

Antiviren-Schutz muss sein! Aber kann das Prüfen denn nicht ein bisschen schneller gehen? Viele Anwender müssen immer minutenlang warten, bis ihr Windows endlich mal durchgestartet ist – wegen der Antiviren-Software. Oder der PC wird unglaublich langsam beim Herunterladen von Dateien oder beim E-Mail-Abruf. Schlimm wird das, wenn der PC schon etwas betagt ist und mit den aktuellen Antiviren-Programmen nicht so richtig klarkommt. Dann wird ein vernünftiges Arbeiten damit eventuell unmöglich. Wir zeigen Ihnen die richtigen Einstellungen, damit es doch schneller geht mit dem Viren-Check.

- Die Qual der Wahl: Welche Antiviren-Programme eignen sich besonders für ältere PCs? A 41/3
- Eine Frage der Konfiguration: Mehr Tempo ohne nennenswerte Sicherheitseinbußen A 41/4
- So tunen Sie Ihre Antiviren-Software A 41/6
- Scan-Module bis zum Abwinken: Welche Module benötigen Sie wirklich? A 41/9

Autor: **Christian Grugel**

**Ein falscher
Klick genügt**

Drei Tage Arbeit und mehrere Dutzend gelöschte private Fotos, Dokumente und E-Mails – so lautet die Bilanz von Jens T. nach der letzten Virenattacke. Eine Antiviren-Software hatte Herr T. bis dato nicht installiert. Damit sich dieser Albtraum beim frisch aufgesetzten Windows nicht gleich wiederholt, ist Jens T. bereit, einiges zu investieren: Für gut vierzig Euro erstet er eine leistungsfähige Antiviren-Software neuester Generation.

**Performance-
Killer: Antivi-
ren-Software**

Doch nach der Installation macht sich Enttäuschung breit: Windows reagiert plötzlich nur noch träge auf Mausklicks, das Öffnen von Dokumenten dauert eine Ewigkeit und der fortlaufend im Hintergrund aktive Virenwächter bremst sein System so stark aus, dass an ein produktives Arbeiten nicht mehr zu denken ist. „Was nutzt mir der beste Virenscanner, wenn die Performance von zwei Jahre alten PCs schon nicht mehr ausreicht, um produktiv mit dem System arbeiten zu können?“, denkt sich Herr T. frustriert.

**Der Preis der
Sicherheit**

So wie Herrn T. geht es vielen Anwendern: Die Notwendigkeit von Antiviren-Software ist zwar unbestritten, doch moderne Antiviren-Programme zehren doch arg an den Rechnerressourcen.

**Auf maximale
Sicherheit
getrimmt**

Ursache sind unter anderem die Standardeinstellungen der Antiviren-Programme: Viele Hersteller konfigurieren ihre Virenscanner ab Werk rigoros auf maximale Sicherheit, was wiederum aktuelle PC-Hardware voraussetzt, soll sich der PC nach der Installation noch einigermaßen flott bedienen lassen. Älteren PCs geht hier zumeist schnell die Luft aus.

**Balance zwi-
schen Sicher-
heit und Per-
formance**

Gefragt sind sinnvolle Kompromisse, die einerseits größtmöglichen Schutz versprechen und andererseits ein flüssiges Arbeiten ermöglichen. Schließlich steht beim PC immer noch die Funktion im Mittelpunkt und nicht die Sicherheit.

Die Qual der Wahl: Welche Antiviren-Programme eignen sich besonders für ältere PCs?



Hinsichtlich Arbeitstempo und Performance-Hunger zeigen sich bei den aktuell auf dem Markt befindlichen Antiviren-Lösungen zum Teil gravierende Unterschiede. Selbst Produkte mit vergleichbaren Scan-Leistungen erledigen ihre Arbeit zuweilen in sehr unterschiedlichen Geschwindigkeiten. Die Spannweite hinsichtlich der benötigten Zeit und Rechenleistung erreicht hier schnell den Faktor vier und höher.

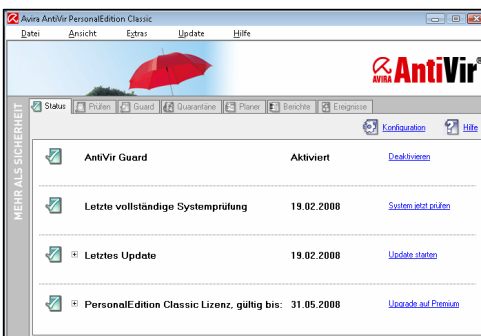
Deutliche Unterschiede

Besitzer älterer PCs sind daher gut beraten, bereits durch die geschickte Wahl des Virenschanners etwaigen Performance-Problemen frühzeitig vorzubeugen.

Performante Lösung wählen

Als schnelle und dennoch vergleichsweise zuverlässige Antiviren-Lösungen für etwas betagtere PCs haben sich in der Praxis „AntiVir Personal Edition Premium“ von Avira (www.avira.de) sowie „avast! Antivirus Professional Edition“ von Alwil (www.avast.com) erwiesen.

Schnelle Virenjäger



Avira AntiVir: Eine sinnvolle Alternative zu den sehr sicheren, aber leider auch extrem performance-hungrigen Scanner-Boliden von Gdata, F-Secure, Kaspersky und Bitdefender.



Kostenloser Schutz

Beide Produkte sind auch in einer kostenlosen Version verfügbar. Der „AntiVir Personal Edition Classic“ fehlten allerdings der E-Mail-Scanner sowie das Anti-Spyware-Modul. Bei der kostenlosen „avast! Antivirus Home Edition“ fallen die Unterschiede zur kommerziellen Version geringer aus.

Hier fehlen lediglich die erweiterten Funktionen der Benutzeroberfläche, ein spezieller Script-Blocker sowie der Kommandozeilen-Scanner. Der Hersteller wirbt bei der kommerziellen Version allerdings mit häufigeren Signatur-Updates.

Für eine Handvoll Euros

Sofern Sie sich für AntiVir entscheiden, empfiehlt sich der Griff zur kommerziellen Version, die mit 20 Euro vergleichsweise günstig zu bekommen ist.

Eine Frage der Konfiguration: Mehr Tempo ohne nennenswerte Sicherheitseinbußen

Scanner- Konfiguration anpassen

Was zunächst wie ein Widerspruch klingt, lässt sich bei genauerer Betrachtung mittels einer geschickten Anpassung der System- und Scanner-Konfiguration erreichen.

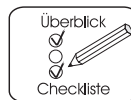
Mehrfachprü- fungen ver- meiden

Nicht selten passiert es, dass bestimmte Scans auf einem System gleich doppelt und dreifach ausgeführt werden, was unnötig Systemressourcen verbraucht und hinsichtlich der Systemsicherheit kaum Vorteile bringt.

Spezialpro- gramme oft obsolet

So ist es inzwischen nicht mehr erforderlich, neben modernen Antiviren-Lösungen zusätzlich Spezialprogramme wie „Spy-Bot – Search & Destroy“ oder „Lavasoft Ad-Aware“ zu installieren, die sich gezielt um die Beseitigung von Spy- und Adware kümmern. Alle gängigen Antiviren-Produkte übernehmen diese Aufgabe inzwischen ebenso zuverlässig wie ihre spezialisierten Pendants.

Einzigste Ausnahme sind bis dato Programme, die den PC auf Rootkits hin untersuchen, wie der kostenlose „F-Secure BlackLight Rootkit Eliminator“ (http://www.f-secure.com/security_center) oder der „RootkitRevealer“ von Sysinternals (<http://www.microsoft.com/germany/technet/sysinternals/utilities/RootkitRevealer.msp>). Hinsichtlich der Erkennung von Rootkits sind viele Virens Scanner noch auf beiden Augen blind.



Suche nach Rootkits

Besonders schnell passieren Mehrfachprüfungen auf Vista-Systemen. Grund: Nach der Installation ist „Windows-Defender“ standardmäßig aktiviert. Das Windows-Programm überwacht Ihren PC in Echtzeit auf Ad- und Spyware und schlägt Alarm, sobald es die Installation einer verdächtigen Datei bemerkt. Zusätzlich führt das Tool regelmäßige – in der Standardkonfiguration tägliche – Komplettskans des Systems durch.

Läuft Windows- Defender?

Läuft Windows-Defender parallel zu einem installierten Antiviren-Programm, werden Dateien gleich durch zwei Instanzen auf Ad- und Spyware gescannt. Dabei summieren sich nicht nur die Wartezeiten – prinzipiell können sich die Module auch gegenseitig in die Quere kommen.

Steigende Bearbeitungs- zeiten vorpro- grammiert

Allerdings ist der Nutzen von Windows-Defender als Schutz vor Ad- und Spyware eher mäßig: Das Programm erkennt deutlich weniger Schädlinge als gängige Antiviren-Lösungen, benötigt für seine Arbeit aber vergleichbar viel Zeit.

Beschränkter Nutzen

Haben Sie bereits ein Antiviren-Programm installiert, können Sie Windows-Defender daher getrost deaktivieren:

Windows- Defender deaktivieren

1. Öffnen Sie die „Systemsteuerung“ und starten Sie unter „Sicherheit/Windows-Defender“ die Konfigurationsoberfläche des Programms.

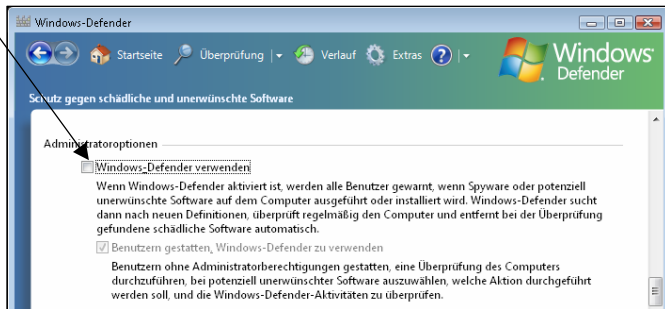
Die „Optionen“ öffnen

2. Klicken Sie in der oberen Symbolleiste auf „Extras“ und anschließend unter der Rubrik „Einstellungen“ auf „Optionen“.

Konfiguration anpassen

3. Scrollen Sie an das untere Ende der angezeigten Seite, entfernen Sie unter der Rubrik „Administratoroptionen“ das Häkchen vor „Windows-Defender verwenden“ und bestätigen Sie die Änderung mit einem Klick auf „Speichern“.

Hier deaktivieren Sie Windows-Defender mit nur einem Mausklick.



Eine installierte Antiviren-Software vorausgesetzt, können Sie Windows-Defender getrost deaktivieren und Ihr System so nachhaltig entlasten.

So tun Sie Ihre Antiviren-Software

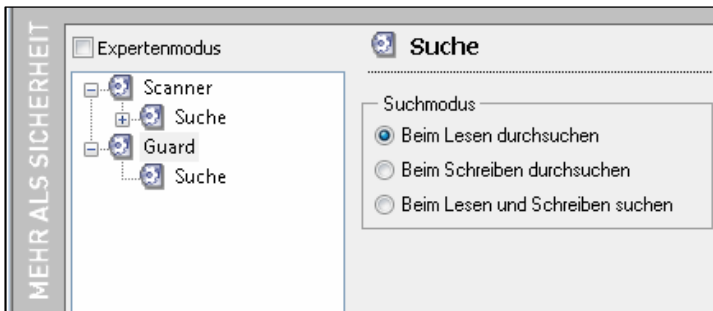
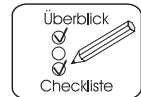
Performance-Bremse: Hintergrundwächter

Bremst das Antiviren-Programm Ihren PC im Alltag über Gebühr aus, liegt dies meist am Echtzeitschutz.

Die Hintergrundwächter sind ab Werk häufig so vorkonfiguriert, dass Dateien nicht nur beim Öffnen, sondern auch beim anschließenden Zurückschreiben auf die Festplatte nach Viren und anderen Schädlingen untersucht werden.

Der Sicherheitsvorteil dieser doppelten Prüfung ist hingegen

marginal. Die Wartezeit lässt sich daher ruhigen Gewissens um die Hälfte reduzieren, indem Sie die Prüfung auf den Lesevorgang beschränken.



In der Regel reicht es völlig aus, wenn die Antiviren-Software Dateien nur beim Lesen auf Viren hin überprüft.

Falls ein produktives Arbeiten mit dem System nach wie vor an mangelnder Performance scheitert, bietet es sich in einem zweiten Schritt an, die untersuchten Dateitypen einzugrenzen.

Den Echtzeit-Scan eingrenzen

Zwar ist es unbestritten die sicherste Methode, stets alle Dateien durch den Wächter prüfen zu lassen, aber bevor Sie den Wächter allenthalben in den Pause-Modus versetzen, um beispielsweise größere Kopieraktionen zügig durchführen zu können, ist es sicherlich sinnvoll, den Prüfungsvorgang stattdessen zu beschleunigen, indem Sie diesen auf bestimmte besonders gefährdete Dateitypen eingrenzen.

Besser gezielt prüfen als gar nicht

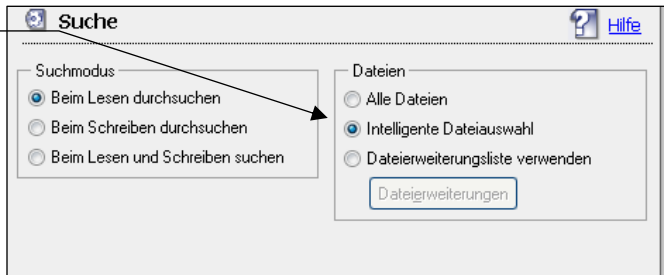
Hinzu kommt, dass viele Hersteller von sich aus entsprechend vorkonfigurierte Listen innerhalb der Programmkonfiguration bereitstellen, die sich bei der Suche auf die erfahrungsgemäß häufig als Virenträger missbrauchten Dateiformate beschränken.

Nutzen Sie den Service der Hersteller

Automatische Aktualisierung

Meist werden diese Listen von den Herstellern automatisch aktualisiert, sodass sich der Konfigurationsaufwand in aller Regel auf einen Klick an der richtigen Stelle beschränkt.

Die „Intelligente Dateiauswahl“ beschleunigt die Echtzeitprüfung.



Der Einstellung „Intelligente Dateiauswahl“ liegt eine vom Hersteller gepflegte Liste mit potenziell risikobehafteten Dateitypen zugrunde. So lässt sich die Echtzeitprüfung gegenüber der Einstellung „Alle Dateien“ deutlich beschleunigen, ohne ein allzu großes Sicherheitsrisiko einzugehen.

Archive von der Echtzeitprüfung ausnehmen

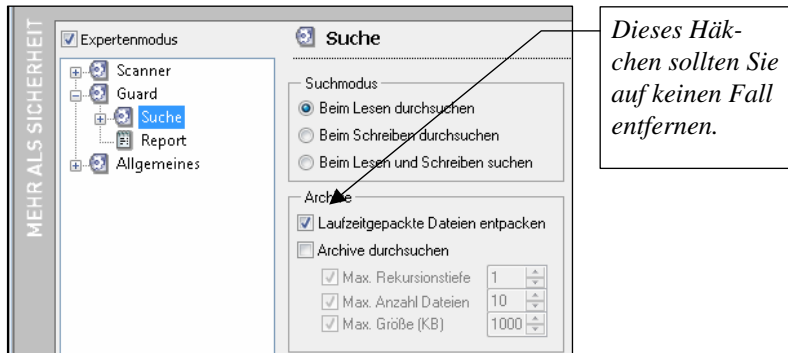
Weitere Rechenzeit lässt sich einsparen, wenn Sie die automatische Überprüfung von gepackten Dateiarchiven deaktivieren – schließlich müssen Sie die Archive zunächst einmal entpacken, bevor ein eventuell enthaltener Schädling aktiv werden kann. Und spätestens beim Entpacken würde der Hintergrundwächter ohnehin Alarm schlagen.

Vorsicht beim Weiterleiten

Einziger Nachteil: Leiten Sie Archive ungeprüft an Dritte weiter, kann es sein, dass Sie eventuell bei der Verbreitung enthaltener Schädlinge helfen.

Ausnahme: Laufzeitgepackte Archive

Einzige Ausnahme sind sogenannte laufzeitgepackte Archive. Das sind Archive in Form ausführbarer Dateien, die beim Öffnen zunächst in den Speicher geladen und dort direkt entpackt und ausgeführt werden.



Vorsicht: Die Überprüfung laufzeitgepackter Archive (Option: „Laufzeitgepackte Dateien entpacken“) sollten Sie tunlichst eingeschaltet lassen. Ansonsten steigt das Risiko, sich einen neuen Schädling einzufangen, beträchtlich.

Als Kompromiss bietet es sich an, stattdessen bei den regelmäßigen Komplettskans alle Dateitypen und Archive mit maximaler Suchtiefe prüfen zu lassen. Eine geschickte Wahl des Überprüfungszeitpunkts vorausgesetzt, ist es dann kaum entscheidend, ob der Komplettskan nun eine oder zwei Stunden benötigt.

Scan-Module bis zum Abwinken: Welche Module benötigen Sie wirklich?

Moderne Antiviren-Programme installieren meist einen ganzen Schwung spezieller Scan-Module, angefangen vom E-Mail-Modul über Netzwerk- und P2P-Modul sowie Scanner, die speziell auf die Überwachung von Instant-Messenger-Programmen zugeschnitten sind.

Insbesondere auf nicht mehr ganz taufrischen Systemen lohnt daher ein prüfender Blick, welche Module auf Ihrem System überhaupt sinnvoll einsetzbar sind und welche Sie zugunsten

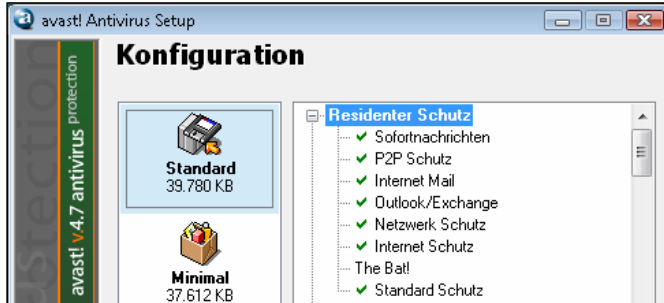
Intensive Prüfung bei Komplettskans

Spezialisierte Scan-Module

Überflüssige Module deaktivieren



einer höheren System-Performance getrost deaktivieren können.



Beispiel „avast! Antivirus Setup“: In der Standardkonfiguration verrichten nicht weniger als sieben Scan-Module ihren Dienst.

Surfen in der Sandbox

Auf Vista-Systemen ist beispielsweise der „Internet Schutz“ obsolet, sofern Sie mit dem Internet Explorer 7 surfen. Grund: Ist die Option „Geschützter Modus“ im Browser aktiviert, läuft dieser inklusive sämtlicher Erweiterungen in einer Sandbox, abgeschottet vom Rest des Systems. Etwaige virenverseuchte Downloads meldet hingegen auch der „Standard Schutz“.

Sandbox-Programme nutzen

Prinzipiell sind Sandbox-Programme wie „Sandboxie“ (www.sandboxie.com) eine sinnvolle und im Vergleich zu Scan-Modulen vor allem performante Alternative, um E-Mail-, Instant-Messenger- oder Tauschbörsenprogramme abgeschottet vom System zu betreiben.

Systemschutz auf Mausclick

Das verhindert zwar prinzipiell nicht, dass sich Viren einschleichen können, aber schlägt der Hintergrundwächter Alarm oder meldet der nächste Komplettscan einen Virenfund, genügt ein Mausclick, und der Spuk hat ein Ende.