Schotten dicht!

Mit Restric’tor zum sicheren Windows

In die Windows-Ausgaben, die für den Einsatz in Unternehmen vorgesehen sind, baut Microsoft Funktionen ein, um sie zuverlässig vor Hacker-Angriffen zu schützen. Anwendern mit Windows Home bleibt der Zugang zu diesen Funktionen verwehrt – bislang: Mit dem c’t-Programm Restric’tor können Sie alle Windows-Editionen konfigurieren.

Von Hajo Schulz

Schadprogramme wie Viren oder Trojaner sind darauf angewiesen, Code auf dem Opfer-Rechner auszuführen. Um schädliche Programme auszusperren, scannt beispielsweise Antivirensoftware die Dateien auf der Festplatte und versucht, Code zu entdecken, der dem bereits bekannter Schädlinge ähnelt. Je nach dem Geschick der Entwickler gelingt ihr das mehr oder weniger erfolgreich.

Der perfekte Schutz eines idealen Systems bestünde wohl darin, es schlicht gar keinen Code mehr ausführen zu lassen, dessen Harmlosigkeit nicht zweifelsfrei belegt ist. Tatsächlich enthält Windows einen Mechanismus, mit dem man diesem Ziel sehr nahekommen kann: die „Richtlinien für Softwareeinschränkung“, englisch „Software Restriction Policies“ oder kurz SRP. Damit lassen sich Regeln definieren, die Windows anweisen, nur noch Programme aus einer zuvor festgelegten Liste auszuführen – unbekannter Code hat keine Chance mehr, Schaden anzurichten oder sich gar dauerhaft im System einzunisten.

Gedacht sind diese Richtlinien eigentlich dazu, dass Administratoren in Unternehmen den Katalog der erlaubten Anwendungen definieren und über Gruppenrichtlinien an alle Rechner in der Windows-Domäne verteilen. Werkzeuge zum Bearbeiten der Regeln bringen folgerichtig nur die für den Einsatz in Firmen vorgesehenen Professional-, Enterprise- und Ultimate-Ausgaben von Windows mit. Technisch sind diese Regeln aber nichts anderes als automatisch generierte Registry-Einträge. Wenn sie vorhanden sind, richtet sich auch ein Windows Home nach ihnen. Das nutzt unser Tool Restric’tor aus, das wir im Folgenden vorstellen: Es läuft unter allen Windows-Editionen seit Windows 7 und lässt Sie einigermaßen komfortabel die Registry-Schlüssel und -Werte der SRP bearbeiten.

Gibt es für Home-Anwender außer dem mühsamen und fehlerträchtigen Herumfrickeln direkt in der Registry kaum eine Alternative zu Restric’tor, müssen sich Pro- und Ultimate-Anwender entscheiden: Mit dem in ihrem Windows ent-

haltenen „Editor für lokale Gruppenrichtlinien“ (gpedit.msc) oder der „Lokalen Sicherheitsrichtlinie“ (secpol.msc) lassen sich in puncto SRP praktisch dieselben Einstellungen vornehmen wie mit Restric’tor. Hinter den Kulissen ist die Vorgehensweise aber eine komplett andere: Während Restric’tor direkt die zuständigen Registry-Einträge liest und schreibt, laden die Microsoft-Werkzeuge die Einstellungen zunächst in der lokalen Gruppenrichtlinie ab, von wo Windows sie beim Speichern und bei jedem Systemstart in die Registry übernimmt. Anders gesagt: Restric’tor stellt stets die aktuell gültigen Systemeinstellungen dar, während die Windows-eigenen Editoren eher indirekt arbeiten. Daher sollten Sie es vermeiden, mal dieses und mal jenes Tool zu verwenden – Verwirrung wäre programmiert. Um Richtlinien zum Verteilen in einer Domäne vorzubereiten, eignet sich Restric’tor nicht; hier sind die Windows-eigenen Werkzeuge alternativlos.

Den Restric’tor gibt es unter ct.de/y9wc zum Download. Für ein erstes Ausprobieren können Sie die EXE-Datei einfach in irgendeinen Ordner auf Ihrer Festplatte kopieren – auf eine sichere Installation für die regelmäßige Benutzung gehen wir weiter unten noch ein. Restric’tor erfordert ein installiertes .NET Framework ab Version 4.0; die Windows-Versionen ab Windows 8 haben alles Benötigte von vornherein an Bord, unter Windows 7 rüsten die „Empfohlenen Updates“ .NET 4.5 nach. Das Programm benötigt Administratorrechte.

Kennenlernen

Wenn Sie sich auf Ihrem PC noch nie mit Software Restriction Policies beschäftigt haben, wird auf der Seite „Allgemein“ von Restric’tor einzig die von Windows vorgegebene Option „Administratoren einschließen“ ausgewählt sein; die Liste der Regeln auf der zweiten Seite ist leer. Zu diesem Zustand (der Schutzlosigkeit) können Sie jederzeit zurückkehren, indem Sie im Menü den Befehl „Datei/SRP-Richtlinie komplett löschen“ wählen. Dies ist übrigens die einzige Aktion in Restric’tor, die sich sofort auf Ihr Windows auswirkt. Alle anderen Einstellungen, die Sie in dem Programm vornehmen, werden erst aktiv, nachdem Sie die Schaltfläche „Anwenden“ am unteren Fensterrand anklicken.

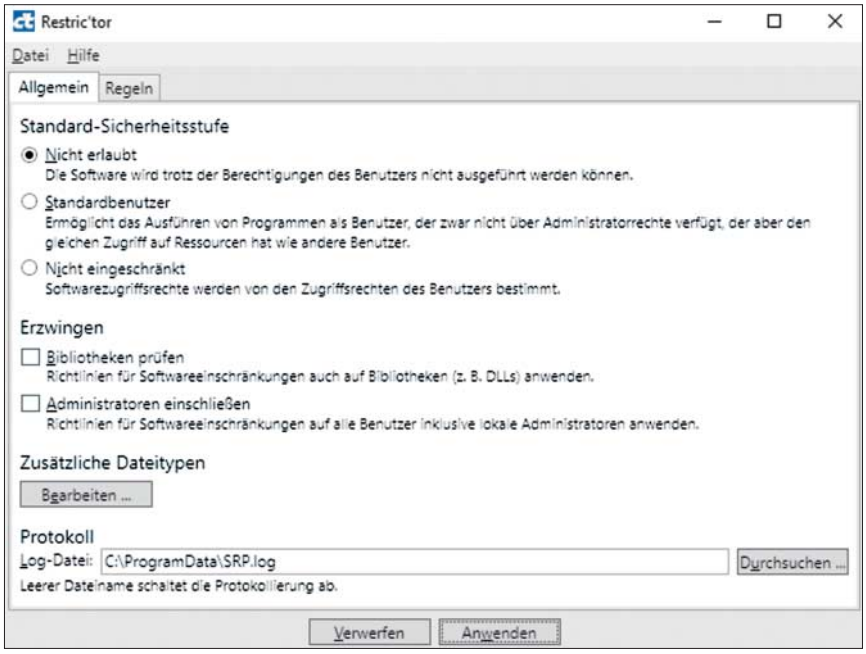
Sollten Sie sich mit den Optionen von Restric’tor mal versehentlich so verhaspelt haben, dass das Programm selbst sich nicht mehr starten lässt, können Sie die SRP direkt in der Registry zurücksetzen: Löschen Sie einfach den kompletten Schlüssel `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\safer`. Extrem experimentierfreudigen Naturen könnte es sogar gelingen, die SRP so zu konfigurieren, dass selbst das Programm regedit nicht mehr startet. Ihnen bleibt dann nur, Windows im abgesicherten Modus zu starten: Dort werden die Richtlinien nicht beachtet und der Registrierungs-Editor lässt sich auf jeden Fall benutzen.

Der Hauptschalter für die SRP besteht in Restric’tor aus den Optionen unter „Standard-Sicherheitsstufe“. „Nicht eingeschränkt“ entspricht dem Auslieferungszustand von Windows: Die passenden Benutzerrechte vorausgesetzt führt das Betriebssystem jedes Programm ungefiltert aus. Eingeschaltet wird die SRP-Prüfung mit „Nicht erlaubt“: Damit ist zunächst einmal die Ausführung sämtlicher Programme verboten – nicht einmal die EXE-Dateien, die zum Betriebssystem gehören, würden starten; Windows wäre ohne weitere Vorkehrungen unbenutzbar. Beim Klick auf „Anwenden“ prüft Restric’tor aber, ob so ein Zustand eintreten würde, und verweigert im Zweifel das Schreiben in die Registry mit einer Fehlermeldung.

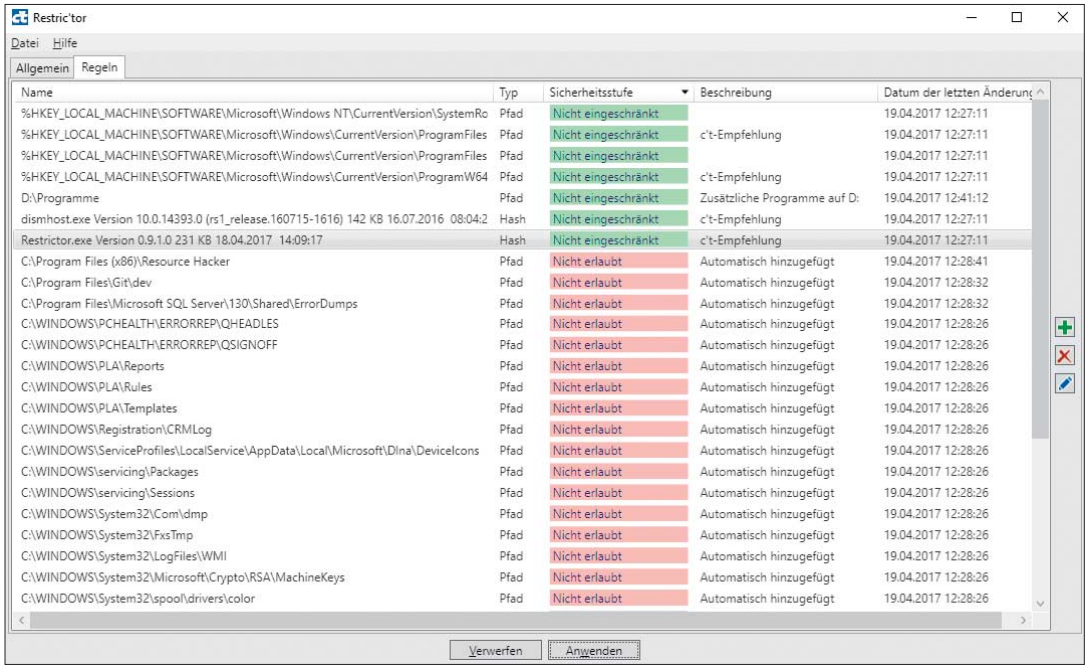
Die Option „Standardbenutzer“ hat eigentlich nur unter Windows Server eine Bedeutung und ist auf dem Desktop nicht zu empfehlen. Restric’tor bietet sie lediglich der Vollständigkeit halber an. Ihr Effekt entspricht im Wesentlichen der Einstellung „Nicht erlaubt“.

Der Schalter „Bibliotheken prüfen“ bringt zwar etwas zusätzliche Sicherheit, drückt aber sehr stark auf die Gesamt-Performance des Systems und ist deshalb nicht zu empfehlen. Er ist in Restric’tor eigentlich nur deshalb vorhanden, damit Sie ihn ausschalten können, falls er durch ein anderes Werkzeug aktiviert wurde.

Dasselbe gilt für die widersinnigerweise von Windows selbst aktivierte Vorgabe „Administratoren einschließen“. Damit sägen Sie unter Umständen den Ast ab, auf dem Sie sitzen: Wenn die anderen SRP-Optionen die Ausführung von Restric’tor nicht explizit erlauben, können Sie ihn (und alle anderen Programme) immer noch per Rechtsklick „Als Adminis-



Die wichtigsten Optionen zum Konfigurieren der Software Restriction Policies versammelt Restric’tor auf der ersten Seite. Die Standard-Sicherheitsstufe entscheidet darüber, ob sie überhaupt beim Laden von Programmen eingreifen.



Die zweite Seite von Restric'tor dient dazu, Regeln zu definieren, nach denen die SRP vertrauenswürdige Programme identifizieren. Ohne solche Regeln wäre der Rechner bei eingeschalteten SRP unbenutzbar.

trator starten". Der Schalter „Administratoren einschließen" verhindert das. Mit etwas Unachtsamkeit blockieren Sie so sogar den Registry-Editor und sind auf den abgesicherten Modus angewiesen, um die SRP anders zu konfigurieren.

Damit die Erlaubnis zum Ausführen von Programmen mit Administratorrechten nicht zu einem Loch wird, durch das sich doch wieder unbekannte und möglicherweise gefährliche Software in Ihr Windows einschleicht, sollten Sie in der Systemsteuerung unter „Sicherheit und Wartung" die „Einstellungen der Benutzerkontensteuerung" aufrufen. Schieben Sie den Regler für die Benachrichtigungen mindestens auf die zweite Stufe von oben, besser ganz hinauf. Sollte in der Folge eine der bekannten Sicherheitsabfragen der Benutzerkontensteuerung („Möchten Sie zulassen, dass durch diese App Änderungen an Ihrem Gerät vorgenommen werden?") aus dem Nichts auftauchen, ist das ein sicheres Zeichen dafür, dass irgendein Programm versucht, sich an den SRP vorbeizumogeln. Im Zweifel ist dann „Nein" die richtige Antwort.

Wie schon gesagt dienen die SRP dazu, das Laden von ausführbarem Code zu verhindern, der dem System schaden könnte. Code wird von Windows aber nur gestartet, wenn er in einer Datei steckt, die das System entweder als direkt ausführbar kennt oder die einem Programm zugeordnet ist, das seinerseits den enthaltenen Code ausführen kann. Die Dateitypen, die aus Sicht der SRP in die zweite Kategorie fallen, bestimmt die Liste, die sich in Restric'tor bei einem Klick auf „Bearbeiten" unter „Zusätzliche Dateitypen" öffnet. Um sie nicht von Hand füllen zu müssen, sollten Sie bei der Ersteinrichtung der SRP einen der Befehle „Microsoft-Standardwerte laden" oder besser „c't-Empfehlung laden" aus dem Datei-Menü in Restric'tor auswählen. Die Liste der überwachten Dateitypen unterscheidet sich bei beiden nur in einem Eintrag: .LNK-Dateien zu überwachen, wie Microsoft vorgibt, halten wir für überflüssig, denn eine Verknüpfung ist ja für sich alleine genommen nicht gefährlich, selbst wenn sie ein böses Programm anlegt. Entscheidend ist, dass das Ziel überwacht wird, auf das sie verweist – und darum kümmern sich die anderen SRP-Regeln.

Mit dem Eingabefeld „Log-Datei" können Sie Windows anweisen, sämtliche Programmstarts zu protokollieren. Jeder Eintrag vermerkt, ob die SRP das Programm zugelassen oder blockiert haben und welche Regel für die Entscheidung verwendet wurde. Das ist vor allem sinnvoll, um sich vor dem Scharfschalten der SRP zunächst einen Eindruck davon zu verschaffen, wo im laufenden Betrieb mit Hindernissen zu rechnen ist – siehe den vorangegangenen Artikel auf Seite 76.

Sind die SRP aktiv, gibt es einen besseren Weg, ihre Arbeit unter Beobachtung zu halten: Jedes Mal wenn sie einen Programmstart verhindern, schreibt Windows einen Eintrag in das System-Log, wo sich die Aktivitäten dann mit der Ereignisanzeige verfolgen oder mit geeigneten Werkzeugen automatisch auswerten lassen – siehe Textkasten auf Seite 86.

Regelkunde

Die eben schon erwähnten Restric'tor-Menübefehle zum Laden einer Grundkonfiguration initialisieren nicht nur die Liste der überwachten Dateitypen, sondern legen auch schon einige Regeln an, die in der Liste auf der gleichnamigen zweiten Seite erscheinen. Deren Notwendigkeit erschließt sich, wenn man sich vergegenwärtigt, wie die SRP funktionieren: Mit der Standard-Sicherheitsstufe „Nicht erlaubt" ist zunächst einmal das Ausführen sämtlicher Programme verboten. Damit Windows funktioniert und Sie vernünftig arbeiten können, muss es Ausnahmen geben – und genau die bestimmen Sie mit den Regeln.

Ziel der SRP ist es, nur noch Code zuzulassen, dem Sie vertrauen. Dieses Prädikat verdient zunächst einmal alles, was zu Windows selbst gehört, also der Inhalt des System-Ordners. Der heißt normalerweise C:\Windows, kann aber in Einzelfällen auch mal woanders liegen. Deshalb verweist die zuständige Regel nicht direkt auf C:\Windows, sondern über den Registry-Eintrag `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SystemRoot`. Ähnliches gilt für die Ordner „Programme" und „Programme (x86)", in die Sie normalerweise Anwendungen installieren.

All diesen Ordnern ist gemeinsam, dass dort nur Prozesse schreiben dürfen, die mit Administrator- oder Systemrechten laufen: im Systemordner etwa Windows Update und in den Programmver-

zeichnissen Setup-Programme, die Sie ausdrücklich mit Administratorrechten gestartet haben. Sofern Sie die Sicherheitsabfragen der Benutzerkontensteuerung ernst nehmen, enthalten diese Ordner also nur Code, dem Sie schon einmal explizit vertraut haben.

Pfad-Regeln mit der Sicherheitsstufe „Nicht eingeschränkt“ sind also dazu da, Ordner zu identifizieren, in denen vertrauenswürdiger Code liegt. Damit diese Eigenschaft erhalten bleibt, sollten Sie auf keinen Fall an den Rechten dieser Ordner herumdoktern und normalen Benutzern Schreibzugriff gewähren. Das wäre dann nämlich genau das Einfallstor, auf das die Programmierer etwa von Erpressungstrojanern warten: Ein unbedacht angeklickter Mail-Anhang oder ein Dokument mit versteckten Makros könnte dort Code abladen und sich so ins System einnisten.

Wenn Sie diesen Grundsatz beachten, können Sie in Restric’tor selbstverständlich auch weitere Pfad-Regeln mit der Sicherheitsstufe „Nicht eingeschränkt“ anlegen: Der „+“-Knopf neben der Regelliste bringt ein Menü zum Vorschein, in dem sich unter anderem der Befehl „Neue Pfad-Regel“ findet.

In Frage kommt zum Beispiel ein Ordner auf einem anderen als dem Systemlaufwerk, in den Sie gelegentlich Programme installieren, etwa um den Platz auf der knapp bemessenen System-SSD zu schonen. Dann sollten Sie in diesem Ordner aber auch normalen Benutzern die Schreibrechte entziehen. Bewährt hat sich, in so einem Ordner dieselben Rechte zu vergeben, die auch im standardmäßigen Programme-Ordner gelten. Am einfachsten erreichen Sie das, indem Sie dessen Rechte kopieren, zum Beispiel mit der Befehlsfolge

```
$acl = Get-Acl "C:\Program Files"
Set-Acl "D:\Programme" $acl
```

Eingeben müssen Sie diese Kommandos in eine mit Administratorrechten gestartete PowerShell; in der zweiten Zeile ist der Name des Zielordners gegebenenfalls anzupassen.

Ausnahme von der Ausnahme

Leider enthält schon der Systemordner einer frischen Windows-Installation einige Verzeichnisse, in die man mit eingeschränkten Benutzerrechten schreiben kann. Auch im Programme-Ordner sind uns auf einigen Rechnern von Benutzern beschreibbare Verzeichnisse untergekommen – unverantwortlicherweise stammten auch die offenbar von Installationen von Microsoft-Programmen. Die Rechte dieser Ordner einzuschränken, damit sich dort keine Malware breit machen kann, ist al-

lerdings keine gute Idee, denn das könnte die Funktion der betroffenen Programme beeinträchtigen. Vielmehr sollte man die SRP so konfigurieren, dass das Ausführen von Programmen aus diesen Verzeichnissen verboten ist. Dafür sind Ordnerregeln mit der Sicherheitsstufe „Nicht erlaubt“ gedacht. Um solche Ordner zu identifizieren, enthält Restric'tor den Menübefehl „Datei/Ordner prüfen“. Auf dem Dialog, den er auf den Plan ruft, klicken Sie einfach die Schaltfläche „Ordner suchen“ an. Daraufhin prüft Restric'tor die Rechte in den Unterverzeichnissen sämtlicher Ordner, für die eine „Nicht eingeschränkt“-Ordnerregel konfiguriert ist. Alle Ordner, in die Sie ohne Administratorrechte schreiben dürfen, zeigt er in der Liste auf dem Dialog an. Ein Klick auf OK erzeugt für jeden Eintrag, bei dem Sie nicht das Häkchen entfernt haben, eine Ordnerregel der Sicherheitsstufe „Nicht erlaubt“.

Extrawurst

Auf den meisten Windows-Rechnern finden sich auch außerhalb der Windows- und Programme-Ordner Programme, auf die der Anwender nicht verzichten möchte: Auf die Schnelle heruntergeladene Spezialwerkzeuge ohne eigenes Installationsprogramm gehören ebenso in diese Kategorie wie portable Anwendungen, die man etwa auf einem USB-Stick mit sich herumträgt.

Für die erste Sorte empfehlen wir, einen Unterordner – etwa „Tools“ – im Programme-Ordner anzulegen. Um die Utilities dort abzulegen, braucht man dann einen Dateimanager, den man mit

Reagieren auf SRP-Ereignisse

Von Peter Siering

Wenn eine Software Restriction Policy das Ausführen eines Programms verhindert, notiert Windows ein Event im Ereignisprotokoll für Anwendungen. Die Wichtigkeit stuft das Betriebssystem als Warnung ein, womit die Ereignisse selbst aufmerksamen Betrachtern dieser zentralen Protokollinstanz entgehen dürften. Man muss schon explizit danach suchen, um sie im Wust der von Windows dort notierten Dinge zu finden.

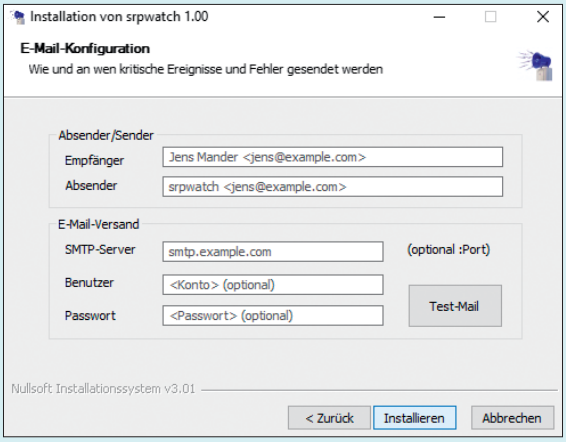
Einfach gelingt die Suche in der Ereignisanzeige über einen Filter, der die Quelle „SoftwareRestrictionPolicies“ auswählt. So erwischt man alle Ereignisarten, auch wenn bei unseren Experimenten nur wenige überhaupt auftreten, die sich darin unterscheiden, welche Art von Richtlinie die Ausführung eines Programms verhindert hat.

Nützlich sind sie durchaus: Einen – meist schnell weggeklickten – Dialog bekommt der Anwender bei einem SRP-Treffer nur zu sehen, wenn er den Programmstart selbst veranlasst hat; Autostarts und geplante Aufgaben scheitern stillschweigend. Im Unterschied dazu werden die Ereignisse im System-Log in jedem Fall erfasst und lassen sich auch später noch nachlesen und vor allem weiterverarbeiten. Letzteres könnte in einer Management-Lösung geschehen, die alle PCs im Netz im Auge behält, oder in kleinerem Rahmen, um Kenntnis eventueller SRP-Treffer auf einem entfernt stationierten PC zu erhalten.

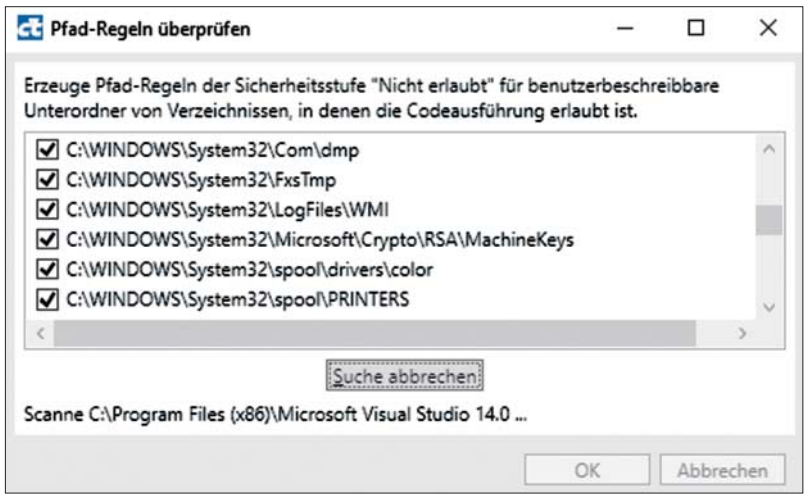
Aus unserer Sicht gut dafür geeignet ist E-Mail, die idealerweise nicht demjenigen zugeht, der den betroffenen PC benutzt, sondern dem, der ihn verwaltet. So lag es nahe, unser in [1, 2] vorgestelltes EventWatch-Projekt für dieses Nutzungsszenario umzubauen: Das dabei herausgekommene SrpWatch funktioniert ähnlich, hat sich aber auf die SRP-eigenen Ereignisse spezialisiert.

SrpWatch lauscht über eine geplante Aufgabe am Ereignisprotokoll. Wenn ein Eintrag mit der oben genannten Quelle ins Anwendungs-Log gerät, läuft das PowerShell-Skript an: Es sendet dann die seit dem letzten Lauf hinzugekommenen Einträge per E-Mail an eine beim Einrichten vorgegebene Adresse. Damit bei akutem Trojanerbefall das Konto nicht geflutet wird, läuft das Skript maximal alle fünf Minuten. In der Zwischenzeit aufgelaufene Ereignisse landen dann gebündelt in einer Nachricht.

Die Installation von SrpWatch müssen Sie nicht wie anfangs die von EventWatch zu Fuß erledigen. Das über den Download-Link (ct.de/y9wc) erhältliche Installationspaket erledigt alles: Es packt die Dateien in die für Programme vorgesehenen Verzeichnisse, fragt die E-Mail-Konfiguration ab, testet sie auf Wunsch und richtet die geplanten Aufgaben ein. Bei der Deinstallation verschwindet all das wieder aus dem System.



Unser Tool SrpWatch lauscht am Ereignisprotokoll für die SRP und benachrichtigt Sie per E-Mail, wenn eine Regel ein Programm blockiert hat. Die Einrichtung erledigt eine eigene Installationsroutine.



Unverständlicherweise lässt Microsoft zu, dass normale Benutzer in einigen Unterverzeichnissen des Systemordners Schreibzugriff haben. Restric'tor hilft dabei, sie zu finden und zu sperren.

Administratorrechten starten kann. Der Favorit des Autors dieser Zeilen heißt Double Commander, als Notnagel kann auch der „Datei öffnen"-Dialog eines mit Administratorrechten gestarteten Notepad herhalten. Ein solcher Tools-Ordner ist übrigens auch der empfohlene Speicherort für den Restric'tor.

Dieses Vorgehen funktioniert allerdings für die meisten portablen Anwendungen nicht: Sie benötigen in ihrem eigenen Ordner Schreibrechte, auch wenn sie unter einem eingeschränkten Benutzerkonto laufen. Den Ordner zu verrammeln scheidet also ebenso aus, wie in ihm enthaltenen Code per SRP-Pfad-Regel zu erlauben. Letzteres ist für Verzeichnisse auf USB-Sticks ohnehin keine gute Idee: Die meisten Sticks sind mit dem Dateisystem FAT32 formatiert. Das kennt aber keine Rechteverwaltung, sodass Benutzerprozesse generell überall schreiben dürfen – ein ideales Einfallstor für Schädlinge.

Für solche Fälle kennen die SRP Hash-Regeln: Mit ihnen identifiziert man jeweils eine einzelne ausführbare Datei als vertrauenswürdig. Entscheidend sind dabei nicht Merkmale wie Dateipfad, -größe oder Änderungsdatum, sondern eben ein Hash, also ein digitaler Fingerabdruck der Datei. Das hat den Vorteil, dass eine Malware keine Chance hat, sich beispielsweise in ein erlaubtes Programm hineinzukopieren: Sie würde den Hash dabei unweigerlich verändern. Weil den Hash-Regeln der Speicherort der Datei egal ist, funktionieren sie außerdem auch, wenn der Stick mit den portablen Programmen mal einen anderen Laufwerksbuchstaben zugewiesen bekommt.

Der Vorteil, Dateien unverwechselbar zu identifizieren, wird allerdings zum Nachteil, wenn die betroffene Anwendung häufig Updates erhält: Dann muss man jedes Mal den Hash neu berechnen, um das Programm wieder zuzulassen. Problematisch sind auch Programme, die sich in einen von Benutzern beschreibbaren Ordner installieren, um sich stillschweigend und ohne Sicherheitsabfrage aktualisieren zu können: Wenn die SRP plötzlich melden, dass sie so ein Programm blockiert haben, muss man als verantwortungsvoller Anwender eigentlich jedes Mal prüfen, ob sich der Hash durch ein legitimes Update geändert hat oder womöglich doch ein Trojaner eingedrungen ist. Wie das mit wenig Aufwand gelingt, erklärt der nachfolgende Artikel.

In Restric'tor legt man eine neue Hash-Regel über den „+"-Knopf neben der Regelliste und Auswahl von „Neue Hash-Regel" an. Über die „Durchsuchen"-Schaltfläche navigiert man zu der gewünschten Programmdatei. Die Dateiinformationen, die Restric'tor daraufhin in das zuständige Feld einträgt, dienen nur dazu, die Regel später in der Liste wiederzufinden. Den Hash berechnet das Programm im Hintergrund – es handelt sich um eine mehr oder weniger zufällige, nichtssagende Zeichenfolge. Um eine Hash-Regel etwa nach einem Update des betroffenen Programms zu aktualisieren, rufen Sie sie per Doppelklick oder über den Stift-Knopf neben der Regelliste auf und wiederholen die Auswahl der Programmdatei. Löschen lassen sich Pfad- und Hash-Regeln mit dem roten X neben der Regelliste.

Falls Sie sich wundern, warum die Regelliste nach dem Laden der c't-Empfehlungen bereits zwei Hash-Regeln enthält: Mit der einen kennzeichnet sich der Restric'tor selbst als vertrauenswürdig. Nach einem eventuellen Update von Restric'tor können Sie das mit dem Menübefehl „Datei/Hash-Regel für Restric'tor hinzufügen" wiederholen. Die zweite betrifft eine Windows-eigene Datei namens dismhost.exe, die partout aus dem Nutzer-Ordner starten will. Hintergrund ist eine systemeigene geplante Aufgabe, die gelegentlich prüft, ob noch ausreichend Platz auf der Platte frei ist. Da Windows dismhost.exe aber jedes Mal aus dem Windows-Ordner dorthin kopiert und nach dem Ende der Aufgabe wieder löscht, erfasst die Pfad-Regel für den Systemordner diese Aktion nicht.

Sonst noch

Wie eingangs erwähnt, eignet sich Restric'tor nicht, um Software Restriction Policies in einem Firmennetz auszurollen. Im privaten Rechnerzoo mag aber durchaus der Wunsch aufkommen, einen mühsam erstellten Regelsatz von einer Maschine auf eine andere zu übertragen. Dazu dienen die Befehle „Konfiguration exportieren" und „Konfiguration importieren" aus dem Datei-Menü. Sie leisten auch gute Dienste, um die SRP-Konfiguration vor einer geplanten Neuinstallation des Betriebssystems in Sicherheit zu bringen.

Unter ct.de/y9wc finden Sie außer dem Download des Programms ein Diskussionsforum, in dem Sie sich mit anderen Benutzern über Erfahrungen mit dem Tool austauschen können. Außerdem halten wir Sie auf der Projektseite über mögliche Updates von Restric'tor und SrpWatch auf dem Laufenden.

(hos@ct.de) c't

Literatur

[1] Peter Siering, Selbstüberwachung, Ereignisprotokolle im Blick, c't 10/12, S. 148
[2] Peter Siering, Pakete schnüren, Installer für Windows-Programme oder -Skripte, c't 16/14, S. 164

Projektseiten zu Restric'tor und SrpWatch: ***ct.de/y9wc***