UAC Virtualisierung

Grundlagen

Bestimmte Programmpfade in Windows 10 (eigentlich schon seit Windows VISTA) können mit Benutzerrechten nicht beschrieben werden. Die Einschränkung, diese Dateien und Pfade nur mit Administratorrechten beschreiben zu können, ist Teil des Sicherheitskonzeptes von Windows und wird User Account Control (UAC) genannt.

Dies betrifft insbesondere

- C:\Windows
- C:\Programme
- C:\Programme (x86)

und andere systemrelevante Pfade.

Ferner können einige Dateitypen grundsätzlich nicht ohne Administratorrechte überschrieben werden, insbesondere

- EXE
- VBA
- BAT

und andere Dateien, die schlimmstenfalls Schadcode beinhalten können. Für weitergehende Informationen sei auf das Dokument von Mark Russinovich verwiesen.

Das Problem

Dadurch entsteht das Problem, dass die gängige Praxis, Nutzerdaten wie z. B. grundlegende Einstellungen im Programmpfad zu speichern, nicht mehr möglich ist, sobald das Programm ohne Administratorrechte läuft. Es reicht vielfach nicht einmal, wenn man als Administrator angemeldet ist, sondern das Programm muss per Mausklick mit rechter Maustaste und „Ausführen als Administrator“ explizit mit den hohen Rechten gestartet werden.

Für das Programm Metric bedeutet das nun, dass die Grundeinstellungen wie Messsysteme, Kalibration, Belichtungszeit und auch Beschaltung von Messtischen und Motortischen, die alle in der Datei „Metric.opt“ im Programmpfad abgespeichert werden, von niemandem mehr überschrieben werden können, es sei denn das Programm Metric wurde mit Administratorrechten gestartet.

Um bei solchen Problemen Abhilfe zu schaffen, hat Microsoft die Technik „UAC Virtualisierung“ erfunden. Wenn ein Programm keine Schreibrechte in das gewünschte Verzeichnis oder auf die gewünschte Datei hat, dann wird eine Kopie an einem speziellen Ort erstellt und diese Kopie anstelle des Originals (oder der gar nicht im Zielverzeichnis vorhandenen Datei) virtuell eingeblendet.

Beispiel: Sie sind als „YouAsAUser“ mit normalen Benutzerrechten angemeldet und wollen die Datei Metric.opt speichern. Da Sie das nicht unter „C:\Programme (x86)\Metric\Metric.opt“ dürfen, speichert Windows die Datei tatsächlich unter

C:\Users*YouAsAUser*\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt

ab. Hier sieht man zweimal die Virtualisierung: Zum einen wird auf deutschsprachigen Systemen „C:\Program Files (x86)“ als „C:\Programme (x86)“ virtuell übersetzt und zum anderen wird die Datei „Metric.opt“ an einem völlig anderen Ort abgespeichert.

Es nutzt dabei gar nichts, wenn der Administrator Ihnen Schreibrechte an „C:\Programme (x86)\Metric“ eingeräumt hat, Windows erkennt einen systemkritischen Pfad und führt automatisch die Virtualisierung durch, außer Sie starten das Programm Metric mit Administratorrechten. Das geht aus Sicherheitsgründen jedoch nicht.

Wenn Sie jetzt die Datei „C:\Programme (x86)\Metric\Metric.opt“ laden möchten, dann wird tatsächlich die Datei aus dem VirtualStrore gelesen.

Für Sie als einzelner Benutzer ist das sehr praktisch. Zum einen haben Sie die hohe Sicherheit durch die UAC Virtualisierung und zum anderen können Sie wie gewohnt die Daten dort speichern, wo auch ihr Programm installiert wurde.

Wenn sich jetzt ein anderer Nutzer als „YourCollegue“ anmeldet, dann passieren zwei Dinge:

1. Der Kollege bekommt beim ersten Programmstart die Originalinstallation der Metric.opt zu lesen
2. Beim Speichern erzeugt der Kollege in seinem eigenen VirtualStore eine Kopie der Metric.opt, die auch nur für ihn eingeblendet wird.

Damit haben Sie zum einen den Vorteil, dass der Kollege ihre Einstellungen nicht verändern kann, zum anderen aber den Nachteil, dass z. B. eine Neukalibration für alle Mitarbeiter getrennt durchgeführt werden muss.

Wenn sich in Ihrem individuellen Fall diese UAC Virtualisierung als Problem herausstellen sollte, dann kann man wie folgt Abhilfe schaffen.

Die Lösung UAC File Exclude

Wie oben erwähnt, gibt es Dateitypen, für die die UAC Virtualisierung nicht angewendet wird. Wenn man jetzt die Dateitype „OPT“ zu dieser Liste hinzufügt, dann verhindert man damit die Virtualisierung der Metric.opt.

Der einzelne Anwender kann dann keine Einstellungen mehr verändern. Nur ein Administrator, der das Programm Metric auch explizit mit Administratorrechten startet, kann dann Einstellungen ändern. Wenn das bereits die gewünschte Lösung ist, ist man an dieser Stelle fertig. Das beigefügte „uac opt exclusion.reg“ beinhaltet nachfolgenden Eintrag in die Registry.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\luafv\Paramete  rs]
"ExcludedExtensionsAdd"=hex(7):6f,00,70,00,74,00,00,00,00,00
```

Die hexadezimale Zeichenkette kodiert für einen String „OPT“ im DBCS-Format und einen leeren String. Durch Doppelklick und entsprechendes Bejahen der UAC-Abfragen wird der Eintrag in die Registry vorgenommen. Anschließend muss das System neu gestartet werden.

Die erweiterte Lösung „Schreibrechte“

Sollen zusätzlich die Nutzer Einstellungen am Programm Metric ändern können, müssen sie darüber hinaus Schreibrechte auf „C:\Programme (x86)\Metric“ bekommen. Hier würde „ändern“ reichen, da eine Neuanlage nicht erforderlich ist. Der Administrator kann hier also die minimalen Rechte einstellen und muss nicht explizit „Vollzugriff“ erlauben.