FAQ
Software Restriction Policies

Antworten auf die häufigsten Fragen

Von Hajo Schulz

Sinn und Zweck

? Was sind überhaupt die Software Restriction Policies?

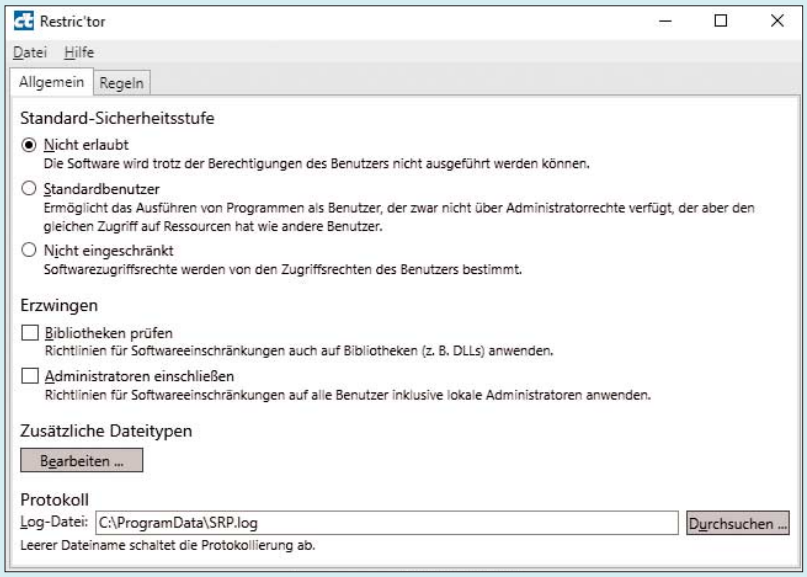
! Mit den Software Restriction Policies – kurz SRP, auf Deutsch „Richtlinien für Softwareeinschränkung“ – kann man Windows anweisen, nur noch bestimmte Software auszuführen. In Unternehmen dient das dazu, den Aktionsradius von Mitarbeitern auf die Programme einzuschränken, die sie für ihre Arbeit brauchen. Auf Privatrechnern kann man sie zur Erhöhung der Sicherheit einsetzen: Wo nur noch vertrauenswürdige Software gestartet werden kann, haben es Trojaner schwer, sich etwa über vermeintlich harmlose Dateianhänge von E-Mails ins System einzuschleichen.

SRP werden typischerweise so konfiguriert, dass sie zunächst einmal alle Programme verbieten. Über einen Satz von Regeln definiert man dann, welche Programme vertrauenswürdig sind. Es gibt unter anderem Pfadregeln, die den Inhalt ganzer Ordner erlauben – sinnvoll zum Beispiel für das Windows-Verzeichnis und die Programme-Ordner mit regulär installierten Anwendungen. Außerdem gibt es Hash-Regeln, die einzelne Programmdateien eindeutig als erlaubt identifizieren. Wichtig beim Einrichten der SRP ist, dass man über die Pfadregeln nur solche Ordner als vertrauenswürdig ausweist, in denen zum Schreiben Administratorrechte notwendig sind.

Restric’tor

? Wie konfiguriert man SRP?

! Normalerweise über die Gruppenrichtlinien (engl. Group Policies). Dazu dienen in den Professional-, Enterprise- und Ultimate-Ausgaben von Windows der Gruppenrichtlinieneditor (gpedit.msc) oder die „Lokale Sicherheitsrichtlinie“ (secpol.msc). In Windows Home fehlen beide. Letztlich sind die Software Restriction Policies aber nichts anderes als Registry-Einträge – wo sie vorhanden sind, beachten sie alle Windows-Versionen einschließlich Home. Das Einrichten über direkte Eingriffe in die Registry ist aber anstrengend und fehlerträchtig. Deswegen hat die c’t das Programm Restric’tor entwickelt, mit dem sich die SRP komfortabel editieren lassen [1, 2].



Mit dem c’t-Programm Restric’tor lassen sich die „Richtlinien für Softwareeinschränkung“ unter allen aktuellen Windows-Editionen recht komfortabel einrichten.

Hässliche Log-Datei

? Im Artikel zu Restric’tor in c’t 10/17 empfehlen Sie, mit den SRP zunächst nichts einzuschränken, sondern erst mal nur eine Log-Datei schreiben zu lassen, um zu beurteilen, ob mit übermäßigen Nebenwirkungen zu rechnen ist. Dieses Protokoll hat ein ziemlich krudes Format, außerdem habe ich den Eindruck, dass Einträge fehlen. Kann Restric’tor das nicht besser machen?

! Restric’tor selbst schreibt keine Logs, verhindert keine Programmstarts und gibt auch keine Fehlermeldung aus, wenn ein Programmstart an den Einstellungen scheitert. Um all das kümmert sich Windows – Restric’tor schreibt lediglich Registry-Einträge und steuert damit die in Windows vorhandenen Protokoll- und Schutzmechanismen. Restric’tor läuft auch nicht im Hintergrund – wenn Sie sein Fenster schließen, verschwindet es komplett aus dem Speicher. Sie könnten es nach dem Festlegen der Einstellungen sogar von der Festplatte löschen und die SRP würden weiterhin funktionieren.

Restric’tor startet nicht

? Ich habe mir Ihr Programm Restric’tor heruntergeladen und wie im Artikel empfohlen auf die Platte kopiert. Es scheint aber nicht zu funktionieren: Ob ich es doppelklicke, per Rechtsklick „Als Administrator ausführe“ oder über die Eingabeaufforderung zu starten versuche: Es passiert einfach nichts.

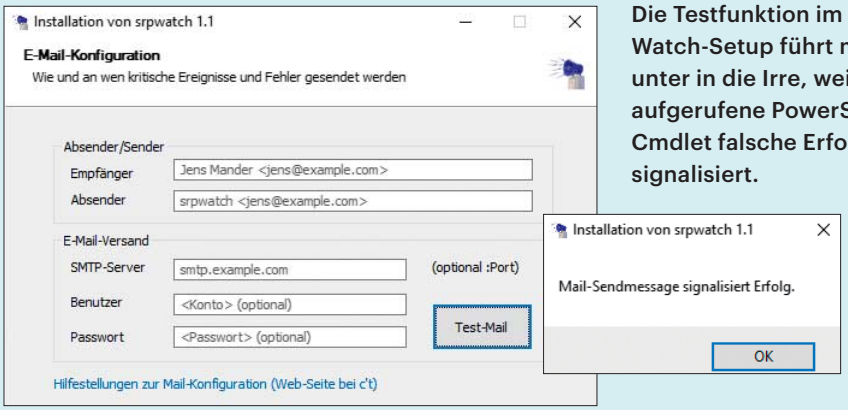
! Haben Sie womöglich auf dem betroffenen Rechner zuvor das c’t-Notfall-Windows 2017 gebaut? Dann sind Sie vermutlich Opfer eines Fehlers geworden, den eines der dabei verwendeten Skripte enthielt. Der Fehler zerstört einige Registry-Einträge, was dazu führt, dass verschiedene Programme nicht mehr starten,

die – wie Restric'tor – mit Microsofts .NET-Framework programmiert wurden. Genaueres dazu steht in [3]; dort finden Sie auch eine Anleitung, um Ihre .NET-Installation zu reparieren.

SrpWatch-Showstopper

? Gern hätte ich auch Euer SrpWatch eingesetzt, aber zwei Gründe haben mich davon abgehalten: Es speichert das Passwort für den Mail-Versand im Klartext. Obendrein misslang mir die Konfiguration für zwei verschiedene Mail-Konten, obwohl die Installation behauptet hat, dass die Test-Mail erfolgreich verschickt worden sei. Könnt Ihr da noch mal beigehen?

! Sind wir: Die Version 1.1, die Sie unter ct.de/yfst zum Download finden, enthält zwei wesentliche Korrekturen. Die erste betrifft den Umgang mit Passwörtern: Die speichert das Programm nicht mehr im Klartext, sondern verwendet die PowerShell-eigenen Mechanismen, um Passwörter so zu sichern, dass Sie nur der Benutzer wieder in Klartext verwandeln kann, der die „Verschlüsselung" veranlasst hat – das stellt zwar keine absolute Sicherheit dar, verbessert aber die Lage aus unserer Sicht. Benutzer in diesem Kontext heißt, dass der erzeugte Hash nur unter seinem Konto und in der Windows-Installation in Klartext zurückwandelbar ist.



Die Testfunktion im SrpWatch-Setup führt mitunter in die Irre, weil das aufgerufene PowerShell-Cmdlet falsche Erfolge signalisiert.

Die zweite Änderung betrifft die Möglichkeit, eine Test-Mail noch aus der Installation heraus zu erzeugen. Wie wir in ausgiebigen Tests des vom Skript verwendeten Cmdlet für die PowerShell (`Send-MailMessage`) festgestellt haben, liefert es oft unsinnige Statusinformationen zurück, die die Installation obendrein zu optimistisch interpretiert. Fehlen zum Beispiel die Domain-Namen in den E-Mail-Adressen, gibt das Cmdlet keinen Fehlercode zurück, sondern signalisiert Erfolg – sieht man genauer nach, hat es aber nicht mal den Versuch unternommen, eine Nachricht zu verschicken. Die neue Version meldet den Sende-Erfolg deshalb weniger euphorisch.

Eine technische Lösung für die Mail-Konfigurationsprobleme gibt es nicht – die alternativ verwendbaren Klassen und Funktionen aus dem .NET-Namensraum `System.Net.Mail` verhalten sich analog und scheinen uns ohnehin nur der Kern zu sein, den auch `Send-MailMessage` aufruft. Was hoffentlich hilft, sind Beispiele: Der Mail-Konfigurationsdialog von SrpWatch enthält einen klickbaren Link, der im Browser die Projektseite mit Beispielkonfigurationen für diverse Mail-Anbieter öffnet. Wenn Sie weitere ergänzen wollen, freuen wir uns über eine E-Mail. *(hos@ct.de)*

Literatur

[1] Axel Vahldiek, Das Hochsicherheits-Windows, c't-Tool aktiviert Profi-Schutz, c't 10/17, S. 76
[2] Hajo Schulz, Schotten dicht!, Mit Restric'tor zum sicheren Windows, c't 10/17, S. 82
[3] Peter Siering, c't-Notfall-Windows 2017 .NET-Fehler: https://heise.de/-3576079

Restric'tor, SrpWatch, Foren: ***ct.de/yfst***

Restric'tor 1.2

Wir haben das Programm Restric'tor weiterentwickelt; die aktuelle Versionsnummer ist jetzt 1.2. Zu den Neuerungen gehört, dass die Routine zum Einlesen der SRP aus der Registry jetzt wesentlich robuster ist. Offenbar existieren andere SRP-Tools, die nicht standardkonforme Einträge in einem Format in der Registry hinterlassen, das Restric'tor in der ersten Version aus dem Tritt gebracht hat.

Außerdem erfüllt Restric'tor einen Wunsch zahlreicher Anwender: Über die Kommandozeilenoption `/NewHash` lässt sich jetzt der Name einer Programmdatei an das Tool übergeben, woraufhin es eine neue Hash-Regel der Stufe „Nicht eingeschränkt" für dieses Programm erzeugt. Die müssen Sie nur noch mit „Anwenden" in die Registry schreiben. Zuvor können Sie wenn nötig Hash-Regeln für ältere Versionen desselben Programms löschen.

Um dieses Feature sinnvoll zu nutzen, erzeugen Sie sich am besten einen Eintrag dafür im „Senden an"-Kontextmenü des Explorers. Dazu markieren Sie zunächst die Datei Restrictor.exe im Explorer und kopieren sie mit der Tastenkombination Strg+C oder dem Kontextmenübefehl „Kopieren" in die Zwischenablage. Geben Sie nun in die Explorer-Adresszeile `shell:sendto` ein und bestätigen Sie mit Enter. Mit einem Rechtsklick in einen freien Bereich des SendTo-Ordners und Auswahl des Befehls „Verknüpfung einfügen" erzeugen Sie einen Restrictor-Eintrag. Den können Sie nach Belieben umbenennen, zum Beispiel in „Restric'tor (Neue Hash-Regel)" – der Name erscheint später im „Senden an"-Kontextmenü. Außerdem müssen Sie noch die Eigenschaften der neu erzeugten Verknüpfung aufrufen und dort das Feld „Ziel" am Ende durch ein Leerzeichen und `/NewHash` ergänzen.

Um für eine EXE-, CMD- oder jede andere Datei eine SRP-Hash-Regel zu definieren, die sie als vertrauenswürdige Ausnahme kennzeichnet, klicken Sie sie im Explorer mit der rechten Maustaste an und wählen den eben erstellten Befehl aus dem Untermenü „Senden an". Möchten Sie das für mehrere Programme nacheinander tun, müssen Sie trotzdem für jedes einzelne im Restric'tor „Anwenden" klicken und das Tool anschließend beenden – eine Datei an eine laufende Restric'tor-Instanz zu schicken funktioniert leider (noch) nicht.