Windows 10
Höchste Sicherheit mit Bordmitteln

Absolute Sicherheit gibt es nicht!

Diese - zugegebenermaßen ziemlich abgedroschene - Binsenweisheit ist auf nahezu jeden Lebensbereich anwendbar und gilt natürlich auch uneingeschränkt im Computer- und Datenbereich. Auf dem Weg zu möglichst idealer Datensicherheit hat Microsofts neuestes Betriebssystem Windows 10 dennoch schon sehr viel richtig gemacht. So bietet der neueste Windows-Ableger schon fast alles, was für ein sicheres Betriebssystem erforderlich ist.
Vorausgesetzt, du hast alle Einstellungen auch richtig gewählt. Am besten ist es dabei natürlich immer, wenn Schadsoftware gar nicht erst auf deinen Rechner gelangt und entsprechende Bereinigungstools erst gar nicht aktiv werden müssen. Doch was machen Smart Screen Filter, Windows Defender und Firewall eigentlich genau? Worauf kommt es an? Auf welche Konfigurationen musst man achten?

Wir bringen etwas Licht ins Dunkle.

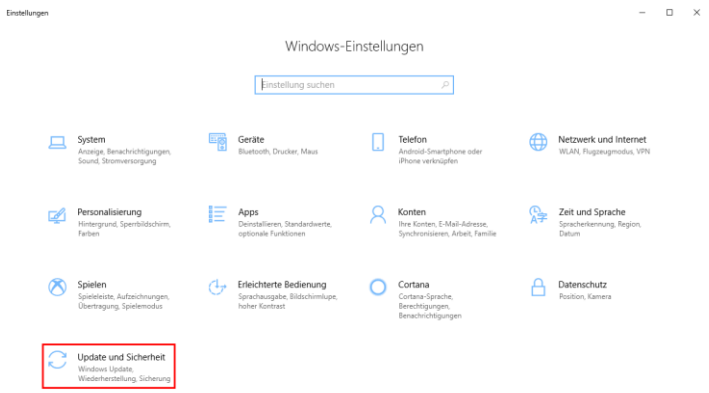
Windows Defender Security Center

Für den Schutz vor gefährlichen Inhalten vor allem aus dem Internet bietet Windows 10 gleich mehrere integrierte Funktionen. Alle relevanten Einstellungen kannst du bequem im sogenannten **Windows Defender Security Center (Windows-Einstellungen)** verwalten und anpassen.

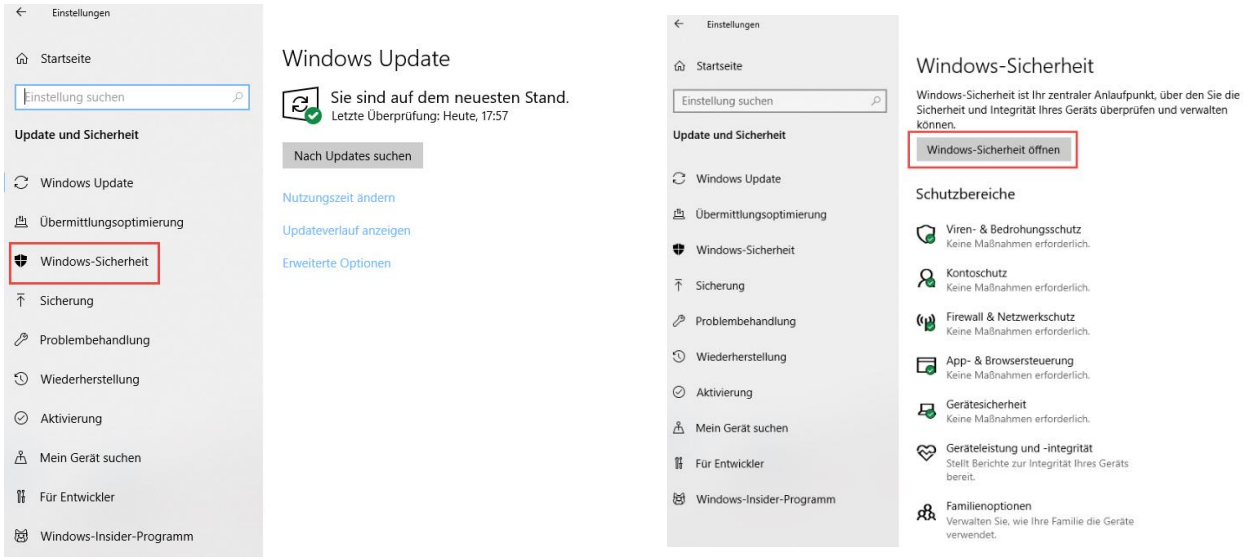
Das Security-Center erreichst du ganz einfach per Klick auf die Startschaltfläche sowie danach auf das Zahnrad für die Einstellungen.

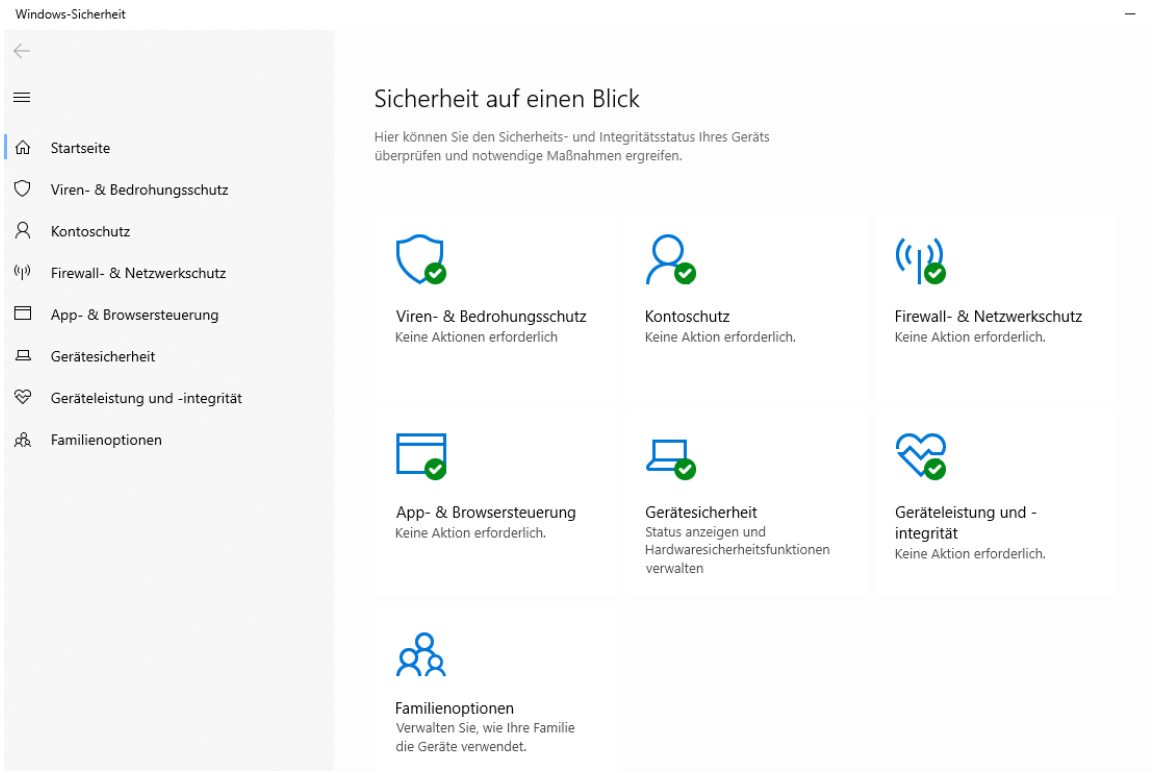
Noch schneller gehts über den Infobereich rechts unten am Bildschirmrand neben der Uhr  .

Folge den nachstehenden Bildern um zu allen notwendigen Einstellungen zu gelangen.



info@pc-home-service.com
www.pc-home-service.com





Die Startseite des Sicherheits-Dashboards liefert einen Überblick mit den wichtigsten Informationen. Wenn alles in Ordnung ist, erscheint bei allen Rubriken ein grünes Häkchen.

SmartScreen

Für den Schutz vor gefährlichen Inhalten aus dem Internet sollte dein SmartScreen korrekt eingestellt sein. Dies ist ein automatischer Filter, welcher schädliche Inhalte von Webseiten und/oder heruntergeladenen Apps ausfindig macht und gegebenenfalls blockiert.

Die Einstellungen kannst du im oben gezeigten Fenster unter „**App- & Browsersteuerung**“ vornehmen.

Bei allen Optionen ist standardmäßig „**Warnen**“ eingestellt. Diese Einstellung ist auch gleichzeitig die sinnvollste, denn bei jedem einzelnen Fund wirst du per Bildschirm-

anzeige über eventuelle Gefahren informiert. Abschließend kannst du aber immer noch selbst entscheiden, ob der Download oder die Website tatsächlich gefährlich ist und geblockt werden soll, oder nicht.

Apps und Dateien überprüfen

„**Apps und Dateien überprüfen**“ ist dabei für alle Downloads aus dem Internet unabhängig vom Browser zuständig. Downloads, die als nicht unbedenklich eingestuft werden, bekommen zunächst einmal einen speziellen Identifier. Willst du die Datei oder App dann öffnen, meldet sich Smartscreen und informiert dich über die Blockade. Auf den ersten Blick siehst du nur die Schaltfläche „Nicht ausführen“ und kannst das Programm folglich nicht starten.
Wenn du dir sicher bist, dass es sich nicht um Schadsoftware handelt, dann kannst du die Datei auch mit der rechten Maustaste anklicken und im Kontextmenü den Punkt „Eigenschaften“ aufrufen. Hinter dem Reiter „Sicherheit“ siehst du dann die Angabe „Die Datei stammt von einem anderen Computer. Der Zugriff wurde aus Sicherheitsgründen eventuell blockiert.“ Klickst du dort auf „Zulassen“ und dann auf „OK“, so kannst du die Datei anschließend ganz normal öffnen.

SmartScreen für Microsoft Edge

„**SmartScreen für Microsoft Edge**“ wirkt sich nur auf Webseiten und Downloads aus, die du im Browser Edge ausführst. Bei Webseiten, die beispielsweise Schadsoftware verbreiten oder ein anderes Risiko für die Sicherheit darstellen, erscheint eine Warnung im Browser. Nach Klicks auf „Weitere Informationen“ und „Ignorieren und fortfahren (nicht empfohlen)“ lässt sich die Website dennoch aufrufen – auf eigenes Risiko.

SmartScreen für Microsoft Store-Apps

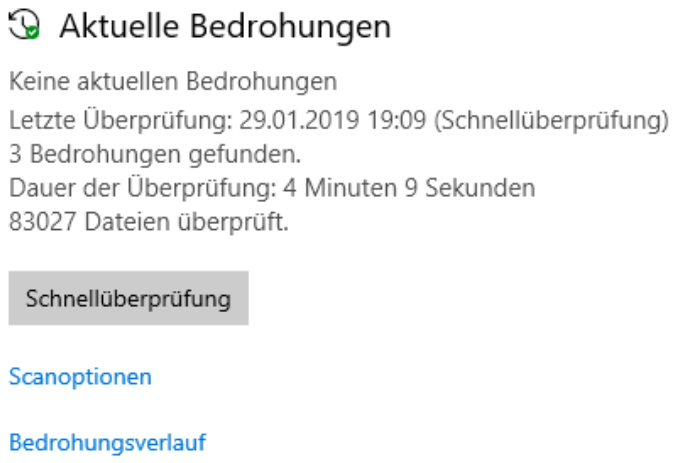
„**SmartScreen für Microsoft Store-Apps**“ funktioniert ähnlich wie beim Browser. Sollte eine App eine als schädlich eingestufte Webseite aufrufen wollen, siehst du eine entsprechende Warnung. Daraufhin kannst du selbst entscheiden, ob die entsprechende App ausgeführt werden soll, oder nicht. Auch hier gilt wie immer, Benutzung auf eigenes Risiko!

Exploit-Schutz

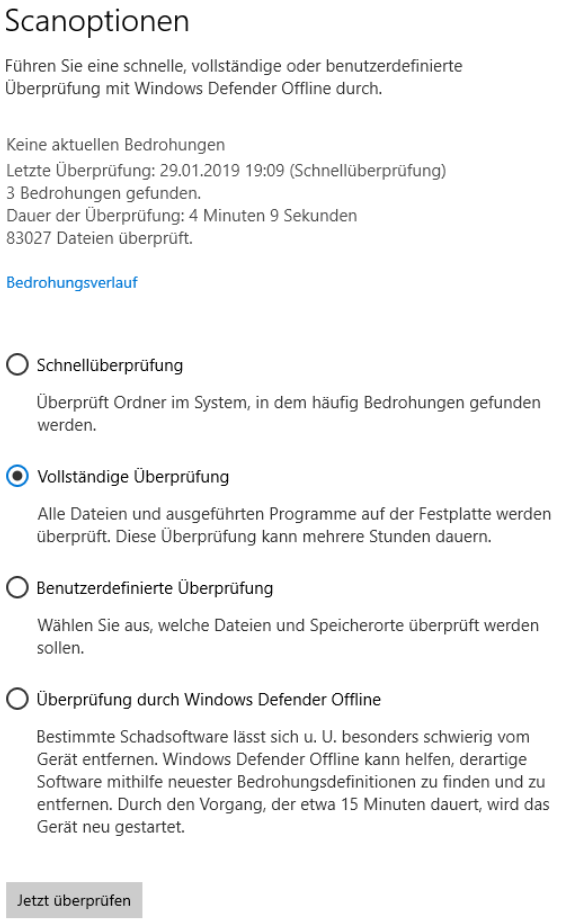
Der vierte Bereich heißt „**Exploit-Schutz**“. Hier ist generell nur eine Änderung der Einstellungen zu empfehlen, wenn du dich im Vorfeld genauestens über die entsprechende Funktionsweise informiert hast. Zu den Optionen gelangst du hier per Klick auf „Einstellungen für Exploit-Schutz“. Unter dem Reiter „**Systemeinstellungen**“ sind alle Optionen bis auf „Zufällige Anordnung für Images erzwingen (obligatorische ASLR)“ standardmäßig aktiviert, wobei du es auch belassen solltest.
Unter „Programmeinstellungen“ findest du eine Liste mit Programmen, für die jeweils Ausnahmeregeln festgelegt sind. Hier kannst du bei Bedarf weitere Programme hinzufügen, oder bestehende Einträge bearbeiten und entfernen. Auch hier ist allerdings Vorsicht geboten und du solltest nur die Einstellungen verändern, über deren Wirkweise du zu 100% Bescheid weißt, wenn du deinen PC nicht einem unnötigen Risiko aussetzen willst. In der Regel erledigt das Windows automatisch.

Virenschutz

Der hauseigene Virenscanner **Windows Defender** kann in puncto Bedienbarkeit und Funktionsumfang ohne weiteres mit anderen bekannten Virenscannern mithalten. Zudem ist er werbefrei und belastet das System mäßig.
Nach einem Klick auf „**Viren- & Bedrohungsschutz**“ im Fenster (s.o.) siehst du das Ergebnis der letzten Schnellprüfung. Diese umfasst alle Systemordner, die besonders häufig das Ziel von Angriffen sind.



Per Klick auf "Scanoptionen" gelangst du stattdessen zu den weiterführenden Optionen. Hier gibt es unter anderem die Option „Vollständige Überprüfung“, mit der sich alle Dateien auf der Festplatte prüfen lassen, sowie „Benutzerdefinierte Überprüfung“, wo du ganz gezielt einzelne ausgewählte Ordner untersuchen lassen kannst.
Die umfassendste Überprüfung bringt „Überprüfung durch Windows Defender Offline“ mit sich. Ein Klick auf „Jetzt überprüfen" startet die ausgewählte Überprüfung.



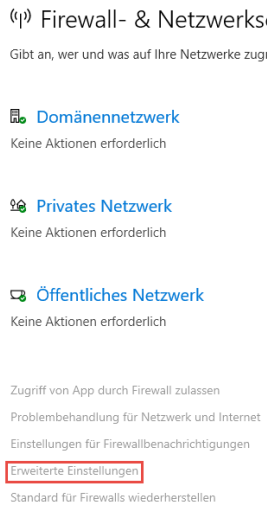
Allerdings ist der manuelle Start der Überprüfung nur in den seltensten Fällen wirklich notwendig. Windows Defender überwacht und prüft dank **Echtzeitschutz** jede Datei, die neu auf deinen PC gelangt.
Wurde bei einem Scan nun eine verdächtige Datei gefunden, bekommst du eine entsprechende Warnmeldung. Per Mausklick kannst du die betroffene Datei dann entweder löschen, in Quarantäne verschieben oder trotz der Warnung ausführen.

Die Firewall

Bei der Windows-Firewall handelt es sich um einen Filter, der Zugriffe über das Netzwerk auf bestimmte Ports unterbindet. Die Firewall blockiert erst einmal alle Anfragen aus dem lokalen Netzwerk, außer du hast zuvor einen Port für die betreffende Anwendung freigegeben. Zugriffe aus dem Internet sind ohnehin nicht möglich, weil hier die Firewall in deinem DSL-Router einspringt. Vorausgesetzt, du hast diese nicht irgendwie anderweitig deaktiviert.

Grundsätzlich gilt

In deiner Firewall sollten immer nur die Ports geöffnet sein, die du tatsächlich auch benötigst. Kontrolliere daher regelmäßig, welche Einstellungen aktiv sind und entferne jegliche veraltete Freigaben. Über das oben genannte Sicherheits-Center findest du unter dem Punkt „Firewall- & Netzwerkschutz“ allerdings nur die grundlegendsten Basisinformationen. Die detaillierte Konfiguration deiner Firewall erfordert noch einen weiteren Klick, nämlich auf den Punkt „Erweiterte Einstellungen“.



Bevor du hier allerdings etwas veränderst, empfiehlt es sich, ein Backup der vorhandenen Regeln anzulegen, um sie im Zweifelsfall unverändert wieder herstellen zu können. Dazu klickst du im linken Teil des Fensters auf die erste Zeile und dann oben im Menü (oder im rechten Fensterteil) auf „Aktion –› Richtlinie exportieren“. Nach Auswahl von Speicherort und Namen wird eine Sicherungskopie angelegt. Sollte es nötig sein, kannst du selbige über „Aktion –› Richtlinie importieren“ problemlos wieder laden.

Eingehende & Ausgehende Regeln

Nun kannst du dir einmal die Einträge unter „**Eingehende Regeln**“ etwas genauer ansehen. Über „Nach Profil filtern“ auf der rechten Seite des Fensters kannst du die Liste beispielsweise mit „Nach öffentlichen Profil filtern“ noch weiter einschränken. Hier sollten dann auch keine Programme auftauchen, die du nur im lokalen Netzwerk nutzen möchtest. Bei den Regeln für das private Profil gilt es dagegen, alle Anwendungen zu entfernen, die nicht mehr benutzt werden.

Für die eingehenden Regeln gilt: Die Firewall blockiert alle eingehenden Verbindungen, außer es gibt eine Freigaberegel. Bei den ausgehenden Regeln ist es umgekehrt. Die Firewall erlaubt alle ausgehenden Verbindungen, außer es ist eine blockierende Regel festgelegt. Nutze ausgehende Regeln beispielsweise für Programme, denen du den Zugang zum Internet verbieten willst, weil diese z.B. unerlaubt Daten an den Hersteller senden.

Wir hoffen, wir konnten dir einen ersten kurzen Überblick über die wichtigsten Sicherheitsfeatures von Windows 10 verschaffen.

Noch Fragen?

Hast du noch vertiefende Fragen oder Anmerkungen? Dann nimm doch einfach Kontakt mit uns auf!