

Tipps & Tricks

Sie fragen – wir antworten!

Backups sicher vor Ransomware aufbewahren

? Sind meine Backups vor Ransomware geschützt, wenn ich sie von meinem Backup-Programm mit AES256 verschlüsseln lasse? Und wie sicher sind 7z- oder Zip-Dateien mit Kennwort?

! Das kommt darauf an, wo Sie die Backups aufbewahren: Wenn sie auf einem Datenträger lagern, der dauerhaft im Zugriff ist, kommt auch eine Ransomware dran. Aus deren Sicht handelt es sich dann ja um Dateien wie alle anderen. Es gibt sogar Ransomware, die nicht nur nach Dokumenten & Co. sucht, sondern auch gezielt nach Dateien mit Endungen typischer Backupformate. Wenn ein Backup verschlüsselt ist, kommen Angreifer nicht an seinen Inhalt heran, können also nicht damit drohen, ihn im Darknet zu veröffentlichen. Mit einer Ransomware können Kriminelle das Backup aber selbst noch einmal verschlüsseln und für die Entschlüsselung ein Lösegeld fordern.

Um Backups so aufzubewahren, dass sie sicher vor Ransomware sind, sollten Sie sie also auf einen externen Datenträger speichern, etwa auf eine USB-Festplatte, die Sie nur dann anschließen, wenn Sie Daten sichern oder wiederherstellen wollen. Ähnlich sicher ist eine Freigabe auf einem NAS-Gerät, für die Sie dann aber ein eigenes Benutzerkonto mit speziellem Passwort einrichten müssen. Auch diese Freigabe binden Sie nur zum Sichern und Wiederherstellen von Daten ein und hängen sie danach wieder aus.

Grundsätzlich gibt es ein gewisses Restrisiko, dass der Schädling genau dann zuschlägt, wenn man den Datenträger gerade angeschlossen hat. Dagegen helfen Systeme, die sich selbstständig um eine Versionierung der gesicherten Daten kümmern, etwa spezielle Backupserver auf dem NAS, Sync-Lösungen wie Syncthing oder Cloudspeicher. Oder Sie sichern

kurzerhand abwechselnd auf zwei USB-Platten.
(hos@ct.de)

HDR10+ oder Dolby Vision?

? Wenn mein Smart-TV sowohl Dolby Vision als auch HDR10+ beherrscht, was bekomme ich dann zu sehen, wenn mein Streamingdienst einen Film in beiden Formaten anbietet?

! Wir haben diesen Fall mit Amazon – dem einzigen Dienst, der in Deutschland bislang überhaupt HDR10+-Filme im Angebot hat – und einem Philips-TV geprüft. Der erhielt von Amazon bei einem Film, der in beiden HDR-Formaten vorliegt, die Dolby-Vision-Variante. Der Fernseher signalisierte das auch mit einem kurzzeitig eingeblendeten Logo.

Auf HDR10+ hingegen weist Amazon in der Filmbeschreibung nicht hin. Man kann deshalb nicht vorab erkennen, ob ein Film dieses Format besitzt. Samsung-TVs blenden bei der Wiedergabe solcher Filme kurz einen Hinweis auf HDR10+ ein.

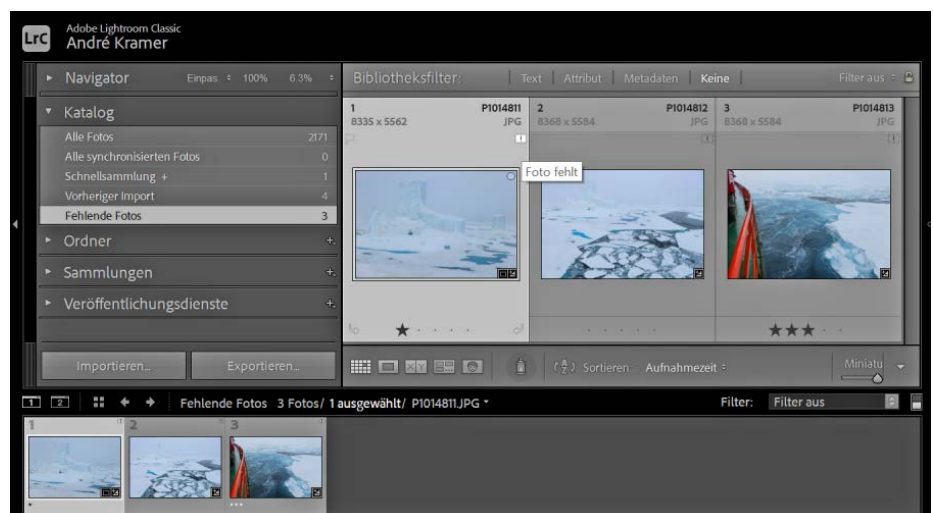
(uk@ct.de)

Fehlende Fotos in Lightroom

? Ich wollte ein älteres Foto in Lightroom Classic bearbeiten, bekam aber eine Meldung, dass das Foto fehlt. Offenbar habe ich es versehentlich gelöscht. Wie kann ich solche Datenbank-Inkonsistenzen aufspüren und beheben?

! Lightroom öffnet Fotos nicht direkt von der Festplatte, sondern importiert zunächst nur deren Metadaten in seine Bibliothek. Erst beim Aufruf im Entwickeln-Modul greift Lightroom auf die Originaldaten zu oder meckert, dass es das betreffende Foto in Abwesenheit nicht bearbeiten kann.

Beim Import erstellt der Raw-Entwickler auch ein Vorschaubild. Die Standardvorschaugröße beträgt bei Lightroom Classic 2048 Pixel an der langen Kante. Der Datenbankeintrag besteht weiter, auch wenn das Originalfoto, auf das er verweist, außerhalb von Lightroom gelöscht oder verschoben wurde. Aufgrund der relativ hohen Vorschauauflösung ist also nicht unbedingt ersichtlich, welche Fotos fehlen.



Der Menübefehl „Nach allen fehlenden Fotos suchen“ listet in Lightroom Classic alle Datenbankeinträge auf, die ins Leere führen.

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.

Im Bibliotheksmodul erscheint ein kleines Ausrufezeichen in der rechten oberen Ecke des Vorschaubilds, wenn das Originalfoto fehlt. Allen ins Leere führenden Verweisen kommt man in der Bibliothek über den Menübefehl „Bibliothek/Nach allen fehlenden Fotos suchen“ auf die Spur. Lightroom durchforstet dann die gesamte Bibliothek inklusive Unterordner und präsentiert sämtliche Karteileichen in einer Übersicht. Im Kontextmenü kann man den Eintrag über „Im Explorer anzeigen“ neu verknüpfen. Die Option „Nach zugehörigen fehlenden Fotos suchen“ verknüpft andere Fotos im betreffenden Ordner gleich mit. Lassen sich die Fotos aber nirgends finden, bleibt nur, den Datenbankeintrag über „Foto entfernen“ zu löschen. Exportieren kann man die von Lightroom erstellten Vorschaubilder nicht. (akr@ct.de)


Normen ausleihen


 In Ihren Artikeln geben Sie ab und zu einschlägige Normen an. Manchmal würde ich einzelne Aspekte gern vertiefen und die Normtexte im Original lesen. Kaufen möchte ich sie aber nicht immer direkt, so weit geht meine Neugier dann doch nicht. Gibt es eine Möglichkeit, diese Dokumente kostengünstig auszuleihen?

 Ausleihen kann man sie nicht direkt, wohl aber kostenlos einsehen. Dafür gibt es in ganz Deutschland verteilt die Normen-Infopoints, in denen man DIN-Normen und VDI-Richtlinien durchsuchen und vor Ort lesen kann. Diese Stellen befinden sich meist in Universitäts- und Fachhochschulbibliotheken. Man muss aber nicht studieren, um Zugang zu bekommen. Eine Übersicht über die Standorte finden Sie über ct.de/y8zx. (jam@ct.de)

Normen-Infopoints: ct.de/y8zx

USB-Maus soll PC schlafen lassen

 Damit mein Rechner nicht immer anspringt, wenn ich versehentlich an meine Funkmaus stoße, habe ich im Windows-Gerätemanager das entsprechende Häkchen entfernt. Doch der PC wacht trotzdem aus dem Suspend auf. Liegt das am USB-Funkempfänger?


 Um das versehentliche Hochfahren des PCs bei Maus- oder Tastaturberührungen zu verhindern, öffnet man üblicherweise den Windows-Gerätemanager (beispielsweise per Rechtsklick aufs Startmenü), sucht dort den Eintrag für die Maus oder Tastatur, öffnet dann per Rechtsklick deren Eigenschaften-Menü, geht in den Reiter „Energieverwaltung“ und schaltet „Gerät kann den Computer aus dem Ruhezustand aktivieren“ aus.


Kommunizieren Maus oder Tastatur allerdings über einen USB-Dongle per Funk mit dem Rechner, müssen Sie zwei Fallen beachten: Als wir die Aufwecksperrung mit einem Microsoft-Dongle für Maus plus Tastatur eingerichtet haben, funktionierte sie erst, nachdem wir den Haken bei beiden Geräten entfernten. Somit dürfen weder Maus noch Tastatur den PC aufwecken – bei Dongles anderer Hersteller könnte das ähnlich sein. Im Gerätemanager haben wir dazu unter „USB-Controller“ den „Microsoft Mouse and Keyboard Detection Driver“ angewählt, im Ansicht-

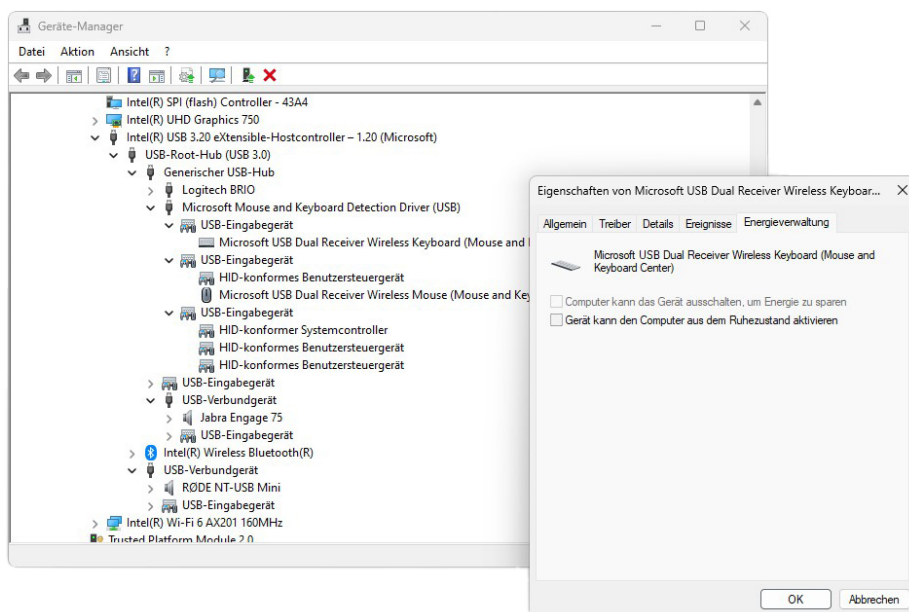
Menü „Geräte nach Verbindung“ gewählt und dann bei allen darunter eingehängten Einträgen (Wireless Mouse, Wireless Keyboard, einige HID-Geräte) den „Ruhezustand“-Haken entfernt. Wir haben keine Möglichkeit gefunden, wie die Tastatur den Rechner aufwecken darf, die Maus aber nicht – oder anders herum.

Zweitens merkt sich Windows diese Einstellung nicht allgemein für den USB-Dongle, sondern spezifisch pro USB-Buchse. Wer den Dongle also umsteckt, muss obige Prozedur wiederholen. Das Gleiche gilt fürs Aufwecken: Sollen Maus und Tastatur den PC aufwecken dürfen, sollten Sie nach jedem Umstecken des Dongles überprüfen, ob die Optionen für diese Buchse korrekt gesetzt sind. (jow@ct.de)

Eigene Domain und Mastodon

 Beim Microblogging-Dienst Mastodon bin ich nur unter <mein-name>@<mastodon-server> zu finden. Ich habe aber eine eigene Domain und möchte auch unter <mein-name>@<meine-domain> zu finden sein. Geht das irgendwie?

 Mastodon nutzt das Protokoll WebFinger (siehe ct.de/y8zx), um die bei einer Suche hinter dem @-Zeichen angegebene Domain zu erkunden. Wenn Sie auf Ihrem Webserver die passende Antwort bereitstellen, wird Mastodon sie anzeigen.



Damit eine per USB-Funk-Dongle angeschlossene Maus-Tastatur-Kombi den Rechner nicht versehentlich aufweckt, muss man das zuständige Häkchen bei sämtlichen Komponenten ausschalten.

Eine einfache Möglichkeit, die Antwort zu erzeugen, ohne dass Sie sich in WebFinger einarbeiten müssen, hat der Entwickler Maarten Balliauw (@maartenballiauw@mastodon.online) gefunden: Speichern Sie einfach den WebFinger-Eintrag Ihres Mastodon-Kontos an der richtigen Stelle auf Ihrem Server ab. Dazu rufen Sie die URL `https://<mastodon-server>/.well-known/webfinger?resource=acct:<mein-name>@<mastodon-server>` auf (Ihren Benutzernamen geben Sie dabei ohne führendes „@“ an) und speichern die Antwort ab: eine Textdatei, die mit `{ "subject": "acct:<mein-name>..."` beginnt. Erzeugen Sie im Hauptverzeichnis Ihres eigenen Webservers das Unterverzeichnis `.well-known` und legen Sie dort die Datei unter dem Namen `webfinger` ab.

Nun müsste jede Suche bei Mastodon nach `<kürzel>@<meine-domain>` als Treffer Ihren Mastodon-Account `<mein-name>@<mastodon-server>` anzeigen. Ein weiterer Vorteil: Wenn Sie auf einen anderen Mastodon-Server umziehen, speichern Sie einfach dessen WebFinger-Antwort auf Ihrem Server, damit `<kürzel>@<meine-domain>` auf Ihren neuen Mastodon-Account verlinkt. In dieser Einfachheit liefert Ihr Server allerdings für jedes angefragte Kürzel dieselbe Datei. Sie können also nicht je nach Kürzel auf verschiedene Mastodon-Konten verweisen oder bei bestimmten Kürzeln eine Fehlermeldung liefern.

Wenn Sie mehrere Domains haben, die Sie per 301-Weiterleitung in `.htaccess` auf Ihre Hauptdomain umleiten, funktioniert das Verfahren möglicherweise nicht, weil die WebFinger-Anfrage nicht korrekt umgeleitet wird. Legen Sie dann einfach im Hauptverzeichnis der verweisenden Domain ebenfalls das Verzeichnis `.well-known` mit der Datei `webfinger` an. Allerdings hilft auch das in der Regel nur dann, wenn Sie der verweisenden Domain ein SSL-Zertifikat spendiert haben (und nicht nur Ihrer Hauptdomain). (jow@ct.de)

Informationen zum WebFinger-Protokoll:
ct.de/y8zx

Procmon lädt keine gespeicherten Filter

Um Windows-Problemen auf die Schliche zu kommen, benutze ich gerne den Process Monitor von Microsoft Sysinternals. Seit einiger Zeit will es mir aber ums Verrecken nicht mehr gelingen,

die angezeigten Ereignisse mit gespeicherten Filtern zu dezimieren. Ich stelle mir die Filteroptionen so ein, wie ich sie brauche, wähle den Befehl „Filter/Save Filter“ und gebe einen Namen ein – zum Beispiel „Policies“. Er erscheint anschließend auch im Menü „Filter/Load Filter“, aber wenn ich den Filter zwischenzeitlich geändert habe und den gespeicherten Eintrag auswähle, passiert einfach nichts. Ich bin mir ziemlich sicher, dass das schon mal funktioniert hat. Was mache ich falsch?

! Nichts. Es handelt sich um einen Bug, den der Process Monitor mindestens seit Version 3.82 mit sich herumschleppt und der auch in der zum Redaktionschluss aktuellen Version 3.92 noch nicht behoben ist.

Für einen Workaround müssen Sie ein bisschen mit der Registry und deren Export-Dateien jonglieren: Zunächst beenden Sie den Process Monitor und exportieren mithilfe des Registrierungs-Editors `regedit` den Schlüssel „HKEY_CURRENT_USER\Software\Sysinternals\Process Monitor“, zum Beispiel in die Datei `procmon_komplett.reg`. In dem genannten Schlüssel speichert der Process Monitor alle seine Einstellungen, darunter auch die Filter.

Die exportierte Datei öffnen Sie nun in einem Texteditor und löschen alles Unnötige. Stehen bleiben nur die ersten paar Zeilen bis einschließlich `[HKEY_CURRENT_USER\Software\Sysinternals\Process Monitor]` sowie die Zeilen ab derjenigen, die – in Ihrem Beispiel – mit `"Filter#Policies"=hex:` beginnt, plus alle folgenden, durch eine Einrückung erkennbar dazugehörenden Zeilen. Zum Schluss ändern Sie noch `"Filter#Policies"` in `"FilterRules"` und speichern das Ergebnis unter neuem Namen, beispielsweise als `procmon_policyfilter.reg`.

Mit Nvidias RTX-4000-Grafikkarten bleibt mancher Bildschirm zu lange dunkel. Dagegen hilft ein Firmware-Update.

Analog basteln Sie sich auch `.reg`-Dateien für weitere gespeicherte Filter.

Wenn Sie nun einen dieser Filter verwenden wollen, stellen Sie zunächst sicher, dass der Process Monitor beendet wurde. Dann importieren Sie die gewünschte Filterregel per Doppelklick über den Registrierungs-Editor oder mit einem Aufruf des Kommandozeilenbefehls `reg import`. Wenn Sie anschließend den Process Monitor starten, sollten die gewünschten Filterregeln voreingestellt sein. (hos@ct.de)

„Blackscreen“ bei Nvidia RTX 4000

? Ich habe mir eine Grafikkarte mit Nvidia RTX 4080 gegönnt. Seit ich die eingebaut habe, bleibt mein Bildschirm beim Einschalten sehr lange dunkel. Ich sehe weder das Boot-Logo noch die Hinweise auf die Tastenkürzel für BIOS-Setup und Bootmenü. Erst wenn Windows die Kontrolle übernimmt, gibt es ein Bild, ab dann funktioniert auch alles perfekt. Wie bekomme ich das Boot-Bild zurück?

! Das ist ein bekanntes Problem, das RTX-4000-Karten im Zusammenspiel mit der UEFI-Firmware mancher Mainboards haben. Für Betroffene hat Nvidia ein Update für die Firmware des Grafikchips herausgegeben. Auf der Download-Seite (siehe ct.de/y8zx) weist der Hersteller aber ausdrücklich darauf hin, dass Anwender das „Nvidia GPU UEFI Firmware Update Tool v1.2“ wirklich nur dann installieren sollten, wenn bei ihrem System das beschriebene Problem auftaucht. (csp@ct.de)

Nvidia-Update-Tool: ct.de/y8zx



Bild: Nvidia