren:

dom.enable_resource_timing = false
dom.enable_user_timing = false
dom.enable_performance = false

Clipboard Events deaktivieren
Mit den Clipboard Events informiert Firefox eine Webseite, dass der Surfer einen Ausschnitt in die Zwischenablage kopiert hat oder den Inhalt der Zwischenablage in ein Formularfeld eingefügt hat. Es werden die Events oncopy, oncut and onpaste ausgelöst, auf die die Webseite reagieren könnte. Man kann diese Events unter "about:config" deaktivieren:

dom.event.clipboardevents.enabled = false

Außer bei Google Docs und ähnliche Javascript-lastigen GUIs zur Dokumenten-bearbeitung in der Cloud ist mir keine sinnvolle Anwendung dieses Features bekannt.

Spekulatives Laden von Webseiten
Firefox beginnt in einigen Situationen bereits mit dem Laden von Webseiten, wenn sich der Mauszeiger über einem Link befindet, also bevor man wirklich klickt. Damit soll das Laden von Webseiten einige Millisekunden beschleunigt werden. Wenn man Verbindungen mit unerwünschten Webservern vermeiden möchte, kann man das Feature unter "about:config" abschalten:

network.http.speculative-parallel-limit = 0

WebIDE deaktivieren
TorProject.org empfiehlt für Firefox 38.0 aus Sicherheitsgründen, die WebIDE unter "about:config" zu deaktivieren:

devtools.webide.enabled = false
devtools.webide.autoinstallADBHelper = false
devtools.webide.autoinstallFxdtAdapters = false

Kill Switch für Add-ons abschalten

Die Extension blocklist kann Mozilla nutzen, um einzelne Add-ons im Browser zu deaktivieren. Es ist praktisch ein kill Switch für Firefox Add-ons und Plug-ins. Beim Aktualisieren der Blockliste werden detaillierte Informationen zum realen Browser und Betriebssystem an Mozilla übertragen.

Ich mag es nicht, wenn jemand remote irgendetwas auf meinem Rechner deaktiviert oder deaktivieren könnte. Unter "about:config" kann man dieses Feature abschalten:

extensions.blocklist.enabled = false

Update der Metadaten für Add-ons deaktivieren
Seit Firefox 4.0 kontaktiert der Browser täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons und die Zeit, die Firefox zum Start braucht. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhägig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. Unter "about:config" kann man diese Funktion abschalten:

extensions.getAddons.cache.enabled = false

HTML5 Beacons deaktivieren
Mit Beacons kann ein Browser beim Verlassen/Schließen einer Webseite Daten zur Analyse an den Webserver senden, die via JavaScript gesammelte wurden. Eine sinnvolle Anwendung außerhalb von "Analyse des Surfverhaltens" (aka Tracking) fällt mir dafür nicht ein. Unter "about:config" kann man dieses Feature abschalten:

beacon.enabled = false

Safebrowsing deaktivieren
Ab Firefox 34 reicht es nicht mehr, die Nutzung von Googles Safebrowsing Datenbank im Einstellungsdialog zu deaktivieren. Zusätzlich muss man den Download der Datenbank unter "about:config" abschalten, wenn man keine Verbindungen zu Google herstellen will.

browser.safebrowsing.enabled false (bis Firefox 49)
browser.safebrowsing.phishing.enabled false (ab Firefox 50)
browser.safebrowsing.malware.enabled false
browser.safebrowsing.blockedURIs.enabled false
browser.safebrowsing.downloads.enabled false
browser.safebrowsing.downloads.remote.enabled false
browser.safebrowsing.updateURL (leerer String)
browser.safebrowsing.appRepURL (leerer String, bis FF 45)

browser.safebrowsing.downloads.remote.url (leerer String, ab FF 46)

Gegen Phishing Angriffe schützen keine technischen Maßnahmen vollständig, sondern in erster Linie das eigene Verhalten. Und gegen Malware schützen regelmäßige Updates des Systems besser als Virenscanner und URL-Listen.

Healthreport deaktivieren
Der Healthreport wird an Mozilla gesendet, kann man unter "about:config" deaktivieren:

datareporting.healthreport.service.enabled = false
datareporting.healthreport.uploadEnabled = false
datareporting.policy.dataSubmissionEnabled = false

Heartbeat User Rating deaktivieren
Mit Firefox 37.0 hat Mozilla das heartbeat user rating system eingeführt. Der User soll Firefox bewerten und wird gelegentlich zur Teilnahme an der Community eingeladen. Mozilla hat selbst erkannt, dass dieses Feature nerven könnte:

We understand that any interruption of your time on the internet can be annoying.

Unter "about:config" kann man das Feature deaktivieren, indem man die folgende URL auf einen leeren String setzt:

browser.selfsupport.url = ""

Wi-Fi Hotspot Portalerkennung deaktivieren
Firefox 52 erkennt die Portalseiten von Wi-Fi Hotspots und öffnet sie in einem neuen Tab (Release Notes). Für die Wi-Fi Hotspot Portalerkennung kontaktiert Firefox bei jedem(!) Start folgende Webseite:

Reveal hidden contents

Unter about:config kann man Firefox dieses Verhalten abgewöhnen, indem man die Portalerkennung deaktiviert (man wird es kaum vermissen):

network.captive-portal-service.enabled = false

Microsoft Family Safety deaktivieren
Microsoft Family Safety ist ein lokaler man-in-the-middle Proxy in Windows 10, der die Zugriffsrechte auf Webseiten steuern kann und damit per Definition ein Zensur-tool ist. Ab Firefox 52 ist die Verwendung von Microsoft Family Safety standardmäßig

aktiviert. Mit folgender Option kann man unter "about:config" die Nutzung von Microsoft Family Safety abschalten:

security.family_safety.mode = 0

Schritt 4: Hardware ID ändern

Die Hardware ID kann unter Umständen durch Programme ausgelesen werden, im schlimmsten Fall kann diese bei einem Abgleich gegen euch verwendet werden. Daher empfiehlt es sich auch diese zu ändern. Dafür gibt es dieses Tool:

DOWNLOADLINK

Das Tool ist selbsterklären und sehr einfach zu bedienen. Ihr startet das Programm, generiert eine neue Hardware ID und drückt auf den "Change HWID-Button" Nach dem Reboot sollte die neue Hardware ID eingestellt sein. Ob die Änderungen aktiv geworden sind.
Geht in Windows auf Start und tippt "regedit" ein und bestätigt euch als Admin. Es öffnet sich ein Fenster. Nun müsst ihr folgendem Pfad folgen um an die richtige Datei zu gelangen: Computer - Hkey_Local_Machine - System - CurrentControlset - Control - ID Config DB - Hardware Profiles - 0001
Dort findet ihr eine Datei mit der Bezeichnung "HW Profile Guid". Rechts daneben ist ein Wert eingetragen. Ändert die letzten 4 Ziffern des Wertes.

Schritt 5: Mikrofon und Kamera des Notebooks deaktivieren

Ja, ich gebe zu, es mag Paranoid klingen. Aber, wer sich ein wenig mit RATs beschäftigt, kann das eventuell verstehen. Wenn euch jemand infiziert, hat er unter Umständen einen kompletten Zugriff auf euren Computer, sobald dieser mit dem Internet verbunden ist. Dazu gehören teilweise auch Zugriff auf Mikrofone und Kameras. Wenn dies der Fall ist, kann der Angreifer theoretisch jederzeit Fotos von euch aufnehmen, aber auch euer Mikrofon aktivieren. Möglich ist das übrigens auch über euer Smartphone. Solange ihr das Mikrofon nicht benötigt, empfehle ich es euch im Gerätemanager zu deaktivieren. Bei der Kamera bin ich einen Schritt radikaler. Ich deaktiviere sie nicht nur, nein ich deinstalliere auch die Treiber dafür. Zusätzlich habe ich meine Kamera auch noch abgeklebt. Geht im Gerätemanager auf "Bilderanbetung oder Imaging Device" und deinstalliert eure dortige Kamera.

Schritt 6: Blue Screen of Death per Tastenkombination aktivieren

Anmerkung: Ich bin durch den User Cloudfire auf diese sehr nützliche Funktion aufmerksam geworden. Es ist eine Tastenkombination, mit der ihr euren PC zum Abstürzen bringt und somit euren PC wieder verschlüsselt. Sollte bei euch aus irg. welchen Gründen ein Zugriff der Staatsgewalt oder ähnliches stattfinden, könnt ihr somit eure Daten vor Vater Staat schützen.

Da nicht ich das Tutorial geschrieben habe, aber es als sehr nützlich empfinde, zitiere ich es einfach hier und verlinke nochmal den Thread auf dem Board. Credits gehen ausschließlich an den User cloudfire, danke dir nochmal:

Hide contents

"Hier ein kleiner Tipp für diejenigen, die von zu Hause Ihr Business betreiben.

Diejenigen, die einen stationären PC nutzen, können diesen im Falle eines uneingeladenen spontanen Besuchs dritter einfach über eine Mehrfachsteckdose mit Schalter sofort ausschalten, so dass das hoffentlich verschlüsselte System sofort wieder encryptet ist.

Bei denen, die aber ein Notebook nutzen, ist das Arbeiten ohne Akku auch nicht das Wahre und wenn man im Falle eines Falles das Notebook sofort ausgeschaltet haben muss, kann ein dritter schnell zum Laptop rennen und diesen "offen" halten.

Für diesen Fall ist es bei Windows Systemen möglich, auf Tastendruck einen Bluescreen of Death (BSOD) auszulösen, was sofort das System zum Absturz bringt und somit die Verschlüsselung scharf schaltet.

Hierzu muss man bei einem aktuell gepatchten Rechner nur folgenden Registry-Key einen DWORD-Wert eintragen:

1. Zum Registry-Pfad "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\kbdhid\Parameters" gehen.

2. Einen neuen Schlüssel als DWORD "CrashOnCtrlScroll" (ohne Anführungszeichen!!!) eintragen

3. dem neu angelegten Schlüssel den Wert "1" eintragen und den Rechner neu starten.

Nach dem Neustart müsst Ihr dann nur im Notfall die folgende Tastenkombination drücken:
Die rechte "Strg"-Taste gedrückt halten und zweimal die Taste "Rollen" drücken.
Wenn Ihr das alles saubergemacht habt, dürft Ihr Euch wohl zum ersten Mal über einen Bluescreen of Death freuen!

Schritt 7: Virtuelle Maschine einrichten

Virtuelle Maschinen werden benötigt, um Szene Tools auszuführen, ohne euer System zu gefährden. Wer längerfristig in der Szene verweilen möchte, kommt ohne eine VM nicht aus. VM Workstation oder VirtualBox (free) installieren.

DOWNLOADLINK

Für die VB nehmt ihr am besten Windows 8 oder 10, da das von den meisten. Nutzern verwendet wird. Alternativ geht es natürlich auch mit Windows 7. Zur Installation der VB wird ein .iso Image des gewählten OS benötigt.

Habt ihr das passende OS gefunden, ladet ihr euch die Iso runter.

VB Erstellen

Schritt #1 (Erstellen einer VM)
http://prntscr.com/ll2p18
Schritt #2 (Konfiguration auswählen)
http://prntscr.com/ll2pdj
Schritt #3 (ISO Datei Ort bestimmen; wo Windows liegt)
http://prntscr.com/ll2phy
Schritt #4 (Version bestimmen)
http://prntscr.com/ll2plv
Schritt #5 (VM benennen)
http://prntscr.com/ll2pqn
Schritt #6 (Festplattenspeicher zuweisen)
http://prntscr.com/ll2pv3
Schritt #7 (VM anpassen)
http://prntscr.com/ll2pza
Schritt #8 (Arbeitsspeicher; RAM zuweisen)
http://prntscr.com/ll2q39

Und zum Schluss die VM starten und das Betriebssystem installieren lassen wie bei einer normalen Installation. VMware hat hierbei für Windows und Ubuntu die EasyInstaller Funktion, wodurch sie sich quasi mehr oder weniger selbstständig auf die VM installieren.