



Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

2 Laufen auf Ihrem PC unsichere Programme?

Prüfen Sie mit meiner Tabelle, ob auf Ihrem PC ein gefährdetes Programm läuft und tauschen Sie es aus.

3 Wie aktuell sind Ihre Programme?

Nur bei einem aktuellen Programm sind die bekannten Sicherheitslücken wirklich geschlossen. So prüfen Sie!

5 Bannen Sie die Betrugsgefahr

Sperren Sie alte, unsichere Programme ein und lassen Sie sie nur bei Bedarf frei. Ich zeige Ihnen wie das geht!

6 Setzen Sie das aktuellste Schutzprogramm ein

EMET 5.52 ist das neueste Schutzprogramm. Dank weniger Mausklicks prallen Angriffe auf Ihren PC ab.

Ihr neuer 4-fach-Schutz bewahrt Sie vor gefährlichen Sicherheitslücken in Ihren Programmen!

Steuern Kriminelle Ihren PC heimlich über das Internet?

Adobe Flash ist wegen Hunderter kritischer Sicherheitslücken das gefährdetste Programm auf Ihrem PC (siehe Tabelle rechts). Mozilla hat bei der neuesten Firefox-Version jetzt endlich reagiert und die Flash-Erweiterung gesperrt. Die einzig richtige Entscheidung.

Doch im Internet wird mit Flash-Werbung viel Geld verdient. Das ist für mich die einzige Erklärung, warum Microsoft Flash weiter unterstützt und es sogar in Windows 10 integriert hat.

Dabei vergeht kaum eine Woche ohne Meldung einer neuen Sicherheitslücke. Nutzt ein Hacker eine dieser Lücken, kann er Ihren PC fernsteuern – und zwar so, als würde er direkt hinter Ihnen stehen und über Ihre Schulter Ihre Tastatur bedienen.

Meine Empfehlung: Machen Sie Adobe Flash unschädlich und lassen Sie es nie wieder auf Ihrem PC aktiv werden. Mit meinen 4 Sicherheitsstufen behalten Sie die Kontrolle über Ihren PC.



Viele Grüße, Ihr



Michael-Alexander
Beisecker,
Deutschlands

PC-Sicherheitsexperte Nr. 1

4.363 kritische Sicherheitslücken Anfang 2018

Machen Sie Ihre PC-Programme sicher

Ihre wichtigsten PC-Programme sind durch Schadprogramme und Hacker-Angriffe gefährdet, denn sie haben kritische Sicherheitslücken. Daher habe ich für Sie die Top 10 der gefährdetsten Programme erstellt und warne Sie eindringlich: Sie kennen alle diese Programme, denn die meisten davon sind auch auf Ihrem PC! Aber keine Sorge: Mit meinem Schutzsystem arbeiten Sie trotz Sicherheitslücken weiterhin mit einem sicheren PC.

Die für Hacker-Angriffe höchst anfälligen Programme auf Ihrem PC haben eine Funktion, etwa das Anzeigen von Videos im Internet (Adobe Flash), das Anzeigen von PDF-Dateien (Adobe Acrobat Reader DC), oder sie werden für andere Programme wie LibreOffice benötigt (Java). Sie können diese Programme daher nicht einfach alle deinstallieren.

Die Top 10 der gefährdetsten Programme mit kritischen Sicherheitslücken

Platz	Unsicheres Programm	Kritische Sicherheitslücken 2017	Empfehlung oder Hinweis
1.	Adobe Flash	875	Das sicherste häufig genutzte Programm hatte gerade einmal 5 Sicherheitslücken!
2.	Microsoft Internet Explorer	601	Bei Windows 10 wurde der Internet Explorer von Microsoft durch Edge ersetzt. Edge wies nur 44 kritische Sicherheitslücken auf.
3.	Mozilla Firefox	506	Verwenden Sie stattdessen Firefox ESR.
4.	Acrobat Reader bis Version 11.0, seit 2015 Adobe Acrobat Reader DC (siehe Platz 5)	436	Entfernen Sie das veraltete PDF-Programm.
5.	Adobe Acrobat Reader DC	387	Stellen Sie diese neueste Version sicher ein (siehe Sicherheitsstufe 3, Seite 5).
6.	Mozilla Thunderbird	358	Auch die Alternative Microsoft Outlook ist gefährdet (siehe Platz 7).
7.	Microsoft Office 2007	342	Verwenden Sie ein aktuelles Office ab 2010.
8.	Adobe Air	342	Entfernen Sie Adobe Air.
9.	Adobe Reader bis Version 5.0, danach umbenannt in Acrobat Reader (siehe 4.)	307	Entfernen Sie das veraltete PDF-Programm.
10.	Google Chrome	209	Ersetzen Sie Chrome durch Firefox ESR.

Internet-Kriminelle konzentrieren sich auf die meistgenutzten Programme auf Ihrem PC!

>>> Lesen Sie bitte weiter auf Seite 2

Mein Schutzsystem bei gefährlichen Sicherheitslücken besteht aus 4 Sicherheitsstufen:

1. Unsichere gegen sicherere Programme tauschen (siehe folgenden Beitrag auf dieser Seite).
2. Update-Funktionen der Programme überprüfen (siehe Seite 3).
3. Sicherheitsfunktionen zum Schutz aktivieren (siehe Seite 5).
4. Anwendungen durch das neue EMET schützen (siehe Seite 6).

Ich führe Sie Schritt für Schritt durch alle 4 Sicherheitsstufen hindurch und zeige Ihnen, bei welchen der 10 gefährdetsten Programme Sie diese Maßnahmen anwenden sollen.

Sind Sie am Ende dieser Spezialausgabe angelangt, ist Ihr PC so gut wie nur irgend möglich vor den Gefahren von Sicherheitslücken geschützt – und zwar nicht nur bei den 10 gefährdetsten Programmen, sondern bei allen neuen Sicherheitslücken sämtlicher auf Ihrem PC befindlicher Programme!

Warnung: Bitte verwenden Sie nur die von mir empfohlenen Tools zur Absicherung Ihres PCs. Ich möchte sichergehen, dass Sie nicht durch eines der zahlreichen Betrugsangebote im Internet gefährdet werden. Diese stehen in den Ergebnissen der Suchmaschinen meist sehr weit vorne, und das gerade bei Sicherheitsthemen.

Stufe 1: Ersetzen Sie gefährdete Programme

Prüfen Sie mit der nachfolgenden Tabelle, ob es für besonders gefährdete Programme auf Ihrem PC eine sicherere Alternative gibt. Es sind sicherlich nicht alle der 10 gefährdetsten Programme auf Ihrem PC installiert. Leider lassen sich manche Programme nicht einfach deinstallieren, so sind zum Beispiel Adobe Flash und Internet Explorer fester Bestandteil von Windows 10 und im Fall des Internet Explorers auch von Windows 7. Sie können solche Programme aber deaktivieren oder sicherere Programme dafür einsetzen.

Ein mit sicheren Programmen betriebener PC ist der beste Schutz vor Kriminellen. Es ist daher sehr wichtig, dass Sie die Anzahl der Sicherheitslücken Ihrer Programme durch eine regelmäßige Versionspflege minimieren. Die Programmversionen aller installierten Programme ständig zu überprüfen, bedeutet jedoch

viel unproduktive Arbeit. Konzentrieren Sie sich daher auf die 10 gefährdetsten Programme. Damit haben Sie die wichtigsten Sicherheitslücken abgedeckt. Ich verspreche Ihnen: Der Rest macht Ihnen durch meine in 5 Minuten eingerichtete Sicherheitsstufe 4 auch keinen Kummer mehr.

Unsicheres Programm	Ihre Alternative oder Sicherheitsvorkehrung
1. Adobe Flash	Durch ständig neue kritische Sicherheitslücken ist kein sicherer Betrieb möglich: Erhöhen Sie die Sicherheit mit meiner Sicherheitsstufe 3 ab Seite 5, indem Sie Adobe Flash in Ihren Browsern deaktivieren.
2. Internet Explorer	Mozilla Firefox ESR: Installieren Sie Mozilla Firefox ESR über den Link https://www.mozilla.org/de/firefox/organizations/all/ . Als zusätzlichen Schutz können Sie den Internet Explorer deaktivieren (siehe Seite 5).
3. Firefox	Mozilla Firefox ESR: Ersetzen Sie Mozilla Firefox durch die sicherere Variante Mozilla Firefox ESR (https://www.mozilla.org/de/firefox/organizations/all/). Zusätzlich empfehle ich Ihnen Browser in the Box (Bitbox) bei Internetseiten und Anwendungen, denen Sie nicht voll vertrauen. Installieren Sie Bitbox über den Link https://www.chip.de/downloads/BitBox-Browser-in-the-Box-Firefox-Edition_48987303.html . Überprüfen Sie die Update-Funktion von Firefox in Sicherheitsstufe 2 (ab Seite 4) und aktivieren Sie die Sicherheitsfunktionen in Sicherheitsstufe 3 (ab Seite 5).
4. Acrobat Reader	Durch abgelaufenen Support kein sicherer Betrieb möglich: Ersetzen Sie Acrobat Reader durch die aktuelle Version Acrobat Reader DC und nehmen Sie die Sicherheitseinstellungen vor oder verwenden Sie das PDF-Anzeigeprogramm Foxit Reader, das Sie vom Link https://www.foxitsoftware.com/de/pdf-reader/ herunterladen.
5. Adobe Acrobat Reader DC	Sichere Einstellungen oder Foxit Reader: Möchten Sie Acrobat Reader DC aus Kompatibilitätsgründen weiterverwenden, aktivieren Sie in Sicherheitsstufe 3 die Sicherheitsfunktionen für PDF-Dateien (siehe ab Seite 5). Damit können Ihnen die kritischen Sicherheitslücken nicht mehr gefährlich werden. Ich empfehle Ihnen ansonsten den Wechsel zu Foxit Reader, der wegen seiner wenigen Sicherheitslücken sicherer ist.
6. Mozilla Thunderbird	Internetseite Ihres E-Mail-Anbieters oder Office: Verwenden Sie nach Möglichkeit die Internetseite Ihres E-Mail-Anbieters, dann brauchen Sie kein E-Mail-Programm wie Thunderbird oder Outlook aus Microsoft Office.

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.

Unsicheres Programm	Ihre Alternative oder Sicherheitsvorkehrung
7. Microsoft Office	Microsoft Office in aktueller Version oder LibreOffice: Wechseln Sie bei einem älteren, nicht mehr unterstützten Office wie 2007 zu einer aktuellen Version. Es wird bei richtiger Einstellung automatisch mit Windows aktualisiert (siehe Seite 4). Möchten Sie den Kaufpreis für Office sparen, wechseln Sie zum kostenlosen LibreOffice.
8. Adobe Air	Durch ständig neue kritische Sicherheitslücken sicherer Betrieb fraglich: Sie sollten Adobe Air deinstallieren, sofern Sie es nicht unbedingt für eine unverzichtbare Windows-Anwendung benötigen.
9. Adobe Reader	Durch abgelaufenen Support kein sicherer Betrieb möglich: Überprüfen Sie Ihre älteren PCs mit Windows 7, Vista oder XP auf Adobe Reader. Das veraltete Programm ist dort häufig vorhanden. Ersetzen Sie Adobe Reader durch die aktuelle Version Acrobat Reader DC und nehmen Sie die Sicherheitseinstellungen vor oder verwenden Sie Foxit Reader.
10. Google Chrome	Mozilla Firefox ESR: Installieren Sie Mozilla Firefox ESR über den Link https://www.mozilla.org/de/firefox/organizations/all/ . Falls Sie bei Google Chrome bleiben möchten, überprüfen Sie in Sicherheitsstufe 2 (siehe Seite 4) die Update-Funktion.


Tauschen Sie die 10 am meisten gefährdeten Programme mit meiner Anleitung einfach aus oder stellen Sie sie sicher ein.

In 5 Schritten setzen Sie meine Empfehlungen um

Die Tabelle enthält wichtige Empfehlungen zum Ersatz der Programme Acrobat Reader, Adobe Reader, Internet Explorer, Firefox und Google Chrome. Haben Sie sich dazu entschlossen, gehen Sie wie folgt vor:

1. Laden Sie das in der Tabelle genannte Ersatzprogramm herunter. Das ist z. B. bei Adobe Acrobat Reader der **Foxit Reader**.
2. Installieren Sie das Ersatzprogramm. Dazu rufen Sie die Download-Liste (den Download-Ordner) Ihres Browsers auf. Das geht mit **(Strg)+(J)** am schnellsten oder bei Firefox über das Symbol . Starten Sie das heruntergeladene Programm mit einem Doppelklick.
3. Bestätigen Sie der Benutzerkontensteuerung das Ausführen des Programms und folgen Sie dem Assistenten.
4. Probieren Sie das Ersatzprogramm ein paar Tage aus, ob Sie mit der Bedienung zurechtkommen. Öffnen Sie damit unbedingt auch häufig von Ihnen benötigte Dateien (PDF-

Dateien im Fall des Adobe Acrobat Reader DC) oder Webseiten im Fall eines Ersatz-Browsers.

5. Verläuft mit dem Ersatzprogramm alles zu Ihrer Zufriedenheit? Dann drücken Sie die Tastenkombination  + **(R)** und geben **control** ein, gefolgt von der Eingabetaste **(Enter)**, um die **Systemsteuerung** aufzurufen. Stellen Sie **Anzeige** oben rechts auf **Große Symbole**.
6. Deinstallieren Sie das alte Programm über **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7). Gefällt Ihnen Ihr bisheriges Programm aber doch besser, deinstallieren Sie das Ersatzprogramm wieder, damit keine ungepflegten Altlasten zurückbleiben.



Mein Tipp: Tauschen Sie ein Programm nach dem anderen aus. Lassen Sie sich damit ruhig bis zur nächsten Ausgabe Ihres PC-Sicherheits-Beraters Zeit. Der Grund: Eventuell auftretende Fehler können Sie dann klar einem Programm zuordnen. Darüber hinaus können Sie sich auf die Einarbeitung in das neue Programm konzentrieren.

Stufe 2: Prüfen Sie die Update-Funktionen


Antiviren-Programme versagen bei Angriffen über Sicherheitslücken von Programmen – ausnahmslos! Ohne eine ganz wichtige Funktion wäre Ihr PC daher wahrscheinlich schon von Dutzenden von Schadprogrammen unrettbar infiziert. Ich rede von den automatischen Update-Funktionen bei Windows und den verbreitetsten Programmen. Kontrollieren Sie daher bei Ihren Programmen, ob die Update-Funktionen sicher eingestellt sind.

Sofern Sie Adobe Flash noch nicht aufgrund einer früheren Empfehlung von mir komplett entfernt haben, beginnen Sie die Kontrolle mit diesem Programm. Auch die auf den Plätzen 4, 5, 8 und 9 stehenden gefährdeten Programme sind vom selben Hersteller. Sie beheben also bis zu fünf Sicherheitsrisiken auf einen Schlag und haben Zeit gespart.

Update-Check 1: So prüfen Sie die automatischen Sicherheitsupdates von Adobe Acrobat/Adobe Reader und Adobe Flash

Ob für die aktuellen Adobe-Programme automatische Updates erfolgen oder nicht, erfahren Sie über einen Eintrag in

der Registrierungsdatenbank von Windows. Stellen Sie in nur 7 Schritten die Update-Funktion ein:

1. Rufen Sie mit  + **(R)** das **Ausführen**-Fenster auf.
2. Geben Sie **regedit** ein und drücken Sie die Eingabetaste **(Enter)**. Bestätigen Sie der Benutzerkontensteuerung per Klick auf **Ja**, dass Sie den Registrierungseditor starten möchten.
3. Navigieren Sie zu folgendem Schlüssel:
**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432-No-
de\Adobe\Adobe ARM\Legacy\Reader\{Produkt Code}**

- Prüfen Sie, ob im rechten Fenster bei **Mode** in der Spalte **Daten** der Wert **3** steht. Das bedeutet: Die Adobe-Updates werden automatisch heruntergeladen und installiert.
- Steht hier ein anderer Wert, wie zum Beispiel **0** (Updates werden weder heruntergeladen noch installiert), klicken Sie **Mode** mit der rechten Maustaste an und wählen **Ändern**. Schreiben Sie **3** in das Feld **Wert** und klicken Sie auf **OK**.
- Schließen Sie den Registrierungseditor per Klick auf die **Schließen**-Schaltfläche rechts oben.
- Starten Sie Windows neu und die automatischen Updates für Ihre Adobe-Programme sind aktiviert.

Update-Check 2: Überprüfen Sie die automatischen Sicherheits-Updates von Internet Explorer, Windows und Office

Windows 10: Rufen Sie das **Start**-Menü, **Einstellungen**, **Update und Sicherheit** und **Windows Update** sowie **Erweiterte Optionen** auf und prüfen Sie diese Einstellungen:


- Setzen Sie einen Haken vor **Updates für andere Microsoft-Produkte bereitstellen**.
- Entfernen Sie – sofern vorhanden – den Haken vor **Upgrades zurückstellen**.

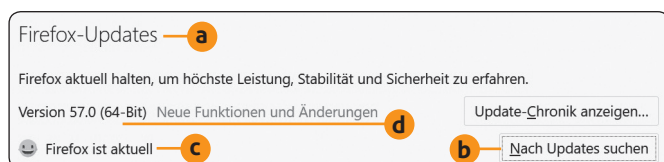
Windows 7: Klicken Sie in der **Systemsteuerung** unter **System und Sicherheit** auf **Einstellungen ändern**. Prüfen Sie, ob unter **Wichtige Updates** das Kontrollkästchen **Updates automatisch installieren (empfohlen)** aktiviert ist. Wenn nicht, setzen Sie per Klick den Haken.

Update-Check 3: Überprüfen Sie die Version und Einstellung von Firefox

Die aktuelle Firefox-Version seit November 2017 ist Firefox 57 „Quantum“ und im Fall des sichereren Firefox ESR ist es 52.5. Führen Sie diesen zweistufigen Check durch, um Ihre Firefox-Version sicher und aktuell einzustellen:

Stufe 1: Haben Sie die aktuelle Version installiert?

- Öffnen Sie **Firefox**, klicken Sie auf das **Menü öffnen**-Symbol  und wählen Sie **Einstellungen**.
- Im Register **Allgemein** blättern Sie nach unten bis zu **Firefox-Updates** **a**. Klicken Sie danach auf **Nach Updates suchen** **b**. Erhalten Sie die Meldung **Firefox ist aktuell** **c**, ist Ihr Firefox auf dem aktuellen Stand. Die aktuelle Version steht oberhalb dieser Meldung **d**.



Klicken Sie auf **Update-Chronik anzeigen**, um einen Überblick der letzten Sicherheits-Updates zu erhalten.

Stufe 2: Stellen Sie diese 3 Sicherheitseinstellungen ein:


- Aktivieren Sie im Register **Allgemein** unter **Firefox-Updates** im Bereich **Firefox erlauben** die erste Option **Updates automatisch zu installieren (empfohlen)**, sofern diese nicht bereits ausgewählt ist.

- Entfernen Sie den Haken bei **Einen Hintergrunddienst verwenden, um Updates zu installieren**. So erfolgen die Updates nicht unbemerkt im Hintergrund und der Dienst kostet keine Systemleistung.
- Entfernen Sie den Haken bei **Suchmaschinen automatisch aktualisieren**, damit diese Funktion nicht durch einen Browser-Entführer missbraucht werden kann.

Warnung: Finden Sie die hier beschriebenen Menüs und Optionen bei Ihrem Firefox nicht, haben Sie entweder bereits Firefox ESR (siehe Tabelle auf Seite 2, Zeile 3) oder ein stark veraltetes und daher durch Hunderte von Sicherheitslücken extrem gefährliches Firefox. Deinstallieren Sie die veraltete Version über die **Systemsteuerung** und **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7). Anschließend installieren Sie das aktuelle Firefox ESR oder Firefox in der aktuellen Version, das Sie am Link <https://www.mozilla.org/de/firefox/new/> finden.

Update-Check 4: Automatische Sicherheits-Updates bei Google Chrome

Google Chrome gehört zwar zu den Top 10 der gefährdetsten Programme, ist aber auch der am meisten angewendete und schnellste Browser. Möchten Sie Chrome daher weiternutzen und nicht zu Firefox ESR wechseln (siehe Tabelle Seite 3, Zeile 10), überprüfen Sie unbedingt die Version:

- Öffnen Sie **Google Chrome**, klicken Sie auf das **Menü öffnen**-Symbol  und wählen Sie **Einstellungen**.
- Wählen Sie **Hilfe** und **Über Google Chrome**.
- Steht rechts nun **Version 62** oder falls bereits erschienen **Version 63**? Dann ist Google Chrome bei Ihnen auf dem aktuellen Stand. Wird Ihnen eine deutlich ältere Version angezeigt, deinstallieren Sie Google Chrome über die **Systemsteuerung** und **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7). Installieren Sie anschließend die neueste Version von Google Chrome über den Link <https://www.google.de/chrome/>.
- Google Chrome findet neue Versionen automatisch und installiert sie auch ohne Rückfrage. Wurde eine neue Version gefunden, erkennen Sie dies an der Schaltfläche **Neu starten**. Klicken Sie einfach darauf und starten Sie Google Chrome neu. Erst nach dem PC-Neustart ist Ihr Browser wieder sicher!



Mein Tipp: Die aktuelle Windows-Version 10 sowie Windows auf einem Notebook werden kaum noch heruntergefahren. Sie erwachen beim Einschalten aus dem Stromsparmodus.

Ein geöffneter Firefox- oder Google-Chrome-Browser bleibt somit über Tage oder gar Wochen geöffnet. Das ist gefährlich, denn erst beim Neustart werden sicher alle Updates installiert. Der Speicherverbrauch kann zum Absturz und zu Datenverlusten führen. Um die Sicherheit Ihrer Daten zu gewährleisten, schließen Sie daher Ihren Browser mindestens einmal am Tag.

Stufe 3: Verringern Sie die Betrugsgefahr mit 3 sicheren Programmeinstellungen

Die vielen Sicherheitslücken in den 10 gefährdetsten Programmen werden Ihnen nicht gefährlich, wenn Sie diese Programme wie Adobe Flash erst gar nicht auf Ihren Rechner lassen. Ohne Programme macht ein PC aber keinen Sinn. Daher werden Sie die meisten Programme trotz Sicherheitslücken weiter nutzen müssen. Das ist mit den folgenden Sicherheitseinstellungen auch kein Problem mehr.

Adobe Flash wird bei Internet Explorer, Edge und Google Chrome automatisch mit dem Browser bzw. mit Windows 10 aktualisiert und bekannte Sicherheitslücken werden geschlossen. Diese Flash-Updates erfolgen jedoch mit zeitlicher Verzögerung von bis zu mehreren Wochen nach dem Bekanntwerden der Flash-Sicherheitslücken. Sie sind in der Zwischenzeit immer in Gefahr, solange Sie Flash nicht deaktivieren.

Firefox ab Version 57 entfernt den Original-Flash-Player von Adobe (Shockwave Player) automatisch. Das Flash-Risiko bleibt jedoch auch bei Firefox bestehen, denn Mozilla erlaubt weiterhin die Installation eines der vielen anderen Flash-Player als Firefox-Erweiterung.

Sie sollten daher auch bei Firefox eine Flash-Überprüfung durchführen und das integrierte Flash der anderen Browser auf Ihrem PC abschalten.

Sicherheitscheck 1: Deaktivieren Sie Adobe Flash in allen installierten Browsern

Erhöhen Sie die Sicherheit Ihres PCs, indem Sie Adobe Flash deaktivieren. So geht's:

1. Öffnen Sie **Microsoft Edge**.
2. Klicken Sie auf das **Menü-Symbol** ☰ oben rechts und wählen Sie **Einstellungen**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **Erweiterte Einstellungen anzeigen**.
4. Klicken Sie auf den Schalter unter **Adobe Flash Player verwenden**, um diesen auf **Aus** zu stellen.

Verwenden Sie Google Chrome, deaktivieren Sie in nur 4 Schritten den Adobe Flash Player in Chrome:

1. Klicken Sie auf das **Menü-Symbol** ⋮ oben rechts und wählen Sie **Einstellungen**.
2. Blättern Sie in den Einstellungen nach unten und klicken Sie auf **Erweitert**.
3. Klicken Sie unterhalb von **Sicherheit und Datenschutz** auf **Inhaltseinstellungen**.
4. Klicken Sie auf **Flash** und dann auf **Zuerst fragen (empfohlen)**. Der Schalter wird grau und der Text ändert sich in **Ausführen von Flash für Websites blockieren**. Jetzt wird unter Chrome kein Flash mehr ausgeführt.

Firefox achtet schon von sich aus darauf, dass Ihnen Adobe Flash nicht gefährlich wird. Überprüfen Sie trotzdem die Firefox-Sicherheitseinstellung:

1. Öffnen Sie **Mozilla Firefox**.

2. Klicken Sie auf das **Menü-Symbol** ☰ oben rechts und wählen Sie **Add-ons** und dann links das **Puzzle-Symbol** 🧩.
3. Überprüfen Sie, ob hier ein Eintrag mit dem Namensbestandteil **Flash** vorhanden ist, wie zum Beispiel **YouTube Flash Player**, **YouTube Flash Video Player** oder **Flash Video Player for Facebook**. Klicken Sie hinter jeder dieser Erweiterungen auf **Deaktivieren** oder klicken Sie auf **Entfernen**, wenn Sie die Erweiterung nicht mehr benötigen. Ich empfehle Ihnen das Entfernen sämtlicher installierter Flash-Player, damit sie nicht durch ein Schadprogramm wieder aktiviert werden können.



Mein Tipp: Sollten Sie eine Flash-Erweiterung einmal benötigen, klicken Sie zuvor auf **Aktivieren**. Wenden Sie Flash-Erweiterungen aber nur bei Internetseiten an, denen Sie vertrauen, und deaktivieren Sie die Flash-Erweiterung nach der Anwendung wieder.

Sicherheitscheck 2: Deaktivieren Sie den Internet Explorer

Der Internet Explorer ist nicht nur wegen seiner vielen Sicherheitslücken eine Gefahr (siehe Tabelle auf Seite 1, Zeile 2). Er beinhaltet auch das gefährliche ActiveX (erlaubt Internet-Kriminellen das Ausführen von Skriptprogrammen) und das unsichere Silverlight.

Die Gefahr für Ihren Windows-PC besteht selbst dann, wenn der Internet Explorer von Ihnen gar nicht verwendet wird. Hacker und Schadprogramme können seine Funktionen aufrufen und über die Sicherheitslücken darin Ihren PC infizieren.

Deaktivieren Sie den Internet Explorer daher, denn deinstallieren lässt er sich nicht:

1. Öffnen Sie mit der Tastenkombination **Windows + R** das **Ausführen-Fenster**. Geben Sie **control** gefolgt von der Eingabetaste **[Enter]** ein, um die **Systemsteuerung** aufzurufen.
2. Stellen Sie in der **Systemsteuerung** bei **Anzeige** oben rechts **Große Symbole** ein und klicken Sie auf **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7).
3. Klicken Sie links auf **Windows-Features aktivieren oder deaktivieren** (Windows 10) oder **Windows-Funktionen aktivieren oder deaktivieren** (Windows 7).
4. Blättern Sie nach unten bis zur Option **Internet Explorer 11** und entfernen Sie per Mausklick den Haken davor.
5. Im Fall von Windows 10 erscheint eine Warnung. Bestätigen Sie diese mit einem Klick auf **Ja**.

Hinweis: Keine Sorge, sollten durch das Deaktivieren des Internet Explorers tatsächlich Fehler bei Anwendungen auftreten, können Sie den Internet Explorer jederzeit wieder aktivieren. Dazu führen Sie diese Anleitung erneut aus und setzen in Schritt 4 wieder den Haken vor **Internet Explorer 11**.

6. Klicken Sie auf **OK** und starten Sie den PC neu, wenn Sie dazu aufgefordert werden.



Mein Tipp: Sehen Sie nach jedem größeren Windows-Update nach, ob der Internet Explorer noch deaktiviert ist. Die nächste Kontrolle sollten Sie im Mai 2018 nach dem Frühjahrs-Creators-Update vornehmen.

Sicherheitscheck 3: Schalten Sie alle gefährlichen Funktionen von Adobe Acrobat Reader aus

In Sicherheitsstufe 2 habe ich Ihnen den Wechsel zu Foxit Reader empfohlen. Haben Sie diesen Wechsel durchgeführt und Adobe Acrobat Reader entfernt, gehen Sie direkt weiter zur Sicherheitsstufe 4. Benötigen Sie Adobe Acrobat Reader jedoch weiter, schalten Sie unbedingt voreingestellt die potenziell gefährlichen Funktionen aus:

1. Öffnen Sie **Adobe Acrobat Reader**.

2. Öffnen Sie das Menü **Bearbeiten** und wählen Sie **Voreinstellungen**.
3. Wählen Sie links das Register **Sicherheit (erweitert)**.
4. Stellen Sie die Optionen unter **Sandbox-Schutz** und **Erweiterte Sicherheit** so ein, wie es in der folgenden Abbildung zu sehen ist. Dann schließen Sie die Einstellungen wieder.

Der Sandbox-Schutz führt geöffnete PDF-Dateien in einem eigenen, fest zugewiesenen Speicherbereich aus, aus dem kein Angriff auf andere Anwendungen oder Windows möglich ist – Ihr PC ist geschützt.



Mein Tipp: Diese Sicherheitseinstellung lässt Sie PDF-Dateien weiter wie bisher lesen, aber zum Beispiel nicht mehr ausdrucken oder mit Kommentaren versehen. Dazu müssen Sie die Sicherheitseinstellung zuvor bewusst wieder aufheben. Machen Sie dies nur bei PDF-Dateien, bei denen Sie sich wirklich sicher sind, dass sie keine Gefahr darstellen.

Stufe 4: Schützen Sie Ihren PC bei Windows 7 mit EMET 5.52

Die Sicherheitslücken in Ihren Anwendungen lassen sich nicht alle schließen. Es kommen täglich neue Lücken hinzu. Teilweise werden Sicherheitslücken erst nach Jahren entdeckt und meist erst Wochen oder gar Monate später geschlossen. Das trifft auf Hunderte von Sicherheitslücken auf Ihrem PC zu. Sie können nicht verhindern, dass Internet-Kriminelle Sie darüber angreifen. Die Sicherheitsfunktionen von Windows 10 lassen solche Angriffe jedoch ohne Folgen verpuffen. Dafür hat Microsoft im Herbst 2017 das Schutzprogramm EMET in Windows 10 integriert. Sie erfahren hier, welche Schutzfunktionen Ihnen EMET bietet. Windows 7 fehlt dieser Schutz. Arbeiten Sie noch mit Windows 7? Ich verrate Ihnen, wie Sie es mit EMET 5.52 auf den Sicherheitsstand von Windows 10 bringen.

Windows 10 enthält zu Ihrem Schutz 15 spezielle Funktionen mit kryptischen Namen wie ASLR, DEP oder SEHOP. Eine Erklärung der wichtigsten Funktionen finden Sie in der nachfolgenden Tabelle. Die meisten Programmhersteller nutzen diese Funktionen jedoch nicht. Das liegt hauptsächlich daran, dass mit diesen Funktionen der Testaufwand steigt und daher die

Entwicklungskosten deutlich höher werden. Die Entwickler sparen also auf Kosten Ihrer Sicherheit! Schalten Sie diese Funktionen bei Windows 7 ein, denn erst dann schützt Sie Windows 7 zuverlässig vor Schadprogrammen. Windows 10 aktiviert diesen Schutz automatisch und führt viele Programme erst gar nicht aus, wenn ein vorausgesetzter Schutz fehlt.

Sicherheitsfunktion	Bedeutung
ASLR (Address Space Layout Randomization = zufälliges Anlegen des Adressspeichers)	Früher griffen Programme immer über feste Adressen auf ihre Daten oder auch Programmbestandteile im Arbeitsspeicher zu. Das ermöglichte Angreifern, diese Adressbereiche mit eigenen Daten zu überschreiben oder Daten daraus zu lesen, sie zu verändern und zu stehlen. Sichere Programme ändern daher die Adressen laufend über einen sicheren Zufallszahlengenerator. Aktivieren Sie diese Funktion, werden ältere Programme für Windows XP oder Vorgängerversionen nicht mehr laufen. Solche Programme sollten Sie aus Sicherheitsgründen aber auch nicht mehr einsetzen.

Sicherheitsfunktion	Bedeutung
ASR (Attack Surface Reduction = Verringerung der Angriffsfläche)	Reduziert die Anzahl der Angriffspunkte (engl. „attack vectors“), an denen ein Angreifer („attacker“) unbefugt auf Ihre Daten zugreifen oder Daten aus einer Programmumgebung herausziehen kann.
Block untrusted fonts = nicht vertrauenswürdige Schriften sperren	Diese ab Windows 10 verfügbare Schutzfunktion soll eine Infektion Ihres PCs über eine manipulierte Schriftartendatei verhindern. Ältere Schriften verfügen nicht über das erforderliche Zertifikat und werden daher gesperrt.
Certificate Trust/Pinning = nur zertifizierte Sicherheit erlauben	Hier wird über Zertifikate überprüft, ob dem betreffenden Programm zu trauen ist. Das Problem: Viele Programmhersteller verwenden aus Kostengründen keine Zertifikate oder gehen damit nicht sorgfältig genug um. Es kann somit beim Aktivieren dieser Funktion zu Fehlern kommen.
DEP (Data Execution Prevention = Datenausführung verhindern)	Windows 10 teilt den Arbeitsspeicher in Bereiche ein, in denen Daten ausgeführt („executable“) oder nicht ausgeführt („nonexecutable“) werden dürfen. DEP verhindert, dass Schadprogramme auf nicht vorgesehene Bereiche zugreifen. Ältere Programme können dadurch abstürzen, da sie die Anforderungen moderner Betriebssysteme nicht beachten. Solche Programme gehören aber nicht auf Ihren sicheren PC.
SEHOP (Structured Exception Handler Overwrite Protection = Schutz vor dem Überschreiben strukturierter Ausnahmebehandlungen)	Verhindert einen Angriff über einen Speicherüberlauf (Buffer Overflow) oder einen anderen, durch Schadprogramme provozierten Fehler. Das ist sehr wichtig, denn Schadprogramme ändern die Programmschritte für die Ausnahmebehandlung („exception handling“). Beim Auftreten des Fehlers wird dann die Routine des Schadprogramms vom gehackten Programm ausgeführt.

Die Erklärung der wichtigsten Sicherheitsfunktionen von Windows 10 und der Einstellungen von EMET.

Für Ihren Schutz brauchen Sie das aktuellste EMET

Microsoft bietet zum einfachen Aktivieren dieser Schutzfunktionen bei Ihrem Windows 7 das Tool EMET 5.52 an. Sehen Sie im **Start**-Menü nach, ob dort bereits **EMET GUI** eingetragen ist. Falls EMET noch nicht vorhanden ist, überspringen Sie den nächsten Abschnitt mit den Versionshinweisen. Ist EMET vorhanden, rufen Sie es auf und überprüfen die Version. Dazu klicken Sie auf das blaue **Help**-Symbol (Hilfe) und wählen **About** (Über). Die Version wird Ihnen nun angezeigt.

Achten Sie bei EMET auf das Support-Ende

Wie Sie in der nachfolgenden Tabelle sehen, ist der Support für EMET 5.5 am 27. Januar 2017 abgelaufen. Sie benötigen aus Sicherheitsgründen daher die aktuellste Version 5.52. Aller-

dings liefert Microsoft nach dem 31. Juli 2018 für EMET 5.52 auch keine Sicherheits-Updates mehr. Laut Microsoft ist es „nicht geplant, nach dem 31. Juli 2018 Support oder Sicherheits-Updates für EMET anzubieten“.

EMET-Version	Support-Beginn	Support-Ende
EMET 5.5	29. Januar 2016	27. Januar 2017
EMET 5.52	27. Januar 2017	31. Juli 2018

Derzeit sollten Sie nur noch EMET 5.52 verwenden, wobei der Support von Version 5.52 im Sommer ausläuft und Sie dann nur noch als Anwender von Windows 10 durch EMET sicher geschützt sind.

Wichtig für EMET 5.52:

Ist „.NET Framework 4.5“ auf Ihrem PC installiert?

EMET benötigt „.NET Framework 4.5“, das bei Windows 10 bereits enthalten ist. Arbeiten Sie mit Windows 10, müssen Sie nichts unternehmen. Haben Sie Windows 7, finden Sie mit dieser Anleitung heraus, welches „.NET Framework“ bei Ihnen installiert ist:

1. Laden Sie das Tool **netversioninfo.bat** von unserer sicheren Service-Webseite www.pc-sicherheitsberater.de herunter.



Mein Tipp: Microsoft liefert für Windows 7 zwar noch bis zum 14. Januar 2020 Sicherheits-Updates, behandelt es aber praktisch als „Windows 2. Klasse“. Für neu entwickelte Prozessoren gibt es keine Treiber mehr, der Internet Explorer und der Movie Maker werden nicht mehr weiterentwickelt und Sicherheits-Updates werden gar nicht oder mit wochenlanger Verzögerung im Vergleich zu Windows 10 geliefert. Ich rate Ihnen daher, bis spätestens Ende Juli 2018 zu Windows 10 zu wechseln.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Dieses monothematische Supplement
„Software-Sicherheitslücken schließen“
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 telefoni-
sche Auskünfte, ausgeschlossen. Vervielfältigungen jeder
Art sind nur mit Genehmigung des Verlags gestattet.

Copyright 2019 by Verlag für die Deutsche Wirtschaft AG;
Bonn, Bukarest, Manchester, Melbourne, Warschau



- Rufen Sie es mit einem Doppelklick auf. Es öffnet sich die Eingabeaufforderung und darin werden die vorhandenen „.NET-Framework“-Versionen angezeigt **a**.

```

C:\ Auswählen C:\WINDOWS\system32\cmd.exe
File: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Microsoft
InternalName: Microsoft.Build.Tasks.v4.0.dll
OriginalFilename: Microsoft.Build.Tasks.v4.0.dll
FileVersion: 4.6.1038.0 built by: NETFXREL2
FileDescription: Microsoft.Build.Tasks.v4.0.dll
Product: Microsoft .NET Framework
ProductVersion: 4.6.1038.0
Debug: False
Patched: False
PreRelease: False
PrivateBuild: True
SpecialBuild: False
Language: Englisch (Vereinigte Staaten)

Drücken Sie eine beliebige Taste . . .


```

Blättern Sie mit dem Laufbalken rechts nach unten, dann gelangen Sie zu den höheren Versionsnummern – im Beispiel ist die höchste Version 4.6 **a**.

- Finden Sie keine Version 4.5, laden Sie „.NET Framework 4.5“ über den Link <https://www.microsoft.com/de-de/download/details.aspx?id=30653> herunter.

In 5 Minuten erledigt: EMET installieren und einstellen


Mit meiner Hilfe installieren Sie EMET in wenigen Minuten:

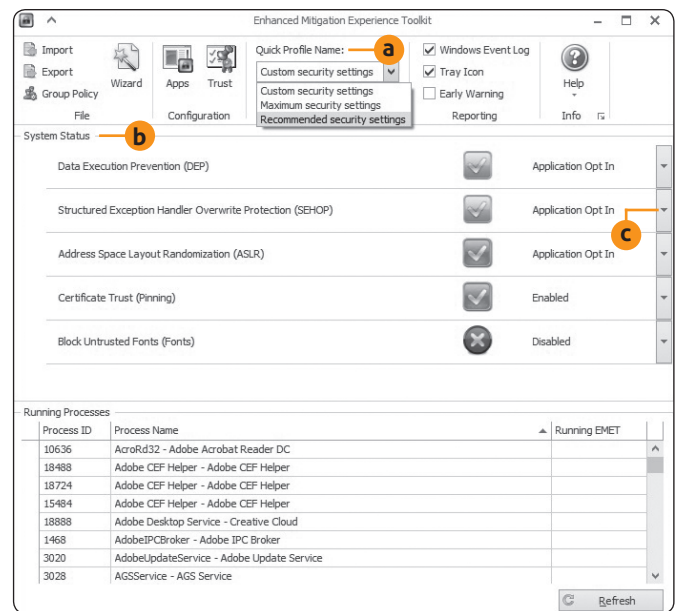
- Laden Sie die neueste Version von EMET am Link <https://support.microsoft.com/de-de/help/2458544/the-enhanced-mitigation-experience-toolkit> herunterladen. Diese EMET-Version läuft mit allen aktuellen Windows-Versionen.
- Öffnen Sie die Download-Liste Ihres Browsers (**(Strg)+[J]** oder Symbol  bei Firefox) und starten Sie die heruntergeladene Datei **EMET_Setup.msi** mit einem Doppelklick.
- Der Installations-Assistent von EMET begrüßt Sie in englischer Sprache. Eine deutsche Version gibt es derzeit nicht. Doch keine Sorge, ich führe Sie durch alle Einstellungen.
- Klicken Sie auf der ersten und zweiten Seite unten rechts auf **Next >** (Weiter).
- Sie sind jetzt auf der Seite **License Agreement** (Lizenzvereinbarungen). Klicken Sie hier die Option **I Agree** (Ich stimme zu), an, um die Lizenzbedingungen anzuerkennen. Klicken Sie auf dieser und der nächsten Seite rechts unten auf **Next >** (Weiter).
- Bestätigen Sie die Nachfrage der Benutzerkontensteuerung von Windows, ob EMET installiert werden soll, und warten Sie, bis die Installation abgeschlossen ist. Ein Laufbalken zeigt den Fortschritt an.
- Sie gelangen auf eine Seite mit Konfigurationseinstellungen. Wählen Sie **Use Recommended Settings** (Empfohlene Einstellungen verwenden). Zum Abschluss der Installation klicken Sie auf **Finish** (Beenden).

So aktivieren Sie EMET blitzschnell

Sie haben EMET nun installiert und brauchen nur noch die Sicherheitsfunktionen zu aktivieren. Mit maximal fünf Mausklicks wird Ihr Windows 7 um bis zu 500 Prozent sicherer. Ihr

Windows-PC ist dann vor der Mehrzahl der Windows-Schadprogramme zuverlässig geschützt:

- Öffnen Sie bei Windows 7 das **Start**-Menü, klicken Sie auf  und bestätigen Sie den Programmaufruf.
- Sehen Sie in den Einträgen unter **System Status** **b** ein gelbes oder rotes Symbol, klicken Sie dahinter auf den **Pfeil nach unten** **c** und wählen je nach Auswahl entweder **Always On** (Immer eingeschaltet) oder **Enabled** (Aktiviert). Das Symbol sollte anschließend grün dargestellt werden.



Über die Liste unter **Quick Profile Name** **a** (sinngemäß „schneller Profilwechsel“) wechseln Sie zwischen **Custom security settings** (Ihren selbst gewählten Einstellungen), **Maximum security settings** (höchstmögliche Sicherheitseinstellungen) und **Recommended security settings** (von Microsoft empfohlene Einstellungen).

- Beenden Sie EMET über die **Schließen**-Schaltfläche rechts oben und starten Sie Ihren PC neu.

Ihr Windows 7 ist jetzt durch die aktiven Sicherheitsfunktionen geschützt und trotz offener Sicherheitslücken nicht mehr so leicht angreifbar. Rufen Sie Ihre häufig verwendeten Programme auf und testen Sie, ob diese fehlerfrei funktionieren.

Meine Empfehlung: Treten nach der Anwendung von EMET Fehler auf, nehmen Sie die geänderten Sicherheitseinstellungen wieder zurück. Aktivieren Sie diese dann eine nach dem anderen, starten Sie dazwischen immer Windows 7 neu und testen Sie, bei welcher Einstellung der Fehler auftritt. Finden Sie den Fehler nicht, helfen Ihnen meine Mitarbeiter aus der Redaktion und ich gern über den Computerwissen Club: <https://club.computerwissen.de>.

Meine Sicherheitsgarantie: Mithilfe meiner 4 Sicherheitsstufen schützen Sie Ihren PC vor den Gefahren, die von den gefährdetsten Programmen ausgehen: Ganz unsichere Programme deaktivieren Sie, andere können Sie nach dem Aktivieren von sicheren Einstellungen weiter einsetzen. Jetzt sind Ihr PC und Ihre sensiblen Daten bestmöglichst vor Sicherheitslücken in Programmen geschützt.