Sie fragen – wir antworten!

DISM: Ein Image für mehrere Partitionen

Bei der Lektüre Ihrer Einführung zum Windows-Kommandozeilenprogramm DISM (c't 24/2020, S. 156) hat mich ein Punkt irritiert: Sie schreiben, dass ein Image keine Daten enthalten kann, die im Original über mehrere Partitionen verteilt liegen. Zudem haben Sie erklärt, dass Setup.exe während einer Windows-Installation bloß ein Image entpackt und mit einem Bootloader versorgt. Doch nach einer Windows-Installation enthält ja nicht nur C: Daten, sondern auch die im Explorer nicht sichtbare Recovery-Partition. Denn dort liegt ja Windows RE. Kann DISM also doch die Daten mehrerer Partitionen enthalten? Oder trickst Setup.exe hier irgendwie?

Weder noch: Das Image enthält nur die Daten einer einzigen Partition, und die Recovery-Partition wird nicht von Setup.exe befüllt. Es funktioniert anders: Direkt nach dem Entpacken des Images auf Laufwerk C: liegt auch Windows RE auf C:. Genauer: Windows RE steckt in der Datei Winre.wim, und die liegt in diesem Moment unter C:\Windows\System32\Recovery. Was das entpackte Image ebenfalls enthält, ist eine spezielle Anweisung, die Datei Winre.wim beim ersten Hochfahren auf die Recovery-Partition zu verschieben (`Reagentc.exe /enable`).

Auf eine ähnliche Weise können Sie auch selbst die Daten mehrerer Partitionen in einem Image vereinigen: Kopieren Sie alles auf die Quellpartition für das Image und erzeugen Sie zusätzlich in `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` eine Verknüpfung zu einem Skript, welches die Dateien beim ersten Hochfahren auf D: verschiebt (Reagentc.exe verschiebt ausschließlich Winre.wim). Registry-Einträge unter `RunOnce` löscht Windows nach der Ausführung.

(axv@ct.de)

Fritzbox 7390 weiter betreiben

Ich würde gerne meine von AVM abgekündigte Fritzbox 7390 noch nicht auf den Schrott werfen. OpenWrt kann man aber nicht installieren. Und Freetz setzt auf das FritzOS auf und wird somit auch nicht mehr aktualisiert. Die 7390 kann ich also nicht wie geplant mit alternativem Betriebssystem und WireGuard laufen lassen. Selbst als Repeater oder Access Point scheint sie mir ungeeignet, da sie ja kein Mesh unterstützt. Ist sie jetzt nur noch ein besserer Switch?

Tatsächlich sind die Tage der 7390 gezählt. Das verwendete SoC wird nicht von OpenWrt unterstützt, also darf man sich keine Hoffnung machen, dass da noch etwas kommt. Aber Sie müssen die Box nicht zwangsläufig ins AVM-Mesh einbuchen können, um sie als Access Point zu betreiben. Die Box kann, wenn nicht gerade die 250 MBit/s einer SVDSL-Anbindung per WLAN weitergegeben werden sollen oder die Luft voll mit anderen WLANs ist, problemlos noch als Lückenfüller dienen, wenn sie mit dem LAN verbunden ist.

Vom Betrieb als Repeater würde ich jedoch abraten – außer Sie leben auf dem Land mit wenigen oder gar keinen (WLAN-)Nachbarn. Die Box kann ausschließlich Wi-Fi 4 (300 MBit/s brutto) und der Repeater-Betrieb halbiert die Bandbreite mindestens. Kommen dann noch WLANs in der Umgebung dazu, die den Kanal belegen, kann man sich den Repeater auch schenken.

Alternativ können Sie die 7390 auch verkaufen. Aktuell gehen die Geräte für 10 bis 25 Euro bei eBay weg – anscheinend gibt es Leute, denen die Aktualität der Software nicht so wichtig ist. Vom Erlös können Sie eine gebrauchte 7362 SL kaufen, die von OpenWrt unterstützt wird, oder 20 bis 40 Euro drauflegen und eine ebenfalls unterstützte gebrauchte 4040 kaufen. Letztere dürfte Ihnen deutlich länger einen guten Dienst mit OpenWrt erweisen, da sie einen vergleichsweise leistungsstarken ARM-Prozessor hat und Wi-Fi 5 (802.11ac) in beiden Bändern beherrscht. Details dazu lesen Sie in c't 10/2019, Seite 28.

(amo@ct.de)

Schlüsselfragen zu PGP

Ich habe festgestellt, dass man eine PGP-verschlüsselte E-Mail mit dem privaten Schlüssel des Absenders entschlüsseln kann. Ich dachte, dass dazu nur der Empfänger mit seinem privaten Schlüssel in der Lage ist. Darf das so sein?

Ja, das ist so und das ist korrekt. Standardmäßig verschlüsselt PGP alle Mails mit den (öffentlichen) Schlüsseln aller Empfänger und dem des Absenders, sodass auch letzterer die Mails später noch lesen kann. Das ist auch durchaus sinnvoll – denn warum sollte man seine eigenen Mails vor sich selbst geheim halten?

Das Verschlüsseln für mehrere Empfänger erzeugt durch einen Trick nur wenig Overhead. Es wird dabei nicht etwa die komplette Nachricht mehrfach mit verschiedenen RSA-Schlüsseln chiffriert. Stattdessen verschlüsselt PGP den Inhalt mit einem zufällig gewählten (symmetrischen) AES-Schlüssel nur ein Mal. Diesen AES-Schlüssel chiffriert PGP dann mit den öffentlichen RSA-Schlüsseln aller Empfänger (einschließlich des eigenen) und hängt all diese Chiffrate an den AES-Ciphertext an. Das macht nur ein paar zusätzliche Byte aus. Der Empfänger kann mit seinem geheimen RSA-Schlüssel dann den AES-Key entschlüsseln und damit dann wiederum die eigentliche Nachricht.

(ju@ct.de)

Aktiviert man im Kontextmenü die Vorschau, erscheint der Desktop, wenn man mit dem Mauszeiger auf das Feld ganz rechts in der Taskleiste fährt. Gerade auf Multimonitorsystemen ist das Feld aber oft zu klein.

Windows-Desktop anzeigen

Wenn man unter Windows ganz rechts unten mit dem Mauszeiger auf die Taskleiste klickt, erscheint der Desktop. Unter Windows 10 ist die Schaltfläche so winzig, dass sie vor allem auf Multimonitor-Systemen kaum noch zu treffen ist – zu schnell ist der Mauszeiger auf den anderen Monitor hinübergerutscht. Kennen Sie einen Weg, die Schaltfläche zu vergrößern?

Leider nicht. Es gibt aber Tastenkombinationen, die weiterhelfen könnten. Windows+D zeigt den Desktop, erneutes Drücken versucht den vorigen Zustand wieder herzustellen – „versucht“, weil das nicht immer zuverlässig klappt.

Windows+M minimiert alle Fenster, allerdings nur jene, die auch minimierbar sind. Eigenschaften-Dialoge beispielsweise gehören meist nicht dazu. Diese Tastenkombination ist daher nützlich, um solche im Fensterwirrwarr verloren gegangenen Dialoge schnell wiederzufinden.

Windows+, (also Windows+Komma) schließlich ist die Tastenkombination für Aero Peek: Drücken Sie die Windows-Taste und halten Sie sie gedrückt, anschließend kurz die Komma-Taste. Dann scheint der Desktop durch, allerdings nur als Ansicht, in der Sie nichts anklicken können. Der vorherige Zustand ist wieder zu sehen, sobald Sie die Windows-Taste loslassen.

(axv@ct.de)

NoScript im Tor Browser nachschärfen

Mit Version 9 des Tor Browsers wurden die Standardeinstellungen des enthaltenen NoScript-Plug-ins verändert. Es sind nun etwa JavaScript und externe Fonts standardmäßig aktiviert. Das gefällt mir nicht. Änderungen an den Einstellungen werden aber nach jedem Neustart wieder zurückgesetzt, ich muss JavaScript stets von Neuem abschalten. Kann man nicht die Standardeinstellungen dauerhaft ändern?

Das NoScript-Plug-in und dessen Einstellungen sind als (signierte) XPI-Datei im Unterverzeichnis extensions im Benutzerprofil des Tor-Browsers gespeichert. Das Profilverzeichnis befindet sich unter Windows in %USERPROFILE%\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser*.default, unter Linux in ~/.local/share/torbrowser/tbb/x86_64/tor-browser_/Browser/TorBrowser/Data/Browser/.default und unter macOS X in ~/Library/Application Support/TorBrowser-Data/Browser/*.default. Der Dateiname besteht überwiegend aus einer hexadezimalen Nummer und trägt die Endung .xpi.

Das XPI-Dateiformat ist eine Zip-Datei mit einem besonderen Aufbau, die Sie unter Linux mittels `unzip` in ein leeres Verzeichnis entpacken können. Unter Windows sollten Sie für diese Arbeitsschritte ein Tool wie 7-Zip zu Hilfe nehmen. Die Rechte werden in der Datei common/Policy.js verwaltet, suchen Sie dort nach `Permissions.IMMUTABLE` und fügen Sie vor der Definition für `UNTRUSTED` die neuen Standardrechte ein:

```
DEFAULT: {
  "fetch": true,
  "frame": true,
  "script": false,
  "object": false,
  "media": false,
  "font": false,
  "webgl": false,
  "other": false,
  "ping": false,
},
```

Speichern Sie die Änderungen und aktualisieren Sie die Policy-Datei im XPI-Archiv mit dem Kommando:

```
zip -u *.xpi common/Policy.js
```

Die geänderte XPI-Datei kopieren Sie zurück in das Unterverzeichnis extensions unterhalb des Tor-Browser-Profils. Anschließend starten Sie den Tor Browser, öffnen die Browser-Einstellungen über die URL „about:config“ und deaktivieren die Signaturprüfung für XPI-Dateien, indem Sie `xpinstall.signatures.required` auf `false` setzen. Nach einem Neustart des Tor Browsers steht Ihnen dann NoScript mit den von Ihnen vorgegebenen Standardeinstellungen zur Verfügung.

Damit Ihre Einstellungen nicht bei einem der häufigen automatischen Updates von NoScript wieder zurückgesetzt werden, deaktivieren Sie in den Browser-Einstellungen die automatischen Updates für die Erweiterungen. Dazu setzen Sie `extensions.update.autoUpdateDefault` und `extensions.update.enabled` auf `false`. Es ist jedoch ratsam, spätestens nach jedem Update des Tor Browsers ein manuelles Update des NoScript-Plug-ins durchzuführen, wobei Sie dann die Einstellungen in der Datei Policy.js wiederholen müssen. *(mid@ct.de)*

Fragen richten Sie bitte an

hotline@ct.de

c't Magazin

@ctmagazin

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter **www.ct.de/hotline.**

Tor Browser 10 unter Debian 10

Seit dem Update auf Version 10 lässt sich der Tor Browser nicht mehr unter Debian 10 starten. Der manuelle Aufruf von `~/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/start-tor-browser -v` im Terminal führt zu einer Fehlermeldung, dass die Bibliothek libstdc++.so.6 nicht geladen werden könne. Ich habe jedoch die neueste Version dieser Bibliothek installiert und mit dem veralteten Tor Browser 9 funktioniert sie einwandfrei. Wie klappt das Update auf die aktuelle Version des Tor Browsers?

Die Ursache für die Fehlermeldung ist, dass der Tor Browser 10 eine eigene Version der libstdc++.so.6 mitbringt, von AppArmor aber daran gehindert wird, sie anstelle der systemweit installierten Bibliothek zu laden. Dieses Verhalten von AppArmor dient grundsätzlich der Sicher-

heit: Es verhindert, dass Angreifer eine präparierte Version der Standardbibliothek ins System einschmuggeln und so das Verhalten von Systemprogrammen, die die Bibliothek einbinden, kompromittieren können.

Der Tor Browser 10 benötigt deshalb eine Ausnahme in Form einer zusätzlichen Regel. Dazu fügen Sie folgende Zeile im Profil `torbrowser_firefox` in der Datei /etc/apparmor.d/torbrowser.Browser.firefox ein. Unter Debian 10 am besten hinter Zeile 75, kurz nach den anderen Regeln für `torbrowser_home_dir`:

```
owner @{torbrowser_home_dir}/
↳TorBrowser/Tor/libstdc++/
↳libstdc++.so.* mr,
```

Anschließend lassen Sie AppArmor die Regeln für den Tor Browser neu laden:

```
sudo apparmor_parser -r /etc/
↳apparmor.d/torbrowser.Browser.firefox
```

So funktioniert der aktuelle Tor Browser auch unter Debian 10. Es ist davon auszugehen, dass die zusätzliche AppArmor-Regel in einem der nächsten Updates von AppArmor oder des Pakets `torbrowser-launcher` von Debian 10 enthalten ist.

(mid@ct.de)

NAS nach Routerwechsel wieder einbinden

Ich habe meinen Provider-Router kürzlich durch eine Fritzbox ersetzt. Nun funktioniert die Windows-Dateifreigabe meines Netzwerkspeichers nicht mehr. Wie kann ich wieder darauf zugreifen?

Öffnen Sie die Konfigurationsseite der Fritzbox im Browser (http://fritz.box) und schauen Sie im Menü unter Heimnetz/Netzwerk nach. Dort finden Sie die Liste der bekannten Netzwerkgeräte. Das NAS sollte unter dem eingestellten Namen erscheinen, beispielsweise „meinnas“.

Versuchen Sie, die NAS-Freigaben unter dem Namen `\\meinnas\` zu erreichen. Klappt das nicht, ergänzen Sie die Endung .fritz.box und versuchen es damit: `\\meinnas.fritz.box\`. Scheitert auch dieses, dann nehmen Sie die in der Liste angezeigte IP-Adresse, beispielsweise: `\\192.168.178.24\`. Falls noch nicht geschehen, löschen Sie die alte Laufwerksbindung auf dem Windows-PC und legen Sie sie mit dem funktionierenden Namen neu an.

(ea@ct.de)

Fingerabdruckscanner unter Linux erkennt nichts

Ich habe mir einen Touch-Fingerabdruckscanner gekauft, der unter Linux mit Fprintd arbeiten soll. Der Scanner wird auch korrekt von Fprintd erkannt und speichert wohl Fingerabdrücke. Jedoch scheitert das Erkennen meiner Fingerabdrücke. Um einen Hardwaredefekt auszuschließen, habe ich den Scanner auch unter Windows getestet. Dort arbeitet er schnell und sehr zuverlässig. Warum arbeitet er unter Linux nicht?

Schuld ist diesmal nicht die Hardware, sondern Fprintd, oder genauer gesagt dessen Erkennungskonzept. Fprintd wurde für Fingerabdruckscanner entwickelt, die ein vollständiges Bild des Fingerabdrucks liefern. Die heutzutage populären Touch-Fingerabdruckscanner erkennen jedoch nur einen sehr kleinen Ausschnitt des Fingerabdrucks. Dieser Ausschnitt ist zu klein für Fprintd. Sie können versuchen, langsam und gleichmäßig mit der gesamten Fingerkuppe über den Scanner zu streichen beim Einrichten und Entsperren. Eventuell funktioniert die Erkennung damit, ist aber nicht so komfortabel und schnell wie unter Windows oder wie beim Smartphone.

Windows ist beim Erkennen so schnell, weil es beim Hinterlegen des Abdrucks aus vielen kleinen Einzelbildern ein vollständiges Abbild des Fingerabdrucks erzeugt. Es erkennt den Fingerabdruck dann auch anhand eines kleinen Abschnitts. Das Problem ist den Fprintd-Entwicklern bekannt, aber erfordert wohl die Implementation eines neuen Erkennungsalgorithmus.

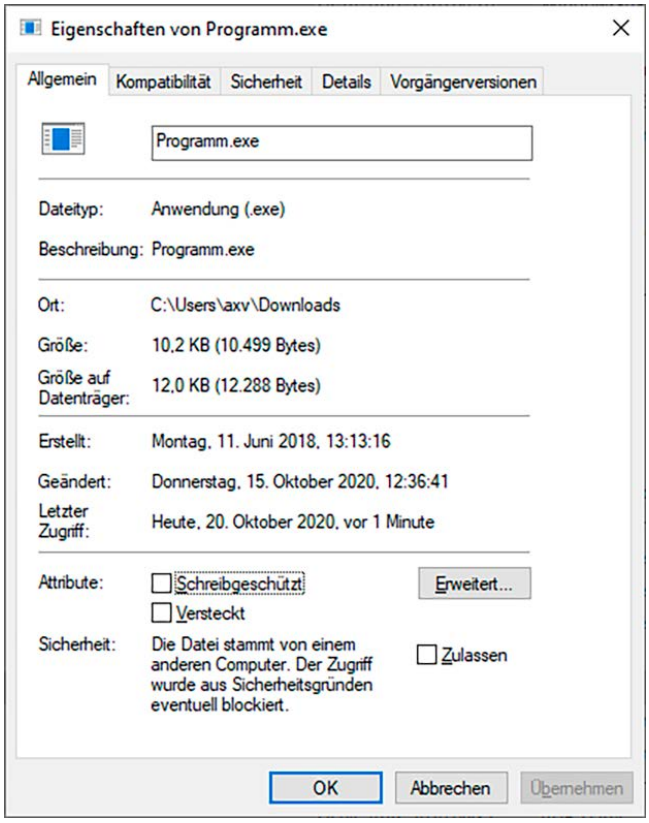
(mls@ct.de)

Windows fragt bei heruntergeladenen Programmen

Ich habe ein Programm aus dem Internet heruntergeladen. Wenn ich es aufrufe, fragt mich Windows jedes Mal, ob ich das auch wirklich zulassen will. Wie stelle ich diese Nachfrage ab?

Das können Sie in den Eigenschaften der Datei vornehmen: Bei solchen Programmen finden Sie im Reiter „Allgemein“ ganz unten beim Punkt Sicherheit den Hinweis, dass die Datei von einem anderen Computer stammt. Setzen Sie hier ein Häkchen vor „Zulassen“, dann erscheint die Abfrage beim Aufruf nicht mehr.

(axv@ct.de)



Mit einem Häkchen an der richtigen Stelle lässt sich die Sicherheitsabfrage bei jedem Aufruf unterbinden.