DIETMAR WALKER - PC-BLITZHELFER-NOTDIENST
Nationalgasse 14 • 72124 Pliezhausen • ∅ Tel. 07127 / 89194 - Fax 89118
Internet: http://www.pc-blitzhelfer.de – Mobil 0172-882 79 55

Anleitung Überwachter Ordnerzugriff

Eine der Neuerungen von Windows 10 Version 1809 ist der

Überwachte Ordnerzugriff

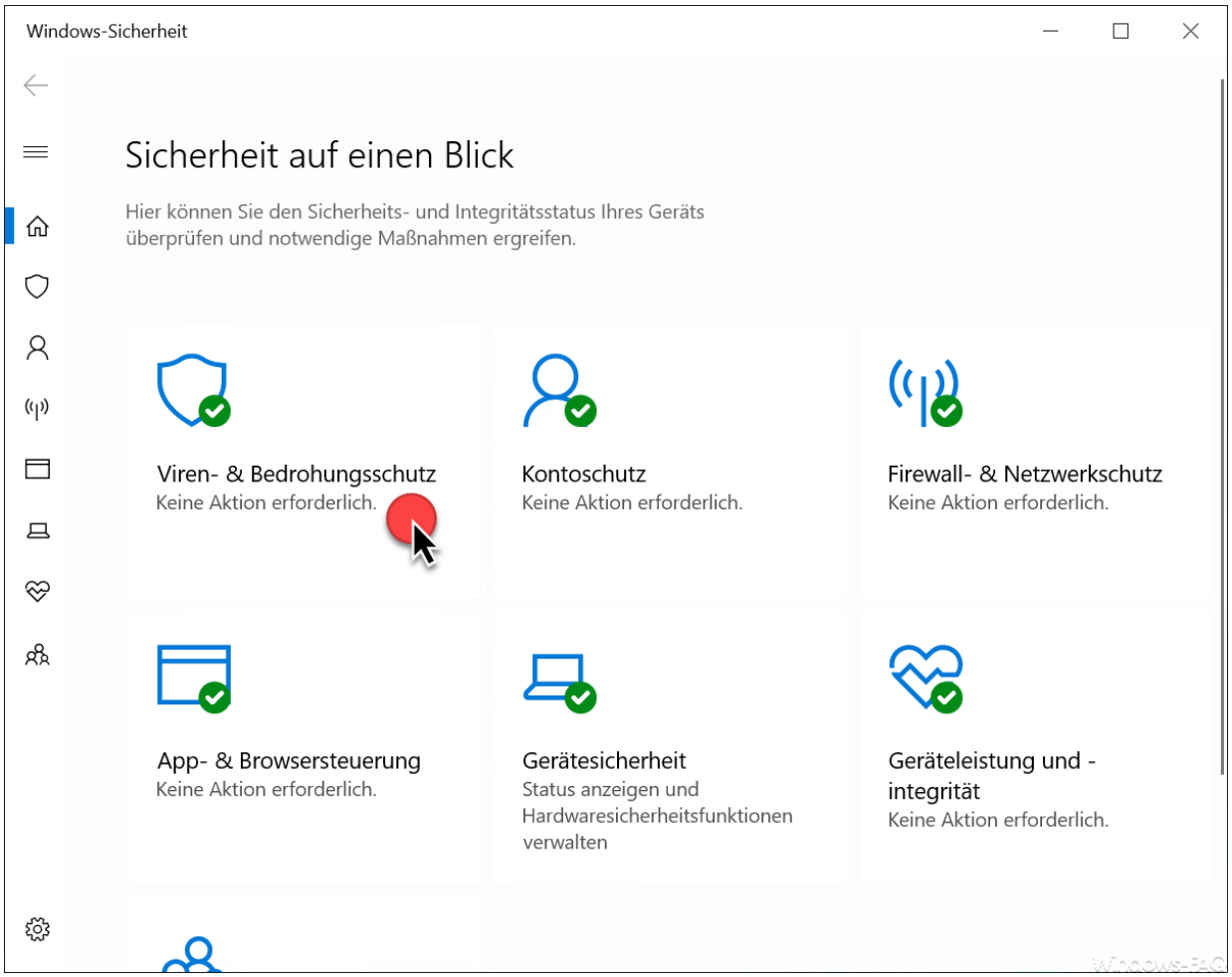
der in den Windows Defender bzw. in die **Windows 10 Sicherheitssoftware „Windows-Sicherheit“** eingeflossen ist. Durch diese Überwachung spezieller Ordner und Apps versucht die Windows 10 Sicherheits-App, evtl. **Verschlüsselungsversuche** von infizierten Windows PCs mit **Ransomware** zu unterbinden. Windows 10 überwacht im Hintergrund permanent die angegebenen Verzeichnisse auf Veränderungen und reagiert entsprechend, wenn Ransomware die **Verschlüsselung von Dateien oder Ordnern** startet.

Überwachten Ordnerzugriff aktivieren und einrichten

Zunächst ruft Ihr das Programm

Windows-Sicherheit

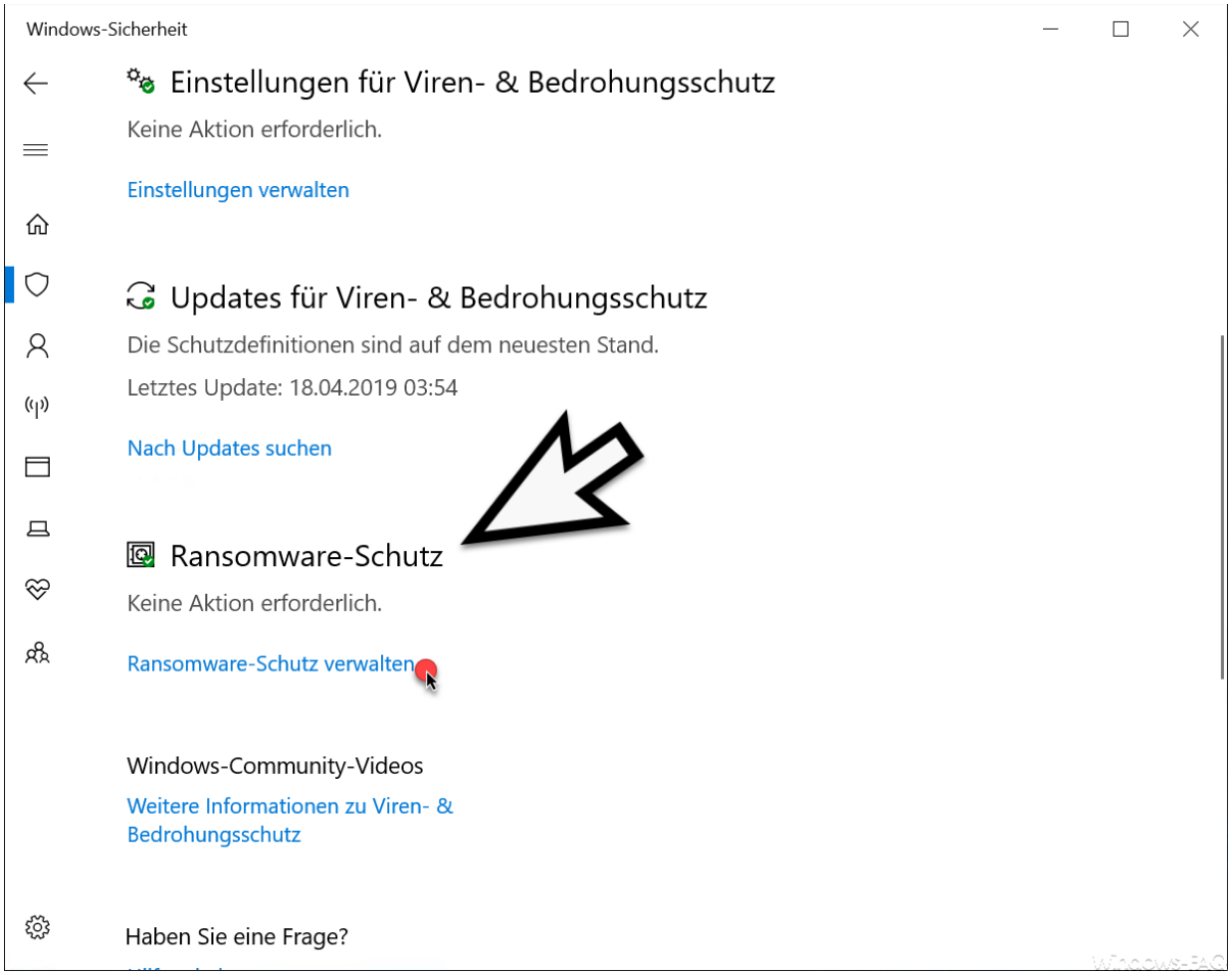
auf, worauf Ihr folgendes Fenster angezeigt bekommt.



Um zu den **Einstellungen des überwachten Ordnerzugriffs** zu kommen, müsst Ihr die folgende Option aufrufen.

Windows-Sicherheit Viren- und Bedrohungsschutz

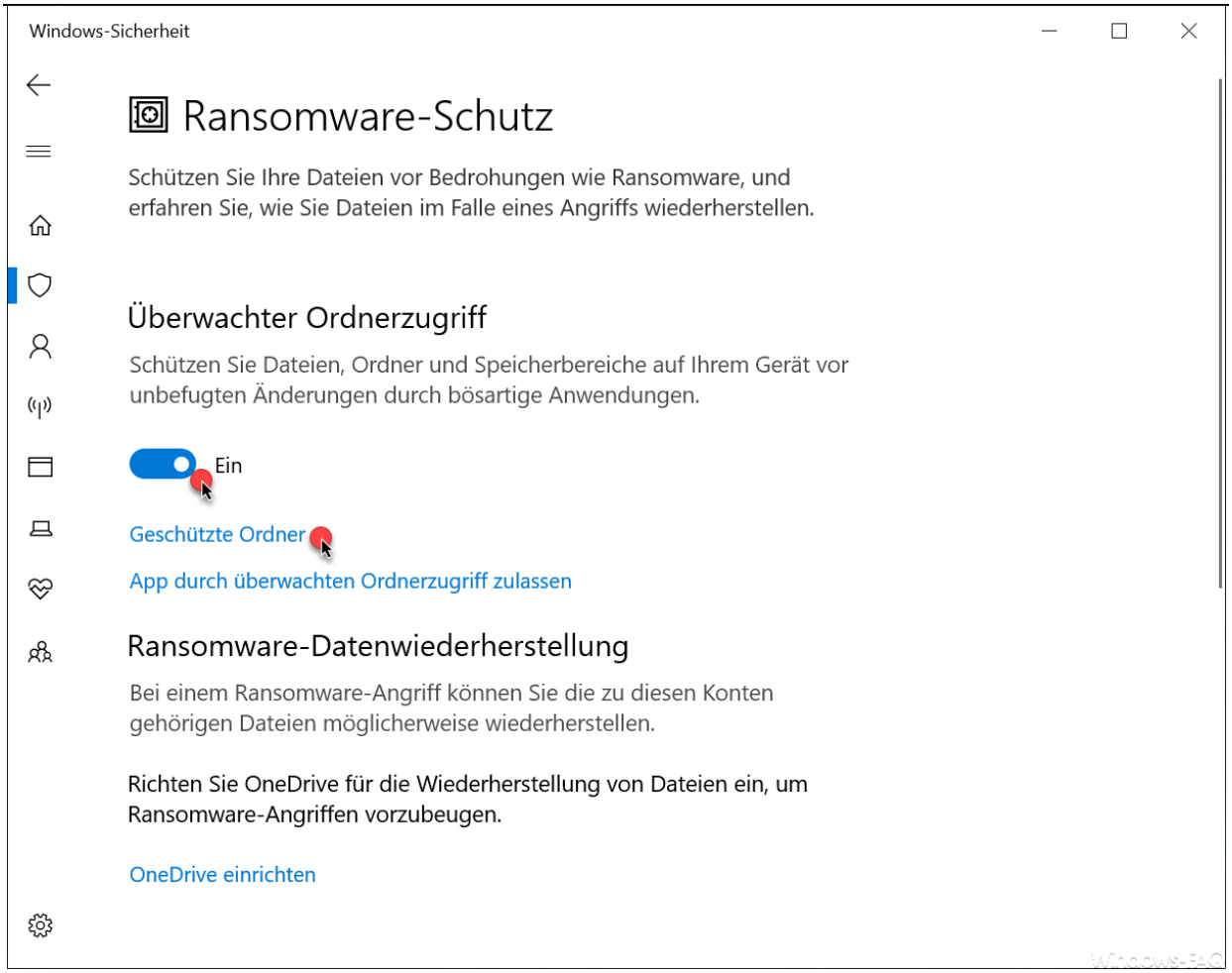
Anschließend verändert sich die Anzeige wie folgt.



Hier findet Ihr den Bereich

Ransomware-Schutz

und Ihr könnt über den Link „**Ransomware-Schutz verwalten**“ alle notwendigen Einstellungen zu der **Ordnerüberwachung** einstellen.



Hier seht Ihr in der Mitte der möglichen Optionen den Punkt

Überwachter Ordnerzugriff

Microsoft erklärt dies wie folgt.

Schützen Sie Dateien, Ordner und Speicherbereiche auf Ihrem Gerät vor unbefugten Änderungen durch bösartige Anwendungen.

Hier ist der Schiebeschaler für den überwachten Ordnerzugriff auf

Ein

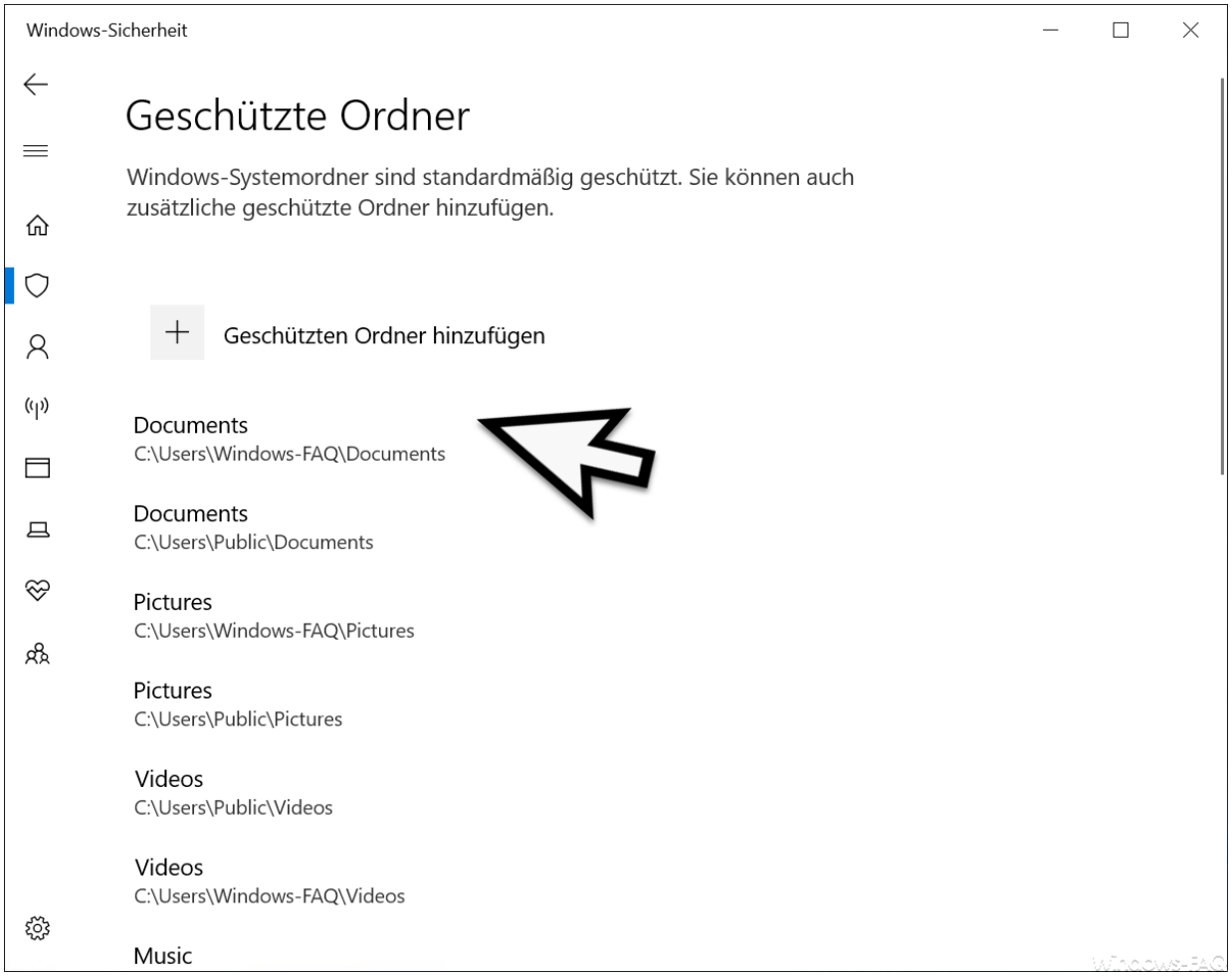
zu stellen. Darunter findet Ihr dann noch die Einstellungen für

Geschützte Ordner

und

Apps durch überwachten Ordnerzugriff zulassen

Im Bereich der „**geschützten Ordner**“ seht Ihr dann, welche Verzeichnisse in die **Ransomware-Überwachung** integriert sind.



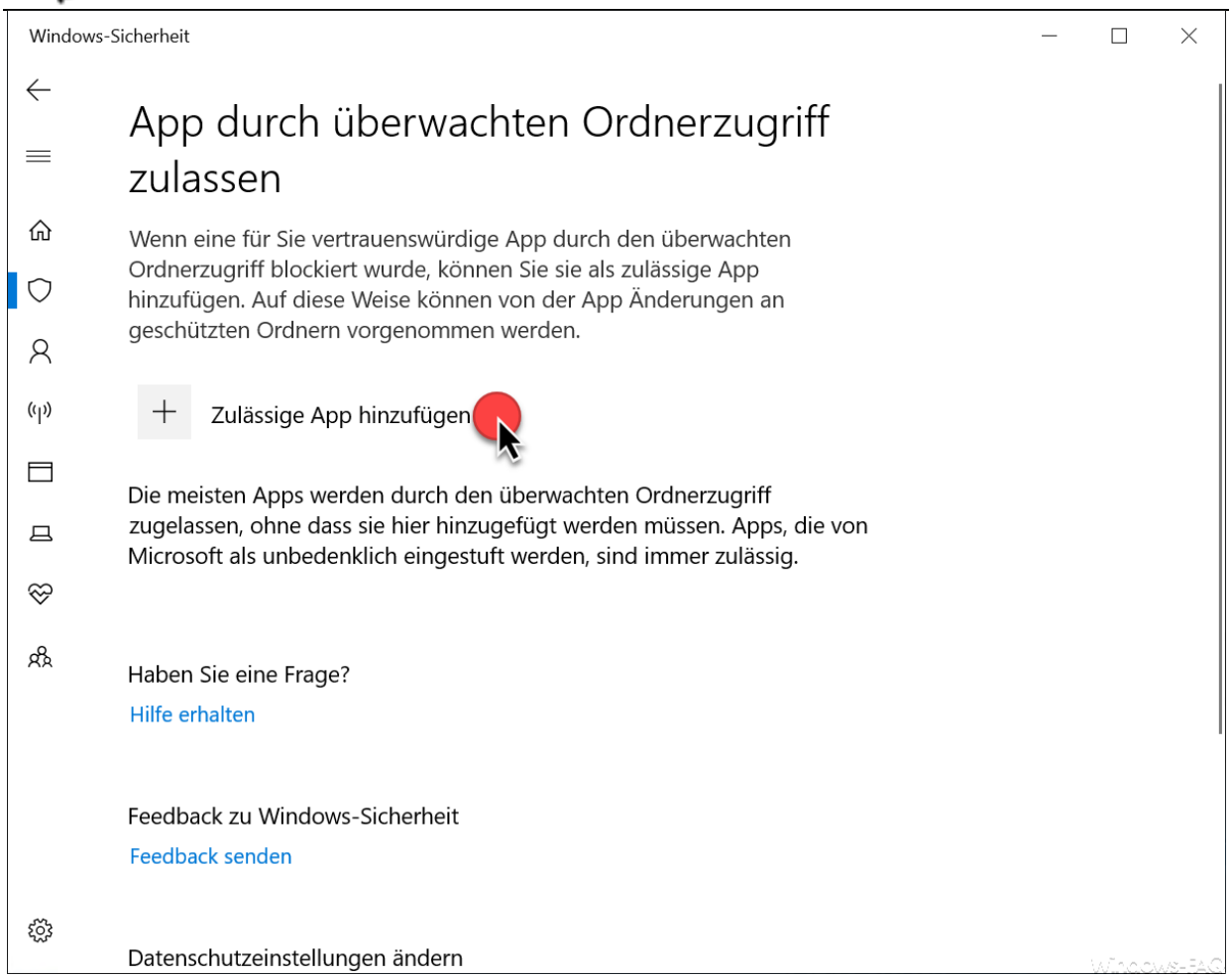
Zu den Standard-Ordnern, die **Windows-Sicherheit gegen Ransomware schützt**, gehen die Windows-Systemordner und viele Bereiche des Userprofilordners, wo der Anwender in der Regel seine lokalen Daten ablegt.

Wenn Ihr weitere **Ordner in die Überwachung aufnehmen** möchtet, so könnt Ihr das über folgende Option durchführen.

Geschützten Ordner hinzufügen

Dazu müsst Ihr einfach den gewünschten Ordner der Liste hinzufügen. Danach wird dieser automatisch durch Windows-Sicherheit überwacht.

Apps für überwachten Ordnerzugriff zulassen



Im Bereich

App durch überwachten Ordnerzugriff zulassen

könnt Ihr eine oder mehrere vertrauenswürdige Apps freigeben, die durch den **überwachten Ordnerzugriff blockiert** wurden. Die freizugebenen Apps könnt Ihr über den folgenden Link freigeben.

Zulässige App hinzufügen

Alle Apps, die ihr hier freischaltet, können Änderungen an den geschützten Ordner vornehmen. Apps, die von Microsoft als unbedenklich eingestuft werden, sind hingegen immer zulässig und brauchen nicht explizit freigeschaltet werden.

Wenn Ihr diese Funktion der **überwachten Ordnerzugriffe** nutzt, so verfügt Euer PC über einen **erweiterten Ransomware-Schutz**. Ein 100%iger Schutz ist es nicht und wird es auch nicht geben, aber es ist auf jeden Fall ein gutes Hilfsmittel, um die Windows Sicherheit zu erhöhen. Trotzdem erspart diese Funktion auf keinen Fall die **regelmäßige Datensicherung**, die auf jeden Fall durchgeführt werden sollte.

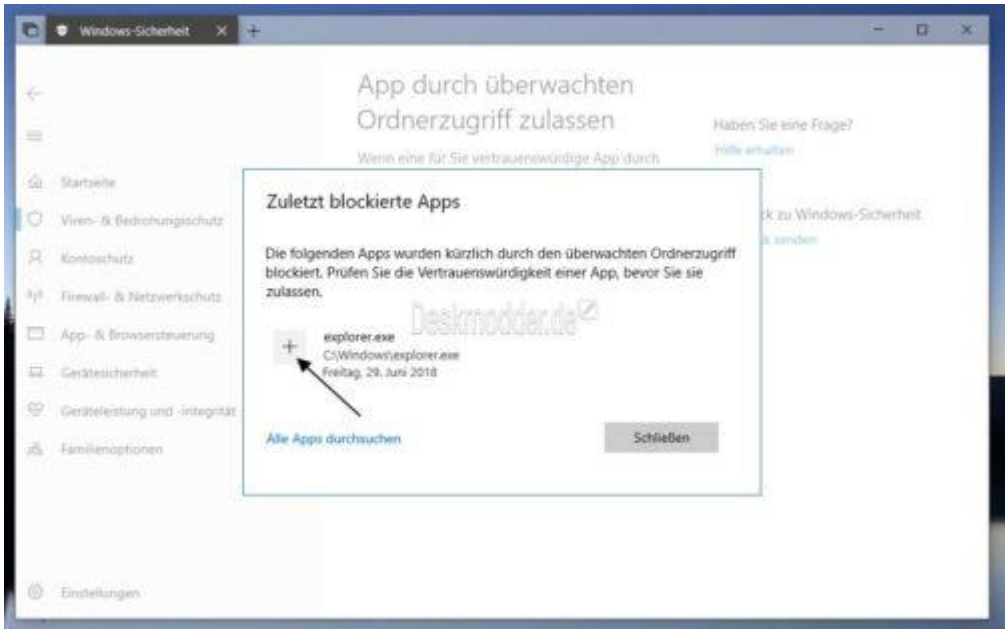
Quelle: https://www.windows-faq.de/2019/06/05/ueberwachter-ordnerzugriff-bei-windows-10-schutz-gegen-ransomware-aktivieren/

Weiter auf der nächsten Seite

[Update 29.06.2018] Ich hole de Beitrag einfach mal hoch: Nach langer Zeit und sicherlich vielen Einträgen im Feedback-Hub wird Microsoft den überwachten Ordnerzugriff in der Windows 10 1809 um einiges verbessern. Hatte man bisher das Problem, dass der Pfad nicht erkenntlich ist, so hat man nun die Einstellungen dazu hinzugefügt, bei der die „zuletzt blockierte App“ angezeigt und durch ein Klick auf das Pluszeichen nun komfortabel hinzugefügt werden kann.

Aber das ist noch nicht alles, was geändert wurde. Das Tutorial dazu haben wir im Wiki mit Bildern für euch parat. Ob man den Schutz vor Ransomware nun aktiviert, oder den Ordnerzugriff ausgeschaltet lässt, bleibt jedem natürlich selbst überlassen. Ich denke durch die neuen Änderungen, die im September / Oktober kommen werden, wird es auf jeden Fall einfacher alles zu konfigurieren.

Überwachter Ordnerzugriff Die neuen Einstellungen Windows 10



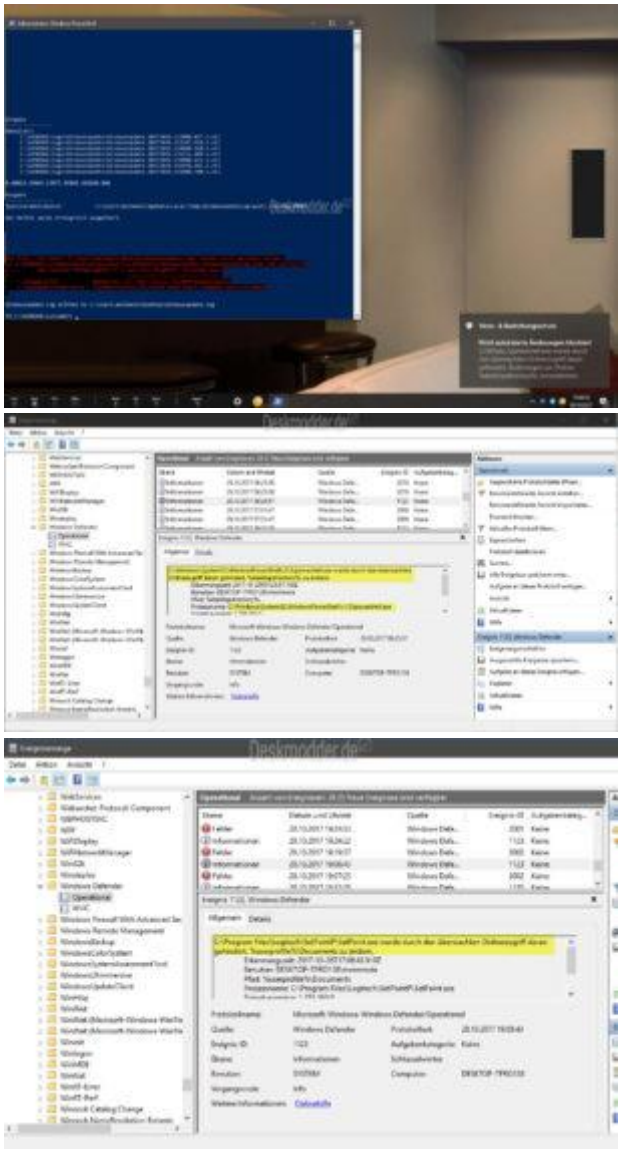
1. Okt 2017: Mit der neuen Windows 10 1709 (Fall Creators Update) hat Microsoft eine neue Sicherheit in den Defender integriert. Der „überwachte Ordnerzugriff“ schützt vor böswilligen Programmen, die in vorab festgelegten Ordnern Änderungen in Dateien vornehmen wollen. Eine gute Sache für den Schutz, aber aktuell noch zu kompliziert für den normalen Nutzer gestaltet.

Wer Probleme beim Speichern von Dateien, der sollte entweder das Programm in die Ausschlüsse hinzufügen, oder den Überwachten Ordnerzugriff komplett deaktivieren. **Windows Defender Security Center öffnen -> Viren- & Bedrohungsschutz -> Einstellungen für Viren- und Bedrohungsschutz -> Überwachter Ordnerzugriff** auf Aus stellen. Danach wird das Speichern kein Problem mehr darstellen.

Gibt man zum Beispiel in PowerShell als Administrator gestartet den Befehl **Get-WindowsUpdateLog** erhält man auf dem Desktop eine Log-Datei über die Windows Updates. Aber da der Ordnerschutz aktiviert ist, wird die Meldung eingeblendet „Nicht autorisierte Änderung blockiert“. „Die .exe wurde

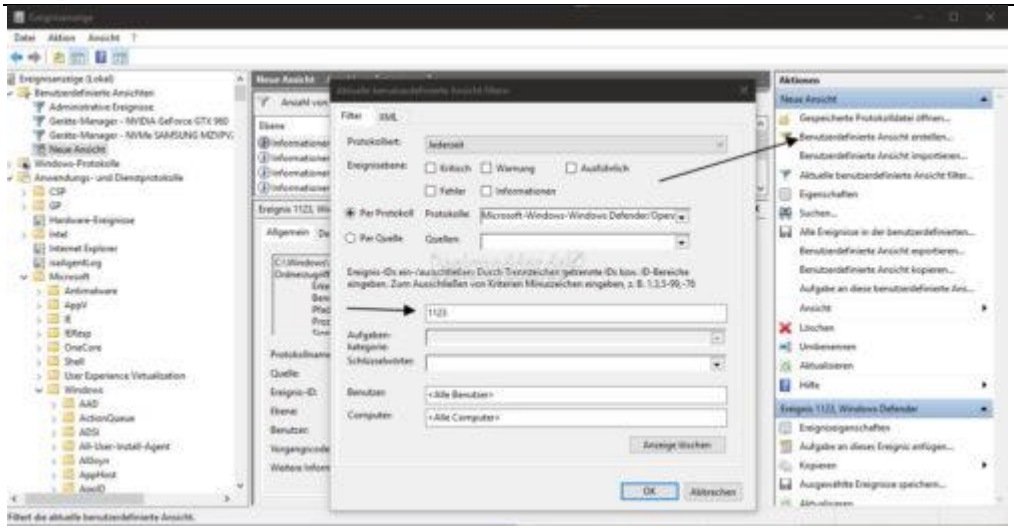
durch den überwachten Ordnerzugriff daran gehindert, Änderungen am Ordner %desktopdirectory% vorzunehmen.“

Das Problem dabei ist der Pfad zu lang, lässt sich schwer nachvollziehen, welches Programm, bzw. welche *.exe daran gehindert wurde. Somit hat man keine Chance, diese unter „Zulässige App hinzufügen“ einzutragen. Man ist also frustriert und schaltet den doch eigentlich nützlichen Schutz auf Aus.

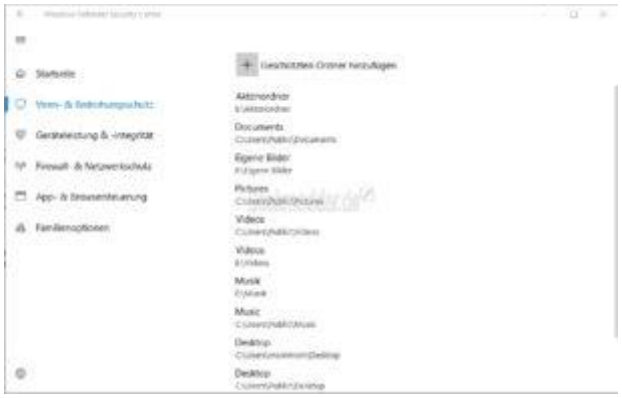


Also hab ich mich einmal auf die Suche gemacht und die Meldung in der Ereignisanzeige aufgespürt. Man gibt Ereignisanzeige in die Suche der Taskleiste ein, oder gibt unter Windows-Taste + R eventvwr.msc ein. Dann geht es los. **Ereignisanzeige -> Benutzerdefinierte Ansichten -> Anwendungs- und Dienstprotokolle -> Microsoft -> Windows -> Windows Defender -> Operational**. Hier findet man nun alle Einträge, die auch die Ordnerzugriffe betreffen.

Als Tipp hinterher: Wenn man sich nicht immer den Pfad entlang hangeln will, kann man sich eine benutzerdefinierte Ansicht erstellen. Rechts auf „Benutzerdefinierte Ansicht erstellen“ klicken Die ID 1123 eingeben und abspeichern. Diese erscheint dann in der Ansicht ganz oben.

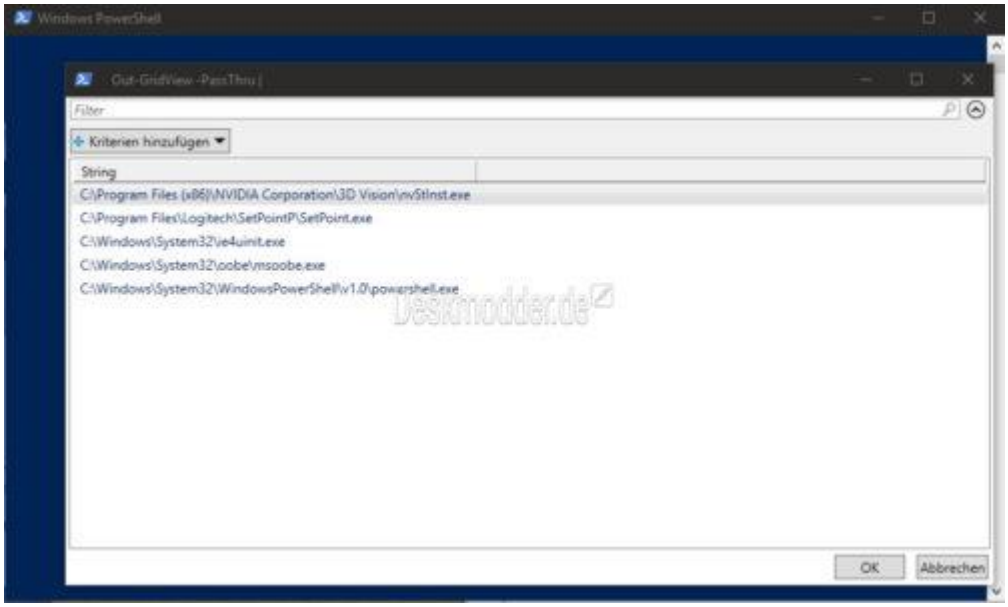


Jetzt kann man den kompletten Pfad auslesen und kann diesen dann als „Zulässige App hinzufügen“ suchen und eintragen. Man kann nur hoffen, dass Microsoft hier noch nacharbeitet. Eine Angabe im Popup „Soll die Anwendung hinzugefügt werden Ja / Nein wäre schon angebracht. Denn so ist der Schutz frustrierend. Denn so muss man immer das **Windows Defender Security Center öffnen -> Viren- & Bedrohungsschutz -> Einstellungen für Viren- und Bedrohungsschutz -> Überwachter Ordnerzugriff** um dann dort eine App / Programm hinzuzufügen.



Blockierte Apps und Programme mit einer PowerShell Datei auslesen

Mithilfe eines PowerShell-Skripts (AddApplicationToControlledFolder.ps1) kann man die Programme aus der Ereignisanzeige schnell auslesen. Diese werden über die ID 1123 herausgefiltert und die Pfade angezeigt. So kann man dann schneller zu den Ausnahmen navigieren und die Programme hinzufügen. Die zip-Datei einfach auf gist.github.com herunterladen und entpacken. Die *.ps1 Datei dann per Rechtsklick „Mit PowerShell ausführen“. Das Ergebnis sieht dann so aus.

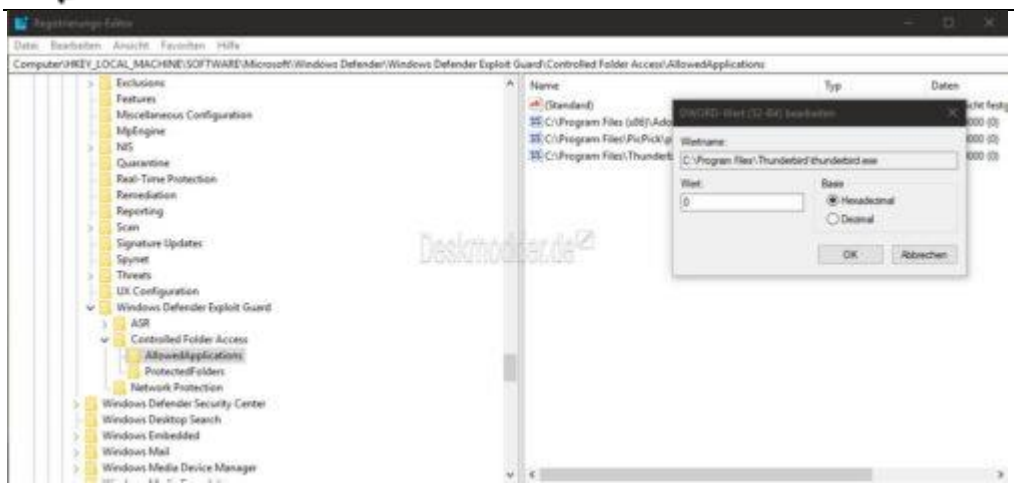


Danke an Sebow für den Hinweis

Apps und Programme durch überwachten Zugriff zulassen in der Registry

Noch als Nachtrag hinterher: Windows schreibt die Apps und Programme, die ihr als Ausnahme (Whitelist) hinzufügt in der Registry unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access\AllowedApplications** Diese sind als DWORD-Wert (32-Bit) eingetragen mit dem Wert 0. Wer jetzt aber denkt, dass man so schnell alle Programme eintragen kann, wird an den Berechtigungen scheitern. Diese müssten erst geändert werden, um Einträge hinzuzufügen. Nur hat sich Microsoft hier schon etwas dabei gedacht. Denn wenn man diese verändert und nicht zurücksetzt hat auch jedes böswillige Programm die Möglichkeit sich dort selbst einzutragen.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



Windows 10 Tutorials und Hilfe

Quelle: https://www.deskmodder.de/blog/2018/06/29/ueberwachter-ordnerzugriff-blockierungen-in-der-ereignisanzeige-anzeigen-id-1123-windows-10/