



Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

3 Sind Ihre Windows-Systemdateien infiziert?

Fiese Schadprogramme verändern Ihr Windows-System. Entfernen Sie die Störenfriede. Erst danach ist Ihr PC wieder sicher.

4 Finden Sie Schadprogramme im Speicher

Mit meinem Spezial-Antiviren-Tool für den Arbeitsspeicher finden Sie alle schädlichen Prozesse. Ihr PC ist störungsfrei.

6 Soforthilfe: So stoppen Sie PC-Spionage

Stöbern Sie unerwünschte Spionageprogramme auf und löschen Sie sie mit einem Mausklick.

7 Störende Programme komplett ausschalten

Meine Schutzgarantie: Mit meinem Tool löschen Sie diese fiesen Programme und Ihr PC ist frei von Schadprogrammen.

+++ Keine Angst vor den neuen Gefahren im Jahr 2019: So vernichten Sie fiese Schadprogramme zuverlässig +++

Schützt Sie Windows 10 gut genug vor Schadprogrammen?

Windows 10 ist das bisher sicherste Betriebssystem von Microsoft. Zusätzlich zu zahlreichen neuen Schutzfunktionen ist das Antiviren-Programm Windows Defender enthalten.

Es schützt Sie nach dem derzeitigen Stand optimal vor Schadprogrammen und ist laut dem Prüfinstitut AV-Test ein „Top-Produkt“.

Sie brauchen also als Windows-10-Anwender kein teures Fremdprogramm mehr. Völlig sicher sind Sie aber auch mit Windows Defender nicht. Jedes Antiviren-Programm lässt sich überlisten.

Meine Empfehlung: Verlassen Sie sich nicht auf Ihr Antiviren-Programm, sondern führen Sie zusätzlich meine 7 Sicherheitskontrollen aus diesem Leitfaden aus, um kein Risiko einzugehen.

Diese Kontrollen sind besonders dann wichtig, wenn sich Ihr PC verdächtig verhält, also zum Beispiel auffällig viel Werbung anzeigt oder sehr langsam arbeitet.



Viele Grüße, Ihr

Michael-Alexander
Beisecker,
Deutschlands

PC-Sicherheitsexperte Nr. 1

Führen Sie diese Kontrollen mindestens einmal im Monat durch

Spüren Sie mit nur 7 Kontrollen alle verborgenen Schadprogramme auf

Das Jahr 2018 ist noch nicht zu Ende, da bieten Ihnen die Hersteller von Antiviren-Programmen schon die neuen Versionen für 2019 an. Diese neuen Antiviren-Programme sollen neue, heute noch nicht bekannte Schadprogrammtypen besser erkennen. Verlassen Sie sich aber nicht allein darauf, sondern machen Sie sich zum Schutz Ihres PCs mit den folgenden 7 Kontrollschritten vertraut und führen Sie diese ab sofort regelmäßig aus.

Vereiteln Sie die Angriffe der neuen Schadprogramm-Generationen schon von Anfang an konsequent, indem Sie in Kontrollschritt 1 deren Start verhindern. Wurde Ihr Windows-System bereits verändert, erkennen Sie das in Kontrollschritt 2.

Haben Sie einen besonders raffinierten Gegner, der trotz aller Ihrer Bemühungen noch handlungsfähig ist, kappen Sie seine Wurzeln. Sie finden und beenden die Schadprogramm-Prozesse in Kontrollschritt 3. Jetzt wird Ihr Antiviren-Programm nicht mehr getäuscht und erkennt in Kontrollschritt 4 plötzlich Schadprogramme, die sich vielleicht schon wochenlang auf Ihrem PC versteckt hielten.

In den zusätzlichen Kontrollschritten 5 bis 7 erfahren Sie, wie gut Ihr Antiviren-Programm Sie wirklich schützt. Sie werden überrascht sein, was in diesen Kontrollen noch an unerwünschten Schadroutinen gefunden wird.

Mit diesen 7 Kontrollschritten erreichen Sie Ihr Ziel eines schadprogrammfreien PCs





- | | |
|--------------------|---|
| Kontrollschritt 1: | Hindern Sie potenzielle Schadprogramme am Start (siehe Seite 2). |
| Kontrollschritt 2: | Entfernen Sie potenzielle Schadprogramme in Windows (siehe Seite 3). |
| Kontrollschritt 3: | Stoppen Sie verdächtige Schadprogramm-Prozesse (siehe Seite 4). |
| Kontrollschritt 4: | Scannen Sie die gesamte Festplatte mit Ihrem Antiviren-Programm (siehe Seite 5). |
| Kontrollschritt 5: | Finden und entfernen Sie Werbeprogramme mit dem Tool The PC Decrapifier (siehe Seite 6). |
| Kontrollschritt 6: | Finden Sie mit dem Tool Malwarebytes AdwCleaner nicht gemeldete unerwünschte Programme (siehe Seite 7). |
| Kontrollschritt 7: | Holen Sie noch eine dritte Sicherheitsmeinung mit HitmanPro.EU-Cleaner ein (siehe Seite 8). |

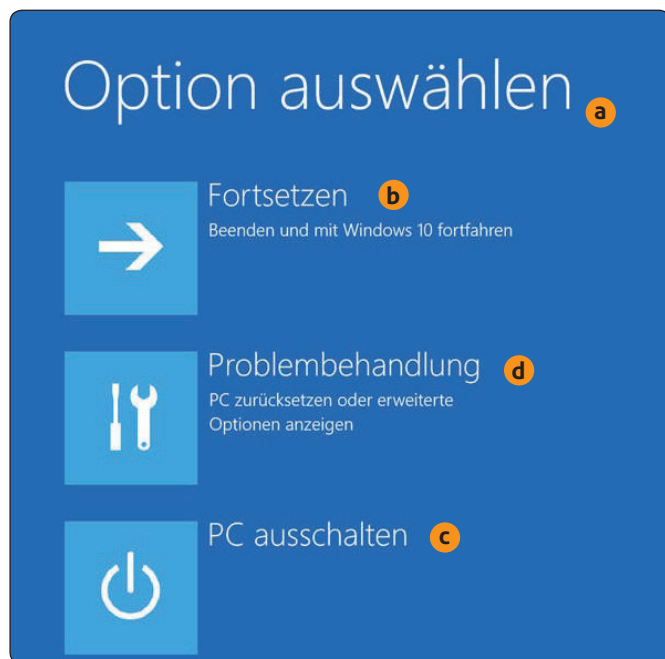
Meine Garantie: Nehmen Sie sich einmal im Monat die Zeit und überprüfen Sie Ihr PC-System anhand dieser 7 Kontrollschritte. Sie benötigen nicht länger als 60 Minuten und erhalten dafür einen sicheren PC.

>>> Lesen Sie bitte weiter auf Seite 2



Kontrollschritt 1: Hindern Sie potenzielle Schadprogramme am Start



Als mich Herr Peters, ein langjähriger Leser und seit Jahrzehnten erfahrener PC-Anwender um Hilfe bat, war ich sehr erstaunt. Ich fand 17 Schadprogramme auf seinem PC, ohne dass sein Antiviren-Programm auch nur ein Schadprogramm gemeldet hätte. Ein Tarnkappen-Virus hatte sein Antiviren-Programm getäuscht und anschließend über ein Dutzend weitere Schadprogramme installiert. Doch solche Schadprogramme haben eine Schwachstelle, an der Sie sie mit meiner Hilfe packen und vernichten: Denn im abgesicherten Modus funktioniert der Tarnmechanismus nicht und Ihr Antiviren-Programm kann die Schadprogramme leichter erkennen und meist restlos entfernen. Starten Sie Ihren PC daher im abgesicherten Modus.


1. Entfernen Sie von Ihrem PC alle Wechseldatenträger wie z. B. eine eingelegte Diskette, CD oder DVD, angesteckte USB-Sticks, Speicherkarten-Lesegeräte oder eingelegte Speicherkarten.
2. Öffnen Sie das **Start**-Menü  und klicken Sie auf das **Ein/Aus**-Symbol . Drücken Sie die Umschalttaste  und halten Sie diese gedrückt, während Sie auf **Neu starten** klicken. Warten Sie ab, bis der Bildschirm **Option auswählen**  erscheint.



In diesem Dialog rufen Sie die **Problembehandlung** auf.

Hinweis: Haben Sie diesen Bildschirm versehentlich geöffnet, gelangen Sie mit **Fortsetzen**  wieder zu Windows 10 zurück und mit **PC ausschalten**  wird Ihr Rechner vollständig heruntergefahren.

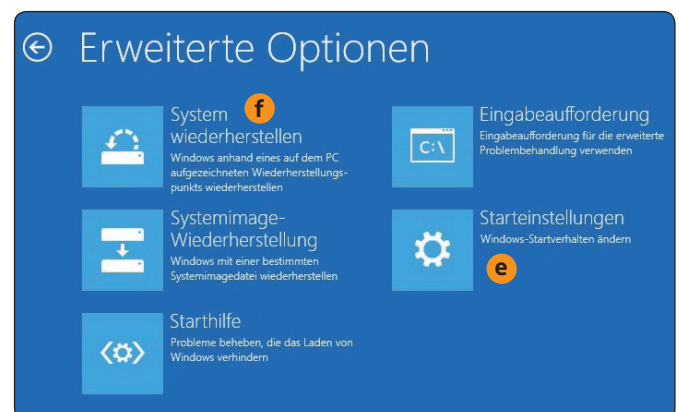
3. Klicken Sie im Bildschirm **Option auswählen** auf **Problembehandlung**  und im nächsten Bildschirm auf **Erweiterte Optionen**. Hier wählen Sie **Starteinstellungen**  und **Neu starten**. Dann drücken Sie die Taste **[F5]** für die Option **Abgesicherten Modus mit Netzwerktreibern aktivieren**, damit ein Internet-Zugriff möglich bleibt.

Hinweis: Wurde Windows 10 durch ein Schadprogramm irreparabel beschädigt, können Sie es mit **System wiederherstellen**  auf den Auslieferungszustand zurücksetzen oder mit **Systemimage-Wiederherstellung** Ihre Sicherung der Systempartition zurückkopieren.



Mein Tipp: Lässt sich Windows nach dem Angriff eines Schadprogramms nicht mehr bedienen, schalten Sie Ihren PC aus, indem Sie den **Ein-/Aus**-Taster an der Vorderseite ca. 8 Sekunden gedrückt halten. Ihr PC schaltet sich daraufhin aus. Dann starten Sie Ihren PC neu und drücken sofort mehrfach die Tastenkombination **[Strg]+[F8]**.

Treten beim Hochfahren im abgesicherten Modus Schwierigkeiten auf, helfen Ihnen meine Mitarbeiter aus der Redaktion und ich gern über den Computerwissen Club: <https://club.computerwissen.de>.



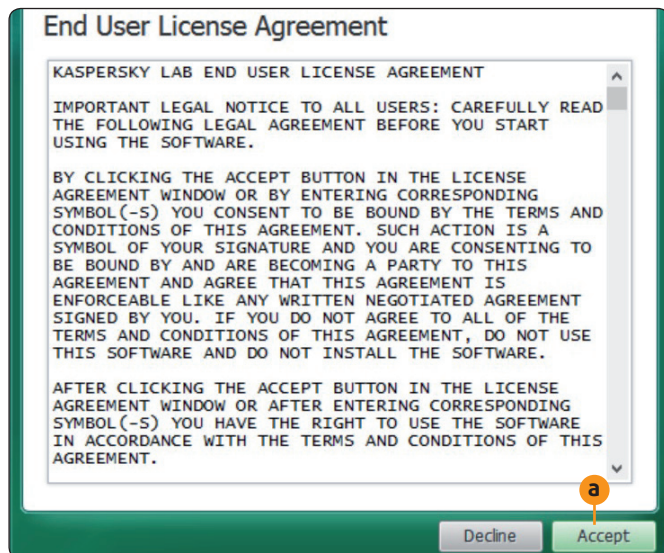
Über die **Starteinstellungen** aktivieren Sie den **abgesicherten Modus**.

Fazit: Ihr Windows ist jetzt im abgesicherten Modus gestartet, in dem keine Schadprogramme mehr aktiv sein sollten. Doch darauf sollten Sie sich nicht verlassen. Daher führen Sie in diesem sicheren Modus nun noch die Kontrollschritte 2 und 3 aus. Nur dann sind Sie sicher, dass Sie beim Entfernen der Schadprogramme nichts übersehen und Ihr PC nicht doch von noch aktiven Schadprogrammen manipuliert wird.

Kontrollschritt 2: Entfernen Sie potenzielle Schadprogramme in Windows

Bei meinem Nachbar Achim wurde der PC über Wochen immer langsamer, bis er mich schließlich fragte, ob er einen neuen PC braucht. Sein Antiviren-Programm meldete kein Schadprogramm. Als ich den PC genauer untersuchte, fand ich veränderte Windows-Systemdateien. Rootkits waren in den Kern von Windows vorgedrungen und konnten das Antiviren-Programm dadurch täuschen. Zum Erkennen von Rootkits gibt es spezielle Antiviren-Programme. Ich empfehle Ihnen den Einsatz des kostenlosen Kaspersky TDSSKiller.

1. Laden Sie das Tool **Kaspersky TDSSKiller** über unsere sichere Service-Webseite www.pc-sicherheitsberater.de herunter.
2. Danach starten Sie das heruntergeladene Programm **tdsskiller.exe** und bestätigen die Nachfrage der Benutzerkontensteuerung mit **Ja** und die Lizenzbedingungen von Kaspersky sowie das **KSN Statement** mit **Accept** (Akzeptieren) **a**.



Sie können diese Lizenzbedingungen unbesorgt bestätigen, sie enthalten keine Formulierungen, die Ihre Sicherheit oder Privatsphäre beeinträchtigen.

3. Klicken Sie auf **Change Parameters**, um die Einstellungen von TDSSKiller zu ändern. Setzen Sie einen Haken bei **Detect TDLFS file system** (TDLFS-Dateisystem erkennen) und bei **Loaded Modules** (Geladene Schadprogramm-Module). Klicken Sie dann auf **Reboot now** (Jetzt neu starten). Ihr PC wird neu gestartet und es wird der erforderliche Treiber installiert.
4. Sobald Ihr PC neu startet, drücken Sie noch vor dem Windows-Boot-Vorgang wiederholt **(Strg)+(F8)**, um wieder

im abgesicherten Modus zu starten (siehe Kontrollschritt 1).

5. Rufen Sie TDSSKiller erneut auf (siehe Schritt 2) und klicken Sie auf **Start scan**, damit Ihr PC überprüft wird. Die Prüfung dauert weniger als eine Minute.



*Ihr Rootkits-Check: Steht hinter **Processed** (Verarbeitet) die Meldung **no threats found** **b**, wurden keine Schadprogramme gefunden und Sie können mit Kontrollschritt 3 weitermachen.*

6. Meldet Ihnen Kaspersky TDSSKiller in roter Schrift Schadprogramme, löschen Sie diese einzeln über **Delete** (Löschen) oder nehmen sie mit **Cure** (Behandeln) in Quarantäne.
7. Ist Ihnen das einzelne Löschen der Schadprogramme zu umständlich, klicken Sie unten rechts auf **Continue** (Weiter). Kaspersky TDSSKiller entfernt jetzt automatisch alle angezeigten Schadprogramme.

Gehen Sie kein Risiko ein, wenn TDSSKiller Schadprogramme gefunden hat. Selbst wenn TDSSKiller die Schadprogramme restlos entfernt, ist Ihr Windows-System beschädigt und damit nicht mehr zuverlässig. Es können auch noch Backdoors (Hintertüren) bestehen, über die wieder neue Schadprogramme einfallen. Beachten Sie daher meine Empfehlung, damit Sie eine zeitaufwändige Windows-Neuinstallation sparen.

Meine Empfehlung: Retten Sie Ihre Windows-Installation nach einem erkannten Rootkit-Schadprogramm, indem Sie es über den Bildschirm **Erweiterte Optionen** und **System wiederherstellen** oder **Systemimage-Wiederherstellung** erneut von allen Schadprogrammen befreien (siehe Bild 2 auf Seite 2).

LESERSERVICE


Redaktionshilfe: Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

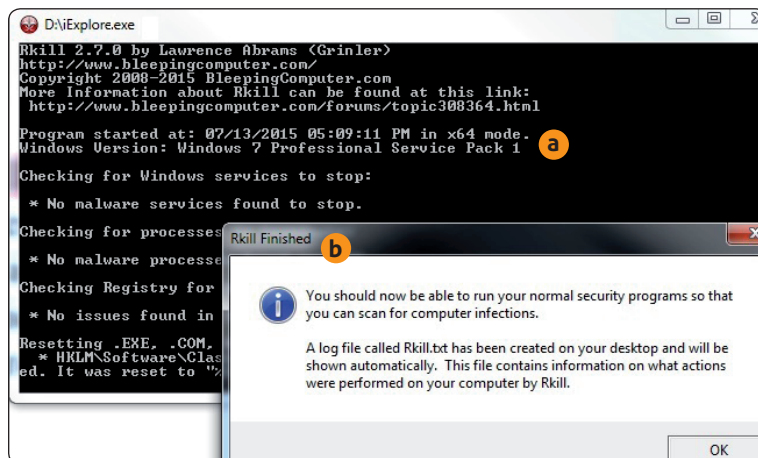
Melden Sie sich dazu einfach kostenlos unter <https://club.computerwissen.de> an und stellen Sie ihm dort Ihre Fragen.

Michael-Alexander Beisecker und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

Kontrollschritt 3: Stoppen Sie verdächtige Schadprogramm-Prozesse

Sie haben bereits mit Kontrollschritt 1 die automatisch gestarteten Schadprogramme gestoppt und im Kontrollschritt 2 Ihr Windows-System auf Rootkits überprüft. Nun überprüfen Sie mit dem Tool RKill noch die laufenden Programme, um ganz sicher zu sein, dass aktuell keine schädlichen Aktivitäten mehr stattfinden.

1. Laden Sie das Tool **RKill** über unsere sichere Service-Webseite www.pc-sicherheitsberater.de herunter.
2. Öffnen Sie mit **(Strg)+[J]** die Download-Liste Ihres Browsers und starten Sie das heruntergeladene Programm **rkill-unsigned.exe**. Bestätigen Sie der Benutzerkontensteuerung per Klick auf **Ja**, dass das Programm ausgeführt werden soll.
3. Das Tool **rkill-unsigned.exe** wird automatisch an der Eingabeaufforderung ausgeführt und meldet Ihnen die Ergebnisse seiner Überprüfung **a** (siehe auch Tabelle unten).
4. Der Dialog **Rkill Finished** **b** (Rkill beendet) erscheint und die vorhandenen, gefährlichen Prozesse sind beendet. Klicken Sie auf **OK**. Schauen Sie zuvor jedoch erst einmal in den Bericht von RKill und sehen Sie nach, ob hier Hinweise auf Schadprogramme zu finden sind.
5. Nach dem Ausführen von RKill sehen Sie in der Taskleiste das **Editor-Symbol** . Klicken Sie darauf,



Im Dialog **Rkill Finished** **b** wird Ihnen mitgeteilt, dass Sie jetzt Ihr Antiviren-Programm aufrufen können (Kontrollschritt 4).



wird die Datei **rkill.txt** mit dem Überprüfungsbericht angezeigt. Finden Sie hier bedrohlich erscheinende Meldungen wie gefundene Schadprogramm-Dienste, Prozesse oder Registry-Einträge, laden Sie die Textdatei beim Computerwissen Club hoch. Meine Mitarbeiter aus der Redaktion und ich helfen Ihnen gern weiter: <https://club.computerwissen.de>.

RKill-Meldung	Deutsche Übersetzung	Dieses Ergebnis bedeutet: Keine Gefahr für Ihren PC
Checking for Windows services to stop	Es wird überprüft, ob Windows-Dienste gestoppt werden müssen.	* No malware services found to stop. = Keine Schadprogramm-Dienste gefunden, die gestoppt werden müssten.
Checking for processes to terminate	Es wird überprüft, ob schädliche Prozesse zu unterbrechen sind.	* No malware processes found to kill. = Keine Schadprogramm-Prozesse gefunden, die gestoppt werden müssen.
Checking Registry for malware related settings	Es wird überprüft, ob die Registrierungsdatenbank von Windows (Registry) schädliche Einstellungen enthält.	* No issues found in the Registry. = Keine schädlichen Einträge in der Registry gefunden.
Performing miscellaneous checks	Es werden verschiedene Prüfungen durchgeführt.	* Windows Defender Disabled. = Windows Defender wurde deaktiviert. Haben Sie ein anderes Antiviren-Programm installiert, wird Windows Defender automatisch deaktiviert.
Checking Windows Service Integrity	Die Windows-Dienste werden auf Vollständigkeit geprüft.	* Dienstname [Missing Service]. = Dienstname [fehlender Dienst]. Überprüfen Sie, welche Aufgabe dieser Dienst hat und ob er für die Sicherheit wichtig ist.
Searching for Missing Digital Signatures	Es wird nach fehlenden digitalen Signaturen gesucht.	* No issues found. = Keine fehlenden Signaturen gefunden.
Checking HOSTS file	Die HOSTS-Datei wird überprüft.	* HOSTS file entries found: = „HOSTS“-Dateieintrag gefunden: 127.0.0.1 localhost. Die Adresse 127.0.0.1 ist die Adresse, unter der sich Ihr PC selbst erreichen kann und damit harmlos. Alle anderen Einträge sollten durch Aufruf der angegebenen IP-Adresse überprüft werden.

Vergleichen Sie die Muster-Meldungen in der dritten Spalte mit den Ergebnissen aus Ihrem RKill-Bericht. So wissen Sie, ob Schadprogramm-Aktivitäten gefunden wurden und welcher Art diese sind.

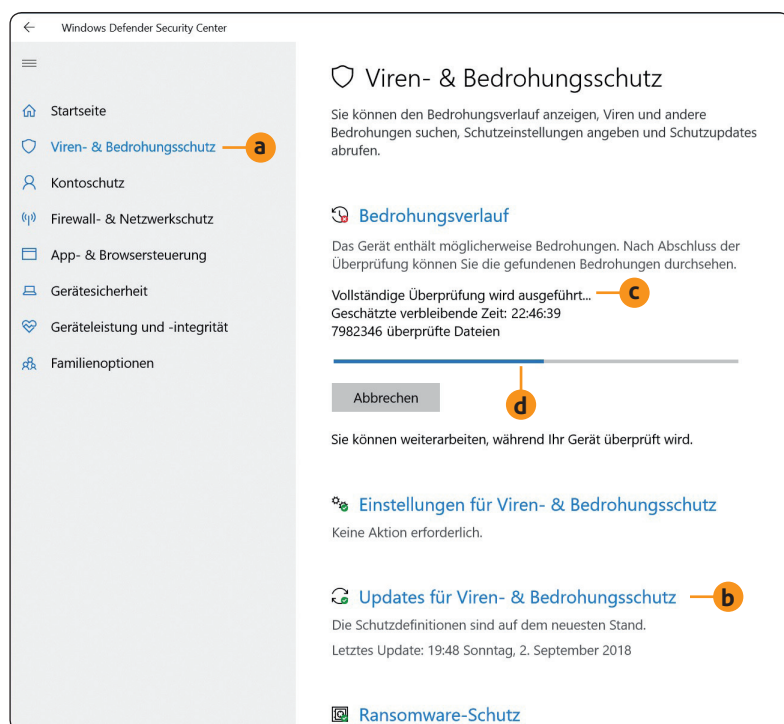
Kontrollschritt 4: Scannen Sie die gesamte Festplatte mit Ihrem Antiviren-Programm

Mit den ersten 3 Kontrollschritten haben Sie alle Hindernisse aus dem Weg geräumt, die verhindern, dass Ihr Antiviren-Programm auch Schadprogramme mit Abwehr- und Tarnfunktionen erkennt. Überprüfen Sie daher mit Ihrem Antiviren-Programm nun gründlich die Festplatte Ihres PCs. Das kann mehrere Stunden dauern. Haben Sie einen leistungsstarken PC, können Sie ihn parallel weiter nutzen. Andernfalls lassen Sie diese Kontrolle über Nacht laufen, dann verlieren Sie keine Zeit.

1. Rufen Sie Ihr Antiviren-Programm auf, also zum Beispiel das zusammen mit Windows 10 gelieferte Windows Defender: Öffnen Sie das **Start-Menü**  und klicken Sie auf das **Zahnrad-Symbol** . Wählen Sie **Update und Sicherheit**, links das Register **Windows-Sicherheit** und klicken Sie rechts auf **Windows Defender Security Center öffnen**.
2. Überprüfen Sie, ob die aktuellen Virensignaturen vorhanden sind, und führen Sie bei Bedarf ein Update durch. Dazu klicken Sie bei Windows Defender auf **Viren & Bedrohungsschutz** **a**, **Updates für Viren- & Bedrohungsschutz** **b** und **Nach Updates suchen**. Warten Sie, bis die Suche beendet ist. Die Updates sind dann installiert.
3. Rufen Sie die Funktion für den Virenschutz auf und starten Sie die Rechnerprüfung. Bei Windows Defender klicken Sie zum Beispiel links auf das Register **Viren & Bedrohungsschutz** und dann auf den Link **Neue erweiterte Überprüfung ausführen**. Lassen Sie die Option **Vollständige Überprüfung** aktiviert und klicken Sie auf die graue Schaltfläche **Jetzt überprüfen**.
4. Warten Sie das Ende der Prüfung ab. Die Dauer der Überprüfung hängt vom verwendeten Programm, der Anzahl der zu überprüfenden Dateien und der Rechnerleistung ab. Sie kann mehrere Stunden betragen, wundern Sie sich also nicht. Windows Defender zeigt Ihnen die geschätzte Überprüfungszeit an **c**, sodass Sie in der Zwischenzeit etwas anderes tun und danach an den PC zurückkehren können.
5. Findet Ihr Antiviren-Programm während der Überprüfung Schadprogramme, lassen Sie diese entfernen.



Mein Tipp: Ihr Antiviren-Programm fragt Sie bei Schadprogramm-Dateien womöglich, ob Sie diese löschen oder in Quarantäne verschieben möchten. Entscheiden Sie sich für die Quarantäne. Antiviren-Programme haben gelegentlich Fehlalarme und markieren fälschlich wichtige Dateien. Im Fall eines Irrtums lassen Sie sich die Dateien in der Quarantäne anzeigen und holen die betreffende Datei wieder heraus.



Während Windows Defender Ihren PC gründlich untersucht, zeigt Ihnen ein Fortschrittsbalken **d** den Verlauf an.

6. Kontrollieren Sie zum Abschluss auch die Sicherheitseinstellungen Ihres Antiviren-Programms. Im Fall von Windows Defender ist diese Kontrolle ganz einfach. Windows Defender informiert Sie mit der Meldung **Keine Aktion erforderlich**, wenn Sie sichere Einstellungen gewählt haben. Sollte eine Einstellung nicht sicher genug sein, werden Sie darauf hingewiesen.

Meine Empfehlung: Haben Sie Windows Defender durch ein anderes Antiviren-Programm ersetzt? Überprüfen Sie bei diesem Antiviren-Programm, ob die vorhandenen Sicherheitsfunktionen vollständig aktiviert sind. Solche Funktionen sind zum Beispiel das Überprüfen von Downloads und E-Mail-Anhängen sowie das Melden potenziell unerwünschter Programme. Haben Sie Fragen zu Einstellungen, helfen Ihnen meine Mitarbeiter aus der Redaktion und ich gerne über den Computerwissen Club: <https://club.computerwissen.de>.

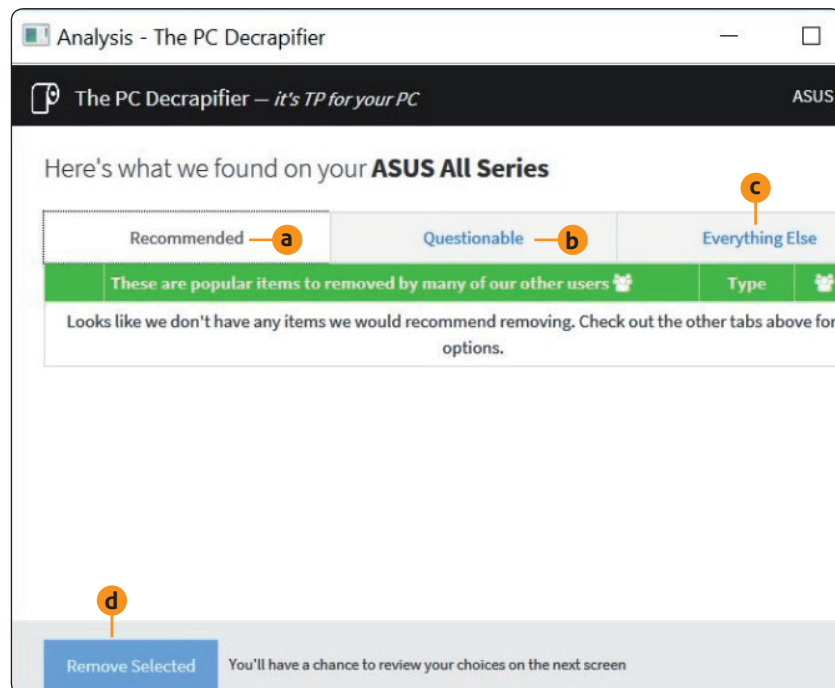
Kontrollschritt 5: Finden und entfernen Sie Werbeprogramme mit dem Tool The PC Decrapifier

Untersuchen Sie Ihren PC jetzt noch auf unerwünschte Werbe- und Spionage-Programme, die auf neuen PCs sogar schon vorinstalliert sind. Häufig sind zum Beispiel mindestens ein Antiviren-Programm, Programme zur Datensicherung und Dokumentenverwaltung, Update-Programme und sogar Spionageprogramme vorhanden, dazu kostenpflichtige Zugänge zu Musik- und Videoportalen. Je länger Sie Ihren PC nutzen, umso mehr dieser Programm-Parasiten gelangen über Download-Portale, Installationsprogramme und kostenlose Tools auf Ihren PC. Diese Werbeprogramme sind so gut wie raffinierte Schadprogramme versteckt und ohne Hilfsmittel kaum zu finden. Daher rate ich Ihnen zu einer Kontrolle mit dem Tool The PC Decrapifier.

1. Laden Sie die kostenlose Free-Version von **The PC-Decrapifier** über unsere sichere Service-Webseite ganz bequem herunter: www.pc-sicherheitsberater.de.
2. Öffnen Sie mit **[Strg]+[J]** die Download-Liste Ihres Browsers und starten Sie danach das heruntergeladene Programm **pc-decrapifier-Versionsnummer.exe**, wobei **Versionsnummer** für die aktuelle Version steht.
3. Bestätigen Sie die Nachfrage der **Benutzerkontensteuerung** mit **Ja** und The PC Decrapifier startet sofort ohne Installation.
4. Klicken Sie auf **Analyze** – danach untersucht das Tool Ihren PC. Die Programme auf Ihrem PC werden in drei Register einsortiert: **Recommended** **a** (Entfernen empfohlen), **Questionable** **b** (Fragwürdig, eventuell benötigte Programme) und **Everything Else** **c** (Alles andere, restliche Programme).
5. Sehen Sie sich die Einträge in den drei Registern an und setzen Sie per Mausklick einen Haken vor alle Programme, die Sie entfernen möchten.
6. Klicken Sie auf **Remove Selected** **d** (Ausgewählte Programme entfernen) und The PC Decrapifier deinstalliert diese Programme.

Meine 3 Regeln für einen werbeprogrammfreien PC

1. Säubern Sie einen neuen PC als Erstes von allen Werbeprogrammen, bevor Sie den PC für sich einrichten.



Finden Sie im Register **Recommended** keine Einträge, haben Sie Ihren PC sauber aufgeräumt.

2. Installieren Sie nur die unbedingt nötigen Programme und die von mir installierten Sicherheitsprogramme.
3. Prüfen Sie bei jeder Programminstallation, ob Sie auf der Webseite des Anbieters oder während der Installation Hinweise auf zusätzliche Programme finden, und deaktivieren Sie dann die entsprechenden Optionen.

Fazit: Ihr PC ist nun frei von Werbe- und Spionageprogrammen. Dadurch startet und reagiert Windows schneller. Sie werden auch nicht mehr durch Werbefeldschirme genervt und durch vorinstallierte Programme ausspioniert.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Dieses monothematische Supplement
„Ihr Leitfaden für Ihren schadprogrammfreien PC“ gehört zu dem Titel
„Ihr PC-Sicherheits-Berater“.
Computerwissen, ein Verlagsbereich der
VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop
Chefredakteur: Michael-Alexander Beisecker
(V.i.S.d.P.), Oberhausen
Herausgeberin: Patricia Sparacio
Adresse: Verlag für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2-4, 53177 Bonn
Telefon: 0228/9550190, Fax: 0228/3696350

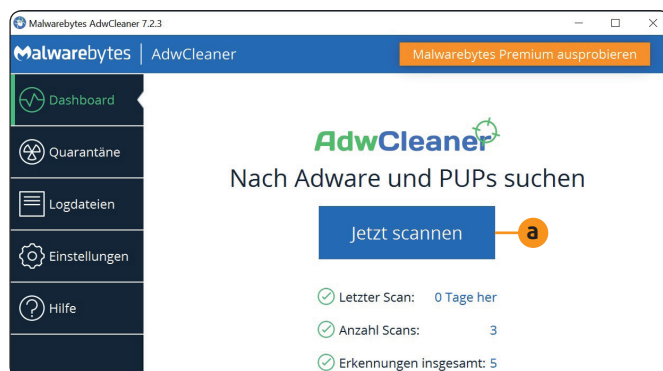
Eingetragen: Amtsgericht Bonn HRB 8165
Die Beiträge in „Ihr PC-Sicherheits-Berater“ wurden mit
Sorgfalt recherchiert und überprüft. Sie basieren jedoch
auf der Richtigkeit uns erteilter Auskünfte und unterliegen
Veränderungen. Daher ist eine Haftung, auch für telefonische
Auskünfte, ausgeschlossen. Vervielfältigungen jeder Art sind
nur mit Genehmigung des Verlags gestattet.
© Copyright 2019 by Verlag für die Deutsche Wirtschaft AG;
Bonn, Bukarest, Manchester, Warschau



Kontrollschritt 6: Finden Sie mit dem Tool Malwarebytes AdwCleaner nicht gemeldete unerwünschte Programme

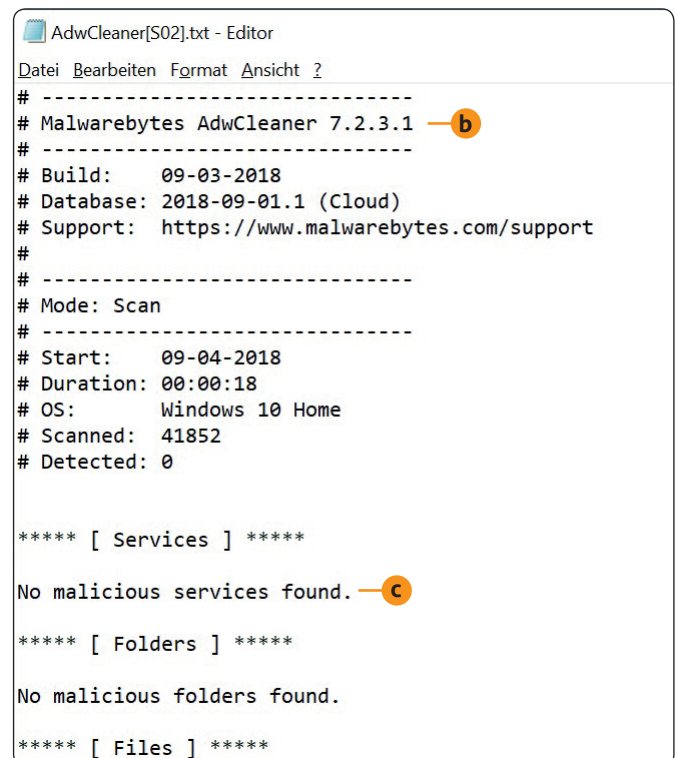
Unerwünschte Programme sind der Grund sehr vieler Hilferufe im Computerwissen Club. Bei Leser Ernst W. wurde zum Beispiel unbemerkt eine Browser-Erweiterung installiert, die zu äußerst störenden Fehlermeldungen beim Aufruf von Internetseiten führte. Als Ernst W. mit Malwarebytes AdwCleaner seinen PC überprüfte, wurde das unerwünschte Programm gefunden und entfernt. Sein Antiviren-Programm hatte ihn nicht vor diesem Programm gewarnt. Starten Sie daher auch eine Kontrolle mit Malwarebytes AdwCleaner.

1. Laden Sie **Malwarebytes AdwCleaner** über unsere sichere Service-Webseite www.pc-sicherheitsberater.de herunter.
2. Öffnen Sie über die Tastenkombination **(Strg)+[J]** die Download-Liste Ihres Browsers und starten Sie das heruntergeladene Installationsprogramm **adwcleaner_Version.exe**, wobei **Version** für die aktuelle Version steht.
3. Bestätigen Sie der Benutzerkontensteuerung das Ausführen des Programms mit **Ja** und Malwarebytes AdwCleaner steht Ihnen sofort zur Verfügung. Eine Installation ist nicht erforderlich.
4. Klicken Sie auf **Jetzt scannen** **a** und warten Sie das Ergebnis der nur wenige Minuten dauernden Suche ab.

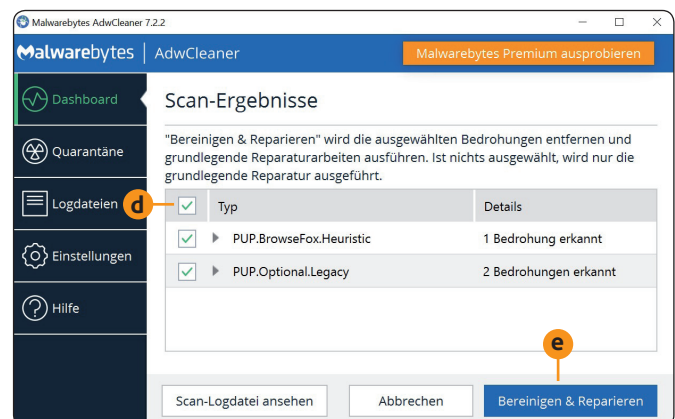


Ein Klick reicht und die Schadprogramm-Suche startet.

5. Klicken Sie auf **Scan-Logdatei ansehen**. Es werden Ihnen alle gefundenen verdächtigen Dateien und Registrierungsdatenbank-Einträge angezeigt **b**. Diese Berichtsdatei können Sie bei Fragen im Computerwissen Club hochladen. Meine Mitarbeiter aus der Redaktion und ich erläutern Ihnen die Einträge gerne: <https://club.computerwissen.de>.
6. Malwarebytes AdwCleaner zeigt Ihnen die gefundenen Bedrohungen auch direkt an. Falls Sie einen Eintrag für eine Falschmeldung halten, entfernen Sie den Haken davor. Zum Entfernen der Bedrohungen markieren Sie die Einträge **d** und klicken auf **Bereinigen & Reparieren** **e**.



Die Scan-Logdatei von Malwarebytes AdwCleaner informiert Sie hier mit der Meldung **No malicious services found** **c**, dass keine schädlichen Windows-Dienste vorhanden sind.



Hier wurden zwei Bedrohungen vom Typ PUP (potenziell unerwünschte Programme) gefunden.

Meine Empfehlung: Malwarebytes AdwCleaner findet wie das Tool The PC Decrapifier ebenfalls Werbe- und Spionageprogramme, kann The PC Decrapifier jedoch nicht ersetzen und umgekehrt. Beide Sicherheitsprogramme ergänzen sich und Sie sollten daher beide verwenden und nicht auf eines davon verzichten.

Kontrollschritt 7: Holen Sie noch eine dritte Sicherheitsmeinung mit HitmanPro.EU-Cleaner ein

Sie haben in den Kontrollschritten 1 bis 6 alles dafür getan, dass kein Schadprogramm mehr aktiv ist und auch etwaige Reste in der Registrierungsdatenbank gefunden werden. Doch kein Antiviren-Programm ist perfekt. Wird auch nur ein Schadprogramm übersehen, war die ganze Mühe umsonst. Das eine Schadprogramm kann ein Dutzend neuer Schadprogramme nachladen. Machen Sie daher zur Sicherheit noch eine Abschlusskontrolle mit dem neuen Tool HitmanPro.EU-Cleaner. So prüfen Sie, ob wirklich 100 Prozent aller Schadprogramme gefunden und entfernt wurden.

HitmanPro.EU-Cleaner ist das ideale Programm für Ihre Abschlussprüfung, denn es wurde so entwickelt, dass es zu keinen Konflikten mit Ihrem installierten Antiviren-Programm kommt.

Die Prüfung dauert nur 5 Minuten und das ist nicht viel Zeit für die zusätzliche Sicherheit einer dritten Meinung. Warten Sie allerdings nach der Installation nicht lange mit Ihrer Prüfung, denn die Nutzung ist nur 30 Tage kostenlos.

1. Laden Sie **HitmanPro.EU-Cleaner** über unsere sichere Service-Webseite www.pc-sicherheitsberater.de herunter. Klicken Sie dazu je nach Ihrem Betriebssystem auf **Download für Windows 32BIT** oder **Download für Windows 64BIT**.



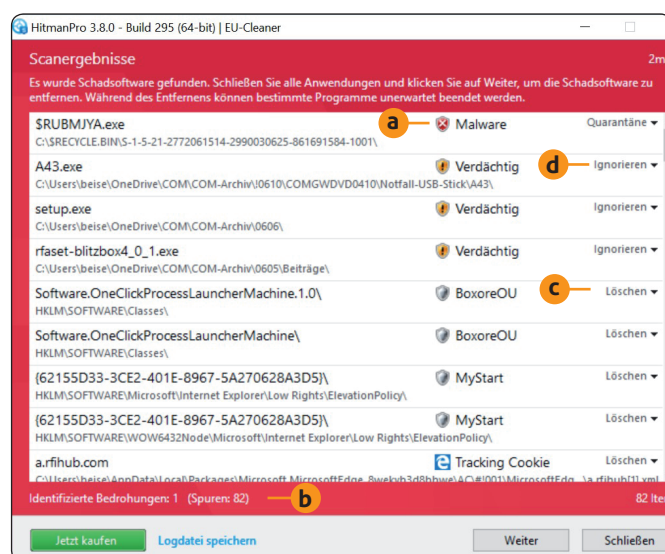
Mein Tipp: Kennen Sie den Betriebssystem-Typ nicht, drücken Sie **Win + Pause** und lesen hinter **Systemtyp** ab, ob Ihr Windows ein **32-Bit-Betriebssystem** oder **64-Bit-Betriebssystem** ist.

2. Klicken Sie im Fenster **Datenschutz- und Datensicherheitshinweis für HitmanPro.EU-Cleaner** auf **ZUSTIMMEN** und der Download beginnt.
3. Öffnen Sie mit der Tastenkombination **Strg+J** die Download-Liste Ihres Browsers und starten Sie das heruntergeladene Programm **hitmanpro.exe** (32-Bit-Version) oder **hitmanpro_x64.exe** (64-Bit-Version). Bestätigen Sie das Ausführen des Programms mit **Ja** und HitmanPro.EU-Cleaner steht Ihnen nach dem Update sofort zur Verfügung. Klicken Sie auf **Weiter**.
4. Setzen Sie einen Haken vor **Ich akzeptiere die Bedingungen dieses Lizenzvertrags** und klicken Sie auf **Weiter**.
5. Wählen Sie die Option **Nein, ich möchte nur einen Einmalscan zur Überprüfung dieses Computers ausführen** und klicken Sie auf **Weiter**.
6. Wurden alle Schadprogramme mit den Kontrollschritten 1 bis 6 gefunden, meldet Ihnen HitmanPro.EU-Cleaner: **Es wurde keine Bedrohungen gefunden** oder es werden Dateien mit dem Eintrag **Malware** angezeigt **a**.

HitmanPro.EU-Cleaner kann zudem verdächtige Programme und Tracking-Cookies finden, mit denen Sie im Internet ausspioniert werden. Am Ende des Fensters finden Sie hinter **Spuren** **b** die Gesamtzahl solcher verräterischer Dateien.

7. Klicken Sie bei den angezeigten Gefahren auf **Löschen** **c**, um diese von Ihrem PC zu entfernen.

Meine Empfehlung: Steht hinter einem Eintrag **Ignorieren** **d**, ist HitmanPro.EU-Cleaner nicht sicher, ob hier eine Gefahr besteht. Fragen Sie uns über den Computerwissen Club, ob Sie die betreffende Datei löschen sollen. Meine Mitarbeiter aus der Redaktion und ich helfen Ihnen gern: <https://club.computerwissen.de>.



Hier wurden noch ein Schadprogramm im Papierkorb (C:\\$RECYCLE.BIN) und über 82 Tracking-Cookies mit Informationen über Ihr Surfverhalten im Internet gefunden.

Meine Sicherheitsgarantie: Sie haben Ihren Windows-PC nun sehr gründlich auf Schadprogramme überprüft. Führen Sie diese Kontrollschritte einmal im Monat durch, dann bleibt kein Schadprogramm über längere Zeit unentdeckt. Und das Beste: Keines der Programme in diesem Beitrag müssen Sie kaufen, auch das Tool HitmanPro.EU-Cleaner nicht. Mithilfe dieses Programms führen Sie die Abschlusskontrolle durch.