Geschützt mit Windows

Der kostenlose Microsoft Defender ist Bestandteil von Windows und schützt das System vor Viren, Trojanern und sogar vor fieser Ransomware. **Mit den folgenden Praxistipps arbeitet der Windows-Beschützer noch schneller und sicherer.** ● **VON MARKUS SELINGER**

Früher war der Microsoft Defender (hiess ehemals Windows Defender; wird teils von Microsoft noch immer so genannt) tatsächlich kein gutes Schutz-Tool für Windows. Aber die Zeiten sind lange vorbei! Auch das unabhängige Testlabor AV-Test bestätigt seit mindestens fünf Jahren die gute Schutzleistung gegen Viren, Trojaner und Ransomware der Windows-internen Antiviren-Software samt Firewall. Allerdings zeigen die Tests auch immer wieder, dass der Defender das Windows-System unnötig langsam macht.

Und an genau dem Punkt haken wir ein und zeigen Ihnen, mit welchen Tipps Sie den Defender beschleunigen, wie er weniger Speicher verbraucht, Scans zu Wunschzeiten macht und perfekt eingestellt wird.

Nahtlos in Windows

Der Defender ist keine gesonderte Applikation, sondern in vielen Programmteilen von Windows integriert. Ein paar Einstellungen finden sich in der *Windows-Sicherheit*, ein paar in der *Firewall*, einige in den *Gruppenrichtlinien* oder auch im Webbrowser Edge. Hier ist es schwer die Übersicht zu behalten. Daher stellen wir Ihnen gleich zu Beginn das kleine Gratis-Tool Defender UI vor, mit dem Sie alle Einstellungen auf einer Oberfläche einfach per Klick an- und ausschalten. Mit diesem Tool haben Sie Zugriff auf dutzende Einstellungen des Defenders und Optionen in Windows. Sie erhalten die praktische Software kostenlos unter der Internetadresse **defenderui.com**. Sie funktioniert unter Windows 10 und 11. Die Installation des Helfers ist mit ein paar Klicks erledigt und er-

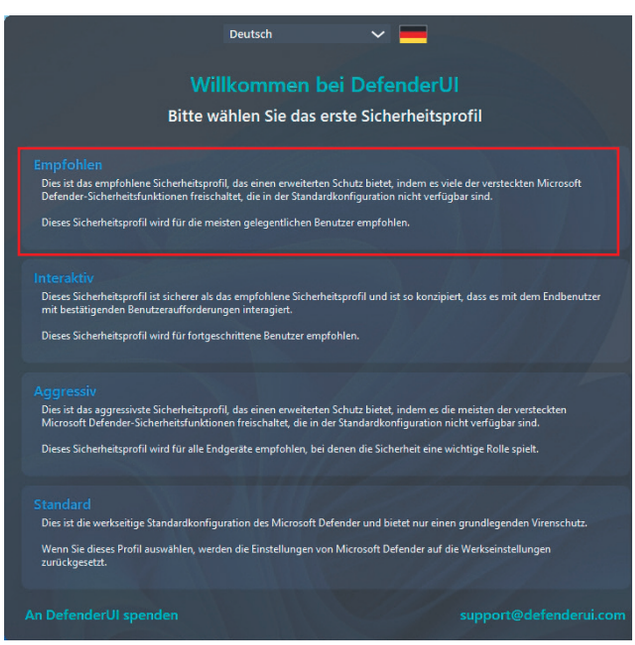

Bild 1: Das kostenlose Tool Defender UI bietet nach dem ersten Start vorgefertigte Profile – nutzen Sie am besten *Empfohlen*

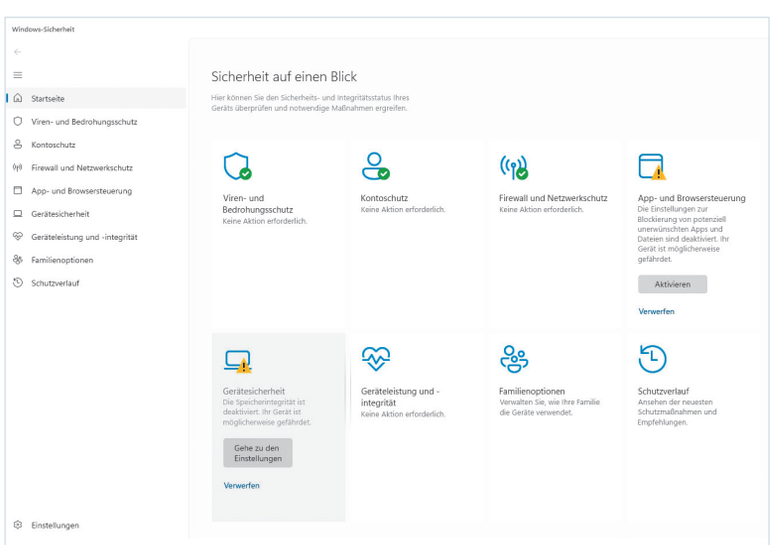

Bild 2: Bei einem neuinstallierten Windows ist der Defender zwar aktiv, aber leider nicht mit allen Schutzkomponenten

Bild: Shuttertock/Boyko.Pictures

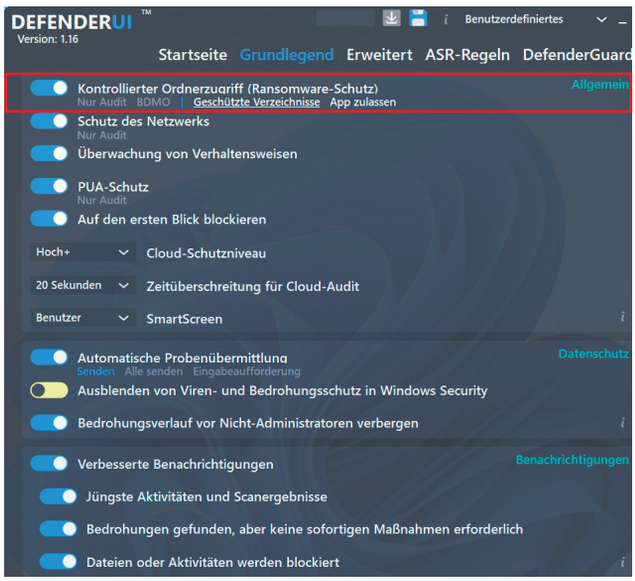

Bild 3: Der Ransomware-Schutz ist zwar für die Systemdaten aktiv, aber *Überwachter Ordnerzugriff* ist standardmässig aus

fordert keine besonderen Rechte unter Windows, sofern Sie als Windows-Administrator arbeiten. Nutzen Sie die vordefinierte Regel *Empfohlen*, Bild 1.

Nach dem ersten Start zeigt sich gleich, dass die meisten Funktionen unter Windows für den Defender bereits korrekt eingeschaltet sind. Aber: Sie werden auch Funktionen entdecken, die unverständlicherweise nicht aktiviert sind. Etwas trügerisch: Auch wenn auf der Startseite der *Windows-Sicherheit* alle Optionen auf «grün» stehen, heisst das nicht, dass alle zusätzlichen Schutzkomponenten aktiv sind, Bild 2.

Tipp: Klicken Sie in Defender UI auf eine unterstrichene Option, öffnet sich automatisch die originale Einstellungsseite in Windows. Aber: Nur wenige Optionen sind auf diese Weise direkt verlinkt, da Sie deren Werte normalweise via Registrierungseditor ändern müssten.

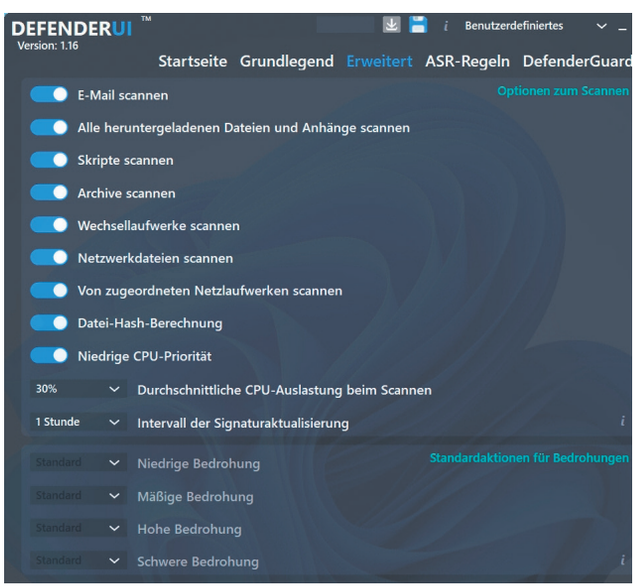

Bild 4: Stellen Sie den Defender so ein, damit er öfters seine Signaturen holt und weniger CPU-Kraft verbraucht

Ransomware

Windows kann sehr gut vor fieser Ransomware schützen; Ransomware sind Erpresser-Trojaner, die Dateien verschlüsseln und nur gegen ein Lösegeld wieder freigeben.

Wer OneDrive als Cloud-Speicher nutzt, kann diesen ebenfalls vor einer Ransomware-Attacke schützen. Der eigentliche Schutz – die Erkennung und Abwehr von Ransomware – ist zwar standardmässig aktiv, aber der *Kontrollierte Ordnerzugriff* nicht. In Defender UI ist das der erste Punkt im Reiter *Grundlegend*, Bild 3. Sobald dieser aktiviert wird, erscheinen auch noch diverse Unterfunktionen.

Sie finden die Funktion in Windows auch unter *Windows-Sicherheit/Viren- und Bedrohungsschutz/Ransomware-Schutz*. Klicken Sie dort auf den Punkt *Ransomware-Schutz verwalten* und schalten Sie die Option *Überwachter Ordnerzugriff* ein.

Unter *Geschützte Ordner* sind nur die Windows-Systemordner des Benutzers geschützt. Sie können dort weitere Ordner angeben und schützen lassen. Wird später einem Programm der Zugriff auf den Ordner verwehrt, tragen Sie es einfach beim Menüpunkt namens *App durch Überwachten Ordnerzugriff zulassen* ein.

Sofern Sie OneDrive-Nutzer sind, finden Sie noch den Punkt *Ransomware-Datenwiederherstellung*. Falls eine Ransomware Ihre Daten auf der Festplatte und somit auch auf OneDrive verschlüsseln würde, können Sie die Daten mit wenigen Klicks wiederherstellen. OneDrive bemerkt sogar das massenweise Verschlüsseln und stoppt den Vorgang. Hier arbeiten der Defender und OneDrive perfekt zusammen.

Schneller und sicherer

Anderer Schutzprogramme aktualisieren mindestens stündlich ihre Antiviren-Signaturen für bösartige Dateien. Der Defender macht das nur alle zwei Stunden. Zusätzlich verlangsamt er den PC, da er standardmässig beim Scannen 50 Prozent der Prozessorleistung in Anspruch nimmt. Wir empfehlen die Werte etwas zu ändern, den aktuelle Signaturen sind besonders wichtig und wenn der Prozessor entlastet ist, können Sie einen Zusatzschutz einschalten.

Stellen Sie in Defender UI auf dem Reiter *Erweitert* das *Intervall der Signaturaktualisierung* auf *1 Stunde* und die *Durchschnittliche CPU-Auslastung beim Scannen* auf *30 Prozent*. Zusätzlich aktiveren Sie noch *Niedrige CPU-Priorität*, Bild 4.

Um den Windows-Schutz zu verbessern, schalten Sie die *Datei-Hash-Berechnung* ein. Ein Hash-Wert sorgt dafür, dass das System eine Veränderung einer Datei bemerkt, sobald diese passiert ist. Der erweiterte Schutz berechnet für jede ausführbare Datei, die keinen Hash-Wert hat, einen solchen Wert und speichert ihn. Der Vorteil: Damit sind auch Dateien geschützt, die Windows nicht im Fokus hat und Cyberangreifer gerne nutzen, um versteckt anzugreifen.

Geheimfunktionen

Wer Windows 10 oder 11 in der Pro-Variante nutzt, kann mit dem *Gruppenrichtlinien-Editor* von Windows auch versteckte Sicherheitsfunktionen aktiveren, Bild 5.

SCANS AUTOMATISCH NACHHOLEN

War zum Beispiel Ihr PC nicht eingeschaltet und hat dadurch den automatisierten Scan von Defender verpasst, dann holt das Windows nicht nach, sondern wartet auf den nächsten Termin. Das sollten Sie mithilfe des *Gruppenrichtlinien-Editors* ändern. Dazu geben Sie einfach im Windows-Suchfeld `gpedit` ein und wählen *Öffnen*. Danach klicken Sie sich durch zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Microsoft Defender Antivirus/Scan*. Klicken ➜

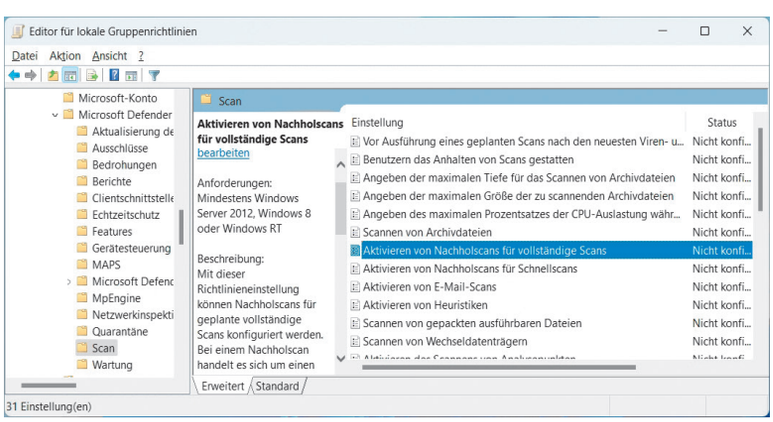

Bild 5: Windows-Pro-Nutzer können mit dem *Gruppenrichtlinien-Editor* auch die geheime Funktion für Nachholscans aktivieren

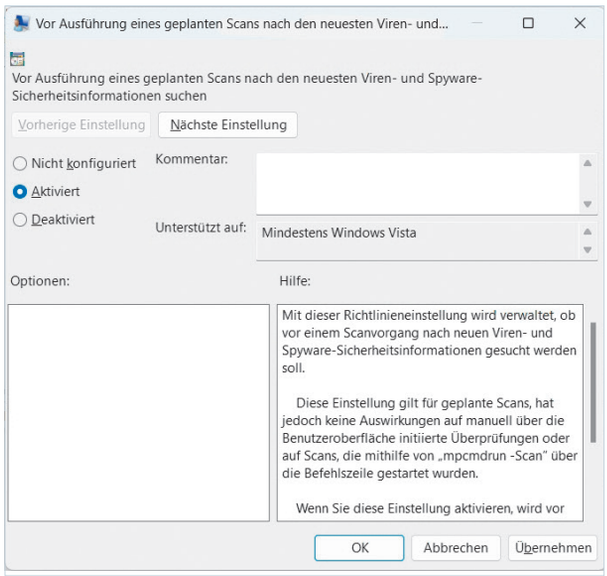

Bild 6: Mit einem versteckten Befehl zwingen Sie Defender vor einer PC-Prüfung die Security-Infos zu aktualisieren

Sie den Eintrag *Aktivieren von Nachholscans für Schnellscans* doppelt an und wählen Sie die Optionen *Aktiviert* und *OK*. Wenn Sie verpasste Komplett-Scans ebenfalls nachholen lassen wollen, schalten Sie zusätzlich den Punkt *Aktivieren von Nachholscans für vollständige Scans* ein.

E-MAIL-ANHÄNGE SOFORT PRÜFEN

Der Microsoft Defender prüft zwar alle E-Mail-Anhänge auf Trojaner & Co. – aber erst, sobald diese auf der Festplatte landen. Sie können den Defender so einstellen, dass er die Mailanhänge sofort prüft, sobald diese im E-Mail-Programm ankommen. Allerdings: Das funktioniert nur mit wenigen E-Mail-Programmen, da das Ganze formatabhängig ist. Microsoft selbst schreibt dazu «Derzeit werden mehrere E-Mail-Formate unterstützt, z. B. pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).» Zum Aktivieren der Option folgen Sie der Beschreibung von *gpedit* und öffnen unter dem Punkt *Scan* das Menü *Aktivieren von E-Mail-Scans* per Doppelklick und bestätigen mit *OK*.

Wenn Sie prüfen wollen, ob der Antivirus-Scan funktioniert, können Sie sich die ungefährliche Eicar-Testdatei per E-Mail schicken lassen. Der Testcode ist zwar vollkommen ungefährlich, wird aber von Virenjägern als Viruscode identifiziert. Nutzen Sie dazu beispielsweise den Service unter dem Link dont.panic.at und dort die Option *Online-Tools/Eicar Testvirus*. Tragen Sie hier einfach Ihre E-Mail-Adresse ein und klicken Sie auf die Schaltfläche *Versenden*.

Im Erfolgsfall wird von Microsoft Defender entweder nur der gefährliche Anhang automatisch entfernt oder die ganze E-Mail in die Quarantäne verschoben.

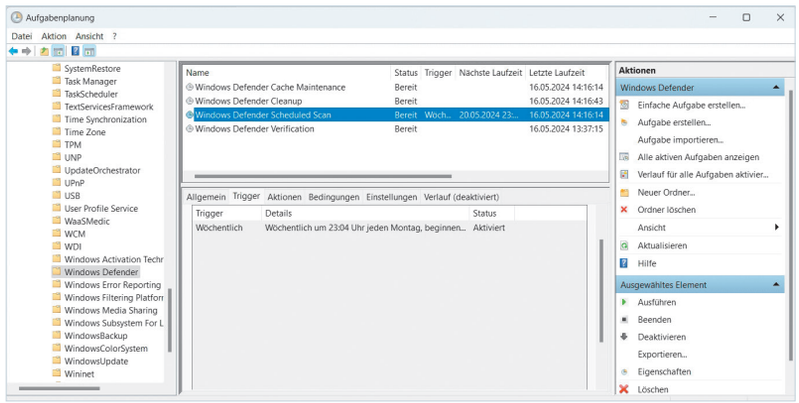

Bild 7: Damit der Defender das System scannt, wann Sie es wollen, müssen Sie in der Aufgabenverwaltung einen Job anlegen

NEUE SECURITY-INFOS

Es ist gut, wenn Sie die Update-Zeit für Ihre Antivirus-Sicherheitsinformationen auf eine Stunde gestellt haben. Es kann aber sein, dass ein automatisierter Scan mit 59 Minuten alten Informationen startet. Sie können auch festlegen, dass der Defender vor jedem automatisierten Scan zuerst die neusten Sicherheitsinformationen abholt und danach loslegt. Dazu müssen Sie nur in *gpedit* wieder zum Ordner *Scan* gehen und öffnen dort per Doppelklick den Punkt *Vor Ausführung eines geplanten Scans nach den neuesten Viren- und Spyware-Sicherheitsinformationen suchen*. Mit einem Klick auf *OK* ist alles aktiv, Bild 6.

Achtung: Der Ordner *Scan* hat noch weitere verlockende Einstellungen parat. Allerdings sind diese zum Teil missverständlich beschrieben. So könnte man meinen, dass die nicht aktive Option *Maximale Tiefe für das Scannen von Archivdateien* die Sicherheit verschlechtert. Aber: Solange der Punkt deaktiviert bleibt, scannt der Defender automatisch alle ZIP- oder CAB-Dateien, und zwar bis in die letzte Ebene!

Scans besser steuern

Wann genau der Defender scannt, ist sein Geheimnis. Allerdings führt er nach jedem Windows-Start einen Schnellscan durch, sofern der Computer keine anderen Aufgaben hat. Ein schneller oder ein normaler Scan lässt sich zwar manuell starten, aber leider nicht in der Oberfläche planen. Das geht wieder nur über eine andere Windows-Funktion: den Aufgabenplaner. Dabei gehen Sie so vor: Geben Sie im Windows Suchfenster `Aufgabenplanung` ein und klicken Sie auf *Öffnen*. Im folgenden Fenster greifen Sie auf der linken Seite zum Menüpunkt *Aufgabenplanungsbibliothek/Microsoft/Windows/Windows Defender*. Danach klicken Sie den Eintrag *Windows Defender Scheduled Scan* doppelt an, Bild 7.

Im folgenden Fenster wechseln Sie zur Registerkarte *Trigger* und wählen *Neu*. In dem sich selbsterklärenden Fenster planen Sie Ihre Scans, so wie diese am besten passen – etwa jeden Tag zum Mittagessen. Sie können aber auch anstatt eines Zeitplans ein Ereignis wählen, etwa bei der *Arbeitsstationssperre*. Der Scan kann dann täglich, wöchentlich oder monatlich zu einer gewünschten Uhrzeit oder nach einem Ereignis erfolgen – genau so, wie Sie es möchten, Bild 8.

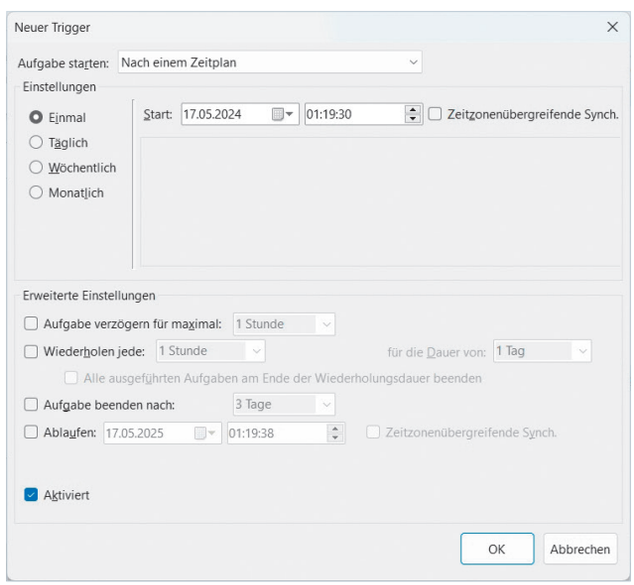

Bild 8: Wie oft und wann Sie die Scans starten wollen, bleibt Ihren Wünschen überlassen

Spezialprüfung

Sie sind der Meinung, im System stimmt etwas nicht und Sie bekommen das vermeintliche Problem nicht in den Griff? Normalerweise erhalten Sie in diesem Fall im Web oft Tipps, wie «Scannen Sie mit einem Boot-Stick». Einfacher, aber genau so sicher geht es so: Der Defender lässt sich in einem speziellen Offline-Modus starten. Dabei erfolgt ein Sicherheits-Scan noch vor dem Start des Windows-Systems. Auf diese Weise kann in der Regel keine bösartige Software bereits arbeiten und eine Erkennung oder Entfernung verhindern. Die Spezialprüfung starten Sie direkt aus Windows heraus: Geben Sie im Windows-Startfeld ein-

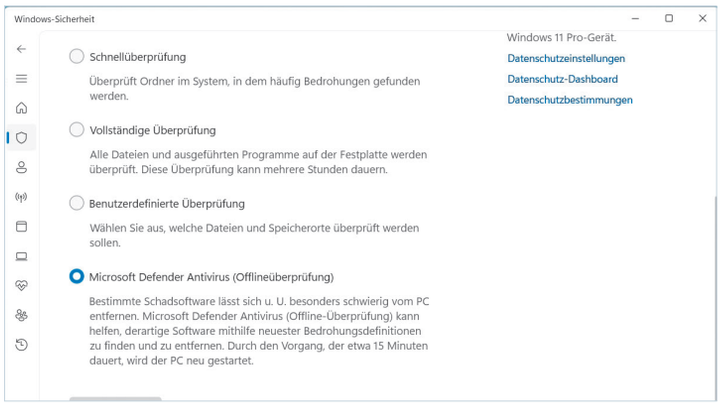

Bild 9: In einem Verdachtsfall ist ein Bootstick unnötig – nutzen Sie einfach *Microsoft Defender Antivirus (Offline-überprüfung)*

fach die bezeichnung `Viren- und Bedrohungsschutz` ein. Danach klicken Sie unter dem Eintrag *Aktuelle Bedrohungen* auf den Menüpunkt *Scanoptionen* und die Option *Microsoft Defender Antivirus (Offlineüberprüfung)*, Bild 9.

Anschliessend startet Windows neu in einem Untersuchungsmodus und scannt den Windows-Rechner. Der Scan dauert zwar etwa 15 bis 30 Minuten, allerdings wird nicht der gesamte Computer untersucht. Aber Malware im System oder Startbereich wird so gefunden und entfernt.

Leistungscheck

Die Leistung einer Schutz-Software wie dem Defender kann natürlich schwanken. Aber ob dem wirklich so ist, können Sie selbst prüfen. Das unabhängige Antiviren-Testlabor AV-Test untersucht im Zweimonatsrhythmus viele Schutz-Suiten für Windows und damit auch den Defender Antivirus. Ein kurzer Blick auf av-test.org/de/antivirus/privat-windows/hersteller/microsoft zeigt Ihnen schnell alle Testergebnisse der letzten Jahre in Zweimonatsschritten. So hat zum Beispiel der

Bild 10: Ist der Defender auf Dauer gut? Checken Sie die Testergebnisse kostenlos in der Langzeitübersicht bei av-test.org

Defender von Februar 2023 bis zum Februar 2024 bis auf einmal (5,5 Punkte) immer die vollen 6 Punkte in der wichtigen Testdisziplin *Schutzwirkung* erreicht. Damit liegt der Defender mit vielen Kaufprodukten gleich auf oder sogar darüber, Bild 10.

TIPP: Kernisolierung an oder aus?

Was bedeutet der Unterpunkt *Kernisolierung* in der *Windows-Sicherheit*? Wir erklären Ihnen, wie wichtig er für Ihre Sicherheit ist. Wird Windows neu installiert, ist dieser Punkt abgeschaltet. Wer keine anderen Systeme wie etwa Linux als zweites System auf dem gleichen PC installiert hat, sollte den zusätzlichen Schutz unbedingt aktivieren (erfordert einen Neustart), Bild 11.

Denn hinter dem Begriff *Kernisolierung* verbirgt sich ein Bündel an Optionen. So ist darin die *Speicher-Integrität* enthalten, die Windows-Prozesse vor der Einschleusung von bösartigem Code schützt. Aber die ist auch nicht sofort aktiv und sollte nachträglich aktiviert werden, Bild 12.

Weiterhin enthalten ist auch der *Hardware-gestützter Stapelschutz im Kernel-Modus*, der ebenfalls vor Codeeinschleusung schützt. Dann gibt es noch den *Schutz durch lokale Sicherheitsautorität*: Er schützt die Benutzeranmeldeinformationen und blockiert das Laden von nicht-signierten Treibern. Der *Microsoft Defender Credential Guard* schützt die Kontoanmeldedaten von Windows vor Angriffen. Der letzte Punkt *Microsoft-Sperrliste gefährdeter Treiber* blockiert Treiber, die mit einem falschen Zertifikat ausgestattet wurden.

Hinweis: Einige der Optionen sind nach dem Einschalten der *Kernisolierung* nicht verfügbar, da sie von Hardware-Komponenten und Optionen im UEFI-Bios oder der Prozessormarke abhängig sind.

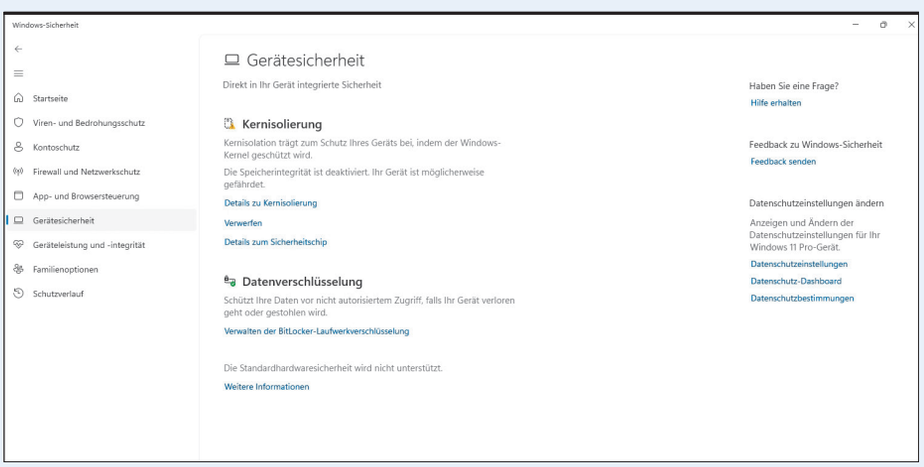

Bild 11: Sofern Sie kein anderes System, wie Linux installiert haben, sollten Sie die Kernisolierung aktivieren

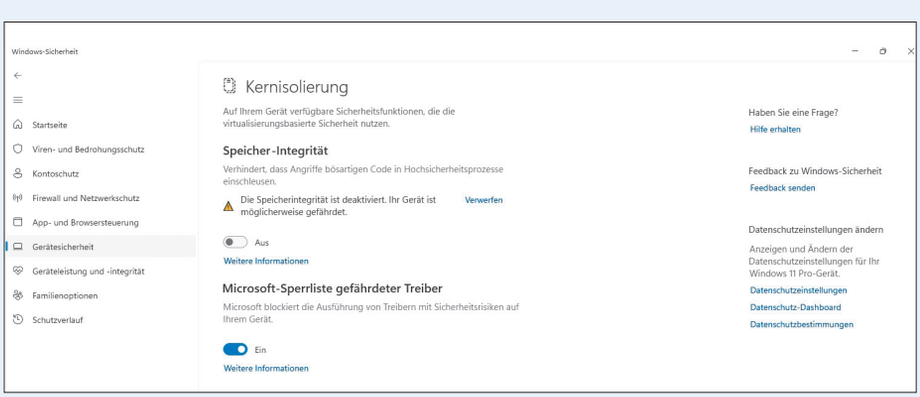

Bild 12: Obwohl die *Kernisolierung* in der *Windows-Sicherheit* aktiv ist, sind nicht alle Funktionen eingeschaltet