Tipps & Tricks

Sie fragen – wir antworten!

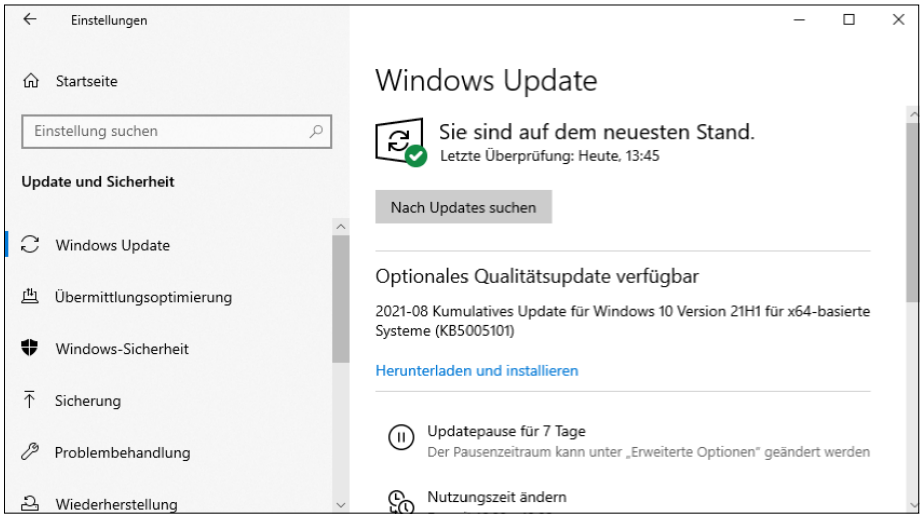
Optionale Windows-Updates

Auf der Seite „Updates und Sicherheit/Windows Update“ in den Einstellungen meines Windows 10 erscheinen gelegentlich „Optionale Qualitätsupdates“. Sollte ich die installieren? Eine Beschreibung, was es mit so einem Update auf sich hat, ist ja meist nicht dabei.

Was genau so ein Update enthält, können Sie auf Microsofts Support-Webseiten nachschlagen: Die Adresse lautet `https://support.microsoft.com/help/<KB-Nummer>`, wobei Sie `<KB-Nummer>` durch die meist siebenstellige Nummer ersetzen müssen, die Windows Update bei der Beschreibung des Patches hinter dem Buchstabenkürzel „KB“ angibt. Die Beschreibung für das derzeit angebotene „2021-08 Kumulatives Update für Windows 10 Version 21H1 für x64-basierte Systeme (KB5005101)“ finden Sie also beispielsweise unter https://support.microsoft.com/help/5005101.

Wenn sich dort kein Fehler findet, unter dem Sie aktuell leiden, lassen Sie besser die Finger von dem optionalen Update. Spätestens im nächsten „offiziellen“ kumulativen (Sicherheits-)Update am nächsten Patchday sind die Änderungen ohnehin meist enthalten. Microsoft nutzt optionale Updates gern mal, um Patches zu testen, bevor sie in den Pflicht-Updates landen. Wenn Sie nicht zum Versuchskaninchen werden wollen, meiden Sie sie also nach Möglichkeit. Sicherheitskritisch sind optionale Updates nie.

(hos@ct.de)



Installieren oder nicht? „Optionalen“ Updates sieht man häufig nicht an, wozu sie gut sein sollen.

Mit LibreOffice sicher vor Trojanern?

Im Zusammenhang mit Phishing, Ransomware oder Trojanern lese ich immer wieder – auch in c’t –, dass Leute dadurch zu Opfern werden, dass sie verseuchte Office-Dokumente öffnen, die als Anhang an betrügerischen E-Mails hängen. Ich besitze gar keine Office-Programme von Microsoft, sondern bearbeite solche Dokumente ausschließlich mit LibreOffice. Eigentlich reagiere ich auch grundsätzlich nicht auf Mails von fremden Absendern und öffne Dokumente nur unter Linux, aber ich wüsste schon gern, was mir passieren kann, wenn mir doch mal ein Dokument unter Windows durchrutscht.

In aller Regel wird nichts passieren. Sämtliche Trojaner-Makros, die wir bisher gesehen haben, sind speziell auf Microsoft Office ausgelegt und funktionieren unter LibreOffice nicht. Aber verlassen kann man sich darauf nicht. Wenn Sie Office-Trojaner-Makros in LibreOffice laden wollen, dann bitte nur auf einem Testsystem, das nicht im Netz hängt. *(ju@ct.de)*

Windows-Profile löschen

Wir experimentieren gerade mit neuen Arbeitsplatzmodellen nach der Pandemie und schaffen feste Arbeitsplätze ab. Das führt dazu, dass sich viele verschiedene Mitarbeiter an unseren Windows-Domänen-PCs anmelden. Mit der Zeit sammeln sich viele ungenutzte Benutzerprofile auf den Maschinen an. Kann Windows die löschen, damit die Festplatten nicht verstopfen?

Eine perfekte Lösung gibt es aktuell nicht. Am besten nutzen Sie die Gruppenrichtline „Benutzerprofile, die älter als eine bestimmte Anzahl von Tagen sind, beim Systemneustart löschen“, die Sie unter Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Benutzerprofile finden.

In der Richtlinie können Sie die Anzahl der Tage konfigurieren. Das klappt leider nicht zu 100 Prozent: Die Erkennung alter Profile kann scheitern, wenn ein Programm – meist ein Virenscanner – die Datei NTUSER.DAT verändert.

(jam@ct.de)

Raspi als WireGuard-Server

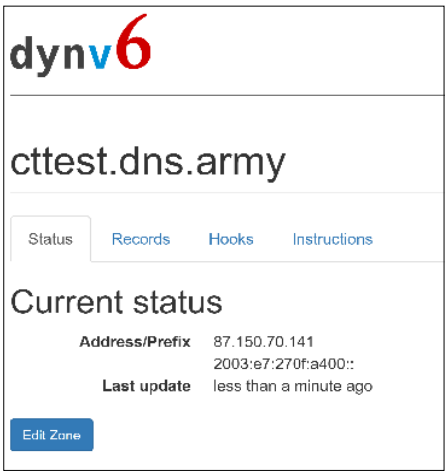
Ich möchte einen Raspberry Pi als WireGuard-Server einrichten. Leider unterstützt der Router, den ich von meinem Provider (Magenta Österreich) bekommen habe, den DDNS-Service nicht, jedenfalls kann ich im Setup des Routers diesbezüglich nichts einstellen. Gibt es eine andere Möglichkeit, den Raspi aus dem Internet erreichbar zu machen, oder muss ich dafür bei neueren Modellen einfach nur die Portweiterleitung im Router aktivieren?

Solange Ihr Router Portfreigaben oder -weiterleitungen unterstützt und Sie eine öffentliche IPv4- oder IPv6-Adresse haben, werden Sie keine Probleme haben, Ihren Raspberry Pi aus dem Internet erreichbar zu machen.

Die IPv4/v6-Adresse Ihres Routers (beziehungsweise bei v6 des benutzten Gerätes) ist ja nicht nur diesem bekannt; sie wird jedes Mal, wenn Sie eine Verbindung ins Internet aufbauen (etwa zu einer Website), mitgeschickt, damit das Ziel weiß, wohin die Daten zurückgehen müssen. Viele DynDNS-Anbieter stellen daher URLs bereit, die Sie nur vom entsprechenden Anschluss aus aufrufen müssen, damit der Anbieter die aktuelle IP-Adresse erhält und für den jeweiligen DynDNS-Eintrag speichert.

Am besten schauen Sie erst einmal auf der Weboberfläche Ihres Routers, ob Sie eine öffentliche IPv4-Adresse sowie eine öffentliche IPv6-Adresse an der WAN-Schnittstelle bekommen und keine private – den Link zu einer Liste mit privaten IPv4-Adressbereichen finden Sie via ct.de/yydy. Aufgrund der IPv4-Adressknappheit verwenden immer mehr Anbieter private IP-Adressen für Endkundenanschlüsse – sogenanntes „Carrier-grade NAT“. Wenn Sie eine öffentliche Adresse haben, können Sie die WireGuard-Portweiterleitung einfach anlegen.

Wenn es eine private IPv4-Adresse ist, fragen Sie bei Ihrem Anbieter, ob Sie auf Anfrage eine öffentliche IPv4-Adresse erhalten können. Wenn nicht, gibt es keinen einfachen Weg (für IPv4). Dann kann nur noch ein anderer Anbieter helfen, der Ihnen die Adresse über einen Tunnel zur Verfügung stellt, oder ein kleiner vServer mit öffentlicher IP-Adresse im Netz, über den Sie ein VPN-Routing einrichten. Nichtsdestotrotz kann Ihr VPN-Vorhaben trotzdem funktionieren, wenn an beiden



Der kostenlose DynDNS-Dienst dynv6.com stellt APIs bereit, mit denen man den eigenen Eintrag auch ohne Router-Unterstützung aktualisieren kann.

verwendeten Anschlüssen IPv6 verfügbar ist.

Vom Anbieter vergebene IPv6-Adressen sind praktisch immer öffentlich (fe80 ist lokal, Check unter ipv6-test.com). Sofern Ihr Router gar keine vergibt, schauen Sie, ob Sie IPv6 auf Ihrem Router und/oder bei Ihrem Anbieter aktivieren müssen. Bietet Ihr Anbieter kein IPv6, schreiben Sie ihm eine Beschwerdemail, in der Sie fragen, wie es sein kann, dass er das Protokoll, das das Problem der Adressknappheit effizient lösen würde, 20 Jahre nach der Veröffentlichung noch nicht eingeführt hat.

Wenn das funktioniert: Da es bei IPv6 genug Adressen gibt, bekommt der Router meist ein öffentliches Präfix zur Vergabe an Geräte, worüber Ihr Raspberry Pi dann eine oder mehrere Adressen erhält. Per Default sind in Raspberry OS die Privacy Extensions aktiviert, die eine temporäre Adresse generieren, die keine eingehenden Verbindungen zulässt. Sie müssen sie also deaktivieren (siehe „IPv6 DynDNS klemmt“, c’t 14/2020, S. 172), wenn die Adresse über eine Verbindung zum Anbieter ermittelt wird. Dann ist IPv6 einsatzbereit und Sie müssen nur noch anhand der Anleitung Ihres Routers die WireGuard-Portfreigabe anlegen.

Anschließend prüfen Sie die Dokumentation Ihres DynDNS-Anbieters. Der Dienst von dynv6.com etwa liefert ein fertiges Shellskript, das auf beliebigen Linux-Computern läuft – also auch auf dem Raspberry Pi (Download via ct.de/yydy). Wenn Sie das oder beispielsweise einen vom Anbieter bereitgestellten `curl`-Befehl regelmäßig als Cronjob auf dem Raspi ausführen, behält der DynDNS-Anbieter auch ohne Zutun des Routers die aktuelle Adresse – der spielt dafür keine Rolle.

(amo@ct.de)

***IP-Adressen, Dynv6-Skript:* ct.de/yydy**

(Power)Shell mit Systemrechten starten

Auf meinem Windows-System gibt es Ordner, an die ich selbst mit Administratorrechten nicht herankomme, weil sie offenbar dem Systemkonto gehören. Gibt es eine Möglichkeit, eine Eingabeaufforderung oder eine PowerShell unter diesem Konto zu starten?

Mit Windows-Bordmitteln ist uns kein Weg bekannt. Abhilfe bietet aber das Tool PsExec von Microsoft Sysinternals (Download via ct.de/yydy). Nachdem Sie das Zip-Archiv entpackt haben, kopieren Sie die Datei psexec.exe zweckmäßigerweise in einen Ordner, der in der Variablen `PATH` (Eingabeaufforderung) beziehungsweise `$Env:Path` (PowerShell) enthalten ist, zum Beispiel nach C:\Windows. Dazu brauchen Sie Administratorrechte.

Jetzt können Sie aus einer Eingabeaufforderung oder einer PowerShell mit Administratorrechten heraus eine Eingabeaufforderung mit Systemrechten starten:

```
psexec -s -i cmd
```

Dabei fordert die Option `-s` Systemrechte an und `-i` sorgt dafür, dass das am Ende angegebene Programm nicht im Hintergrund, sondern auf dem aktuellen Desktop läuft. Eine Liste der weiteren Optionen, die es kennt, liefert das Tool, wenn Sie es ohne Argumente, also einfach als `psexec` aufrufen. Statt `cmd` können Sie so auch beliebige andere Anwendungen unter dem Systemkonto ausführen, zum Beispiel die

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.**

Windows PowerShell mit `powershell` oder den Registrierungs-Editor mit `regedit`.

Beim allerersten Aufruf wird `psexec` Sie einmalig bitten, die Nutzungsbedingungen zu akzeptieren. Das können Sie mit der zusätzlichen Befehlszeilenoption `-accepteula` umgehen.

Das Tool ist Bestandteil der Sysinternals Suite von Microsoft, die noch zahlreiche weitere systemnahe Werkzeuge enthält. Was man mit denen so alles anfangen kann, haben wir in c't 4/2021, Seite 16 beschrieben. *(dz@ct.de)*

***PsExec:* ct.de/yydy**

Firefox per Kommandozeile installieren

In Ausgabe 18/2021 haben Sie beschrieben, wie man Chrome auf einem frischen Windows per Kommandozeile installiert, sich also den Ärger mit Edge und dem Internet Explorer erspart. Ich bevorzuge aber Firefox. Gibt es da auch eine Abkürzung?

Die gibt es. Den aktuellen Firefox in deutscher Sprache laden Sie mit folgendem Befehl herunter:

```
curl.exe -L "https://download.↵
↳mozilla.org/?product=firefox-latest&↵
↳os=win&lang=de" -o ff.exe
```

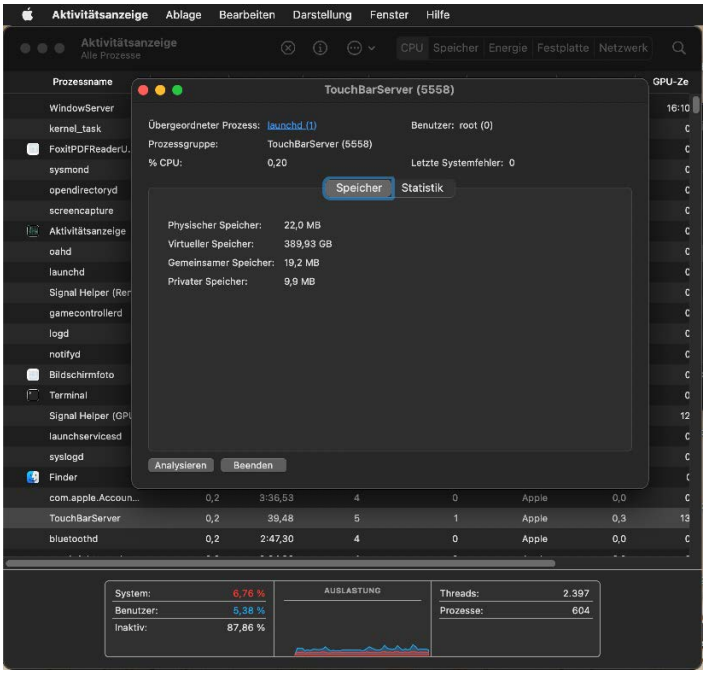
Führen Sie dann den Installer aus, indem Sie `ff.exe` starten. *(jam@ct.de)*

MacBook Pro: Touchbar reagiert nicht

Die Touchbar meines MacBook Pro „klemmt" gelegentlich und zeigt dann zum Beispiel nur die Option „Fertig" an; weitere Funktionen sind nicht verfügbar. Da hilft natürlich immer ein Neustart des MacBook weiter, aber das passt nicht immer. Kennen Sie eine Alternative?

Da gibt es gleich mehrere – allen ist gemeinsam, dass man den „Touch Bar agent" abschießt. Das Betriebssystem startet den Agent dann ruckzuck neu und die Touchbar funktioniert wieder. Ein Beispiel für das Terminal sieht folgendermaßen aus:

```
sudo pkill "Touch Bar agent"
```



Wenn die Touchbar eines MacBook Pro nicht korrekt reagiert, hilft es meist, den TouchBarServer beispielsweise über die Aktivitätsanzeige zu beenden und vom System neu starten zu lassen.

Dafür muss man nach Aufforderung nur noch das Administratorpasswort eingeben.

Alternativ öffnen Sie die Aktivitätsanzeige, klicken auf die Spalte „CPU" und geben in das Suchfeld neben der Lupe „Touch" ein. Doppelklicken Sie dann den Treffer „TouchBarServer". Im nächsten Fenster führt die Aktivitätsanzeige einige Details zu diesem Prozess auf und ganz unten finden Sie den Button „Beenden". Wenn Sie darauf klicken und die folgende Nachfrage bestätigen, wird der Prozess beendet. Schließen Sie das nun überflüssige Fenster und die Aktivitätsanzeige, um Ihre ursprüngliche Arbeit auf dem Mac wieder aufzunehmen. *(dz@ct.de)*

TPM-2.0-Chip arbeitet als TPM 1.2

Um für Windows 11 gerüstet zu sein, habe ich mir einen gebrauchten Bürocomputer mit Trusted Platform Module 2.0 (TPM 2.0) beschafft. Auf dem Mainboard befindet sich auch tatsächlich ein TPM-2.0-Chip von Infineon. Der wird auch unter Windows angezeigt, allerdings als TPM 1.2 – was läuft hier schief?

Ungefähr in den Jahren 2015 bis 2018 haben Firmen wie Dell, Fujitsu, HP und Lenovo Rechner mit TPM-2.0-Chips verkauft, die sich per Firmware-Update nachträglich auf TPM-1.2-Kompatibilität „downgraden" ließen. Betroffen sind vor allem Business-Notebooks und Office-PCs mit Intels vPro-Technik, die unter Windows 7 eingesetzt werden sollten. Das bedeutet auch, dass man alleine anhand der Typenbezeichnung eines TPM auf einem älteren Mainboard nicht sicher sagen kann, ob es als TPM 2.0 funktioniert.

Zumindest bei Dell und HP finden sich noch Support-Webseiten mit Hinweisen und Links zu Firmware-Updates, um die TPM-2.0-Funktion wieder zu aktivieren (siehe ct.de/yydy). Bei Fujitsu und Lenovo konnten wir keine Hinweise dazu beziehungsweise Firmware-Downloads mehr finden.

Die Firmware-Updates müssen genau zum jeweiligen System passen, einerseits weil es unterschiedliche TPM-Chips gibt, andererseits weil Abhängigkeiten zwischen TPM-Firmware und PC-BIOS bestehen. Man kann also nicht etwa das TPM auf einem Fujitsu-Mainboard mit einer Dell-Firmware behandeln. Ob Windows 11 allerdings überhaupt zwingend ein TPM 2.0 (oder fTPM 2.0 in CPU oder Chipsatz) verlangt, ist bislang unklar.

Achtung: Vor einem Update der TPM-Firmware sollten Sie die Hinweise von Microsoft zu diesem Eingriff beachten (siehe ct.de/yydy). Je nach Konfiguration müssen Sie zuvor beispielsweise die BitLocker-Verschlüsselung für Festplatten und SSDs zurücksetzen, weil Sie sonst nicht mehr an die darauf gespeicherten Daten herankommen. *(ciw@ct.de)*

***Firmware-Updates, Microsoft-Doku:* ct.de/yydy**