Das Hochsicherheits-Windows

c’t-Tool aktiviert Profi-Schutz

Erpressungstrojaner sind weiterhin schwer in Mode bei Kriminellen, denn mit ihnen lässt sich leichtes Geld verdienen, weil Windows bei Privatnutzern üblicherweise offen steht wie ein Scheunentor. Das liegt auch daran, dass Microsoft ihnen Sicherheitsfunktionen vorenthält. Ein c't-Tool ändert das.

Von Axel Vahldiek

Windows-PCs in Firmen sind oft so sehr verrammelt, dass man auf ihnen nur jene Anwendungen starten kann, die zuvor vom Administrator ausdrücklich genehmigt wurden. Das soll nicht nur verhindern, dass die Mitarbeiter spielen statt zu arbeiten, sondern schützt auch zuverlässig vor vielen Viren und Trojanern. Zwar gibt es mittlerweile jene seltenen Schädlinge, die sich dateilos ins System einnisten [1], doch die meisten arbeiten anders: Ein Skript auf einer befallenen Website oder ein Makro in einem infizierten Dokument lädt die eigentliche Schädlingsdatei auf die Festplatte herunter und trägt einen passenden Autostart ein, der dafür sorgt, dass die Programmdatei beim Hochfahren des Systems mit gestartet wird. Wenn sie aber nicht in der Liste der genehmigten Anwendungen steht, scheitert auch ihr Start und der Schädling kann nichts anrichten. Das Gleiche gilt auch für Malware, die als ausführbare Datei etwa per Mail beim Nutzer ankommt. Der Mechanismus, der dahintersteckt, heißt „Software Restriction Policies“ (SRP). Dabei handelt es sich letztlich um Listen von erlaubten sowie verbotenen Anwendungen und Dateitypen. Bei neueren Windows-Versionen gibt es eine noch etwas mächtige Variante davon namens Applocker, für den Schutz vor Krypto-Trojanern reichen die bereits mit Windows XP eingeführten SRP aber völlig aus.

Privatanwendern half das bislang allerdings nichts, denn den Home-Editionen von Windows fehlen die zum Konfigurieren der SRP nötigen Werkzeuge – und das, obwohl SRP an sich auch unter Home funktionieren. Wir lösen das Problem: Mit unserem Programm „Restric'tor“ können Sie SRP in allen Windows-Editionen gleichermaßen konfigurieren und verwalten.

Dieser Beitrag erläutert, was SRP eigentlich sind, welche Auswirkungen sie haben und wie Sie auf dem eigenen PC auch ohne Aktivieren der SRP vorab prüfen können, was nach dem Aktivieren wohl alles blockiert werden würde. Das erleichtert die Entscheidung, auf welchen Rechnern Sie SRP wirklich einsetzen wollen, denn eines muss deutlich gesagt werden: SRP sind zwar für viele, aber nicht für alle PCs geeignet. Der nachfolgende Artikel erklärt den Einsatz unseres Werkzeugs Restric'tor und gibt Handreichungen, wie Sie Windows dazu bringen, Sie von sich aus über Verstöße gegen Ihre selbst erstellten Regeln zu informieren. Es folgen Tipps, wie Sie bereits vor dem ersten Start einer Anwendung erkennen können, ob Sie womöglich einen Schädling vor sich haben.

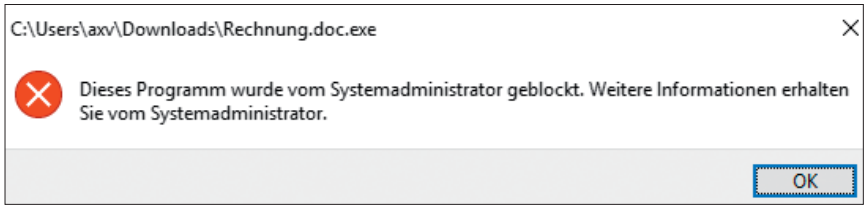
Ein Virenscanner reicht längst nicht mehr.

Falls Sie jetzt ob der Länge der Artikelstrecke zurückschrecken: In der Tat, auch wenn wir mit unserem Restric'tor versuchen, Ihnen möglichst viel Aufwand abzunehmen, kann das Konfigurieren und Pflegen von SRP dennoch mit einem gewissen Aufwand verbunden sein – je nach Einsatzzweck einer Windows-Installation reicht die Bandbreite dabei von Einrichten und Vergessen bis hin zu ständig nötiger Pflege. Sie profitieren aber im Gegenzug von einem für Privatanwender bislang unter Windows unerreichbaren Schutz-Level. Lesen Sie sich also in Ruhe die Artikel durch und wägen Sie danach ab, wie viel Aufwand der Einsatz von SRP auf Ihren Rechnern wohl bedeutet und ob Ihnen der Sicherheitsgewinn das wert ist. Und denken Sie dabei auch an jene PCs, für die Sie im Freundes- und Familienkreis den Admin spielen: Nach unseren Erfahrungen wird Schwiegermutter von aktiven SRP üblicherweise gar nichts merken. Und wenn Sie künftig nicht mehr ständig wegen Virenbefall zu Hilfe gerufen werden, haben Sie selbst dann etwas von SRP, wenn Sie sie auf dem eigenen Rechner gar nicht nutzen.

An der UAC vorbei

Zuerst noch ein paar weitere Worte dazu, warum eine Standard-Windows-Installation auch heutzutage noch offen wie ein Scheunentor ist. Denn immerhin hat Microsoft in den letzten Jahren ja einige Anstrengungen dagegen unternommen. So ist seit dem Service Pack 2 für Windows XP eine Firewall an Bord und seit Windows 8 ein Virenscanner. Seit Vista arbeiten die Nutzer zudem üblicherweise mit eingeschränkten Benutzerrechten, und zwar selbst dann, wenn sie als Administrator angemeldet sind. Um letzteres kümmert sich die Benutzerkontensteuerung, englisch „User Account Control“ (UAC).

Die UAC sorgt dafür, dass jeder Prozess, den ein als Administrator angemeldeter Anwender startet, trotzdem erst mal nur mit eingeschränkten Rechten läuft.



Software Restriction Policies (SRPs) sorgen dafür, dass nur noch zuvor genehmigte Anwendungen starten – Schädlinge werden hingegen blockiert.

Das gilt selbst für den Explorer. Mangels Admin-Rechten hat man unter anderem nicht mehr überall Schreibrechte: Sie fehlen beispielsweise im Windows- und im Programme-Ordner. Möchte ein Prozess dort etwas hinschreiben oder hinkopieren, muss er bereits mit Administratorrechten gestartet worden sein oder sie sich nachträglich verschaffen. Beides löst eine der bekannten „Sind Sie sicher?"-Nachfragen aus. Alle weiteren Prozesse starten trotzdem wieder mit eingeschränkten Rechten.

Die Nachfragen sind immer dann etwas nervig, wenn man gerade selbst geklickt hat, da man sich ja üblicherweise schon beim ersten Klick sicher war. Sollte hingegen eine Sind-Sie-sicher-Frage aus dem Nichts erscheinen, versucht wohl irgendein Programm im Hintergrund, sich Administratorrechte zu verschaffen – und es besteht immer die Gefahr, dass das ein Schädling ist. Und wenn man in so einem Moment einfach so auf „ja" klickt, hat man verloren, falls es es sich wirklich um einen Schädling handelt. Denn ein Prozess mit Admin-Rechten darf genau alles auf dem System. Zwar kann man selbst Administratoren Rechte wegnehmen, doch wenn ein Prozess erst mal mit vollen Rechten läuft, kann er sich fehlende Zugriffsrechte einfach wieder selbst einräumen. Allenfalls der Virenscanner könnte in diesem Moment noch einschreiten, doch ein mit Admin-Rechten laufender Schädling kann sich vor dem problemlos verstecken oder ihn einfach abschalten.

Die Schädlingsprogrammierer gehörten zu den ersten, die begriffen, dass UAC-Nachfragen den Benutzer auf einen Angriff hinweisen können. Daher unterlassen ihre Machwerke längst alle Aktionen, die so eine Nachfrage auslösen könnten. Wozu auch? Wenn ein Erpressungstrojaner den UAC-geschützten Windows-Ordner verschlüsseln würde, könnte man Windows einfach neu installieren. Die ohne UAC-Abfrage verschlüsselbaren Ordner im Benutzerprofil hingegen enthalten die persönlichen Bilder, Videos und Dokumente des Benutzers, und wer davon kein Backup hat, lässt sich viel leichter zur Zahlung von Lösegeld erpressen. Weil zudem auch für Nutzer mit eingeschränkten Rechten Stellen existieren, an denen sie Autostarts eintragen können, können sich Schädlinge problemlos auch ohne Administratorrechte auf Dauer einnisten – genau deshalb ist Windows in der Standardeinstellung wie erwähnt offen wie ein Scheunentor.

SRP können Viren stoppen, aber nicht den Nutzer.

Zum Lösen des Problems könnte man zwar UAC-Abfragen auch für die Benutzer-Ordner einbauen, doch dann wäre an sinnvolles Arbeiten kaum noch zu denken: Bei jedem Speichern und Zwischenspeichern von Dokumenten würde es Nachfragen hageln, ebenso bei jedem Kopiervorgang und bei jedem Löschen einer Datei und so weiter. Das würde also mehr Probleme verursachen als lösen.

Abhilfe SRP

Software Restriction Policies schützen anders: Sie sorgen dafür, dass Windows nur noch den Start zuvor festgelegter Anwendungen erlaubt. Als Folge kann sich ein Schädling zwar noch im Nutzerprofil einnisten, von dort aus aber nicht starten und somit keinen Schaden anrichten. Die Beschränkungen gelten dabei ausschließlich für ausführbare Dateien, also Dateitypen wie exe, bat, vbs und so weiter; die Liste ist anpassbar. Dokumente hingegen werden von SRP nicht überwacht: Das Öffnen von Texten, Tabellen, Videos et cetera ist also auch bei aktiven SRP problemlos möglich. Wichtig ist nur, dass die jeweils mit dem Dokumenten-Dateityp verknüpfte Anwendung erlaubt ist, beispielsweise das Office-Paket.

Es gibt verschiedene Arten von Regeln, die den Start von Programmen erlauben. Für einzelne ausführbare Dateien empfiehlt sich eine „Hash-Regel". Beim Erstellen einer solchen Regel erzeugt Windows selbst einen Hash – eine Art einzigartiger Fingerabdruck – der Datei und gleicht künftig bei jedem Aufruf einer ausführbaren Datei ab, ob sie einen der erlaubten Hashes besitzt – nur dann wird sie ausgeführt. Dank des Hashes ist egal, an welchem Ort die Datei liegt und wie sie heißt, wichtig ist nur, dass sie unverändert ist. Ein Schädlingsbefall hingegen würde die Datei ändern, was zu einem nicht mehr passenden Hash führt.

Nun wäre es recht umständlich, für alle Programme, die man braucht, jeweils eine Hash-Regel zu erstellen. Deshalb gibt es einen weiteren Regeltyp: die Pfad-Regel. Damit ist gemeint, dass man per Regel den kompletten Inhalt eines Ordners mitsamt seiner Unterordner erlaubt. Sinnvoll ist das unter anderem bei den Ordnern „Windows" und „Programme" – ohne Ausnahmen für sie würde nicht nur keine der installierten Anwendungen mehr starten, sondern auch nicht mehr Windows selbst. Man würde stattdessen vor einem schwarzen Bildschirm sitzen. Daher erzeugt Windows Pfad-Regeln für diese beiden Ordner grundsätzlich von selbst beim Aktivieren des SRP-Mechanismus.

Beim Erstellen von Pfad-Regeln muss man aufpassen, dass man nur Pfade erlaubt, in denen Benutzer mit eingeschränkten Rechten keine Schreibrechte besitzen. Es gilt also, die Rechtekombination „Schreiben" und „Ausführen" zu verhindern. Denn in einem Ordner, in dem beides gleichzeitig erlaubt ist, kann sich ein Schädling wieder unbemerkt einnisten. Beim Programme-Ordner besitzt ein Nutzer mit eingeschränkten Rechten keinen Schreibzugriff, daher kann er problemlos einfach so als Pfad-Regel eingerichtet werden. Beim Windows-Ordner sieht es leider anders aus: In seinen Tiefen gibt es einzelne Unterordner, in denen Nutzer und Prozesse auch ohne Admin-

Rechte schreiben dürfen. Restric'tor bietet daher eine Option, solche Unterordner zu suchen und mit zusätzlichen Pfad-Regeln zu blockieren. Denn SRP können nicht nur erlauben, sondern auch verbieten. In verbotenen Ordnern können Sie einzelne Dateien trotzdem per Hash-Regel erlauben.

Bequem machen

SRP können nicht nur für Nutzer mit eingeschränkten Rechten gelten, sondern auch für Administrator-Konten. Davon ist aber im Normalfall abzuraten, denn das erschwert das Arbeiten unnötig: Wenn die SRP nur für Nutzer mit eingeschränkten Rechten gelten, können Sie bei Bedarf ein Programm per Rechtsklick „Als Administrator ausführen" und so beliebige Programme starten. Für Programme, die ohnehin Admin-Rechte brauchen, müssen die dann auch keine Regeln erstellen. Und falls der Abgabetermin mal wieder wichtiger als alles andere ist, können Sie so auch bei aktiven SRP mal eben das gerade lebensnotwendige Programm starten, selbst wenn es dafür noch keine Ausnahmeregel gibt.

Auch das Installieren von Anwendungen ist problemlos möglich: Starten Sie das Setup-Programm einfach als Admin. Wenn es die Anwendung korrekt in den Programme-Ordner installiert, brauchen Sie anschließend nicht mal eine neue Ausnahmeregel dafür zu erstellen.

Nur mal gucken!

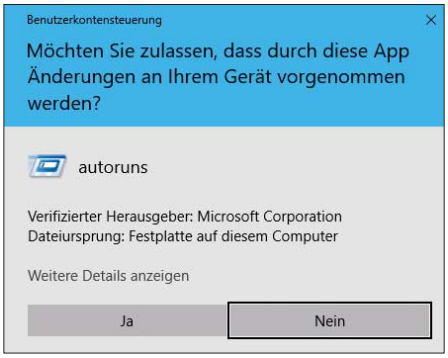
Wer nun wissen will, wie sich SRP auf dem eigenen Rechner auswirken, kann einen harmlosen Probelauf starten und lässt Windows in einer Log-Datei sämtliche Programmstarts protokollieren, die bei aktiven SRP von den Regeln überwacht worden wären. Auf diese Weise können Sie herausfinden, was SRP auf Ihrem Rechner bewirken würden, ohne sie dafür aktivieren zu müssen.

Dazu laden Sie sich unter ct.de/ym5g unser Programm „Restric'tor" herunter und starten es als Administrator. Im ersten Reiter ganz unten können Sie die Log-Datei erzeugen. Hangeln sie sich im „Durchsuchen"-Dialog zu einem beliebigen beschreibbaren Ordner durch, tippen Sie einen Dateinamen ins entsprechende Feld und klicken Sie auf Speichern. Nun noch auf „Anwenden" klicken, die Nachfrage bestätigen und schon erstellt Windows die Log-Datei. Lesen können Sie sie beispielsweise mit Notepad.

Die Log-Datei enthält keine persönlichen Informationen, sondern nur wenige Angaben zum jeweils protokollierten Ereignis: Jeder Eintrag beginnt mit dem Namen des auslösenden Prozesses, also beispielsweise svchost.exe beim Start von Diensten oder explorer.exe, wenn Sie selbst Anwendungen aus dem Startmenü oder eben aus dem Explorer starten. Es folgen die Prozess-ID (PID), Name und Pfad des gestarteten Programms sowie schließlich die ID jener Regel, die den Start erlaubt hat. Da Windows nicht mehr Informationen speichert und nur bei Programmstarts etwas in die Log-Datei schreibt, bleibt sie normalerweise auch nach Wochen wenige MByte klein.

Um sich einen Überblick zu verschaffen, wie viele Ausnahmeregeln zusätzlich zu den Standard-Regeln für den Windows- und den Programme-Ordner wohl nötig werden, nutzen Sie Ihren PC nach dem Aktivieren der Log-Datei einfach ein paar Tage wie gewohnt weiter. Danach schauen Sie in die Log-Datei. Tipp: Falls Sie sie zu unübersichtlich finden, kopieren Sie den kompletten Inhalt kurzerhand in eine Tabelle eines Office-Pakets und sortieren nach der Spalte mit den Pfadangaben. Interessant sind nur die Zeilen, in denen die Pfade anders beginnen als mit den genannten Ausnahmen „C:\Program Files" und „C:\Windows"; unter einem 64-bittigen Windows erfassen die Standard-Regeln zusätzlich den Ordner „C:\Program Files (x86)".

Bei unseren Tests passierte es mitunter, dass Windows bei tagelanger Laufzeit irgendwann das Protokollieren in der Log-Datei bis zum nächsten Neustart stoppte. Einen Grund dafür haben wir nicht finden können. Dramatisch ist das allerdings nicht, denn erstens reicht ein Neustart zum Lösen des Problems und zweitens gibt es weitere Optionen der Überwachung der SRP, die zuverlässig funktionieren – mehr dazu im Kasten auf Seite 86.



Solche Nachfragen mögen nerven, wenn man das fragliche Programm gerade selbst gestartet hat. Doch falls solche Nachfragen aus dem Nichts erscheinen, sind sie ein deutliches Alarmsignal.

Änderungen durch SRP

Auch wenn alle Apps aus dem Store sowie die meisten herkömmlichen Programme problemlos bei aktivierter SRP laufen, muss man sich doch mitunter umgewöhnen. So erkennt Windows beispielsweise Programme, die Administratorrechte brauchen, entweder anhand einiger festgelegter Dateinamen wie setup.exe oder install.exe oder aber an einem in der Datei steckenden Manifest, welches die Rechte

Noteingänge

Software Restriction Policies schützen vor dem Start unerwünschter Anwendungen, aber wie jeder andere Schutzmechanismus kann das mitunter im falschen Moment passieren: Wenn die auf dem Desktop-PC erstellte Präsentation auf dem Notebook nicht starten will, weil das Office-Paket noch nicht erlaubt wurde, will man kaum vor den Augen des Chefs erst mit Regeln hantieren, sondern nur, dass es jetzt sofort geht. Kein Problem: Rechtsklick auf das Programm, „Als Administrator ausführen", läuft.

Falls es nicht um einen hektischen Einzelfall geht, sondern Sie sich beim Konfigurieren der Regeln verhaspelt haben, hilft Noteingang Nummer 2: Einfach alle Regeln löschen und von vorn anfangen. Falls selbst Restric'tor nicht mehr laufen sollte, löschen Sie mit regedit den kompletten Registry-Schlüssel `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\safer`. Schlimmstenfalls erledigen Sie das im abgesicherten Modus – da sind SRP grundsätzlich nicht aktiv. SRP können Sie von Ihrem Rechner daher nicht dauerhaft aussperren.

anfordert. Die Überwachung durch die SRP schlägt aber in allen Fällen vorher zu und verhindert so das Anfordern und damit den Start des Programms. Auch hier hilft wieder, das Programm einfach per Rechtsklick und „Als Administrator ausführen“ zu starten. Sie erkennen solche Programme am kleinen Schild unten rechts im Programmsymbol.

Wer gern portable Anwendungen nutzt, die ohne Installation auskommen, kann das auch bei aktiven SRP. Für portable System-Utilities, die ohnehin nur mit Admin-Rechten laufen, sind nicht mal Regeln erforderlich. Für alle anderen erzeugt man kurzerhand Hash-Regeln. Problematisch werden nur portable Anwendungen, die gelegentlich oder gar häufig Updates brauchen, wie Browser oder Mail-Client. Hier müssten Sie dann jedes Mal die Regeln anpassen, und zwar sowohl für das Update-Programm als auch für das Programm selbst sowie gegebenenfalls für das Wrapper-Programm, das dafür sorgt, dass die Anwendung überhaupt portabel ist. Das ist nach unseren Erfahrungen auf Dauer nur was für Menschen mit sehr belastbarem Nervenkostüm. Wir empfehlen stattdessen, statt der portablen die installierbaren Versionen solcher Programme zu verwenden, denn im Programme-Ordner klappts auch mit dem Update.

In Einzelfällen kann es aber auch bei installierten Anwendungen zu Schwierigkeiten kommen. So lässt sich Googles Browser Chrome je nach Fassung wahlweise ins Nutzerprofil installieren, von wo aus er aber nur mit zusätzlichen Regeln laufen würde - die dank regelmäßiger Updates immer wieder anzupassen wären. Empfehlenswert ist hier, Chrome stattdessen in den Programme-Ordner zu installieren: Dann klappt alles inklusive Updates auch ohne zusätzliche Regeln. Noch etwas anders liegt der Fall bei Spotify: Der Client will sich grundsätzlich ins Benutzerprofil installieren, was dank ständiger Updates immer wieder eine Regel-Pflege erfordert. Doch auch hier gibt es Abhilfe: den Webplayer. Er läuft ganz ohne Ausnahmeregeln im Browser; Sie finden ihn unter play.spotify.com. Weitere Schwierigkeiten sind uns mit Electron-Apps wie Whatsapp aufgefallen, die ebenfalls im Benutzer-Ordner liegen, sowie mit Onedrive, Steam und Origin. Hier waren jeweils Ausnahmeregeln erforderlich.

Mitunter gibt es jedoch auch bei im Programme-Ordner installierten Anwendungen Schwierigkeiten beim Update. Der PDF-Viewer Foxit Reader beispielsweise erzeugt eine Updater.exe im Temp-Ordner des Benutzerprofils, doch von dort darf sie bei aktiver SRP nicht starten. Eine Pfad-Regel als Ausnahme hinzuzufügen verbietet sich, weil der Benutzer hier ja Schreibrechte hat. Abhilfe bringt hier, entweder für die updater.exe eine Hash-Regel zu erstellen, die dann aber immer dann aktualisiert werden muss, wenn auch updater.exe aktualisiert wurde, oder aber die automatischen Updates abzustellen und stattdessen gelegentlich den Reader als Administrator zu starten, um ihn Updates installieren zu lassen.

Beim Umgang mit Skripten muss man sich bei aktivierten SRP etwas umgewöhnen, denn als ausführbare Dateien unterliegen sie ja der SRP-Überwachung. Beispielsweise klappt bei Batch-Dateien ein Klick auf „Bearbeiten“ in deren Kontextmenü zum Öffnen mit Notepad nicht mehr. Sie können aber problemlos zuerst Notepad starten und das Skript dann über dessen Menü oder per Drag & Drop aus dem Explorer öffnen und bearbeiten. Das Ausführen des Skripts klappt dann aber wieder nur mit Administratorrechten oder nach dem Erstellen einer passenden Regel.

Die Windows PowerShell läuft bei aktiven SRP in einem „Constrained Language Mode“, in dem der Zugriff auf die meisten COM- und .NET-Objekte verboten ist. Gewöhnliche Cmdlets funktionieren aber wie gewohnt und in PowerShell-Sessions, die mit Administratorrechten gestartet wurden, ändert sich nichts. Details erläutert der Befehl `Get-Help about_Language_Modes`.

In der Log-Datei werden Ihnen auch immer wieder Einträge zu .lnk-Dateien auffallen, die Sie bei der Durchsicht aber einfach ignorieren können. Hier geht es nur um Verknüpfungen, die aus Sicherheitssicht völlig unkritisch sind, weil das Ziel der Verknüpfung ja ebenfalls von SRP überwacht wird – mehr dazu im nachfolgenden Artikel.

Und los ...

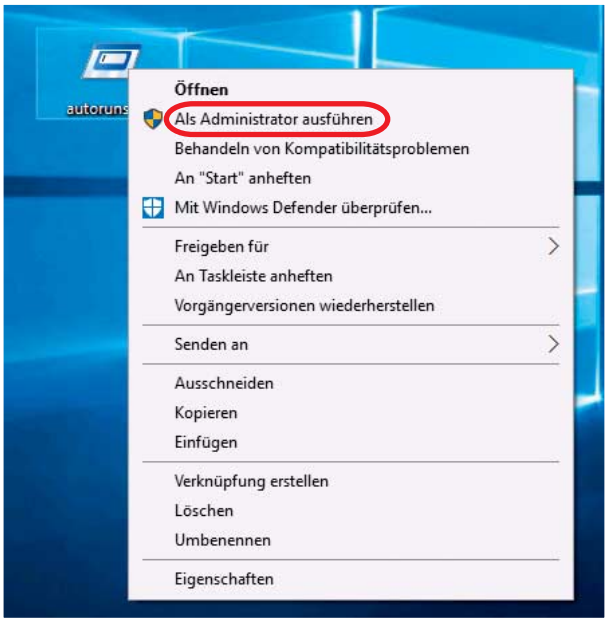
Nach dem Auswerten der Log-Datei können Sie sich entscheiden, auf welchen eigenen oder von Ihnen betreuten PCs Sie SRP aktivieren wollen. Wie genau das mit Restric’tor funktioniert, zeigt der nachfolgende Artikel. Er erläutert auch, wie Sie das Blockieren von Programmen möglichst bequem überwachen können.

(axv@ct.de) c't

Literatur

[1] Olivia von Westernhagen, Jürgen Schmidt, Die unsichtbare Gefahr, Dateilose Infektion umgeht Schutzfunktionen, c’t 7/17, S. 96

Restric’tor: ***ct.de/ym5g***



Richtig konfiguriert, lassen sich auch bei aktivierten SRPs noch beliebige Programme starten, wenn man das ausdrücklich als Administrator macht.