# Tools gegen Verschlüsselungstrojaner

Zurück zum Beitrag Erpresser-Trojaner: Das hilft gegen Ransomware!


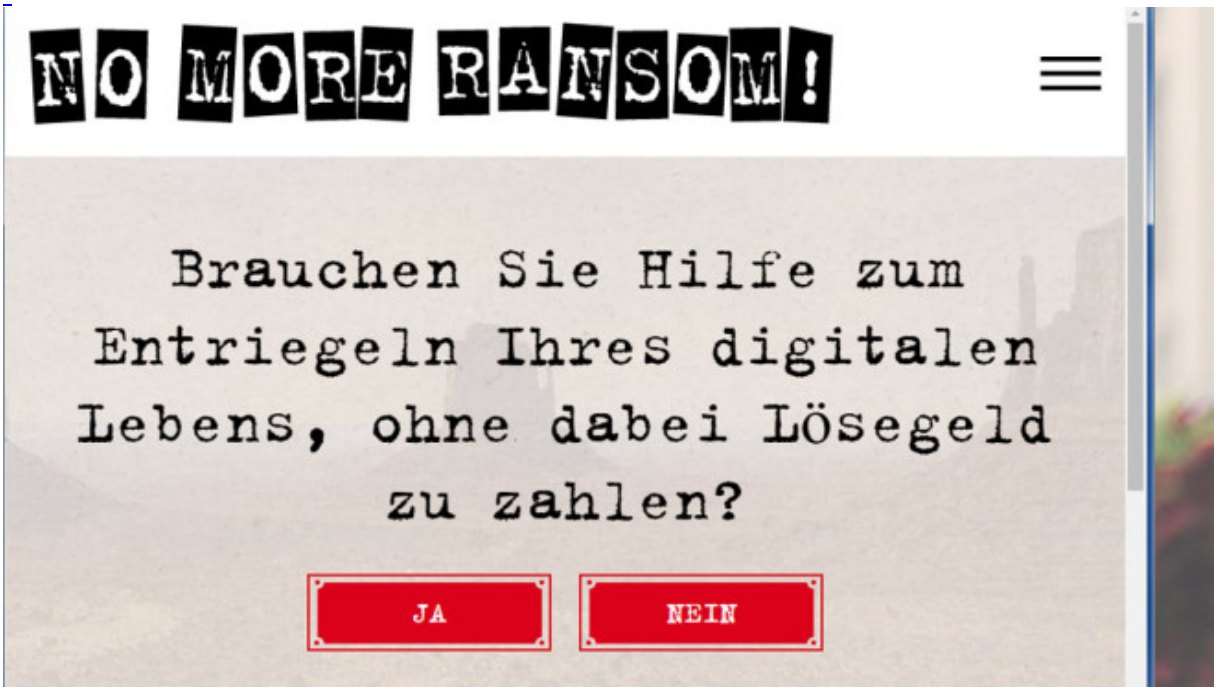


Bild vergrößern

### No More Ransom: Entschlüsselungstool finden

Die erste Anlaufstelle für Opfer eines Erpressertrojaners ist „No More Random“. Dort finden sie ein Entschlüsselungsprogramm für Dateien, die der Schädling hinterlassen hat. Sie laden chiffrierte Exemplare hoch – sodass die Seite den Schädling identifiziert. Mit Glück erhalten Sie ein Werkzeug zur Entschlüsselung zum Download. Hinter der Seite stecken Europol, McAfee und die niederländische Polizei, hinzu kommen unterstützende Sicherheitsfirmen.

» Zum Webdienst: No More Ransom


Bild vergrößern

## ID Ransomware: Art des Schädlings ausmachen

Eine Alternative zu No More Ransom ist ID Ransomware. Der Dienst identifiziert die auf dem PC wütende Ransomware, indem Opfer eine verschlüsselte Datei hochladen. Laut Anbieter erkennt der Dienst 687 verschiedene Verschlüsselungstrojaner (Stand: Mitte Februar 2019).

» Zum Webdienst: ID Ransomware

Bild 3 von 29


Bild vergrößern

## COMPUTER BILD-Erpresserviren-Stopper: Automatischer Systemwächter

Neuere Windows-10-Versionen bringen einen Ransomware-Schutz mit („Überwachter Ordnerzugriff"). Als Alternative bietet sich der COMPUTER BILD-Erpresserviren-Stopper an. Die Gratis-Vollversion arbeitet auch mit älteren Windows-Versionen zusammen und überwacht die Windows-Ordner „Videos", „Bilder", „Dokumente", „Musik". Sie fügen in der Gratis-Version maximal einen weiteren Ordner hinzu. Bemerkt das Programm einen Verschlüsselungsvorgang, fährt es Windows im abgesicherten Modus hoch. Mit Glück startet ein etwaiger Verschlüsselungstrojaner hier nicht automatisch – sodass weitere Verschlüsselung gestoppt ist und Sie eine Datensicherung und Malware-Prüfung durchführen.

» Download: COMPUTER BILD-Erpresserviren-Stopper (AntiRansomware 2019) herunterladen

Bild 4 von 29

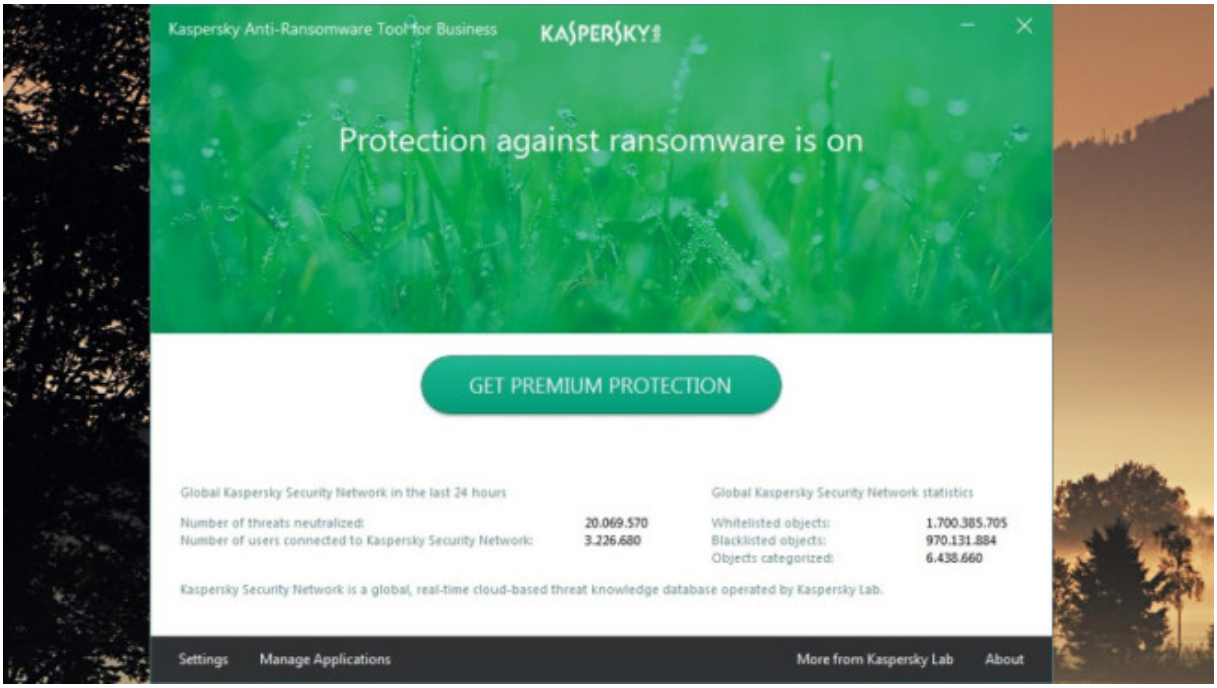


Bild vergrößern

## Kaspersky Anti-Ransomware Tool: Echtzeit-Schutz

Das englischsprachige Kaspersky Anti-Ransomware-verspricht, Verschlüsselungstrojaner zu blockieren. Installieren und vergessen – nach der Installation behütet ein Hintergrundwächter das System, zu erkennen anhand eines Infobereich-Symbols. Das kostenlose Programm ist fürs Business-Umfeld konzipiert und nutzt es Technologien von Kaspersky Endpoint Security. Laut Hersteller ist es kompatibel mit fast jeder Sicherheitssoftware und DSGVO-konform (Datenschutz-Grundverordnung).

» Download: Kaspersky Anti-Ransomware Tool herunterladen

Bild 5 von 29

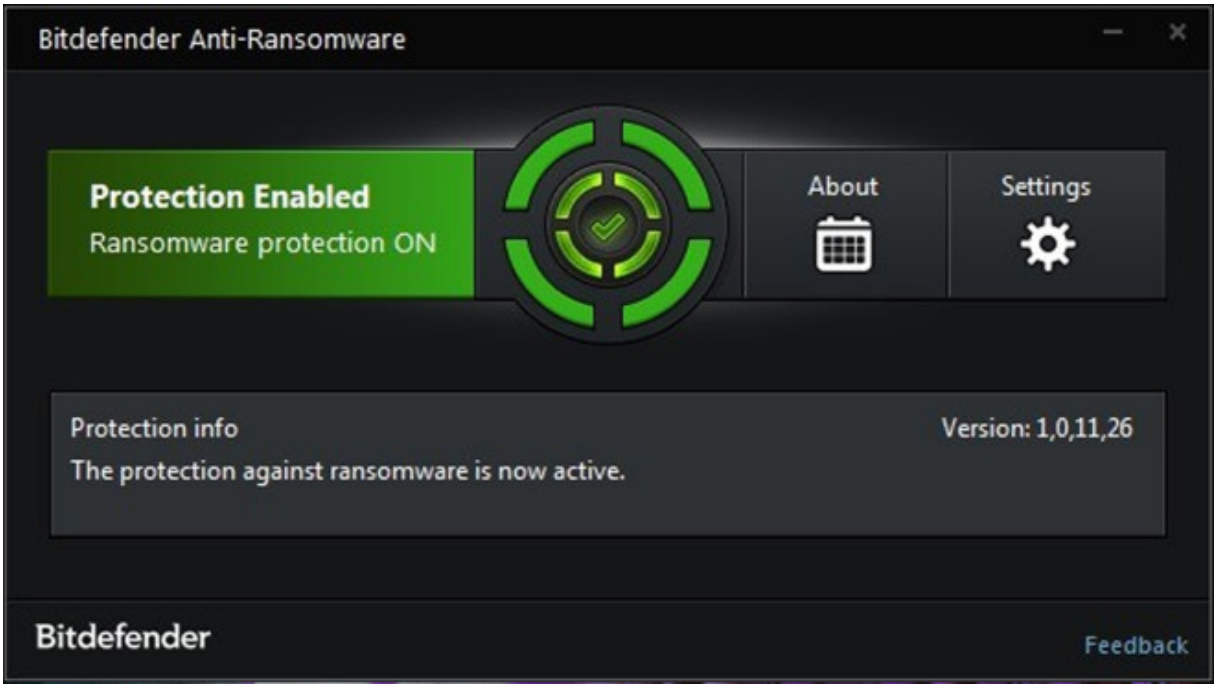


Bild vergrößern

## Bitdefender Anti-Ransomware: Echtzeit-Schutz

Ähnlich Kaspersky Anti-Ransomware Tool ist die Bedienoberfläche von Bitdefender Anti-Ransomware minimal. Das Schutztool läuft im Hintergrund und ergänzt einen Antivirus. Für den Zugriff aufs Tool dient ein Infobereich-Symbol.

» Download: Bitdefender Anti-Ransomware herunterladen

Bild 6 von 29


Bild vergrößern

## Acronis Ransomware Protection: Echtzeit-Schutz

Backup-Spezialist Acronis bietet mit „Ransomware Protection“ Schutz vor Verschlüsselungstrojanern. Der Echtzeitwächter überwacht das System und warnt, wenn er einen verdächtigen Prozess erkennt. Sie sollen den Vorgang dann zulassen oder blockieren können. Der Hersteller integriert einen Backup-Upload, worüber das Tool Dateien in einen 5 Gigabyte großen Cloud-Speicher überträgt. Ob Ransomware oder Festplattenschaden, aus der Acronis Cloud laden Sie via Webbrowser vermisste Dateien wieder herunter.

» Download: Acronis Ransomware Protection herunterladen

Bild 7 von 29

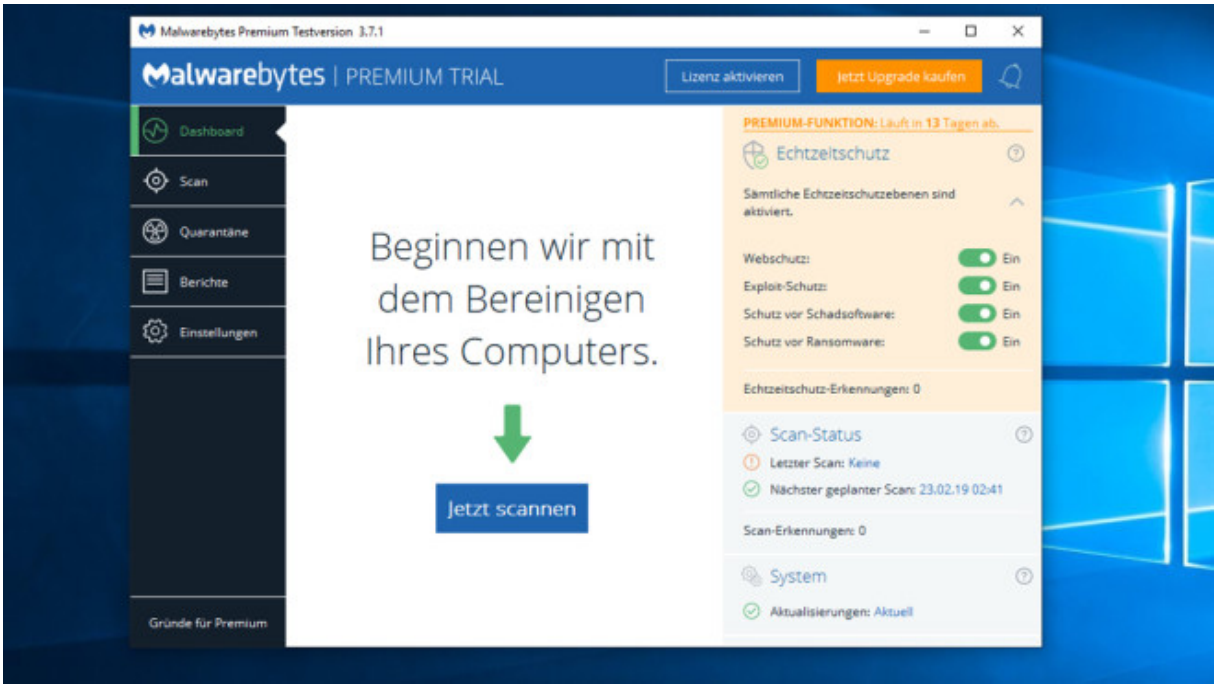


Bild vergrößern

## Malwarebytes: Echtzeit-Schutz

Das beliebte Malwarebytes (ehemals: Malwarebytes Anti-Malware) ergänzt den Virenschutz, sucht und entfernt Schadprogramme. Die kostenpflichtige Premium-Version bietet übers Bereinigen hinaus vier Echtzeitschutzebenen: gegen Angriffe von Schadsoftware, das Sperren von Dateien durch Ransomware, außerdem Webschutz und Spyware-Erkennung. 14 Tage Testzeit der Premium-Funktionen sind vorgesehen.

» Download: Malwarebytes herunterladen

Bild 8 von 29

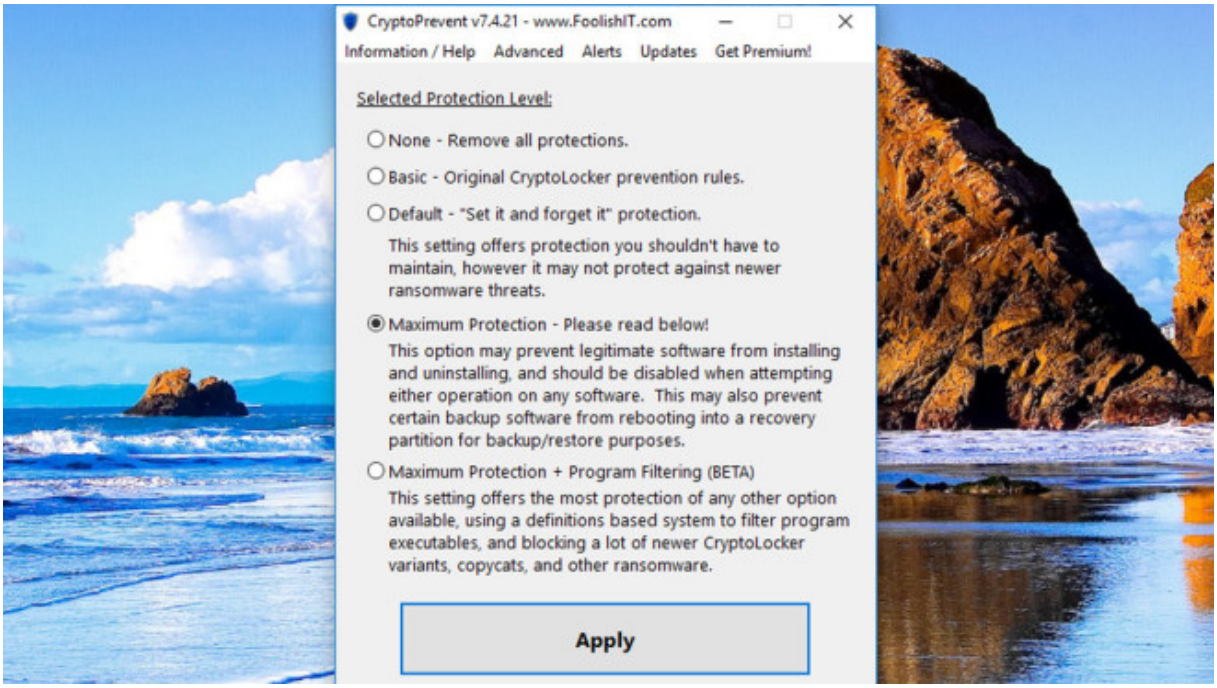


Bild vergrößern

## CryptoPrevent: System härten

CryptoPrevent ändert Windows-Einstellungen, um das System gegen Infektionen zu schützen. Mehrere Schutzstufen stehen zur Wahl, zu jeder zeigt das Tool nach Markieren eine Erklärung. Nach Aktivieren der gewünschten Schutzklasse führen Sie einen Neustart durch. Das Tool verhindert unter anderem, dass Batch-Dateien aus bestimmten Ordnern starten. Außerdem blockiert es die Ausführung von EXE-Dateien einiger Programme – mitunter harmlosen (hier schießt das Tool übers Ziel hinaus).

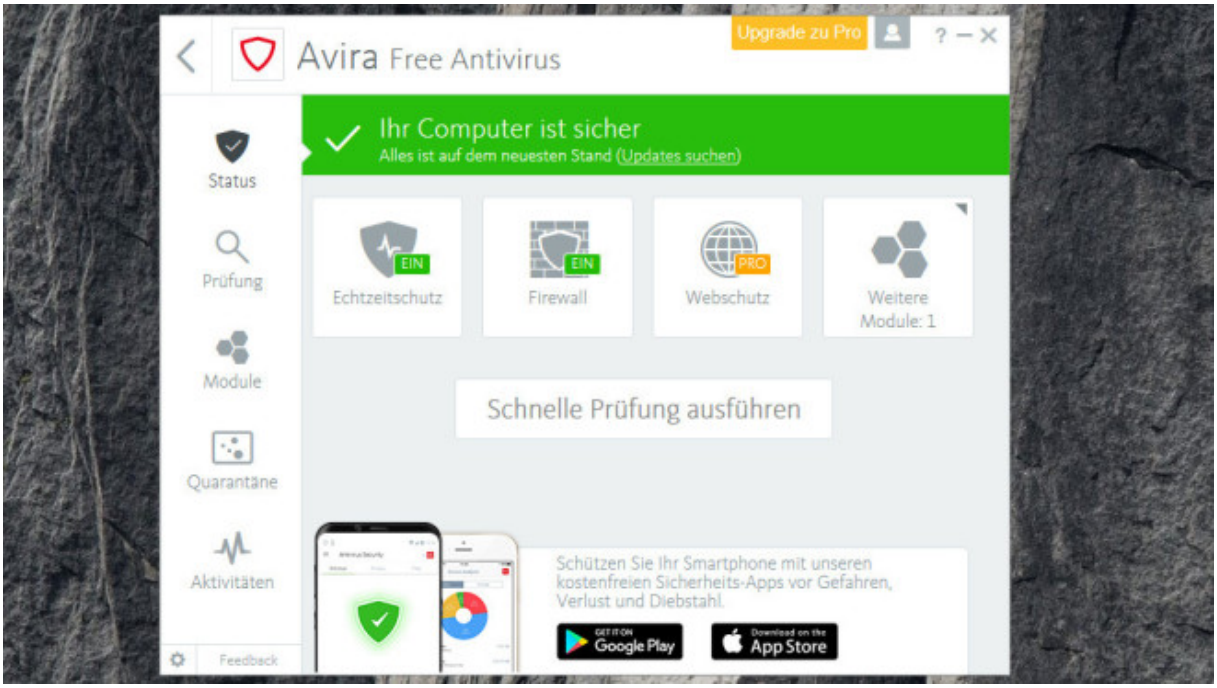


Bild vergrößern

## Avira Free Antivirus: Antivirentool

Ein Antivirenprogramm (AV) sollte auf keinem PC fehlen, empfehlenswert ist etwa Avira Free Antivirus. Die Installation eines externen AV-Produkts ist unter Windows 7 anzuraten, ab Windows 8 nicht zwingend – dessen integrierter Windows Defender bietet soliden Grundschutz. Das Avira-Tool sollten Sie installieren, wenn Sie das Virenschutz-lose Windows 7 noch nicht mit einem Schutzprogramm versehen haben – oder dem Defender unter Windows 8.1/10 nicht vertrauen.

» Download: Avira Free Antivirus herunterladen


Bild vergrößern

## VirusTotal: Verdächtige Dateien prüfen

Bevor Sie eine unbekannte, interessante Datei ausführen (oder in ein Programm laden), sollten Sie sich die Zeit für eine Prüfung nehmen. Gründlich klappt das mit VirusTotal: Der Cloud-Dienst untersucht hochgeladene Dateien mit zahlreichen Antivirus-Engines. Mit dabei sind Engines namhafter und bekannter Anbieter wie Ad-Aware, Avast, AVGt, Avira, BiDefender, ClamAV, Comodo, DrWeb, ESET, F-Secure, GData, Sophos, Malwarebytes, McAfee, Microsoft, Panda, Symantec, TrendMicro, Webroot, ZoneAlarm by CheckPoint. Attestiert die Mehrheit der (wichtigeren) Dienste keinen Malware-Fund, ist die geprüfte Datei wohl sauber – andernfalls verbietet sich ihre Nutzung.

» Zum Webdienst: VirusTotal

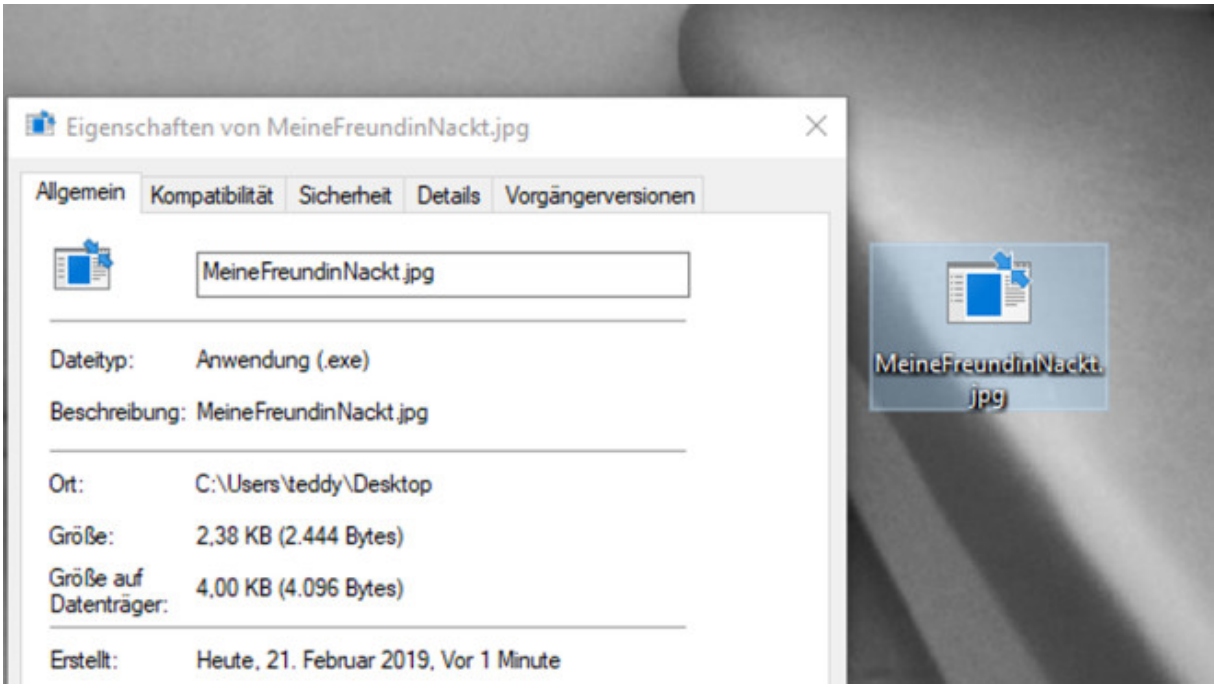


Bild vergrößern

## Dateiendungen anzeigen

Mithilfe des hier angebotenen REG-Skripts erzwingen Sie, dass Windows bei den meisten Dateien die Endung zeigt. Zum Download steht ein ZIP-Archiv bereit: Die eine REG-Datei blendet Dateiendungen ein, die andere aus. Durch das Einblenden haben Sie Gewissheit, um was für einen Dateityp es sich bei Festplattenelementen handelt. Hacker tarnen verseuchte Dateien etwa mit dem Namen „MeineFreundinNackt.jpg.exe“. Windows blendet normalerweise das bedrohlich wirkende .exe aus – ein wenig versierter Nutzer öffnet die Datei, da er JPG mit Bilddatei assoziiert und Bilder für harmlos hält.

» Download: Dateiendungen anzeigen herunterladen

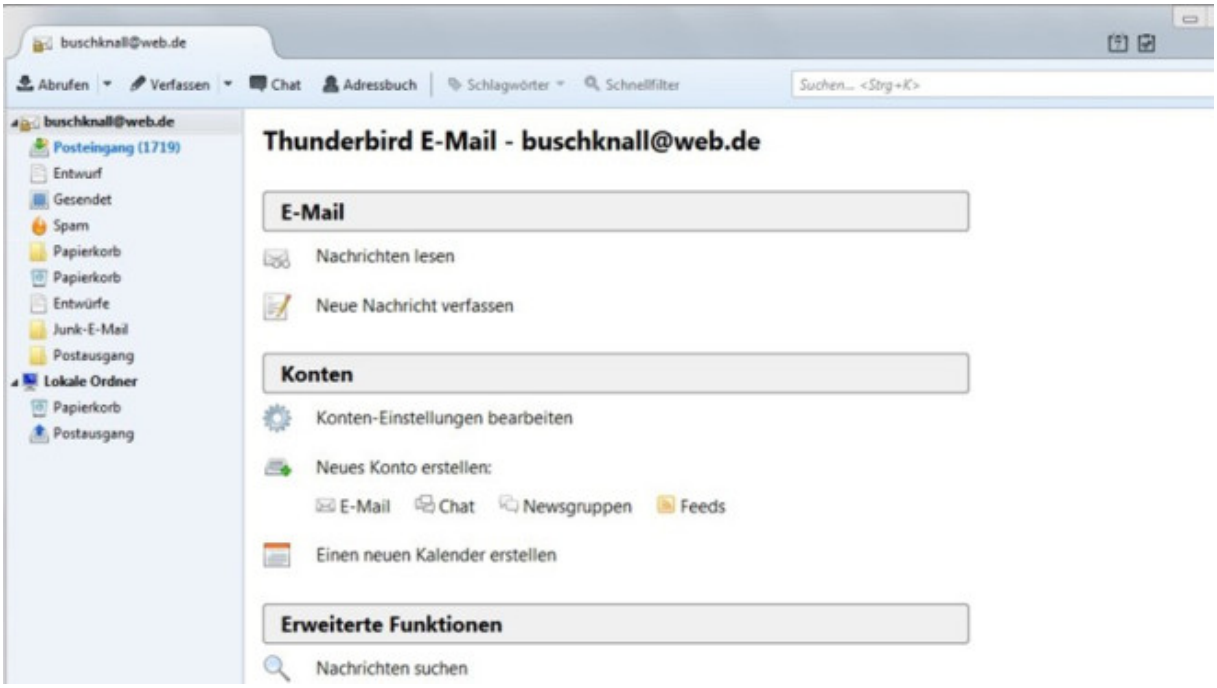


Bild vergrößern

## Thunderbird: Verseuchte E-Mails aussortieren

Wer seine E-Mail-Adresse öffentlich im Internet preisgibt, erhält irgendwann Spammails. Versender solcher mitunter mit schadhaften Dateien gespickten Nerv-Nachrichten finden Ihre Mailadresse sogar ohne Ihr Mitwirken: Es genügt, die Adressbücher gekaperter PCs zu durchsuchen. Da Verschlüsselungstrojaner häufig per Mail auf PCs gelangen, wappnen Sie sich mit einem E-Mail-Programm mit Anti-Spam-Funktion. Thunderbird bringt einen lernenden Spam-Filter mit und sortiert unangenehme Post heraus.

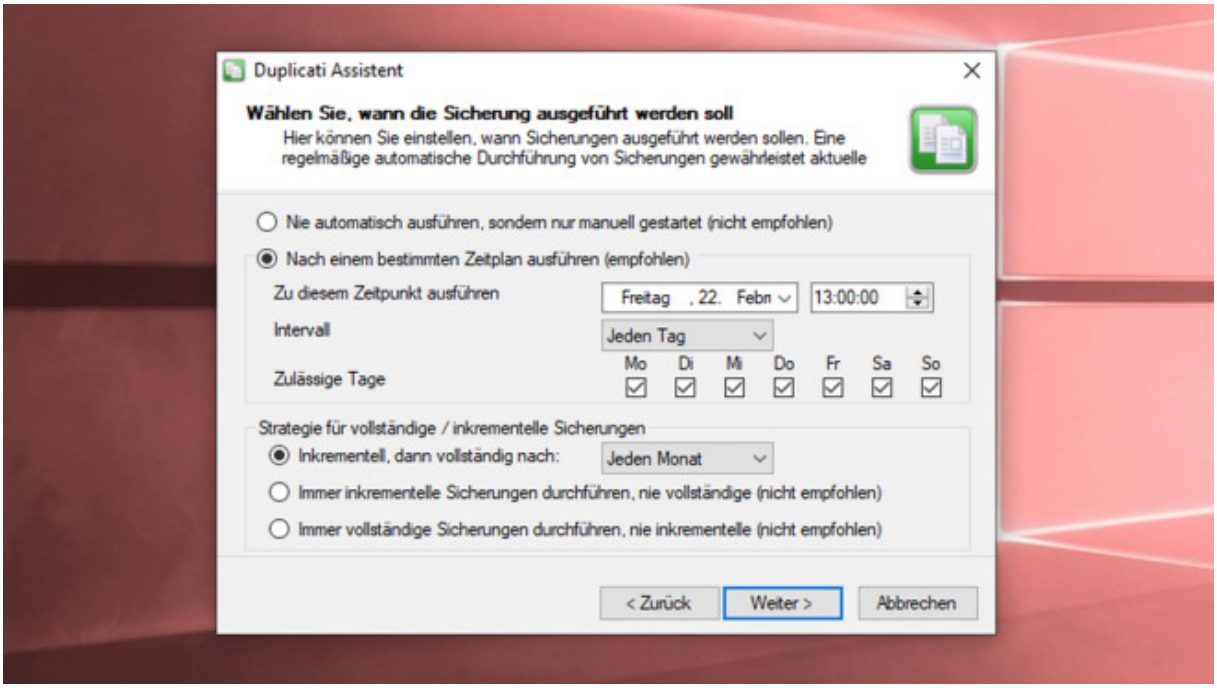


Bild vergrößern

## Duplicati: Lokal oder entfernt Daten sichern

Wer wichtige PC-Daten verliert, ist froh, wenn er irgendwo eine Sicherungskopie gebunkert hat. Duplicati ist ein simpel gestricktes Backup-Werkzeug für einzelne Dateien, das viele Sicherungsziele zur Wahl stellt. So deponieren Sie Ihre Datenschätze an mehreren Orten. Auf Wunsch erfolgen Backups automatisch, verschlüsselt, inkrementell.

» Download: Duplicati (32 Bit) herunterladen
» Download: Duplicati (64 Bit) herunterladen

Bild 17 von 29

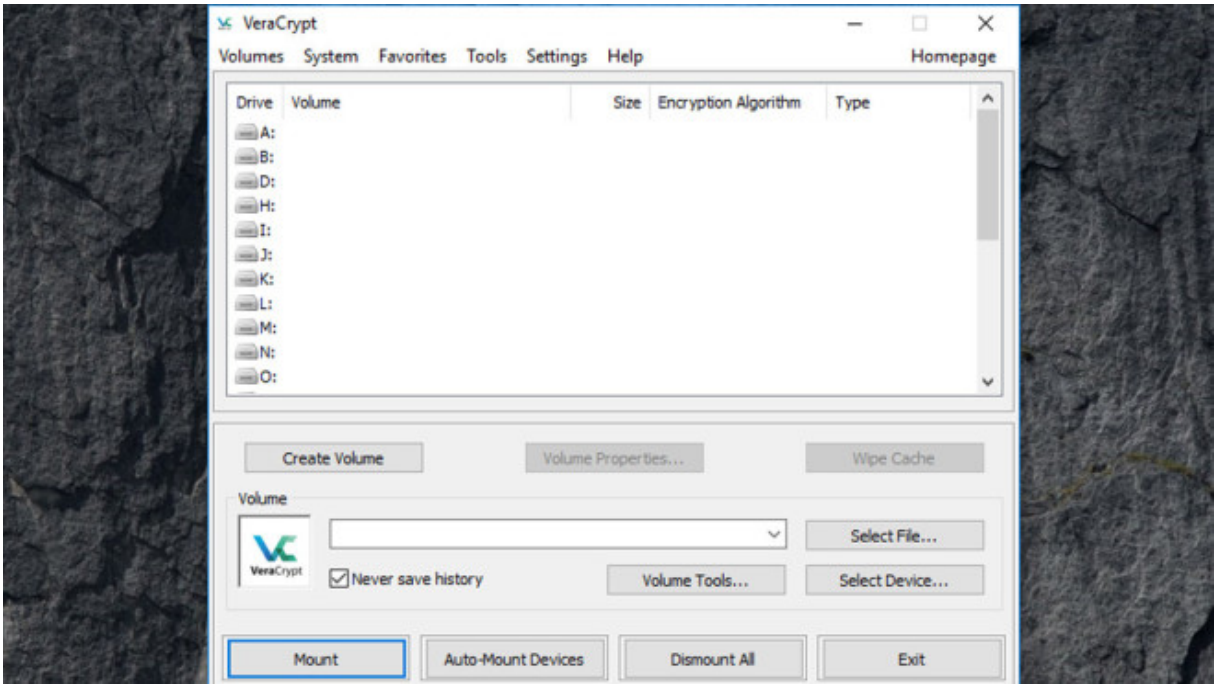


Bild vergrößern

## VeraCrypt: Verschlüsselung gegen Verschlüsselung

Bewusst herbeigeführte Verschlüsselung ist okay – immerhin kennen Sie das Passwort – und schützt unter Umständen vor feindseligen Verschlüsselungen, da einige Trojaner nur Dateien bestimmter Formate unverwertbar machen. Packen Sie Dateien in einen per Kennwort gesicherten Tresor von VeraCrypt, sehen bösartige Programme nur die übergeordnete Container-Datei. Die übergeht Ransomware vielleicht – und die enthaltenen Inhalte bleiben unangetastet. VeraCrypt ist der Nachfolger des populären TrueCrypt, das die Entwickler aufgrund von Sicherheitsbedenken eingestellt haben.

» Download: VeraCrypt herunterladen

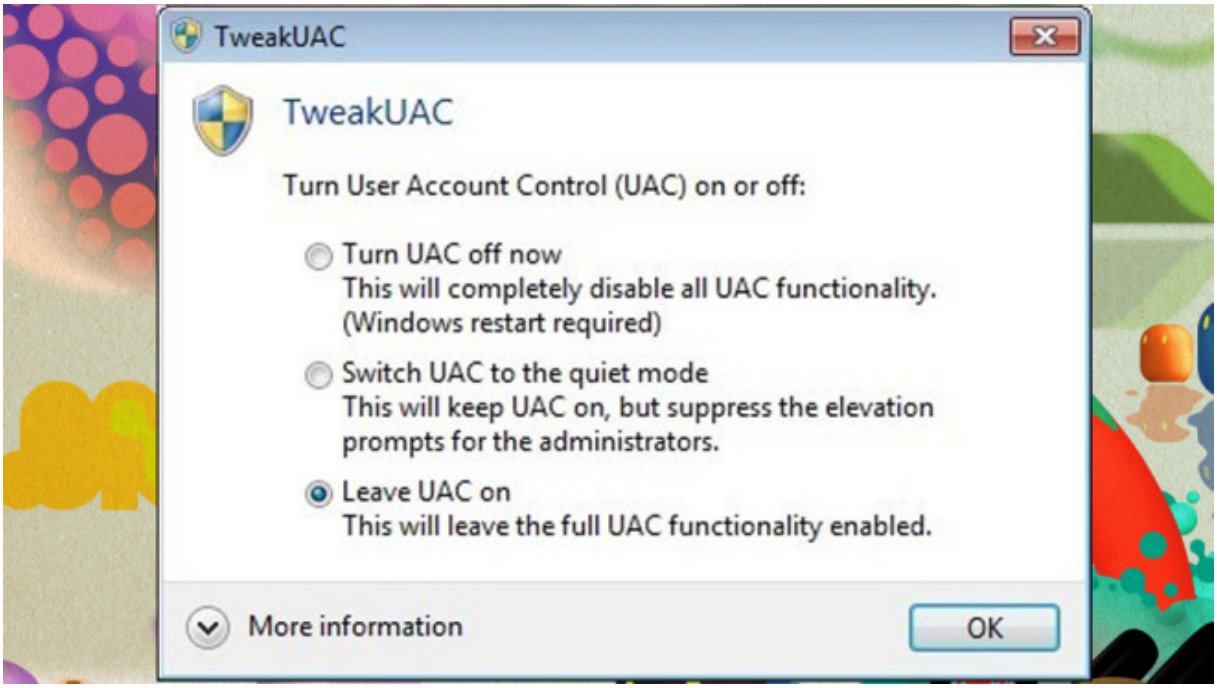


Bild vergrößern

## TweakUAC: Benutzerkonten-Steuerung scharf stellen

Windows legt im Hintergrund im Zusammenspiel mit Wiederherstellungspunkten Sicherungen von Dateien an. Solche älteren Dateiversionsstände bleiben einige Zeit vorrätig. Bei Windows 10 entstehen sie, wenn Sie die ab Werk deaktivierte Systemwiederherstellung einschalten. Die Backups ließen sich nutzen, um an die Ursprungsfassung einer verschlüsselten Datei zu kommen. Das wissen Schädlingsprogrammierer, die die Windows-Funktion vssadmin.exe nutzen, um Schattenkopien zu löschen. Das verhindert die Windows-Benutzerkonten-Steuerung (UAC, User Account Control): Blendet sie ein Warnfenster ein, erteilen Sie nicht unüberlegt die Erlaubnis für die jeweilige Aktion. Sie vereiteln damit neben Systemeingriffen Schadsoftware-Installationen. Damit Ihnen UAC-Meldungen begegnen, schalten Sie gegebenenfalls UAC ein. Um es auf die höchste Schutzstufe zu setzen und so viele Warnungen wie möglich zu erhalten, eignet sich TweakUAC.

» Download: TweakUAC herunterladen

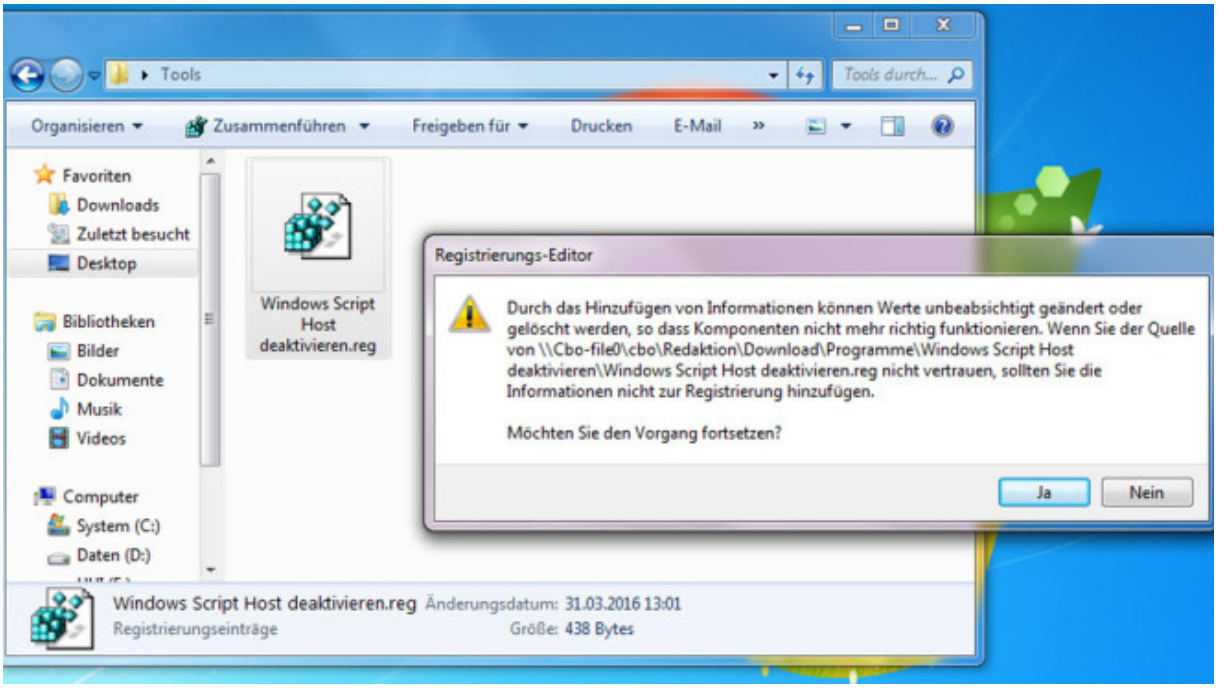


Bild vergrößern

## Windows Script Host deaktivieren: Trojaner-Dateien blocken

Ransomware verbreitet sich über viele Wege und hat das Ziel, den Besitzer des Opfer-PCs zu einer Geldzahlung zu überreden. Zuvor ist Nutzer-Mithilfe gefragt: Der User entpackt etwa ein ZIP-Archiv und führt eine Skroipt-Datei aus, die als Trojaner (Dropper) agiert und den Schädling nachlädt. Indem Sie verhindern, dass Windows Skript-Dateien ausführt, entziehen Sie darauf basierenden Schadprogrammen den Nährboden. Hierzu hat COMPUTER BILD das Tool „Windows Script Host deaktivieren“ entwickelt: Per Doppelklick unterbindet es, dass künftig VBS-Inhalte laden. Ein Doppelklick auf eine weitere mitgelieferte REG-Datei nimmt die Änderung zurück.

» Download: Windows Script Host deaktivieren herunterladen

Bild 20 von 29

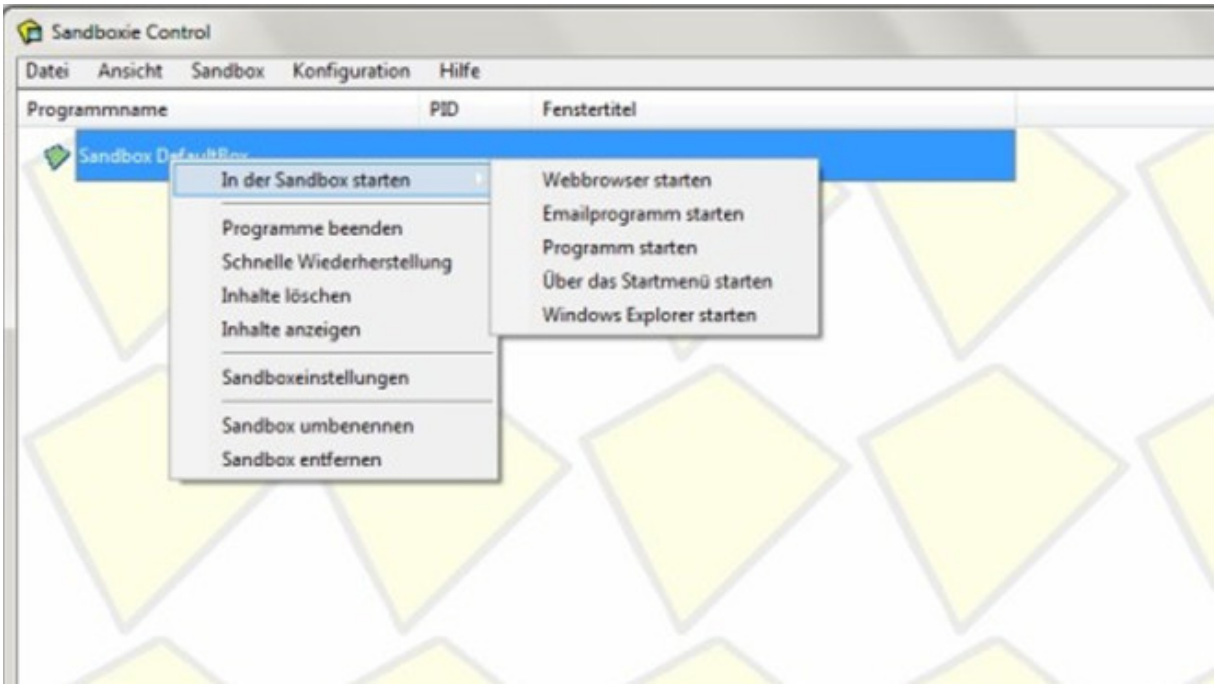


Bild vergrößern

## Sandboxie: Risikoarme Testumgebung

Der Verlockung zu widerstehen, eine interessante neue Datei aus dem Netz auszuprobieren, fällt nicht immer leicht. Sandboxie verschafft Neugierigen mehr Sicherheit. Es führt Programme in einem von Windows isolierten Bereich aus, versuchte Änderungen an Systemeinstellungen scheitern. Handelt es sich bei einer geladenen Datei um Schadsoftware, reduziert sich dank Sandboxie die Infektionsgefahr fürs Haupt-Betriebssystem beträchtlich. Ein farbiger Rahmen um ein Fenster zeigt, dass das jeweilige Tool gekapselt durch Sandboxie den Dienst verrichtet.

» Download: Sandboxie herunterladen

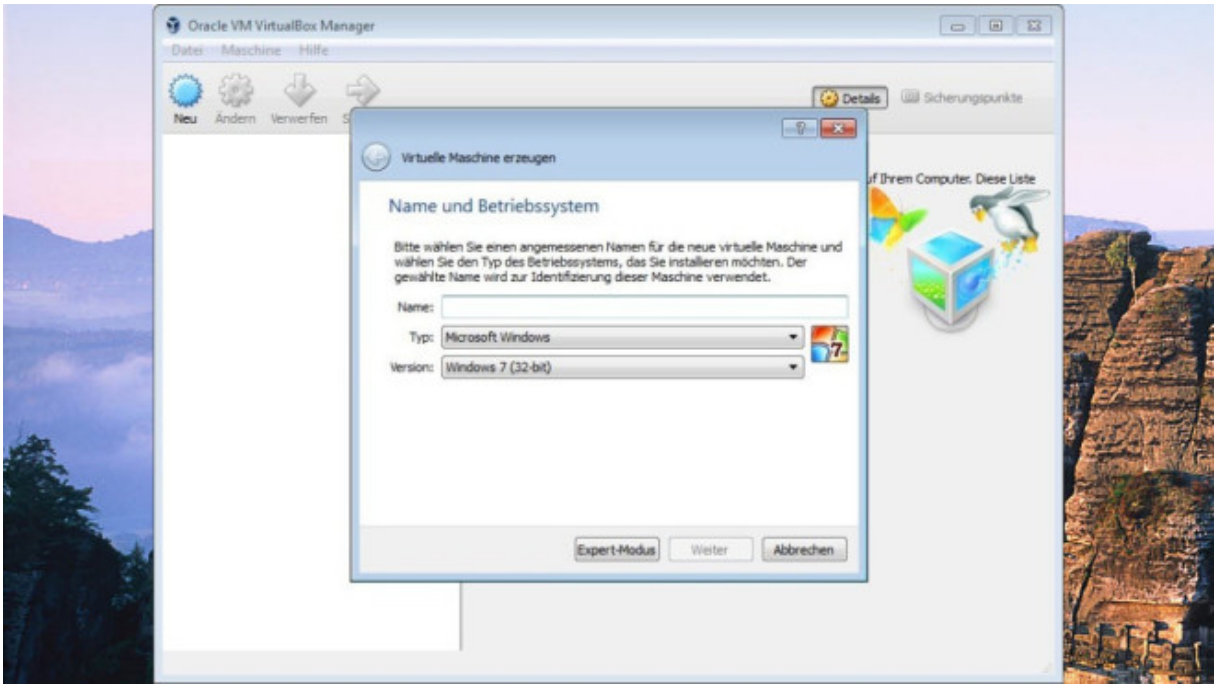


Bild vergrößern

## VirtualBox: Betriebssystem im Betriebssystem nutzen

Sandboxie leistet gute Arbeit, was die Prävention im Zusammenspiel mit unbekannter Software anbelangt. Einen Schritt weiter geht VirtualBox: Es startet Programme ebenfalls abgeschottet. In seinem Fenster führt es jedoch ein komplettes Betriebssystem aus. Das ist aufwendiger als bei Sandboxie und fordert mehr RAM. Aus Sicherheitsgründen der Rat: Verzichten Sie auf ein gemeinsames Verzeichnis für den Datenaustausch zwischen realem und Simulations-Windows, sonst hätten Krypto-Trojaner innerhalb der VirtualBox eine Schnittstelle zum Hauptbetriebssystem.

» Download: VirtualBox herunterladen
» Download: Portable VirtualBox herunterladen

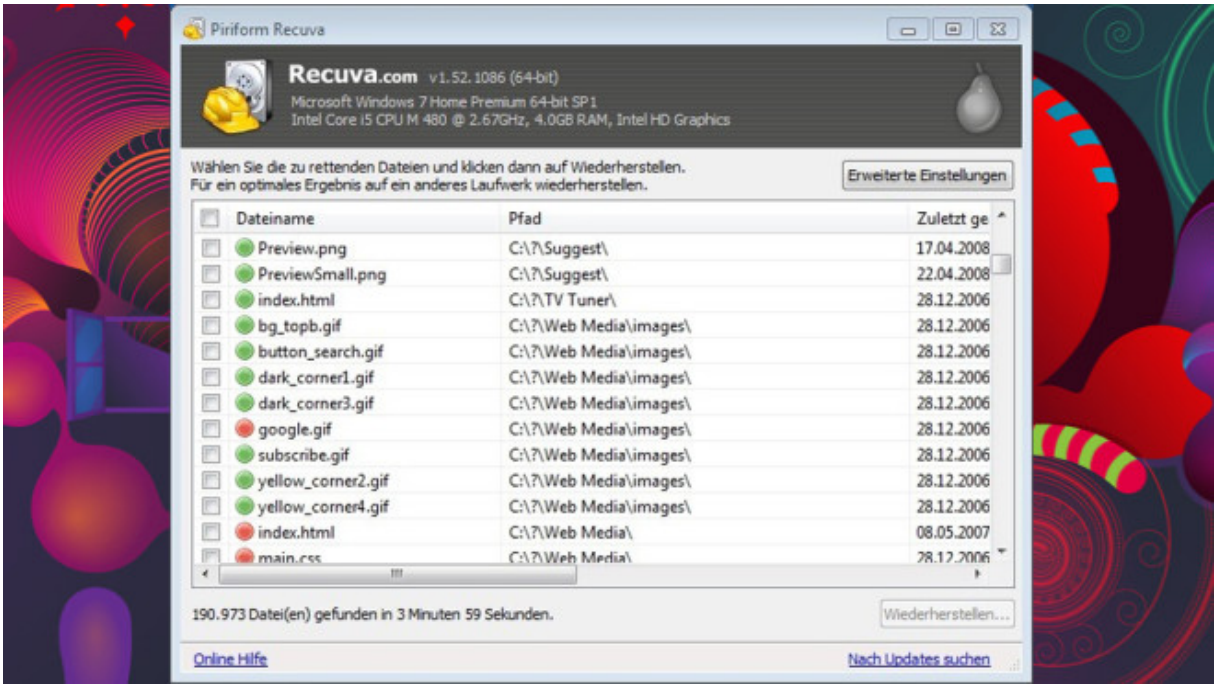


Bild vergrößern

## Recuva: Gelöschte Dateien wiederherstellen

In der Regel verschlüsseln Krypto-Trojaner wertvolle Dateien nicht nur, sie löschen außerdem die Originalinhalte. Vorausgesetzt, Letzteres erfolgte nicht mit Schredder-Technik, bestehen Chancen auf Datenrettung mit Recuva. Das Programm stammt von den CCleaner-Machern, scannt das gewählte PC-Laufwerk auf wiederherstellbare Dateien. Vor einem Rettungsversuch sehen Sie anhand farbiger Markierungen, in welchem Zustand ein aufgespürtes Dateiobjekt vorliegt. Sollte Recuva bei der ersten Nutzung keine gelöschten unverschlüsselten Dateien anzeigen, starten Sie einen zweiten Versuch mit der zeitaufwendigen Tiefensuche: Die prüft nicht nur die Windows-MFT (Master File Table) auf Bereiche mit Gelöscht-Flag/-Kennzeichnung, sondern grast zusätzlich den Datenträger nach sogenannten Datei-Header-Informationen ab – was den Rettungserfolg beflügelt. Tipp: Damit Recuva keine Festplattenbereiche mit gelöschten Inhalten überschreibt, laden Sie die Portable-Fassung auf einen USB-Stick herunter.

» Download: Recuva herunterladen
» Download: Recuva Portable herunterladen

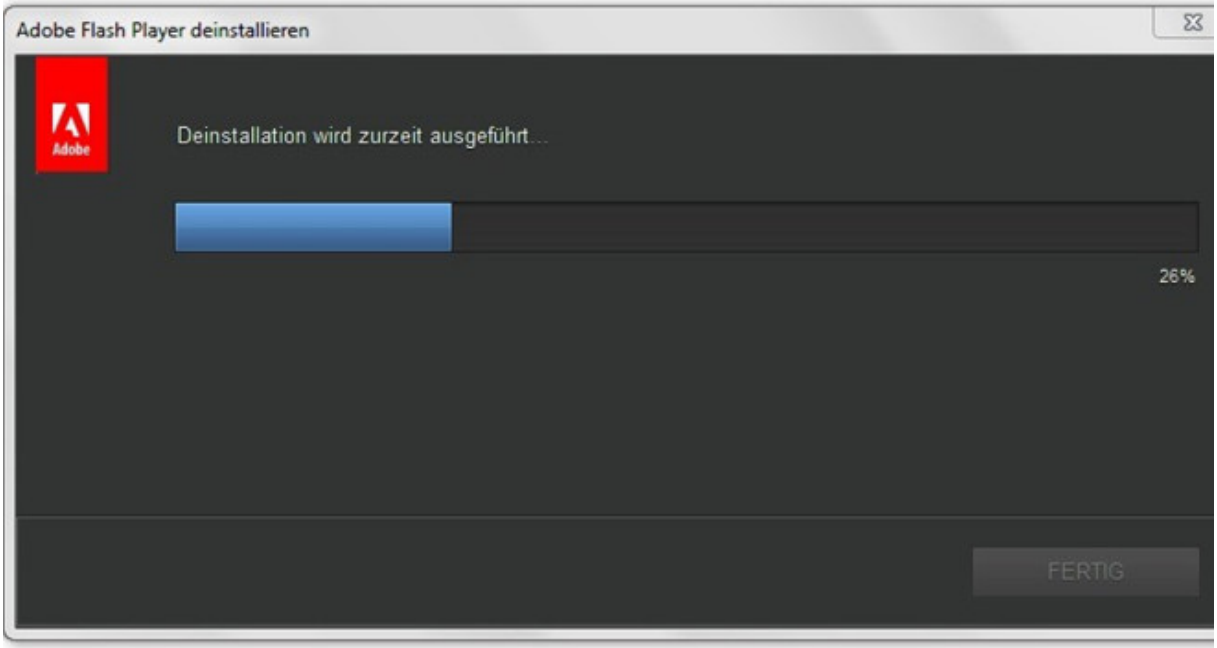


Bild vergrößern

## Adobe Flash Player Uninstaller: Riskantes Plug-in entfernen

Der Flash Player kommt aus der Mode: Größere Webseiten verzichten darauf, 2020 stellt Adobe seinen Webclient-Player ein. Er zeigt Videos, Animationen, Werbung, Spiele. Um das Malware-Einfallstor Flash zu beseitigen, deaktivieren Sie das Plug-in im Browser. Konsequenter: den Adobe Flash Player Uninstaller zur Deinstallation einsetzen. Der fegt Flash runter vom PC – kein tragischer Verlust, denn mit HTML5 gibt es eine sicherere und ressourcenschonendere Alternative.

» Download: Adobe Flash Player Uninstaller herunterladen

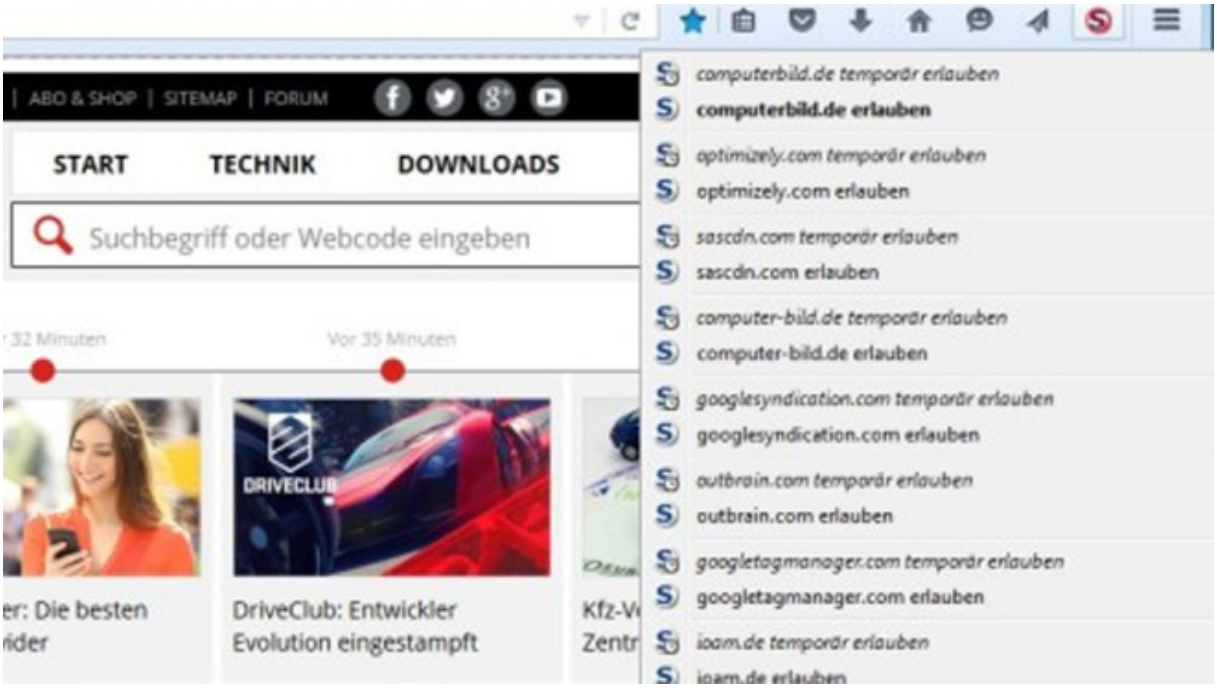


Bild vergrößern

## NoScript, ScriptSafe: Böse Webseiten-Inhalte aussperren

NoScript verhindert, dass Webseiten Sie über Tracking-Mechanismen wiedererkennen und ein detailliertes Nutzerprofil erstellen. Es reduziert die Zahl der Merkmale, die der PC bei Seitenaufrufen an die angesteuerten Server überträgt. Ferner hindert das Programm Webseiten daran, Inhalte in JavaScript auszugeben. Seiten, denen Sie vertrauen, geben Sie für die Skriptsprache frei (URL-Whitelisting). Welchen Seiten zu trauen ist, offenbart ein Check auf URLVoid nach Eingabe der gewünschten Adressen. Wer mit Chrome surft, greift zu ScriptSafe.

» Download: NoScript für Firefox herunterladen
» Download: ScriptSafe für Chrome herunterladen

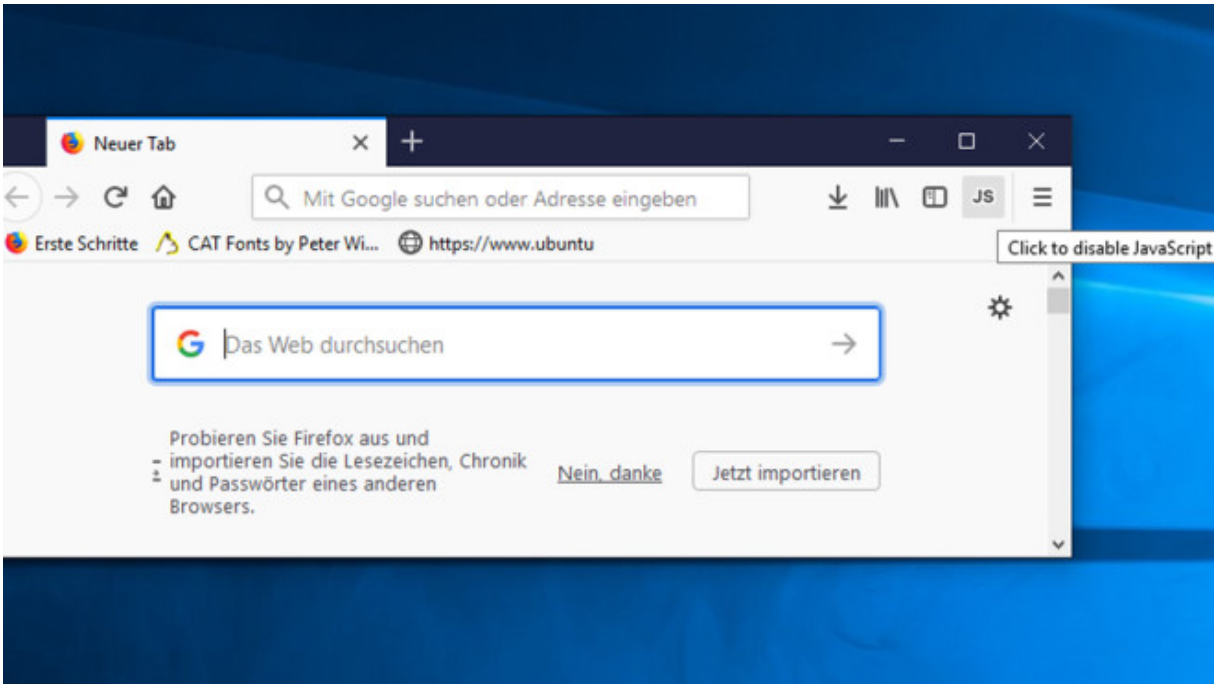


Bild vergrößern

## JavaScript Toggle On and Off für Firefox: Ein-/Aus-Schalter für Skripte

Eine Alternative zu NoScript ist JavaScript Toggle On and Off. Es ist einfacher bedienbar: Per Klick aufs Symbol in der Navigations-Symbolleiste (also neben der Adressleiste) schalten Sie JavaScript  für alle Webseiten aus oder ein. Planen Sie den Aufruf einer unbekannten Webseite (und wollen dafür keine schützende virtuelle Maschine, kein von CD gebootetes Live-Linux oder eine Dual-Boot-Linux-Distribution) nutzen, ist das zeitweise Deaktivieren des Malware-Einfallstors für die Dauer des Seitenbesuchs eine gute Idee.

» Download: QuickJava für Firefox herunterladen