7. Malware: Viren & Co. vermeiden & bekämpfen

Viren und Trojaner – insbesondere auch in der jüngsten Variante der Erpressungstrojaner – sind und bleiben eine beständige Gefahr für jeden Computer, der direkt (Netzwerk) oder indirekt (etwa über USB-Medien) mit anderen Daten austauscht – und welcher Rechner tut das nicht? Deshalb ist es unerlässlich, sich gegen digitale Infektionen zu schützen. Dieser Schutz basiert auf zwei Säulen: einem effektiven Virenschutz mittels entsprechender Software sowie – mindestens ebenso wichtig – einigen elementaren Verhaltensregeln, gepaart mit gesundem Menschenverstand.

7.1 Verhaltensregeln: Schädlinge vermeiden

Auch beim Schutz vor digitalen Schädlingen ist der menschliche Faktor nicht zu unterschätzen: Was nützt ein sicher konfiguriertes System, wenn Anwender Sicherheitswarnungen ignorieren und dubiose Dateien unbedacht öffnen? Und auch mit einem Antivirenprogramm als Rückversicherung sollte man niemals alle Vorsicht über Bord werfen. Praktisch täglich entstehen neue Varianten von Schädlingen. Trojaner-Baukästen ermöglichen es den Urhebern, sich mit wenigen Mausklicks ihren ganz persönlichen Trojaner zusammenzuklicken, der dann eine – etwas – andere Signatur hat und nicht von jedem Scanner sofort erkannt wird. Deshalb müssen die eigene Umsicht und Skepsis stets als weitere Abwehrlinie gegen Infektionen dienen.

Überraschende Rückfragen der Windows-Benutzerkontensteuerung

Für das Einnisten ins System benötigen Schädlinge in der Regel Administratorrechte. Hier kommt die Benutzerkontensteuerung (UAC) von Windows ins Spiel. Richtig eingesetzt, kann sie ein wertvoller Schutz sein. Allerdings muss man die Rückfragedialoge zu diesem Zweck ernst nehmen und zumindest kurz nachdenken, anstatt einfach nur gewohnheitsmäßig zu genehmigen. An sich sollte man ohnehin jedes Mal darüber nachdenken. Aber insbesondere wenn auf einmal scheinbar anlasslos Administratorrechte angefordert werden, sollten die Alarmglocken schrillen.

Fremde Speichermedien prüfen

Früher gehörten Disketten und CDs zu den häufigsten Einfallswegen für digitale Schädlinge. Diese Medien sind aus der Mode gekommen und mit ihnen auch die typischen Viren, die sich darüber verbreitet haben. Trotzdem ist beim Austausch von Daten via DVD oder USB-Medien immer noch Vorsicht angesagt. Nach wie vor gilt, dass man solche Datenträ-

ger umgehend mit dem Virenscanner prüfen sollte, bevor man Dateien von dort öffnet oder kopiert. Ein Risiko besteht auch, wenn man Datenträger im Laufwerk stecken lässt, wenn man den PC ausschaltet. Beim nächsten Start könnte der PC davon booten und dann anstelle des installierten Betriebssystems eigene Software starten. Dies lässt sich aber verhindern, indem man im BIOS/UEFI festlegt, dass grundsätzlich nur von der internen Festplatte gestartet werden soll.

USB – universelle Sicherheitsbedrohung

Von USB-Anschlüssen geht aber noch eine andere Gefahr aus, denn dort kann man nun mal alles Mögliche anschließen. Im Arsenal fortgeschrittener Hacker befinden sich USB-Sticks, die nur äußerlich wie solche aussehen. Technisch aber verhalten sie sich wie Tastaturen. Durch das Anstecken bekommen sie Strom und werden automatisch aktiv. Sie beginnen nun, gesteuert durch ein internes Programm, Tastencodes zu tippen, mit denen sie beispielsweise eine Eingabeaufforderung oder PowerShell öffnen und darin Befehle eingeben. Das reicht, um den Virenschutz des Rechners zu deaktivieren, ein Trojanerprogramm aus dem Internet herunterzuladen und zu installieren.

Schützen kann man sich vor solchen Angriffen kaum, sofern man seine USB-Anschlüsse nicht komplett deaktivieren will. Folgende Verhaltensregeln minimieren die Gefahr aber:

- Stecken Sie niemals unbekannte, gefundene oder unaufgefordert erhaltene USB-Sticks in Ihren Rechner.
- Das Gleiche gilt für alle Arten von USB-Geräten, auch wenn es sich dabei um unscheinbare Gimmicks wie Taschenlampen oder Ventilatoren handelt.
- Verwenden Sie keine öffentlichen USB-Ladeanschlüsse. Man kann nie wissen, ob am anderen Ende wirklich nur ein Netzteil sitzt oder nicht doch ein Mini-PC, der auf das Gerät zugreifen kann. Führen Sie besser stets ein eigenes Ladegerät oder eine Powerbank mit sich.

Vorsicht bei E-Mail-Anhängen

Öffnen Sie niemals unaufgefordert zugesandte E-Mail-Anhänge! Dies gilt insbesondere für Office-Dokumente wie Word-Texte und Excel-Tabellen. Deren aktive Inhalte machen es besonders leicht, einen PC zu manipulieren. Aber auch bei Formaten wie PDF werden immer wieder Sicherheitslücken bekannt. Lassen Sie sich auch von dramatischen Formulierungen wie »Letzte Mahnung« nicht verunsichern. Solche Dokumente bedürfen nach wie vor der Schriftform. Auch über Lotteriegewinne oder Erbschaften wird man in der Regel nicht per E-Mail informiert.

Lassen Sie grundsätzlich die Finger von Dateianhängen, deren Bedeutung Sie nicht kennen! Es gibt eine Vielzahl von Dateiendungen, hinter denen sich letztlich ausführbare Inhalte verbergen können. Wenn Sie nicht sicher sind, worum es sich handelt, sollten Sie es vor dem Öffnen in Erfahrung bringen. Oder einfach ganz darauf verzichten. Lassen Sie sich dabei auch nicht von ZIP-Archiven täuschen. Diese werden gern als Vehikel eingesetzt, dessen Inhalt von Scannern nicht überprüft werden kann (insbesondere wenn er mit einen Kennwort geschützt ist).

Die Chef-Masche erkennen

Vergessen Sie auch niemals, dass E-Mails an sich nicht fälschungssicher sind. Bei der beliebten »Chef-Masche« informieren Angreifer sich zunächst aus öffentlichen Quellen über die Strukturen eines Unternehmens. Dann kontaktieren Sie mittels gefälschter Mails beispielsweise einen Mitarbeiter der Buchhaltung und geben sich als Mitglied der Managementebene aus. Die individualisierte Nachricht schmeichelt dem Empfänger (»Sie wurden mir als sehr vertrauenswürdig empfohlen«) und bittet dann um Mithilfe bei einer wichtigen Transaktion, die aber vorläufig noch streng geheim gehalten werden muss, beispielsweise einer Firmenübernahme. Dazu müsse der Mitarbeiter umgehend eine Überweisung veranlassen. Bei einer anderen Variante bekommt man eine Mail von einem namentlich bekannten Mitarbeiter der IT-Abteilung mit der Bitte, zu Wartungszwecken eine bestimmte Software zu installieren.

Wann immer E-Mails mit ungewöhnlichen, überraschenden Anfragen oder unerwarteten Dateien oder Download-Links kommen, sollten Sie also skeptisch sein und im Zweifelsfall lieber mit einem kurzen Anruf klären, ob damit alles seine Richtigkeit hat.

Datei-Downloads

Downloads aus dem Netz sind ein häufiger Einfallsweg für Viren und Trojaner. Deshalb ist hier etwas Disziplin besonders wichtig:

- Laden Sie nur Dateien herunter, die Sie wirklich benötigen.
- Laden Sie beispielsweise Software am besten direkt von der Website der entwickelnden Firma herunter.
- Andernfalls greifen Sie auf etablierte Softwareverzeichnisse zurück, deren Angebot redaktionell betreut und auf Viren überprüft wird.
- Insbesondere Anbieter von Open-Source-Software geben häufig eine Checksumme bekannt, mit der man die heruntergeladenen Dateien auf Authentizität überprüfen kann (mehr darüber erfahren Sie im folgenden Abschnitt).
- Machen Sie es sich zur Gewohnheit, alle heruntergeladenen Dateien unmittelbar im Anschluss manuell mit Ihrem Virenscanner zu überprüfen.
- Laden Sie heruntergeladene Dateien im Zweifelsfall bei VirusTotal.com hoch, bevor Sie sie erstmals öffnen bzw. ausführen (siehe Seite 260).

Datei-Downloads mit Checksummen überprüfen

Nicht nur, aber insbesondere bei Software rund um Sicherheit und Verschlüsselung ist es sehr wichtig, dass man tatsächlich genau das bekommt, was man erwartet. Beispielsweise bei Open-Source-Anwendungen liegt der Quellcode offen. Ein Angreifer könnte diesen Code nehmen und heimlich beispielsweise um eine eigene Trojaner-Komponente ergänzen. Wenn er diesen eigenen Code kompiliert, erhält er eine Anwendung, die sich äußerlich genau wie das Original verhält, aber eben mit der heimlichen Zusatzfunktion.

Um sich davor zu schützen, geben Open-Source-Entwickler oftmals eine Checksumme zu ihren Downloads bekannt. Die wird nach einem bestimmten Algorithmus aus der Binärdatei berechnet. Eine solche Checksumme ist nicht eindeutig, da theoretisch zwei unterschiedliche Binärdateien dieselbe Checksumme haben können. Aber die Wahrscheinlichkeit ist sehr gering, und es ist praktisch ausgeschlossen, dass eine manipulierte Variante einer Binärdatei dieselbe Checksumme wie das Original hat.

Hashes and Signatures

KeePass 2.42.1

KeePass-2.42.1.zip:
MD5: 6BF0F05A 8188FC2A 35E643AF 4B8A87F0
SHA-1: 01CB0CAE B030CBEC B7DD0012 FFA68566 1E29966D
SHA-256: 67B61A41 0CF0568C F0182A31 E6F940BB 6D00F0C6 FFF44D6D CC514D61 558B86A8
Size: 3202909 B
Sig.: [OpenPGP ASC]

KeePass-2.42.1-Setup.exe:
MD5: 4540BD71 706A429E E1856CCD 1CFE4D88
SHA-1: F3E0B1A5 1ADAAE13 0FD2C6BA 64EE82C4 322D2950
SHA-256: D3BBB617 98DFD230 616D9FF1 9EC227EE 30515798 5D769B9B 7C4AA7DA 59F8800D
Size: 3309104 B
Sig.: [OpenPGP ASC]

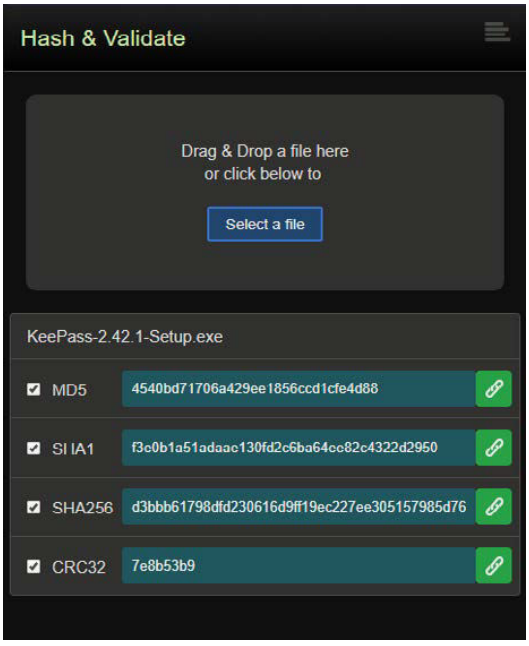
KeePass-2.42.1.msi:
MD5: F81E3519 84B28535 FE325D0E 59E71EEF
SHA-1: F14DE7D5 982443B5 8F07190C 91721A25 BD9DE57F
SHA-256: 3DAD1D63 BE6D57A8 AE721C31 31A2A2BC F53FA87F 220B96B3 384DC789 E0523FA7
Size: 3764736 B
Sig.: [OpenPGP ASC]

KeePass-2.42.1-Source.zip:
MD5: 09E30342 24D7C82C 1822AB3B 015F1495
SHA-1: B40E5469 A1D9E086 F084442C F350E9D3 3233CFEA
SHA-256: 415654E6 2E1E03F1 BC3D0AE7 E5D447C9 DDBCC23C B0394524 24DC5DEF 141976C1
Size: 5163432 B
Sig.: [OpenPGP ASC]

Der Passwort-Manager KeePass gibt zu allen Versionen und Varianten Checksummen auf seiner Website bekannt.

Man kann deshalb nach dem Download einer Datei mit einem Prüfprogramm dessen Checksumme berechnen und mit der Vorgabe des Entwicklers vergleichen. Sind beide identisch, kann man sicher sein, eine Originalfassung der Software ohne Manipulationen erhalten zu haben. Es gibt verschiedene Checksummenverfahren (MD5, SHA1, SHA256, CRC32 etc.). Es gibt auch für alle Plattformen entsprechende Software, mit der man diese Checksummen ermitteln kann. Meine Empfehlung ist eine Web-App, die Sie jederzeit unter www.toolsley.com/hash.html im Browser öffnen können.

Wählen Sie die heruntergeladene Datei aus, oder ziehen Sie sie direkt per Drag-and-drop aus der Download-Leiste des Browsers auf die Web-App. Dann ermittelt die App Checksummen für die vier gängigsten Hash-Verfahren.



Drive-By-Infektionen

Manche halten es für ein hartnäckiges Gerücht, dass man sich nur durch das Aufrufen einer Webseite mit einem Virus infizieren kann. Tatsächlich ist es aber durchaus möglich. »Schuld« daran sind aktive Inhalte von Webseiten wie JavaScript, Adobe Flash, PHP etc. Diese sind im Web allgegenwärtig, um dynamische, attraktive Webseiten zu gestalten. Aber sie lassen sich insbesondere in Verbindung mit Sicherheitslücken oder dem Täuschen uninformierter Anwender auch missbrauchen. Ein beliebter Trick ist es etwa, in einer Webseite plötzlich einen Dialog einzublenden, der einer Warnung des Windows-Betriebssystems auf den ersten Blick täuschend ähnlich sieht. Darin steht, dass auf dem PC eine Sicherheitslücke entdeckt wurde und man umgehend eine bestimmte Webseite besuchen oder eine Software herunterladen soll, um das zu reparieren.

- Verwenden Sie immer nur die jeweils aktuellen Versionen des Webbrowsers sowie ggf. vorhandene Erweiterungen. Dadurch werden eventuelle Sicherheitslücken möglichst schnell geschlossen.
- Halten Sie aus demselben Grund auch das Betriebssystem sowie alle installierten Programme stets aktuell.
- Verwenden Sie stets die aktuellste Version des Virenscanners, und aktualisieren Sie dessen Schädlingssignaturen so häufig wie möglich.
- Lassen Sie den Hintergrundscanner immer laufen, und überprüfen Sie zusätzlich regelmäßig die Festplatte auf Schafsoftware.

- Die Verwendung von Skriptsprachen wie beispielsweise JavaScript lässt sich bei den meisten Webbrowsern deaktivieren. Das ist allerdings eine recht drastische Maßnahme, da viele Webseiten dann nicht mehr (wie gewohnt) funktionieren würden. Auf Seite 292 stelle ich Ihnen Alternativen vor, wie Skripte in Webseiten gezielt kontrolliert werden können.

Risiko Browser-Erweiterungen

Ein weiteres Einfallstor für Schädlinge sind die beliebten Browser-Erweiterungen. Diese können im Prinzip auch alles Mögliche andere machen, als sie vorgeben. Deshalb sollte man beim Installieren von Browser-Erweiterungen genauso vorsichtig wie beim Installieren von Anwendungen oder Apps sein. Ausführlicher wird dieses Thema auf Seite 295 behandelt.

7.2 Infektionen mit Antivirensoftware verhindern

Das A und O einer sicheren Abwehrstrategie ist und bleibt eine Antivirensoftware. Eine der einfachsten und kostengünstigsten Lösungen ist der von Microsoft bei Windows mitgelieferte Defender. Er bietet einen soliden Basisschutz vor gängigen Gefahren, läuft unauffällig im Hintergrund und wird von Windows zuverlässig mit Updates versehen. Allerdings ist die Update-Frequenz nicht ganz so hoch wie bei einigen kostenpflichtigen Alternativen, was die Schutzwirkung gegen ganz frische Schädlinge schmälern kann. Auch in Bezug auf Suchheuristiken zum Erkennen neuer Varianten schneidet der Windows Defender in Vergleichstests regelmäßig schwächer ab. Trotzdem bietet er soliden Schutz und stellt für Benutzer, die sich der Risiken von Mailanhängen und obskuren Download-Links bewusst sind, durchaus eine sinnvolle Option dar. Wer nicht ständig Software aus allen möglichen mehr oder weniger finsteren Ecken des Web ausprobiert, ist damit gut bedient.

Auch die kostenpflichtigen Mitbewerber bieten nicht automatisch ein Rundum-sorglos-Paket. Aber mit Signaturaktualisierungen teilweise mehrmals täglich und raffinierten Suchheuristiken sind sie häufig etwas mehr am Puls der Zeit und stellen vor allem auch für weniger erfahrene Benutzer einen zuverlässigen Begleiter durch die Untiefen des Internets dar.

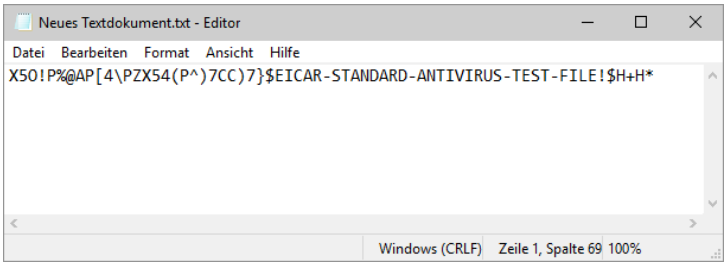
Funktioniert mein Virenschutz?

Wenn Sie noch nie einen Virus auf Ihrem PC gefunden haben, wie können Sie dann sicher sein, dass Ihr Virenschutzprogramm richtig funktioniert? Einen echten Virus zu verwenden, wäre wohl etwas zu riskant. Außerdem hat man den ja meist nicht unbedingt zur Hand. Es gibt aber einen einfachen Test, den jeder an seinem Computer schnell nachvollziehen kann. Unter Windows geht es beispielsweise so:

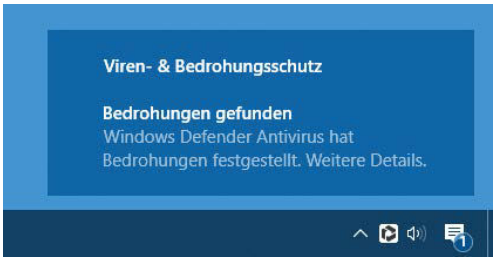
1. Klicken Sie mit der rechten Maustaste in einen Ihrer Ordner oder an eine freie Stelle des Desktops.
2. Wählen Sie im Kontextmenü die Funktion *Neu/Testdokument*. Übernehmen Sie den vorgeschlagenen Namen, oder verwenden Sie einen eigenen.
3. Öffnen Sie die Datei mit einem Doppelklick im Editor. Verwenden Sie zum Bearbeiten nur einen einfachen Texteditor, nicht Word oder Ähnliches.
4. Fügen Sie in die Datei den folgenden Code in einer Zeile ohne Leerzeichen ein:

   `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

   Verwenden Sie dabei nur Großbuchstaben, und das dritte Zeichen ist der Buchstabe O und nicht die Ziffer 0!. Bei dieser Zeichenkette handelt es sich um den EICAR-Virus. Das ist kein echter Schädling, sondern eine spezielle Virensignatur, die jedes Antivirenprogramm kennen und entdecken sollte. Selbstverständlich ist der EICAR-Virus keine echte Gefahr, weil er sich weder selbst repliziert noch irgendeinen Schaden anrichtet.



5. Speichern Sie nun diese Datei mit dem neuen Inhalt.
6. Warten Sie ab, ob Sie daraufhin eine Reaktion Ihres Antivirenprogramms erhalten.



Weil es sich dabei um einen »offiziellen« Testvirus handelt, sollte jedes Antivirenprogramm ihn erkennen und darauf reagieren. Wie diese Reaktion genau aussieht, hängt vom jeweiligen Programm und dessen Einstellungen ab. Wenn Sie keine direkte Reaktion erkennen können, sollten Sie einen Blick ins Protokoll des Antivirenprogramms werfen. Möglicherweise hat es die Datei stillschweigend in Quarantäne verschoben und gelöscht. Sollte die Datei hingegen anstandslos gespeichert werden, sollten Sie überprüfen, warum Ihr Antivirenprogramm diese »Bedrohung« nicht erkannt und darauf reagiert hat. Anscheinend besteht hier Nachbesserungsbedarf.

Den PC mit Windows Defender schützen

Mit dem Windows Defender bringt Windows einen Basisschutz gegen Viren und sonstige Malware mit. Er wird bei der Windows-Installation grundsätzlich erst mal 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 *Windows-Sicherheit* per Doppelklick auf das kleine Symbol im Infobereich der Taskleiste auf. Öffnen Sie dort den Bereich *Viren- & Bedrohungsschutz*.

Hintergrund: 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 Update-Mechanismus kann als Pluspunkt gewertet werden.

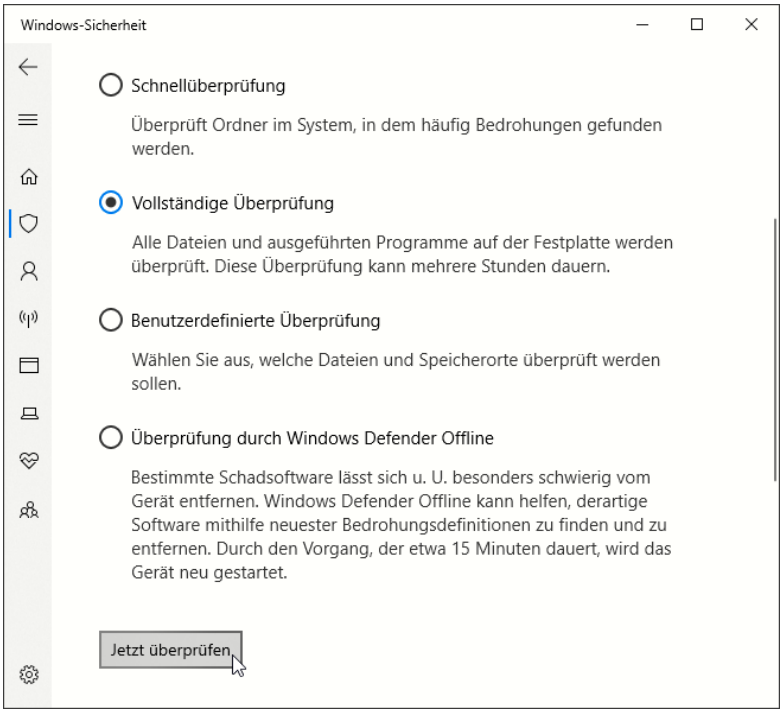
Schwächen offenbart der Defender bei sehr neuen Schädlingen bzw. unbekannten Abarten von Computerviren. Das liegt zum einen an den vergleichsweise langsamen Updates (kommerzielle Programme beziehen teilweise mehrmals täglich Updates, der Defender alle x Tage), zum anderen am Fehlen von effizienten Erkennungsheuristiken. 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.

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.

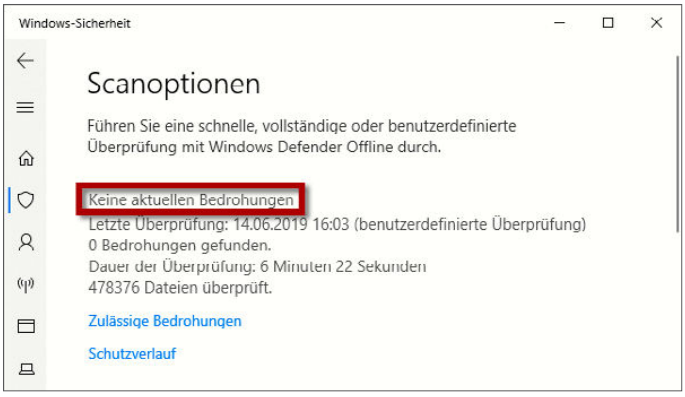
Oder Sie begrenzen das Überprüfen auf einen bestimmten Ordner oder ein einzelnes Laufwerk.

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.

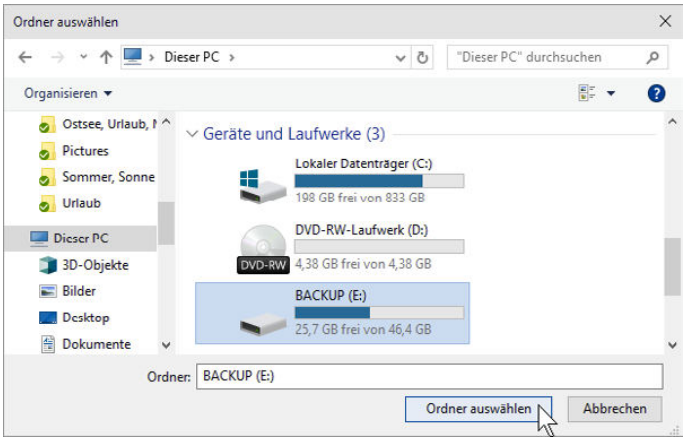
5. Nach Abschluss der Überprüfung zeigt der Defender eine kurze Statistik an. Dieser können Sie entnehmen, wie viele Dateien geprüft wurden und ob dabei Bedrohungen gefunden wurden. Solange hier nur *Keine aktuellen Bedrohungen* steht, ist alles in Ordnung.



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 dann 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.