



Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

3 Ist Ihr Prozessor verwundbar?

Ermitteln Sie den Prozessor in Ihrem PC und überprüfen Sie, ob er in der Liste der gefährdeten Modelle steht.

4 2 Sicherheits-Tools prüfen Ihren PC

Zur Sicherheitsprüfung Ihres PCs empfehle ich Ihnen zwei Tools, die besonders einfach zu bedienen sind.

5 Testen Sie die Sicherheit aller Browser

Überprüfen Sie mit diesem Sicherheitstest, ob Ihr Browser Sie wirksam vor Meltdown- und Spectre-Angriffen schützt.

7 Erst mit neuem BIOS ist Ihr PC sicher

Aktualisieren Sie zusätzlich zum neuen Windows-Update auch unbedingt das BIOS und die Treiber.

+++ Meltdown und Spectre sind für jeden PC gefährlich +++ Schützen Sie sich! +++

Der Sicherheits-Super-GAU: So wird Ihr PC wieder sicher

Fast jeder PC und ein Großteil aller Mobilgeräte sind verwundbar durch die Angriffsmethoden Meltdown und Spectre.

Die Prozessoren der Rechner lassen unbefugte Zugriffe auf Speicherbereiche mit sensiblen Nutzerdaten zu. Drei gefährliche Angriffsmethoden sind bekannt.

Betroffen ist nicht nur Ihr lokaler Windows-PC, sondern auch MacOS X, Linux und Betriebssysteme für Mobilgeräte wie Android und iOS. Sie sind jetzt auf keiner Internetseite mehr sicher.

Weist Ihr PC Sicherheitslücken auf, ist Online-Banking und Online-Shopping ab sofort ein gefährliches Russisch-Roulette-Spiel.

Meine Empfehlung: Vertrauen Sie nicht allein auf das nächste Windows-Update. Das bietet Ihnen keinen umfassenden Schutz und hat Nebenwirkungen (siehe Seite 8). Führen Sie unverzüglich meine 7 Sicherheits-Checks aus. Dann haben Sie die höchste Sicherheit.



Viele Grüße, Ihr

Michael-Alexander
Beisecker,
Deutschlands

PC-Sicherheitsexperte Nr. 1

Anleitung für den Schutz Ihrer Daten

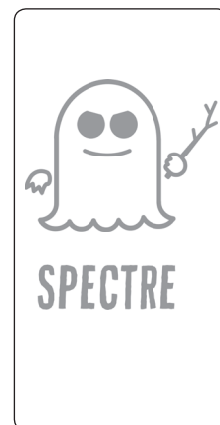
So richten Meltdown und Spectre bei Ihnen keine Schäden an

Google hat zusammen mit der Technischen Universität Graz eine Liste der bislang schlimmsten Sicherheitslücken für PCs und Mobilgeräte veröffentlicht (Quelle: Google Project Zero). Die Liste wird angeführt von Meltdown und Spectre, den gefährlichsten Angriffsmethoden, die ich in meiner über 30-jährigen Laufbahn als PC-Sicherheitsexperte kennengelernt habe. Die Angreifer erhalten Zugriff auf alle auf Ihrem PC gespeicherten oder von Ihnen eingegebenen Daten. Ihr Antiviren-Programm warnt und schützt Sie nicht. Sie brauchen verschiedene Sicherheits-Updates, um diese Gefahr wirksam abzuwenden.

Es gibt drei verschiedene Angriffsmethoden: Spectre 1, Spectre 2 und Meltdown. Spectre missbraucht Optimierungsfunktionen moderner Prozessoren. Sie versuchen, die nächste Speicheradresse und die als Nächstes auszuführenden Befehle vorherzusagen, und arbeiten diese dann spekulativ ab. Bei einem Spectre-Angriff wird der Prozessor dazu gebracht, Befehle durchzuführen und auf Speicher zuzugreifen, auf die er normalerweise nicht zugreifen würde.

Meltdown überwindet die zu Ihrem Schutz vorgesehene Trennung zwischen Speicheradressen für das Betriebssystem und den Speicheradressen von Anwendungen. Auf Speicher des Betriebssystems kann eine Anwendung normalerweise nicht zugreifen, er ist geschützt. Bisher schien das absolut sicher zu funktionieren, zumal die Speicheradressen noch zufällig vergeben werden.

Sofern eine Anwendung oder das Betriebssystem keine Sicherheitslücke hat, kann ein Schadprogramm daher theoretisch nicht auf die Daten anderer Programme zugreifen. Die jüngst entdeckten Sicherheitslücken Meltdown und Spectre zeigen jedoch, dass ein solcher Zugriff bei den meisten Prozessoren möglich ist.



Meltdown ist das englische Wort für „Kernschmelze“ und Spectre das englische Wort für „Gespenst“, daher erkennen Sie Informationen zu diesen neuen Sicherheitslücken in den Medien und im Internet an diesen beiden Logos.

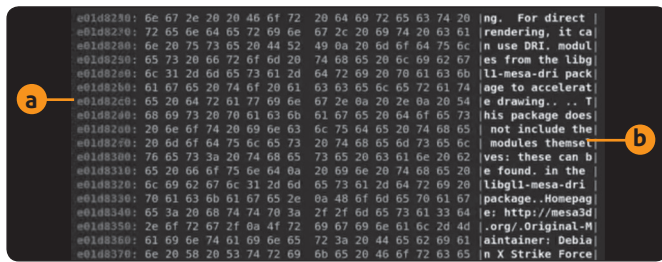
>>> Lesen Sie bitte weiter auf Seite 2

>>> Fortsetzung von Seite 1

Meltdown- und Spectre-Hacks in Aktion: Diese vier Videos veranschaulichen die Vorgehensweise

Die wissenschaftlichen Erklärungen zu diesen Sicherheitslücken sind in englischer Sprache und nur für IT-Spezialisten verständlich. Doch es gibt vier Videos, die Ihnen in weniger als zwei Minuten anschaulich zeigen, wie einfach sich mit den neuen Sicherheitslücken Ihre Daten auslesen lassen, auch Ihre bislang sicheren Passwörter. Zu sehen ist darin Folgendes:

1. Der Inhalt des Arbeitsspeichers wird gelesen **a**.
2. Passwörter werden ausspioniert **c**.

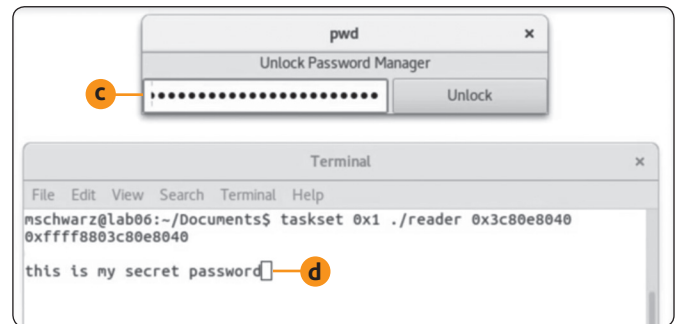


Beispiel 1: Der Inhalt des Arbeitsspeichers wird ausgelesen **a** und der Hacker sieht den Inhalt im Klartext mit allen verarbeiteten Daten **b**.

3. Verarbeitete Grafiken werden wiederhergestellt.
4. Verarbeitete Fotos werden wiederhergestellt.

Diese Videos erreichen Sie über unsere sichere Service-Webseite: www.pc-sicherheitsberater.de.

Warnung: Bitte verwenden Sie nur die von mir nachfolgend empfohlenen Videos, Hilfen und Tools zur Analyse und Absicherung Ihres PCs.



Beispiel 2: Sie geben das Passwort für Ihren Passwort-Verwalter verdeckt ein **c** und ein Hacker kann es über einen Meltdown-Angriff mitlesen **d**.

Sicherheits-Check 1: Fallen Sie nicht auf diese Betrugs-Mail herein

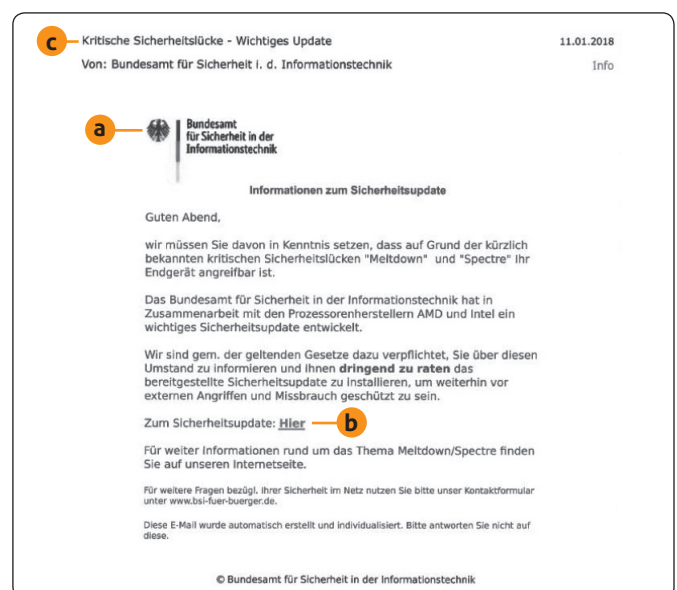
Betrüger nutzen die Verwundbarkeit der Prozessoren und den hohen Bekanntheitsgrad der Meltdown- und Spectre-Sicherheitslücken für einen dreisten Betrugsversuch. Sie verschicken E-Mails mit dem gefälschten Absender des Bundesamtes für die Informationstechnik (BSI) und empfehlen darin die Installation eines angeblichen Sicherheits-Updates. Das BSI warnt vor diesen E-Mails.

Die Phishing-Mails enthalten Absender und Logo des Bundesamtes **a**. In den E-Mails wird behauptet, die Firmen AMD und Intel hätten ein Sicherheits-Update entwickelt, das vor Meltdown- und Spectre-Angriffen schützt. Die Empfänger werden aufgefordert, dieses angebliche Update sofort zu installieren.

Ein Link in den Betrugs-Mails **b** führt auf eine gefälschte Seite, die den Seiten des BSI nachempfunden ist. Die dort zum Download angebotene Software ist ein gefährliches Schadprogramm (Trojaner).

Sie erkennen die Betrugs-Mails am Betreff **Kritische Sicherheitslücke – Wichtiges Update** **c**. Löschen Sie E-Mails mit diesem Betreff sofort, ohne sie zu öffnen.

Warnung: Seien Sie bei jeder E-Mail zum Thema „Update“ sehr vorsichtig, auch wenn sie einen anderen Betreff oder Absender hat. Enthalten solche E-Mails einen Anhang mit einem angeblichen Update oder einen Link zu einer Download-Seite, handelt es sich nahezu immer um einen Betrugsversuch mit einem gefährlichen Trojaner.



Achtung, lassen Sie sich nicht täuschen: Die E-Mail ist sowohl von der Aufmachung als auch vom Inhalt her eine sehr gute Fälschung. Fallen Sie nicht darauf herein!

Sicherheits-Check 2: Gleichen Sie alle Ihre Prozessoren mit der Sicherheitsliste ab

Besonders gefährdet durch Meltdown- und Spectre-Angriffe sind Sie, wenn in Ihrem PC ein Intel-Prozessor verbaut ist. Da die Firma Intel der Marktführer bei PC-Prozessoren ist, wird Ihr PC mit hoher Wahrscheinlichkeit mit einem Intel-Prozessor ausgestattet sein. Es kann aber auch ein Prozessor eines anderen Herstellers verbaut sein und es ist andererseits auch nicht jeder PC mit Intel-Prozessor gefährdet. Nachdem Sie Ihren Prozessor ermittelt haben, schauen Sie daher in der Liste verwundbarer Prozessoren nach, ob Ihr Prozessor dort aufgeführt ist.

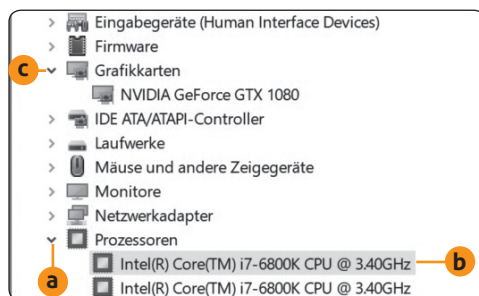
Wenn Sie Glück haben, kann ich Ihnen schon nach Sicherheits-Check 2 für Ihren PC Entwarnung geben. In 7 Schritten finden Sie heraus, welcher Prozessor in Ihrem Gerät verbaut ist.

Verwenden Sie mehrere PCs oder zusätzlich Mobilgeräte, führen Sie die nachfolgenden Anleitungen bei allen Ihren Geräten durch. Sie erhalten bei jedem Gerät ein anderes Ergebnis, sofern Sie keine baugleichen Geräte haben.

Welcher Prozessor ist in Ihrem PC verbaut?

Mit dem Geräte-Manager finden Sie das jetzt sofort heraus:

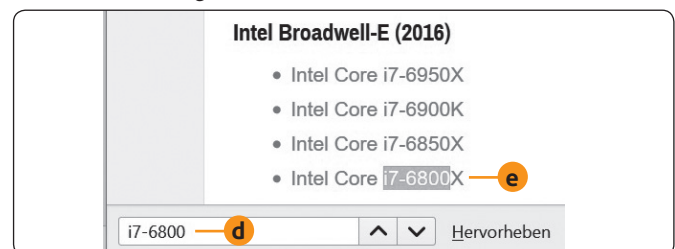
1. Öffnen Sie mit der Tastenkombination **Windows + Pause** blitzschnell das **System**-Fenster. Klicken Sie links auf **Geräte-Manager**.
2. Öffnen Sie den Abschnitt **Prozessoren**. Dazu klicken Sie auf das **Größer-Zeichen** > links davor **a**.
3. Es erscheinen mehrere Einträge für Ihren Prozessor, ein Eintrag für jeden Prozessorkern. Lesen Sie Hersteller und Typ Ihres Prozessors ab **b**.



Hier im Geräte-Manager finden Sie die Angaben über Ihren Prozessor und weitere wichtige PC-Komponenten wie die Grafikkarte.

4. Öffnen Sie den Bereich **Grafikkarten** **c** und lesen Sie Hersteller und Typ Ihres Grafikkadapters ab. Auch hier können mehrere Grafikkadapters eingetragen sein, wenn z. B. eine Grafikeinheit (GPU) in den Prozessor oder die Hauptplatine Ihres PCs integriert ist und zusätzlich eine oder mehrere Grafikkarten in die Steckplätze der Hauptplatine eingesteckt sind. Notieren Sie sich die Angaben, denn Sie benötigen sie im Sicherheits-Check 6 auf der Seite 7 beim Update Ihres Grafiktreibers.

5. Öffnen Sie die vollständige und stets aktualisierte **Liste der verwundbaren Prozessoren** am Link <https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/>. Im Unterschied zur offiziellen Intel-Liste sind hier auch verwundbare Prozessoren der Firmen AMD, Apple und ARM aufgeführt. Die Liste umfasst rund 1.800 Prozessoren.
6. Klicken Sie auf den Link, der zur Übersicht für Ihren Prozessor führt. Die korrekte Liste beginnt mit dem Hersteller Ihres Prozessors, also im Beispiel mit Intel. Im Fall eines Desktop-PCs öffnen Sie beispielsweise die Liste **Intel Desktop CPUs vulnerable To Meltdown + Spectre**. Dagegen klicken Sie bei einem Notebook auf **Intel Mobile CPUs Vulnerable To Meltdown + Spectre**.
7. Suchen Sie in der Liste Ihren Prozessor. Das geht am schnellsten über die Suchfunktion für Internetseiten Ihres Browsers. Drücken Sie **Strg+F** und geben Sie die Typenbezeichnung ins Suchfeld ein **d**, z. B. **i7-6800K** aus dem vorigen Bild **b**.



Schon kleine Unterschiede bei der Typenbezeichnung sind entscheidend für das Ergebnis: Der gesuchte Prozessor **i7-6800K** **b** ist nicht für Meltdown und Spectre verwundbar, das hier gefundene Modell **i7-6800X** dagegen schon **e**.



Mein Tipp: Leistungsfähige Notebooks enthalten teilweise einen Desktop-Prozessor und keinen Prozessor für Mobilgeräte. Einige Mini-PCs wiederum besitzen einen Prozessor für Mobilgeräte, obwohl es Desktop-PCs sind. Finden Sie Ihren Prozessor nicht in der ausgewählten Desktop-CPU- oder Mobile-CPU-Liste, schauen Sie in der anderen Liste nach.

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.

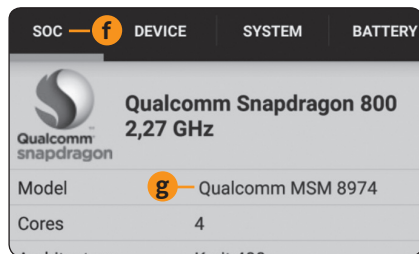
Sind Ihre Mobilgeräte betroffen? So ermitteln Sie den Prozessor bei Ihrem Tablet oder Smartphone

Ihr Smartphone oder Tablet enthält keine Funktion zum Anzeigen des Prozessors. Sie installieren zu diesem Zweck eine App, also ein Programm.

Im Unterschied zu den meisten PCs haben Mobilgeräte keinen separaten Prozessor, sondern das gesamte System befindet sich auf einem Chip (System on a Chip, SoC, „EinChip-Computer“). Sie ermitteln daher den Typ dieses Chips und nicht den des darin integrierten Prozessors.

Ist der Prozessor Ihres Android-Mobilgeräts verwundbar?

1. Installieren Sie über Google Play die App CPU-Z. Das Tool gibt es auch für Windows, es ist Ihnen daher vielleicht bekannt.
2. Im Register SOC finden Sie die Prozessorbezeichnung.



Im Register **SOC** ^f wird Ihnen hinter **Model** der Prozessor-typ angezeigt; hier handelt es sich um einen **Qualcomm MSM 8974** ^g.

3. Vergleichen Sie die gefundene Chip-Bezeichnung mit der Prozessorliste **The ARM CPUs Vulnerable To Meltdown / Spectre**, die Sie am Link <https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/4/> öffnen.

Ist der Prozessor Ihres Apple iPhones oder iPads verwundbar?

Im Fall eines iPhones (Mobiltelefon) oder iPads (Tablet) der Firma Apple finden Sie eine Übersicht aller betroffenen Geräte und Prozessoren in der Liste **The Apple CPUs Vulnerable To Meltdown / Spectre**, die Sie ebenfalls am Link <https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/4/> vorfinden.

Meine Empfehlung: Sie wissen nun, in welchen Ihrer Geräte verwundbare Prozessoren verbaut sind. Diese Geräte benötigen ein Betriebssystem-Update (siehe System-Check 5, Seite 6) und im Fall eines PCs ein Firmware- und Treiber-Update (siehe System-Check 6, Seite 7).

Ich empfehle Ihnen bei Ihrem PC auch dann alle nachfolgenden System-Checks, wenn Ihr Prozessor laut Liste nicht verwundbar ist. Der Grund: Die Liste ist vielleicht nicht vollständig und die genannten System-Checks verbessern in jedem Fall die Sicherheit, Systemleistung und Zuverlässigkeit Ihres PC-Systems.

Sicherheits-Check 3: Führen Sie bei Intel-Prozessoren diese beiden Tool-Checks aus

Im Sicherheits-Check 2 haben Sie herausgefunden, ob Prozessoren Ihrer PCs und Mobilgeräte verwundbar sind. Sie wissen aber noch nicht, ob diese konkret für Spectre, Meltdown oder für beide Angriffsarten anfällig sind. Vielleicht haben Sie auch in der umfangreichen Liste von rund 1.800 Prozessoren Ihren Prozessor übersehen. Daher empfehle ich Ihnen einen Zusatz-Check über die nachfolgenden zwei Sicherheits-Check-Tools. Einer dieser Tests ist nur für Intel-Prozessoren nutzbar. Lassen Sie diesen Test also aus, wenn Ihr PC einen Prozessor eines anderen Herstellers, wie zum Beispiel einen AMD-Prozessor, enthält.

Der Spectre Meltdown CPU Checker ist für jeden PC-Prozessor:


1. Laden Sie am Link <https://www.ashampoo.com/en/usd/pin/1304/security-software/spectre-meltdown-cpu-checker> das Tool **Spectre Meltdown CPU Checker** der Firma Ashampoo herunter.
2. Öffnen Sie mit **[Strg]+[J]** die Download-Liste Ihres Browsers und starten Sie das heruntergeladene Programm **Spectre-MeltdownCheck.exe**. Bestätigen Sie der Benutzerkontensteuerung, dass das Programm ausgeführt werden soll.
3. Das Tool ist ohne Installation sofort lauffähig. Klicken Sie auf **Test starten**. Nach rund einer Minute erhalten Sie das Ergebnis ^a.
4. Ist Ihr Prozessor gefährdet, klicken Sie auf **Was kann ich machen?** ^d. Es erscheint eine Seite mit Informationen zu den Sicherheitslücken in englischer Sprache.
5. Klicken Sie oben rechts auf den Pfeil nach unten neben **English** und wählen Sie **Deutsch** aus.



In diesem Beispiel schützt der Prozessor nicht vor Spectre-Angriffen ^b, durch Meltdown-Angriffe ist er dagegen nicht verwundbar ^c.

6. Lesen Sie sich die Tipps durch, die wertvolle Hinweise darauf geben, wie Sie die Sicherheitslücke beseitigen können.

Der Test für Ihre PCs mit Intel-Prozessor

1. Laden Sie über den Link <https://downloadcenter.intel.com/download/27150?v=t> das **Intel Detection Tool** herunter.
2. Öffnen Sie mit **(Strg)+[J]** die Download-Liste Ihres Browsers und das heruntergeladene Archiv **SA00086_Windows.zip**.
3. Wechseln Sie in den Ordner **DiscoveryTool.GUI** und klicken Sie auf **Intel-SA-00086-GUI.exe**. Bestätigen Sie mit **Alle extrahieren**, dass das Archiv entpackt werden soll, und wählen Sie den gewünschten Ordner für die entpackten Dateien aus. Dann klicken Sie auf **Extrahieren**.
4. Der Windows-Explorer öffnet ein neues Fenster mit dem entpackten Ordner **SA00086_Windows**. Öffnen Sie diesen Ordner und den Unterordner **DiscoveryTool.GUI**.
5. Doppelklicken Sie auf das entpackte Prüfprogramm **Intel-SA-00086-GUI.exe**, das Sie am **Intel-Symbol**  erkennen.

6. Der Test wird sofort ausgeführt und Sie erhalten je nach Ergebnis die Meldung **Dieses System hat Sicherheitslücken** oder **Dieses System hat keine Sicherheitslücken**.

Meine Empfehlung: Im Redaktionstest lieferten der Spectre Meltdown CPU Checker, das Intel Detection Tool und die Sicherheitsliste der verwundbaren Prozessoren teilweise unterschiedliche Ergebnisse. Der Spectre Meltdown CPU Checker meldete auch Prozessoren als verwundbar, die von den anderen Sicherheits-Checks als sicher eingestuft wurden. Bisher ist nicht bekannt, ob der Fehler beim Meltdown CPU Checker oder dem Intel-Tool bzw. der Prozessorliste liegt. Bleiben Sie bei solchen Konfliktfällen auf der sicheren Seite und installieren Sie trotzdem die Sicherheits-Updates, auch wenn ein oder zwei Tests Ihr System für sicher halten.

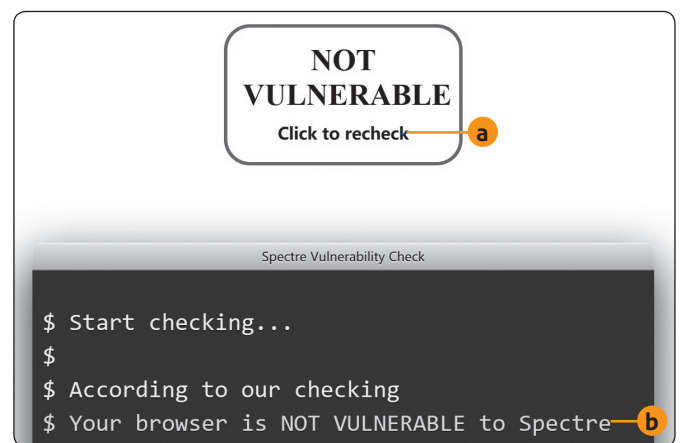
Sicherheits-Check 4: Testen Sie die Spectre-/Meltdown-Sicherheit in allen Ihren Browsern

Mit einem Spectre-Angriff kann ein Hacker wie von Geisterhand auf die Daten anfälliger Anwendungen zugreifen. Das ist beim Browser besonders fatal, denn eine der häufigsten PC-Anwendungen ist heute das Surfen im Internet und Online-Shopping. Verwenden Sie Ihren Browser auch für das Online-Banking, darf er auf keinen Fall bei einem Spectre-Angriff Ihre Daten herausrücken. Mit einem einfachen, schnellen Test über einen speziellen Online-Dienst finden Sie mit einem Mausklick heraus, ob Ihr Browser sicher ist oder nicht.

So führen Sie den Browser-Sicherheitstest durch:

1. Öffnen Sie Ihren Standard-Browser, also zum Beispiel Firefox.
2. Rufen Sie den Spectre-Test auf (https://xlab.tencent.com/special/spectre/spectre_check.html).
3. Klicken Sie auf die Schaltfläche **Click to Check** (Klicken Sie für eine Überprüfung). Nach dem ersten Test steht auf der Schaltfläche **Click to recheck** (Klicken Sie für eine erneute Überprüfung) **a**.
4. Erhalten Sie das Ergebnis **Your Browser is NOT VULNERABLE to Spectre** **b**, besteht bei diesem Browser keine Gefahr. Lautet das Ergebnis dagegen **Your Browser is VULNERABLE to Spectre**, deinstallieren Sie diesen Browser über die **Systemsteuerung** und **Programme und Features** (Windows 10) bzw. **Programme und Funktionen** (Windows 7).

Installieren Sie anschließend die neueste Version des Browsers und führen Sie den Test erneut durch.



Hier ist der getestete Browser sicher und nicht angreifbar. Wäre Ihr Browser über die Spectre-Sicherheitslücke angreifbar, hätten Kriminelle Zugriff auf Ihre E-Mails, Ihre Daten in Online-Speichern und auf Ihre Online-Banking-Konten.



Mein Tipp: Internet Explorer und Microsoft Edge lassen sich nicht deinstallieren und neu installieren. Besteht einer dieser Browser den Sicherheitstest bei Ihnen nicht, setzen Sie diesen Browser nicht weiter ein. Führen Sie den Test nach dem nächsten Windows-Update erneut durch. Besteht Ihr Browser anschließend den Spectre-Test, können Sie ihn wieder verwenden.

5. Führen Sie den Test mit dem nächsten installierten Browser durch, also je nach Windows-Version zum Beispiel mit Microsoft Edge (Windows 10) oder dem Internet Explorer (Windows 7). Machen Sie

den Test mit allen Ihren Browsern. Sollte ein Browser den Test auch in der aktuellsten Version nicht bestehen, verwenden Sie diesen Browser zukünftig nicht mehr.

Meine Empfehlung: Überprüfen Sie unabhängig vom Testergebnis Ihres Firefox-Browsers, ob Sie die neueste Version installiert haben. Dazu klicken Sie auf das **Menü-Symbol**, wählen **Hilfe** und **Über Firefox**. Es wird automatisch eine Versionsprüfung vorgenommen. Bei Bedarf wird

Ihnen eine aktuellere Version angeboten. Die aktuelle Version ist wichtig, damit Ihr Browser keine Sicherheitslücke enthält. Neben dem Spectre-Angriff gibt es noch viele weitere Angriffsmethoden, die einem nicht ganz aktuellen Browser gefährlich werden können.

Sicherheits-Check 5: Bringen Sie das Betriebssystem auf den neuesten Stand

Microsoft hat schnell reagiert und für Windows 10, 8 und 7 Sicherheits-Updates bereitgestellt. Es ist ganz wichtig, dass diese Updates bei Ihrem Windows auch installiert sind. Überprüfen Sie das daher umgehend. Beachten Sie dabei, dass sich die Sicherheits-Updates von Windows 10 je nach Version unterscheiden. Es ist daher wichtig zu wissen, ob Sie das letzte Herbst-Creators-Update und alle großen vorherigen Updates installiert haben oder nicht. Ich zeige Ihnen, wie Sie in 3 Schritten die Version Ihres Windows und die Update-Liste überprüfen.

Schritt 1: Lassen Sie sich die Windows-Version anzeigen

Windows installiert die Updates automatisch und daher ist Ihnen der aktuelle Versionsstand wahrscheinlich nicht bekannt. Doch das macht nichts, denn der Befehl **winver** zeigt Ihnen die benötigte Information an:

1. Drücken Sie **Windows + R**, um das **Ausführen**-Fenster aufzurufen.
2. Geben Sie **winver** ein und drücken Sie die Eingabetaste **↵**.
3. Lesen Sie das Betriebssystem **a** und die Version **b** aus dem **Info**-Fenster ab.



Hier ist Windows 10 **a** in der Version 1709 **b** installiert.

Schritt 2: Ermitteln Sie das benötigte Windows-Update

Die folgende Tabelle enthält eine Übersicht der Updates mit den dazugehörigen Windows-Versionen, sodass Sie die passende Update-Nummer herausuchen können. Im Fall von Windows 10 Version 1709 aus dem obigen Bild ist es zum Beispiel das Update KB4056892.

Windows-Version	Update
Windows 10 Version 1709	KB4056892
Windows 10 Version 1703	KB4056891
Windows 10 Version 1609	KB4056890
Windows 8.1	KB4056898
Windows 7	KB4056897

Windows-Update mit dazugehöriger Update-Nummer.



Mein Tipp: Für hier nicht aufgeführte Windows-Versionen wie Windows 8, Windows Vista oder Windows XP gibt es keine Sicherheits-Updates, da Microsoft diese älteren Betriebssysteme nicht mehr unterstützt. Verbinden Sie einen PC mit einem älteren Windows daher nicht mehr mit dem Internet.

Schritt 3: Schauen Sie nach, ob das Windows-Update vorhanden ist

Rufen Sie nun die Update-Übersicht auf und sehen Sie nach, ob das benötigte Sicherheits-Update vorhanden ist:

1. Drücken Sie **Windows + R**, um das **Ausführen**-Fenster aufzurufen.
2. Geben Sie **control** ein und drücken Sie die Eingabetaste **↵**, um die **Systemsteuerung** aufzurufen.
3. Stellen Sie **Anzeige** oben rechts auf **Große Symbole** und wählen Sie **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7).
4. Klicken Sie links auf **Installierte Updates anzeigen**.
5. Suchen Sie nach dem Sicherheits-Update. Die Nummer ist in Klammern angegeben.
6. Ist das Update nicht vorhanden, suchen Sie nach neuen Updates. Dazu rufen Sie bei Windows 10 über das **Start-Menü** die **Einstellungen** auf und wählen **Update und Sicherheit**. Klicken Sie im Register **Windows Update** auf die Schaltfläche **Nach Updates suchen**. Öffnen Sie bei Windows 7 über das **Start-Menü** die **Systemsteuerung**. Stellen Sie bei **Anzeige** oben rechts **Große Symbole** ein und wählen Sie **Windows Update**. Klicken Sie auf **Nach neuen Updates suchen**.

Warnung: Microsoft weist in seinen Sicherheitsanweisungen zum Schutz vor Meltdown- und Spectre-Angriffen ausdrücklich darauf hin, dass die Windows-Sicherheits-Updates allein nicht ausreichend Schutz bieten. Sie müssen zusätzlich mit Sicherheits-Check 6 noch die Firmware überprüfen und alle Treiber auf den neuesten Stand bringen.

Führen Sie bei Ihren Apple-Geräten ein Software-Update durch

Haben Sie ein iPhone oder iPad der Firma Apple, sollten Sie falls möglich das Betriebssystem iOS aktualisieren:

1. Öffnen Sie die App **Einstellungen**.
2. Wählen Sie **Allgemein**.
3. Tippen Sie auf **Softwareupdate**. Es wird automatisch nach neuen Updates gesucht.

Apple hat die Sicherheits-Updates für Meltdown mit dem Update auf iOS 11.2 und die für Spectre mit dem Update auf iOS 11.2.2 ausgeliefert. Im aktuellen iOS 11.2.5 sind die Sicherheits-Updates also enthalten.

Vertrauen Sie bei Android-Geräten nicht allein auf OTA

Im Fall eines Android-Smartphones oder -Tablets werden die Updates automatisch installiert, wenn Sie in **Einstellungen** und **Software-Updates** die Option **Automatische Aktualisierung** aktiviert haben und die angebotenen Updates zulassen. Das Update kommt per OTA (Over The Air), also per WLAN oder Mobilfunk. Ich rate Ihnen jedoch zu einer manuellen Update-Überprüfung. Sie erhalten das Update dann bis zu zwei Wochen früher als beim automatischen Update. Öffnen Sie **Einstellungen** und **Software-Updates** und wählen Sie **Updates manuell herunterladen**. Sie erfahren dann, welche Updates aktuell für Ihr Mobilgerät bereitstehen.

Warnung: Haben Sie ein älteres iPhone oder iPad, für das Apple kein iOS 11 mehr anbietet, kann es vor Meltdown- und Spectre-Angriffe nicht mehr geschützt werden. Das gilt auch für ältere Android-Smartphones und -Tablets, für die der Hersteller kein Android-Update mehr anbietet. Verwenden Sie diese Geräte aus Sicherheitsgründen nicht mehr, sondern entsorgen Sie sie.

Sicherheits-Check 6: Installieren Sie die neueste Firmware und aktuelle Treiber

Sie haben im Sicherheits-Check 5 überprüft, ob das Sicherheits-Update von Microsoft für Ihre Windows-Version installiert ist. Doch dieses Update allein reicht nicht und verhindert im Ernstfall keinen Datendiebstahl bei einem Meltdown- oder Spectre-Angriff. Die Firmware (BIOS oder Basis-Betriebssystem) Ihres PCs und auch die Treiber für den Chipsatz auf der Hauptplatine und für den Grafikadapter müssen zusätzlich erneuert werden. Sofern vorhanden, finden Sie die benötigten Updates auf der Support-Internetseite des PC-Herstellers oder auf den Support-Seiten für die PC-Komponenten. Lesen Sie in diesem Beitrag, wie Sie die Firmware aktualisieren.

In 3 Schritten zum sicheren BIOS und sicheren Treibern:

1. Rufen Sie die Support-Webseite des PC-Herstellers auf, zum Beispiel die Support-Seite der Firma Medion.
2. Suchen Sie nach der Download-Seite für Ihr Gerät. Wählen Sie bei Medion die Gerätekategorie **PC** oder **Notebook** und das Modell. Bei anderen Herstellern geben Sie den Gerätetyp ein, die Gerätenummer oder die MSN-Nummer (Manufacturer Serial Number, also die Seriennummer).
3. Laden Sie das neue BIOS-Update und die neuesten Treiber herunter und installieren Sie diese. Die Installation der Treiber erfolgt im Normalfall wie bei einem Programm. Sie

brauchen die heruntergeladene Datei also nur anzuklicken. Beachten Sie ansonsten die Informationen des Herstellers zu Treiber-Updates und insbesondere zum BIOS-Update.

Die Sicherheits-Panne: Es gibt kein aktuelles BIOS-Update und keine neuen Treiber für Ihren PC oder Ihr Windows

Ist Ihr PC älter als drei Jahre, ist die Suche nach einem BIOS-Update und neuen Treibern allerdings meist vergeblich. Die meisten PC-Hersteller liefern nur so lange Treiber-Updates, wie die Geräte in der Gewährleistungsfrist oder in der Garantiezeit sind, je nachdem, was länger ist.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299

Dieses monothematische Supplement „Schutz vor den Sicherheitslücken Meltdown und Spectre“ 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

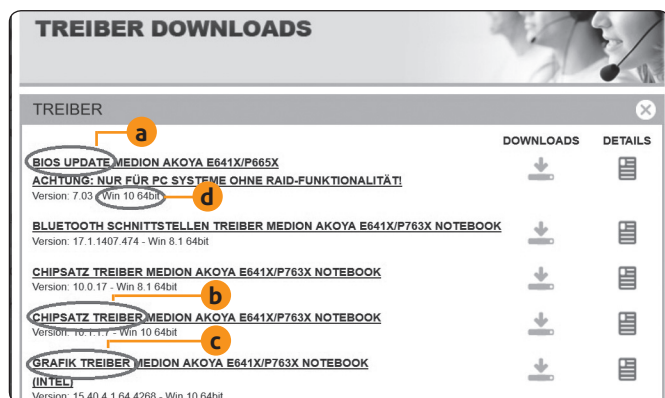
Telefon: 0228/9550190, Fax: 0228/3696350

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, Melbourne, Warschau





Die hier markierten Downloads benötigen Sie: BIOS-Update **a**, Chipsatz-Treiber **b** und Grafik-Treiber **c**. Achten Sie dabei jeweils darauf, dass auch die Windows-Version passt **d**.

Haben Sie Ihren PC mit Windows 7 oder Windows 8 gekauft und dann ein Upgrade auf Windows 10 durchgeführt, bietet der Hersteller wahrscheinlich auch keine neuen Treiber für Ihr Windows 10 an. Sie sind also nicht in der Lage, Ihren PC abzusichern.

Meine Empfehlung: Stellt der PC-Hersteller kein aktuelles BIOS-Update und keine sicheren Treiber für Ihren PC bereit, betreiben Sie mit diesem PC weder Online-Banking noch Online-Shopping. Die Gefahr ist groß, dass Sie dabei viel Geld verlieren. Derzeit empfehle ich Ihnen aber keinen Neukauf, denn sichere Prozessoren wird es voraussichtlich erst ab 2019 geben. Ich informiere Sie, sobald der PC-Kauf aus Sicherheitssicht wieder ratsam ist.

Sicherheits-Check 7: Überprüfen Sie nach den Sicherheits-Updates die PC-Leistung

Das Stopfen der Sicherheitslücken durch Microsoft führt dazu, dass für die Leistung Ihres Prozessors wichtige Funktionen gesperrt werden oder nur noch eingeschränkt nutzbar sind. Dazu gehören die Sprung-Vorhersage und das vorausseilende Ausführen eventuell benötigter Berechnungen. Im Endergebnis läuft Ihr PC daher langsamer als zuvor. Das wirkt sich je nach Alter und Leistungsfähigkeit Ihres PCs unterschiedlich aus. Vielleicht merken Sie den Unterschied gar nicht, aber bei älteren PCs können die Geschwindigkeitseinbußen dramatisch sein.

Zunächst der wichtigste Punkt: Warten Sie mit dem geplanten Kauf eines neuen PCs, bis ich Ihnen dafür grünes Licht gebe und Ihnen die sicheren Prozessoren nenne. Die neuen Prozessoren werden nicht vor Ende dieses Jahres erscheinen. Es wäre zu schade, wenn Sie viel Geld für einen PC ausgeben und die teuer erkaufte Mehrleistung durch das Sicherheits-Update aufgezehrt wird.

Ist Ihr PC schon ein paar Jahre alt und läuft noch mit Windows 7 oder 8, wird er durch die Sicherheits-Updates von Microsoft erheblich ausgebremst, so als wäre er mit einem schlimmen Schadprogramm infiziert (siehe Tabelle).

Hier müssen Sie entweder in den sauren Apfel beißen und den PC ersetzen oder Sie tauschen ein oder mehrere besonders leistungshemmende Komponenten aus.

Der Prozessor lässt sich zum Beispiel bei Desktop-PCs leicht austauschen. Den Arbeitsspeicher können Sie schnell und preiswert erweitern. Auch eine neue Grafikkarte muss

nicht die Welt kosten und kann Ihren PC trotzdem wieder flottmachen.

Lassen Sie sich aber zuerst beraten, bevor Sie hier viel Geld investieren. Nicht jeder Umbau ist das Geld wirklich wert und wenn Sie mehrere Komponenten erneuern müssen, ist ein Neukauf häufig die preiswertere und in jedem Fall von der Leistung her bessere Lösung.

Bremswirkung der Updates	Windows-Version	Prozessor
Gering (wenige Prozent), in der Praxis nicht spürbar	Windows 10	Neueste Intel-Prozessoren ab der 6. Generation (Skylake)
PC wird deutlich langsamer	Windows 10	Ältere Intel-Prozessoren der 5. Generation (Broadwell)
Starke Verlangsamung des PCs	Windows 10 Windows 7 Windows 8	Älterer Intel-Prozessor der 4. Generation (Haswell) oder davor

So wirkt sich das Sicherheits-Update auf Ihren PC aus.

Meine Empfehlung: Ist Ihr älterer PC nach dem Sicherheits-Update merklich langsamer, kaufen Sie nicht sofort einen neuen PC. Es gibt aktuell noch keine PCs mit sicherem Prozessor und Sie können sich die hohen Anschaffungskosten daher sparen. Meine Mitarbeiter und ich beraten Sie gerne über den Computerwissen Club, wie Ihr PC ohne großen Aufwand wieder flott und sicher wird: <https://club.computerwissen.de>.

Meine Sicherheitsgarantie: Mit den 7 Sicherheits-Checks in dieser Ausgabe haben Sie Ihren Rechner auf die gefährlichen Meltdown- und Spectre-Sicherheitslücken überprüft, das Betriebssystem auf den neuesten Stand gebracht und Ihre gespeicherten Daten vor kriminellem Missbrauch geschützt.