18 Vor Viren und Trojanern schützen

Mit dem Windows Defender bringt Windows einen Basisschutz gegen Viren und sonstige Malware mit.

Er wird bei der Windows-Installation grundsätzlich installiert und aktiviert. Nur wenn ein alternatives Sicherheitsprogramm vorhanden ist, das alle Funktionen des Defender übernimmt, deaktiviert Windows ihn automatisch. Nach der Installation erfolgen zunächst eine Aktualisierung und eine schnelle Überprüfung des Systems. Später sorgt dann Windows Update dafür, dass die Virensignaturen stets aktuell bleiben. Das alles läuft vollautomatisch ab, sodass Sie sich nicht darum kümmern müssen. Einmal aktiviert, beruht der Schutz des PCs auf zwei Säulen:

- Das System wird regelmäßig mit einem Scan überprüft. Die Zeitplanung dafür lässt sich individuell anpassen.
- Der Echtzeitschutz überwacht laufend Dateiaktionen und ausgeführte Programme und sucht dabei nach Spuren von Viren.

In der Regel werden Sie den Windows Defender nur selten manuell aufrufen müssen. Wollen Sie die Einstellungen ändern oder einen manuellen Scan vornehmen, rufen Sie dafür die *Windows-Sicherheit* per Doppelklick auf das kleine Symbol im Infobereich der Taskleiste auf. Öffnen Sie dort den Bereich *Viren- & Bedrohungsschutz*.

Was taugt der Windows Defender?

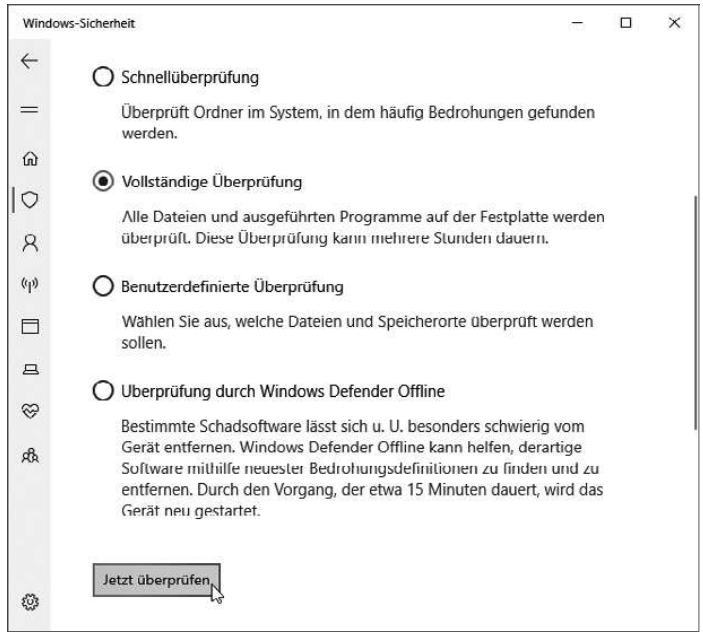
Verschiedene Tests zeigen immer wieder, dass der Defender im Vergleich mit anderen kostenlosen Antivirenprogrammen nicht schlecht abschneidet. Die Erkennungsleistung ist solide und die gute, unauffällige Integration ins Betriebssystem einschließlich Updatemechanismus kann als Pluspunkt gewertet werden. Schwächen offenbart der Defender bei sehr neuen Schädlingen bzw. unbekannten Abarten von Computerviren. Das liegt zum einen an den vergleichsweise langsamen Updates (kommerzielle Programme beziehen teilweise mehrmals täglich Updates, der Defender meist nur einmal pro Tag), zum anderen am Fehlen von effizienten Erkennungsheuristiken. Kommerzielle Produkte bieten darüber hinaus meist weitere Schutzfunktionen, die etwa abgerufene Webseiten überwachen, das versehentliche Weitergeben sensibler Daten auf unsicheren Webseiten verhindern etc. Allerdings machen sich viele dieser Programme auch deutlich stärker bei Speicher und Prozessor bemerkbar. Und Zusatzfunktionen wie den Schutz vor schädlichen Webseiten oder Schutz vor Erpressungstrojanern hat Microsoft inzwischen auch – wenn auch teilweise an anderen Stellen – eingebaut.

HINTERGRUND

18.1 Manuelle Überprüfung nach Bedarf durchführen

Neben den automatischen Überprüfungen können Sie auch jederzeit manuelle Überprüfungen durchführen. So können Sie z. B. ergänzend zu den regelmäßigen schnellen Überprüfungen hin und wieder auch mal eine gründliche vollständige Überprüfung durchführen. Oder Sie begrenzen das Überprüfen auf einen bestimmten Ordner oder ein einzelnes Laufwerk.

1. Für eine manuelle Überprüfung klicken Sie unter der Schaltfläche *Schnellüberprüfung* auf den Link *Scanoptionen*.

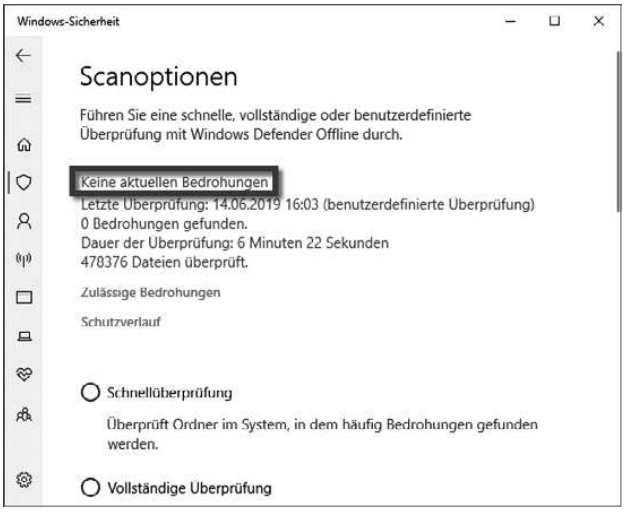


2. Im anschließenden Dialog finden Sie eine Auswahl für die Art der Überprüfung, z. B. *Vollständige Überprüfung*.

3. Wählen Sie die gewünschte Variante aus und klicken Sie dann darunter auf *Jetzt überprüfen*.

4. Der Windows Defender beginnt nun mit der Überprüfung der Dateien. Je nach Umfang kann das vor allem bei einer vollständigen Prüfung etwas dauern. Sie können das Programm aber in der Zeit minimieren und weiterarbeiten.

5. Nach Abschluss der Überprüfung zeigt der Defender eine kurze Statistik an. Dieser können Sie entnehmen, wie viele Dateien geprüft wurden und ob dabei Bedrohungen gefunden wurden. Solange hier nur *Keine aktuellen Bedrohungen* steht, ist alles in Ordnung.



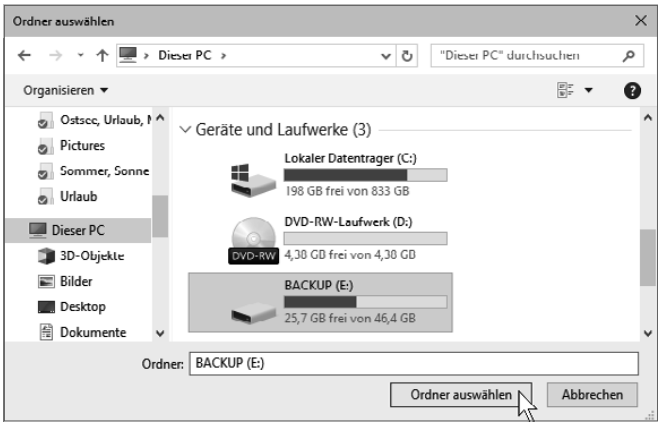
Die Überprüfung auf bestimmte Laufwerke oder Ordner beschränken

Sie können auch gezielt einzelne Ordner oder Laufwerke überprüfen. So lässt sich z. B. eine DVD oder ein USB-Stick ungewisser Herkunft schnell kontrollieren, bevor Sie auf die Daten zugreifen.

1. Wählen Sie dazu die Option *Benutzerdefinierte Überprüfung*.

2. Nach dem Klick auf *Jetzt überprüfen* können Sie in einem zusätzlichen Dialog die zu überprüfenden Bereiche auswählen.

3. Markieren Sie dazu den Ordner bzw. das Laufwerk, das geprüft werden soll. Die Prüfung bezieht sich dabei stets auf den vollständigen Inhalt, also auch auf Dateien in Unterverzeichnissen etc.



4. Klicken Sie dann auf *Ordner auswählen*, um die Überprüfung dieser Bereiche zu starten.

Ausgewählte Dateien oder Ordner direkt überprüfen

Geht es darum, einzelne Dateien oder Ordner zu scannen, die man gerade heruntergeladen oder beispielsweise von einem USB-Stick kopiert hat, kann man eine Überprüfung auch direkt aus dem Windows-Explorer anstoßen. Dazu markieren Sie einfach das oder die Element(e) und klicken die Auswahl mit der rechten Maustaste an. Im Kontextmenü finden Sie die Option *Mit Windows Defender überprüfen*. Sie führt einen Scan der ausgewählten Elemente durch und zeigt das Ergebnis im Defender-Fenster an.

18.2 Virensignaturen überwachen und aktualisieren

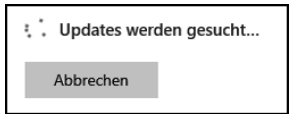
Ein Sicherheitsprogramm steht und fällt mit der Aktualität seiner Signaturdateien. Nur wenn diese ständig aktualisiert werden, ist der Anwender vor neuen Bedrohungen geschützt. Die Signaturen des Windows Defender sind in den Windows-Update-Prozess mit einbezogen und werden darüber regelmäßig aktualisiert. Allerdings ist Windows Update recht zurückhaltend und wartet gern auf Leerlaufzeiten des PCs, um den Benutzer nicht bei seinen Aktivitäten zu behindern. Dadurch können neue Updates schon mal auf sich warten lassen. Deshalb sollten Sie die Situation im Auge behalten und sicherstellen, dass Ihr PC regelmäßig aktuelle Virensignaturen erhält. Wenn Ihr PC beinahe täglich läuft und dabei auch mal zehn Minuten und mehr Leerlauf eintritt, sollten die automatischen Updates häufig genug durchgeführt werden. Ansonsten helfen Sie regelmäßig manuell nach.

1. Im Windows Defender Security Center finden Sie direkt auf der Seite *Viren- & Bedrohungsschutz* ganz unten die Information, wie aktuell die derzeit verwendeten Signaturen sind.

2. Wollen Sie es noch genauer wissen oder besteht Handlungsbedarf, klicken Sie auf *Nach Updates suchen*.

3. Im anschließenden Dialog finden Sie noch mal genauere Angaben zur letzten Aktualisierung und dem jetzigen Stand der Signaturen.

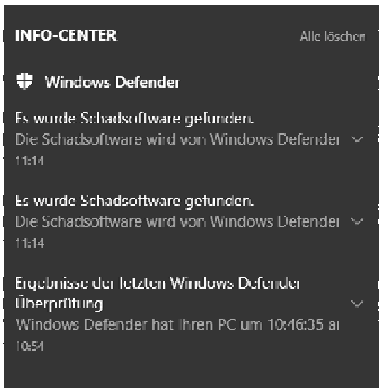
4. Mit einem weiteren Klick auf die Schaltfläche *Nach Updates suchen* können Sie jederzeit manuell den Download der neuesten Signaturen veranlassen. Dieser dauert einige Zeit, Sie können das Programm so lange aber auch minimieren oder schließen und anderweitig weiterarbeiten.



Anschließend ist der Windows Defender erst mal wieder auf dem neuesten Stand und kann Sie zuverlässig schützen.

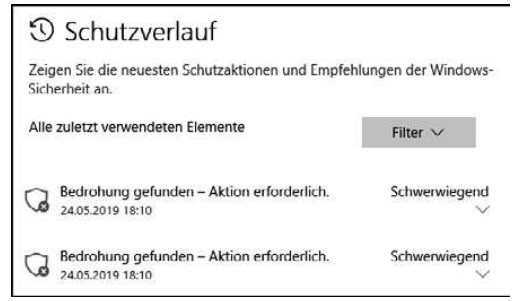
18.3 Im Falle eines Falles: So gehen Sie mit gefundener Malware um

Der Windows Defender läuft permanent im Hintergrund und kontrolliert alle Dateioperationen (sofern Sie nicht den Echtzeitschutz deaktiviert haben). Wird er fündig, erfahren Sie das durch einen Hinweis des Info-Centers. Sollten Sie diesen verpassen, wird aber auch eine Benachrichtigung in der rechten Seitenleiste platziert. Mit einem Klick darauf öffnet die App *Windows-Sicherheit* direkt den Schutzverlauf. Alternativ können Sie jederzeit selbst nachschauen:

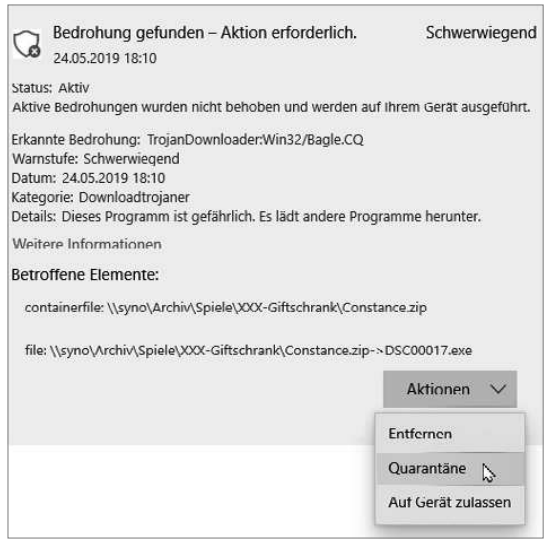


1. Öffnen Sie *Windows-Sicherheit* in der Rubrik *Viren- & Bedrohungsschutz* und klicken Sie dort auf *Schutzverlauf*.

2. Hier können Sie ein vollständiges Protokoll der gefundenen Bedrohungen abfrufen.



3. Jeden der Einträge können Sie durch Anklicken „ausklappen“ und so alle Informationen kompakt erhalten.



4. Unten finden Sie das Auswahlmenü *Aktionen*, mit dem Sie das betroffene Element direkt *Entfernen*, in *Quarantäne* stecken oder zulassen können.

Grundsätzlich verschiebt der Defender alle als schädlich eingestuften Dateien in einen speziellen Quarantäne-Ordner, sodass sie nicht mehr versehentlich geöffnet werden können. Dort verbleiben sie neutralisiert. Diesen Quarantäne-Ordner können Sie jederzeit einsehen und nachschauen, ob und welche Dateien sich darin angesammelt haben. Klicken Sie dazu im *Schutzverlauf* oben rechts neben *Alle zuletzt verwendeten Elemente* auf die Schaltfläche *Filter* und wählen Sie im so geöffneten Menü *Elemente unter Quarantäne*.

18.4 Dateien vor Erpressungstrojanern schützen

Als Erpressungstrojaner bezeichnet man Malware, die sich auf einem PC einnistet und die persönlichen Dateien des Anwenders wie Dokumente, Bilder, Musik und

Videos verschlüsselt. Diese Daten sind dann nicht mehr zugänglich. Um wieder Zugriff darauf zu erlangen, muss der Besitzer einen Entschlüsselungscode erwerben, den man meist per Bitcoin oder anderen nicht verfolgbaren Methoden bezahlen muss. Aber selbst dann ist nicht sichergestellt, dass die Erpresser auch wirklich einen (passenden) Schlüssel liefern.

Um seine Nutzer besser vor dieser Masche zu schützen, bietet Windows 10 die Funktion *Überwachter Ordnerzugriff*. Die Idee dahinter: Bestimmte Ordner wie beispielsweise die mit persönlichen Dokumenten und Bildern werden von Windows zusätzlich geschützt, indem der Zugriff darauf nur Anwendungen erlaubt wird, die entweder von Microsoft selbst stammen oder die der Benutzer ausdrücklich dafür freigegeben hat. Versuchen andere Anwendungen den Zugriff, unterbindet Windows dies. Erpressungstrojaner haben somit keine Chance mehr, solange man als Anwender wachsam ist und wirklich nur vertrauenswürdigen Anwendungen den Zugriff erlaubt.

Überwachten Ordnerzugriff aktivieren

Diese zusätzliche Ordnerüberwachung ist standardmäßig ausgeschaltet. Das liegt daran, dass sie zwar schützt, aber eben auch eine Einschränkung bedeutet bzw. zusätzlichen Konfigurationsaufwand erfordert, um trotzdem reibungslos arbeiten zu können. Was das genau heißt, können Sie aber auf den folgenden Seiten nachlesen. Um die Ordnerüberwachung zu aktivieren, gehen Sie so vor:

1. Öffnen Sie in *Windows-Sicherheit* den Bereich *Viren- & Bedrohungsschutz*.
2. Klicken Sie auf der anschließenden Seite unter *Einstellungen für Viren- & Bedrohungsschutz* auf *Einstellungen verwalten*.
3. In den Einstellungen gehen Sie nach unten, bis Sie den Abschnitt *Überwachter Ordnerzugriff* finden, und klicken dort auf *Überwachten Ordnerzugriff verwalten*.

4. Schalten Sie dort die Option auf *Ein*. Bestätigen Sie die Sicherheitsrückfrage der Benutzerkontensteuerung.

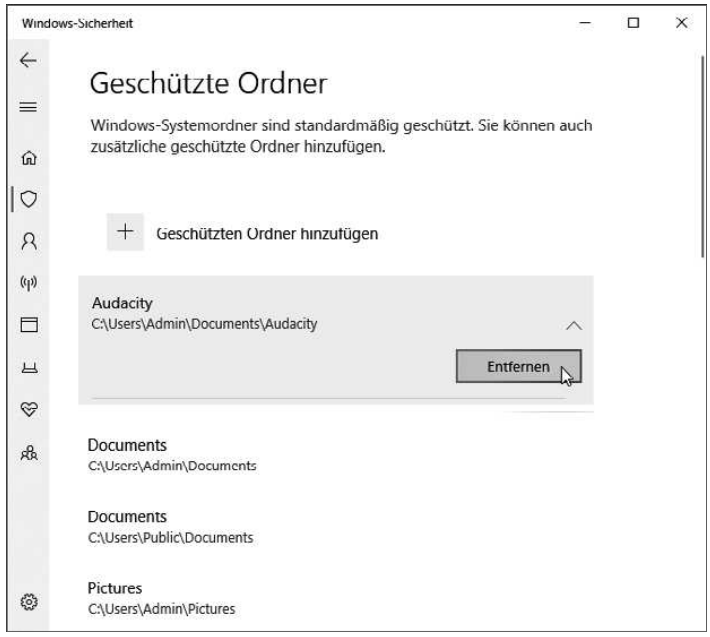
Nach dem Aktivieren der Ordnerüberwachung werden im selben Einstellungsmenü zusätzliche Punkte angezeigt. Wie Sie die Ordnerüberwachung dadurch individuell anpassen und ein komfortables Weiterarbeiten ermöglichen, beschreiben die nachfolgenden Abschnitte.

Ordner zur Überwachung hinzufügen

Der Link *Geschützte Ordner* führt zu einer Liste der von dieser Funktion überwachten Verzeichnisse. Standardmäßig gehören dazu die privaten und öffentlichen Ordner für Dokumente, Bilder, Videos und Musik sowie Desktop und Favoriten. Diese Elemente werden immer kontrolliert (solange diese Funktion aktiv ist) und lassen sich auch nicht entfernen.

Sie können mit dem Plussymbol vor *Geschützten Ordner hinzufügen* aber weitere Ordner in die Überwachung aufnehmen. Wählen Sie dazu einfach im so geöffneten Dialog den gewünschten Ordner aus. Er wird dann mitsamt seiner Unterordner berücksichtigt. Wählen Sie dazu möglichst nur Ordner aus, die Sie selbst für das Ablegen Ihrer Daten erstellt haben. Ordner, die von Windows oder bestimmten Anwendungen für temporäre Dateien oder Einstellungen angelegt wurden, brauchen eigentlich nicht überwacht zu werden, das könnte auch zu unnötigen Komplikationen führen.

Sie können beliebig viele Ordner der Überwachung hinzufügen. Diese Ordner können Sie – im Gegensatz zu den Standardordnern – auch wieder aus der Liste löschen. Klicken Sie dazu auf den entsprechenden Eintrag und dann auf *Entfernen*.



Den Zugriff auf geschützte Ordner steuern

Die andere wichtige Möglichkeit, das Überwachen von Ordnern zu steuern, ist die Auswahl der Anwendungen, denen der Zugriff auf die so geschützten Daten erlaubt wird. Diese Einstellungen finden Sie unter dem Link *App durch überwachten Ordnerzugriff zulassen*. Auch der führt zu einer Liste, die aber zunächst leer ist. Das bedeutet nicht, dass keinerlei Zugriffe möglich wären. Microsoft-eigene Programme wie der Explorer und diverse Systemanwendungen sind als sicher signiert und dürfen unabhängig von dieser Liste immer zugreifen.

Wenn eine andere Anwendung einen potenziell bedrohlichen Zugriff auf einen geschützten Ordner durchführen will, wird das von Windows blockiert. Sie bemerken das an einem Hinweis durch das Info-Center.

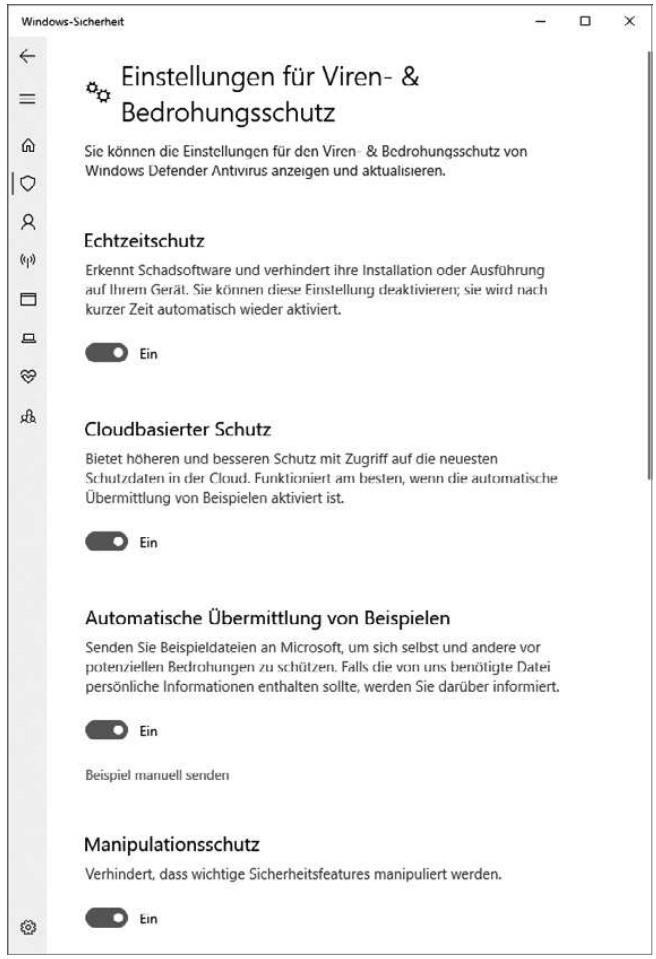
Ist der Zugriff in Ihrem Sinn, weil es sich um eine von Ihnen aktiv genutzte Anwendung handelt, können Sie dieses Programm für die Ordnerüberwachung freigeben. Diese Anwendung hat dann grundsätzlich auf alle überwachten Ordner vollen Zugriff. Eine Abstufung, einzelnen Programmen nur für bestimmte Ordner Rechte einzuräumen, ist bei den geschützten Ordnern bislang zumindest nicht vorgesehen.

Um einer App Zugang zu den geschützten Dateien zu ermöglichen, klicken Sie in der App-Liste auf das Plussymbol neben *Zulässige App hinzufügen*. Navigieren Sie im Dateiauswahldialog in den entsprechenden Ordner – meist unter *C:\Programme* oder *C:\Programme(x86)*. Bestätigen Sie die Rückfrage der Benutzerkontensteuerung. Es wird in der App-Liste dann ein Eintrag für diese Anwendung angelegt, über den Sie das Programm später ggf. auch wieder entfernen können.

18.5 Weitere Einstellungen für den Windows Defender

Die Arbeitsweise des Windows Defender lässt sich mit einigen Einstellungen anpassen. So kann der Echtzeitschutz zumindest vorübergehend deaktiviert werden, um Probleme durch Fehlalarme zu lösen. Aus demselben Grund besteht auch die Möglichkeit, einzelne Dateien, Ordner oder Prozesse von der Überwachung auszunehmen, was der sinnvollere Ansatz ist.

1. Öffnen Sie in *Windows-Sicherheit* die Rubrik *Viren- & Bedrohungsschutz* und klicken Sie darin auf *Einstellungen für Viren- & Bedrohungsschutz*.



2. Hier können Sie ganz oben den *Echtzeitschutz* deaktivieren. Beachten Sie, dass die Selbstüberwachung von Windows dadurch anspringt und Warnungen dazu im Info-Center anzeigt. So kann man nicht vergessen, den Echtzeitschutz später wieder zu reaktivieren. Und selbst wenn man es vergessen sollte: Er wird nach