Sicherheitsstand: Mai 2022

Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

Ami, go home! Warum Facebook hier verschwinden sollte

Facebook verfolgt uns im Internet über seine „Gefällt mir"-Schaltflächen auf Millionen Webseiten.

Dagegen klagten 120 Millionen Amerikaner: Jeder erhält nach Abzug der Rechtskosten rund 50 Cent.

Für uns in Europa gibt es kein solches Almosen, aber wir werden Facebook womöglich bald ganz los!

Meta, die Firma hinter Facebook, denkt offen über das Schließen des Angebots in Europa nach.

Meine Empfehlung: Helfen Sie Meta bei der Entscheidung, indem Sie Ihr Facebook-Konto löschen. Je mehr Nutzer sich in Europa von Facebook verabschieden, umso schneller sind wir die Datenkrake los!

Viele Grüße Ihr

Michael-Alexander Beisecker,
Deutschlands PC-Sicherheitsexperte Nr. 1

Kostenlose Experten-Hilfe
Exklusiv für Sie als Abonnenten: die Sofortauskunft mit zuverlässigen Antworten und professionellen Tipps direkt von der Redaktion. Redaktions-Hotline: **Mittwoch zwischen 15:00 und 18:00 Uhr, Tel.: 02 08/6 90 79 77**

Lassen Sie PC und Router über Nacht laufen

Microsoft warnt: Jedem zweiten Windows-PC fehlen wichtige Updates

Mein Nachbar Achim ist ein Sparfuchs. Damit sein Rechner nicht unnötig Strom verbraucht, hat er ihn an eine Steckdosenleiste mit Schalter angeschlossen. Braucht er seinen PC nicht mehr, legt er den Schalter um. Doch Achim hat ein Problem: Seit er die Steckdosenleiste verwendet, erhält er kaum noch Windows-Updates. Kein Wunder, denn für erfolgreiche Windows-Updates muss ein PC mindestens 8 Stunden am Stück in Betrieb sein und Achim nutzt seinen PC als Rentner höchstens 2 Stunden am Tag und auch nicht jeden Tag.

Die meisten PC-Anwender merken gar nicht, dass ihr Windows nicht auf dem aktuellen Stand ist. Schließlich läuft das Windows-Update ja automatisch im Hintergrund. Jedenfalls sollte man das meinen.

Doch wie Microsoft selbst erst vor Kurzem bei einer Studie herausgefunden hat, funktioniert das Windows-Update bei vielen PCs nicht zuverlässig. Das führt zu verspäteten und fehlenden Updates und ist damit ein hohes Sicherheitsrisiko.

PCs brauchen für ein Update einen ganzen Arbeitstag oder die Nacht

Der Hauptgrund: Ein Windows-PC muss mindestens 2 Stunden ununterbrochen mit Microsoft über das Internet verbunden sein, damit ein Update erfolgen kann.

Zusätzlich muss dieser PC nach dem Erscheinen eines Updates noch einmal 6 Stunden online sein, bevor das Update überhaupt erfolgt. Ihr PC muss also insgesamt 8 Stunden online sein, also einen Arbeitstag lang oder die Nacht über.

Sofern Sie im Home-Office täglich mindestens 8 Stunden arbeiten und den PC nachts auch nicht ausschalten, ist das kein Problem. Nutzen Sie Ihren PC aber überwiegend privat, werden Sie ihn nicht so lange im Betrieb haben.

Machen Sie den Test: Haben Sie das neueste Halbjahres-Update?

Ihr PC ist auf dem aktuellen Stand, wenn darauf Windows 11 oder Windows 10 in der Version 21H2 (ab Mai 2022 auch 22H1) installiert ist und keine neuen Updates gefunden werden. So überprüfen Sie den Windows-Stand mit dem Systemprogramm Winver:

1. Drücken Sie gleichzeitig die Tasten ⊞ + R, um das **Ausführen**-Fenster aufzurufen.
2. Geben Sie **winver** ein und drücken Sie die Eingabetaste ↵. Das **Info**-Fenster erscheint.

>>> Lesen Sie bitte weiter auf Seite 2

>>> Fortsetzung von Seite 1

3. Lesen Sie bei Windows 10 oben links die Version ab, es sollte Version 21H2 oder ab Mai 2022 auch 22H1 sein. Haben Sie eine ältere Version wie 21H1 oder früher, öffnen Sie mit ⊞ + I die Einstellungen, und wählen **Update & Sicherheit**. Im Fall von Windows 11 sollte ab Mai 2022 wie bei Windows 10 die Version 22H1 angezeigt werden.
4. Werden im Register **Windows Update** verfügbare Updates angezeigt, klicken Sie auf **Jetzt installieren**. Suchen Sie nach der Installation nach weiteren Updates und installieren Sie auch diese.

Was Sie bei fehlenden Updates tun sollten

War Ihr PC nicht auf dem aktuellen Stand, dann versetzen Sie ihn ab sofort abends über **Energie sparen** in den Energiesparmodus und trennen Sie ihn nicht vom Strom.

Nutzen Sie Ihren PC als privater Anwender nicht täglich, dann schalten Sie Ihren PC trotzdem mindestens einmal in der Woche abends ein und lassen Sie ihn über Nacht laufen.

Sie können Ihren PC bei längerer Abwesenheit wegen Urlaub oder Krankheit ruhig abschalten. Denken Sie aber daran, dass Sie nach Ihrer Rückkehr als Erstes alle in der Zwischenzeit erschienenen Updates installieren.

Beachten Sie, dass Ihr PC für die Updates nachts auch einen Internet-Zugang benötigt. Sie sollten daher auch den Router nicht über Nacht ausschalten, nicht vom Stromnetz trennen und auch nicht das WLAN zeitgesteuert ausschalten.

Meine Empfehlung: Arbeitet das Windows-Update trotz ausreichender Zeit nicht zuverlässig, dann sollten Sie auf der Support-Webseite des PC-Herstellers nachsehen, ob dort neue Treiber und eventuell ein BIOS-Update angeboten werden, und diese dann installieren. Bringt das keinen Erfolg, ziehen Sie vor dem nächtlichen Update alle angeschlossenen USB-Geräte ab und schließen Sie alle laufenden Programme. Treten dann weiterhin Update-Fehler auf, helfen wir Ihnen gerne über den Computerwissen Club: https://club.computerwissen.de.

Ihre Leserfragen

Schnellste Lösung: Browser wechseln

„Warum wird diese Online-Reise-präsentation nicht abgespielt?"

Frage: *„Ich wollte gestern an einer Reisepräsentation im Internet teilnehmen. Das Unternehmen hatte mir zur Teilnahme einen Link gesendet. Nachdem ich mich angemeldet hatte, erschien eine Meldung, dass das Video wegen eigener Datenschutzeinstellungen nicht zu präsentieren wäre. Somit konnte ich die Präsentation über meinen Laptop nicht sehen, über ein Tablet dann schon. Ich vermute, dass eine Einstellung beim Datenschutz das Abspielen des Videos verhindert. Können Sie mir sagen, welche das ist, damit ich dies vor der nächsten Präsentation entsprechend ändern kann?", fragte uns Leser Jürgen V.*

Lösung: Erhalten Sie diese Meldung, rufen Sie das betreffende Video am besten über einen anderen Browser auf. Versuchen Sie es zum Beispiel mit dem Edge-Browser statt des Firefox-Browsers oder umgekehrt.

Haben Sie Ihren Haupt-Browser nämlich extra sicher eingestellt oder verwenden Sie einen speziellen Sicherheits-Browser wie den Tor-Browser, ist das Abschalten der Sicherheitsfunktionen nicht ganz so einfach.

Sehen Sie diese Meldung, wechseln Sie am besten den Browser, das bringt den schnellsten Erfolg.

Das sind die häufigsten Ursachen dafür, dass statt des gewünschten Videos die oben gezeigte Meldung erscheint:

- **Werbeblocker**: Sie haben als Browser-Erweiterung einen Werbeblocker wie AdBlock Plus installiert. Deaktivieren Sie den Werbeblocker für die betreffende Webseite.
- **Cookies**: Sie haben beim Aufruf der Webseite das Speichern von Cookies abgelehnt oder Ihren Browser so eingestellt, dass Cookies nicht gespeichert werden. Stimmen Sie den Cookies beim Aufruf der Webseite zu und lassen Sie auch beim Browser für die betreffende Webseite Cookies zu, insbesondere solche von Drittanbietern.
- **NoScript**: Sie unterdrücken das Ausführen von Skript-Programmen und das Tracking, also das Verfolgen Ihrer besuchten Webseiten. Dazu dient häufig die Browser-Erweiterung NoScript, die beim Tor-Browser bereits mitgeliefert wird. Deaktivieren Sie NoScript für die betreffende Webseite.
- **Fehlerhafter Link oder Adresseingabe**: Überprüfen Sie zudem die eingegebene Internetadresse. Schon eine kleine Abweichung kann zu einem Fehler führen wie etwa **http://** statt **https://**. Es kann auch einen Unterschied machen, ob Sie eine Adresse mit **www** oder ohne eingeben.

Meine Empfehlung: Tritt bei Ihnen ein solcher Fehler auf, helfen wir Ihnen gern über den Computerwissen Club: https://club.computerwissen.de. Geben Sie jedoch bei Ihrer Anfrage unbedingt an, welchen Browser Sie verwenden, welche Sicherheitseinstellungen Sie daran vorgenommen haben und welche Erweiterungen installiert sind. So können wir Ihnen schnell und gezielt die notwendigen Schritte nennen.

Passwort und Tastatur-Einstellungen überprüfen

„Warum wird mein Passwort von Google nicht anerkannt?"

Frage: *„Google hat mich aufgefordert, mein Passwort zu ändern. Zunächst hat die Anmeldung mit meinem neuen Passwort funktioniert, aber später wurde das gerade geänderte Passwort nicht mehr akzeptiert. Habe ich vielleicht mehrere Konten bei Google oder was ist da schiefgelaufen?", fragte uns Leserin Antje L.*

Lösung: Hier gibt es zwei mögliche Ursachen des Fehlers. Eventuell haben Sie tatsächlich mehrere Google-Konten, zum Beispiel ein beruflich und ein privat genutztes Konto oder ein Konto mit Ihrer aktuellen E-Mail-Adresse und ein Konto mit einer älteren E-Mail-Adresse.

In nur 3 Schritten finden Sie heraus, welches Konto gemeint ist

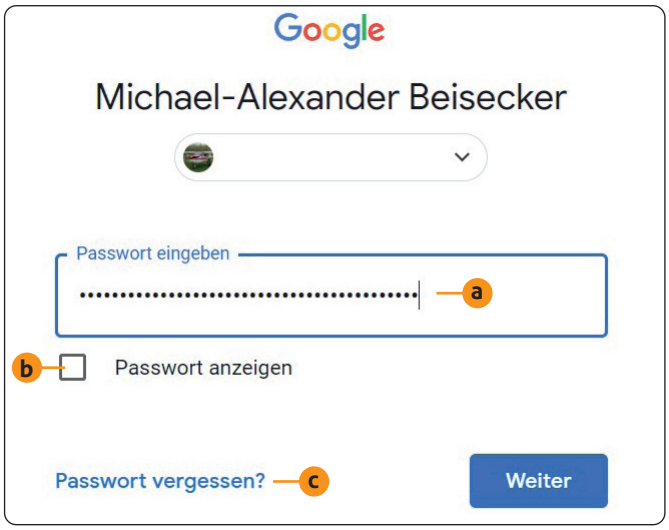
Haben Sie tatsächlich mehrere E-Mail-Adressen, ermitteln Sie so ganz einfach die für Google verwendete Adresse:

1. Rufen Sie www.google.de auf und klicken Sie oben rechts auf **Anmelden**. Geben Sie Ihre E-Mail-Adresse ein und drücken Sie die Eingabetaste ↵.
2. Erscheint die Meldung **Das Google-Konto wurde nicht gefunden**, ist der betreffenden E-Mail-Adresse kein Google-Konto zugeordnet. Sollen Sie jedoch ein Passwort eingeben, ist der Adresse ein Konto zugeordnet. Erfolgt die Passwort-Abfrage bei mehreren Ihrer Adressen, haben Sie tatsächlich mehrere Google-Konten.
3. Sehen Sie sich nun die E-Mail an, die Google Ihnen nach dem Ändern Ihres Passworts gesendet hat. An welche Internet-Adresse wurde diese E-Mail geschickt? Diese E-Mail-Adresse geben Sie nun mit Ihrem neuen Passwort ein, dann sollten Sie sich anmelden können.

Korrektes Passwort wird nicht angenommen

In den meisten Fällen erfolgt die Anmeldung aber nicht beim falschen Konto, sondern es passiert ein Fehler bei der Passwort-Eingabe. So ermitteln Sie den Fehler:

1. Geben Sie das Passwort ein. Sie sehen zunächst nur Sternchen (a).
2. Setzen Sie einen Haken vor **Passwort anzeigen** (b). Jetzt wird das eingegebene Passwort im Klartext angezeigt.



Lassen Sie sich bei Anmeldefehlern das eingegebene Passwort anzeigen, um die Fehlerursache zu finden.

3. Vergleichen Sie das eingegebene Passwort ganz genau mit dem Passwort aus Ihrer Passwort-Liste oder Ihrem Passwort-Buch. Ist vielleicht die Reihenfolge der Zeichen falsch oder ist alles in Großbuchstaben und Sonderzeichen eingegeben?
4. Überprüfen Sie, ob die Feststelltaste für die Groß-/Kleinschreibung aktiviert ist. Sie wird häufig unbewusst betätigt und dann stimmt das eingegebene Passwort nicht. Schalten Sie die Feststelltaste aus und geben Sie das Passwort erneut ein.
5. Prüfen Sie, ob Sie vielleicht statt einer Null den Buchstaben O oder umgekehrt eingegeben haben, und korrigieren Sie den Fehler dann.
6. Finden Sie keinen Fehler, klicken Sie auf **Passwort vergessen?** (c) und vergeben Sie ein neues Passwort.
7. Schreiben Sie sich das neue Passwort auf. Markieren Sie die Null mit einem Querstrich, damit Sie diese nicht mit dem Buchstaben O verwechseln.

Meine Empfehlung: Notieren Sie alle Ihre Passwörter auf einem Zettel oder noch besser in einem kleinen Büchlein. Schreiben Sie dazu den Namen des Online-Kontos, die Internet-Adresse und den Benutzernamen. Haben Sie mehrere Konten bei einem Dienst, wie zum Beispiel bei Google, dann machen Sie auch mehrere Einträge in Ihrer Passwort-Liste oder Ihrem Passwort-Buch.

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.

Gehen Sie kein Trojaner-Risiko ein

Wie Sie große Datenmengen wirklich sicher und anonym übertragen

„Bisher habe ich meine Urlaubsfotos mit dem Online-Dienst WeTransfer an Freunde und Familie geschickt, aber jetzt habe ich Datenschutz-Bedenken." So begann das Gespräch mit meinem Nachbarn Ernst. Ich erklärte ihm, dass er mit WeTransfer tatsächlich keine sensiblen Daten verschicken sollte. Denn die Daten landen unverschlüsselt auf US-amerikanischen Servern und über den Link in den ebenfalls nicht verschlüsselten WeTransfer-Mails können Unbefugte leicht auf die verschickten Daten zugreifen. Doch das stört Ernst nicht mehr, denn jetzt überträgt er seine Daten verschlüsselt und geschützt über das Tool OnionShare. Folgen Sie der nachfolgenden Anleitung und Sie verschicken Ihre Daten genauso sicher.

OnionShare ist ein Open-Source-Tool, das Sie kostenlos herunterladen und nutzen dürfen. Der Programm-Quelltext ist öffentlich einsehbar, sodass die Sicherheit überprüfbar und die Funktion nachverfolgbar ist.

Im Unterschied zu WeTransfer werden die Daten nicht auf fremden Servern gespeichert, sondern direkt von Ihrem PC zum Ziel-PC übertragen, und das natürlich sicher verschlüsselt. Ihre Daten werden dabei über das Tor-Netzwerk übertragen, einen geschützten Teil des Internets.

Dieses Netzwerk verwenden Sie auch, wenn Sie über den Tor-Browser anonym im Internet surfen. Der Tor-Browser kann daher zum Empfang der verschickten Daten verwendet werden (siehe Seite 5), er ist aber keine Voraussetzung dafür.

3 Schritte reichen: Installation von OnionShare

Sie brauchen nur OnionShare für diese sichere Datenübertragung. Folgen Sie zum Installieren von OnionShare dieser Anleitung:

1. Rufen Sie über unsere sichere Service-Webseite die **Webseite der OnionShare-Entwickler** auf: www.pc-sicherheitsberater.de.

2. Klicken Sie zum Download des Einrichtungsprogramms von OnionShare links unter dem Windows-Symbol auf **Downloads**.

Mein Tipp: Die Webseite von OnionShare ist in englischer Sprache. Verwenden Sie den Edge-Browser, denn er bietet Ihnen automatisch das Übersetzen der Webseite an und Sie haben dann eine deutsche Oberfläche.

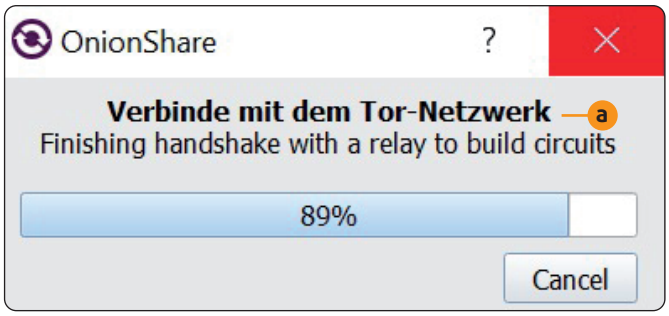
3. Starten Sie das heruntergeladene Programm **onionshare-2.5.msi** durch einen Doppelklick und bestätigen Sie die Lizenzbestimmungen, indem Sie einen Haken vor **I accept the terms in the License-Agreement** setzen. Dann klicken Sie auf **Install** (Installieren) und folgen dem Assistenten mit **Next** (Weiter) und **Finish** (Beenden).

Ihre 1-Klick-Lösung: Daten-Server einrichten

Sie haben gesehen: Die Installation von OnionShare ist einfach. Das gilt auch für das Bereitstellen Ihrer Daten für das Übertragen. Dazu richten Sie einen Server ein:

1. Öffnen Sie das **Startmenü** und starten Sie das neu installierte **OnionShare**. Sie sehen das Hauptmenü mit den Kacheln **Dateien teilen**, **Dateien empfangen**, **Webseite** und **Anonym chatten**.

2. Automatisch wird die Verbindung mit dem sicheren Tor-Netzwerk hergestellt (a). Sobald die Verbindung steht, können Sie über OnionShare Dateien versenden und empfangen.



Bequemer und einfacher geht es nicht: OnionShare macht alles automatisch.

Jetzt ziehen Sie Ihre Dateien zur Übertragung in das OnionShare-Fenster

Mit den folgenden Schritten stellen Sie Ihre Dateien für den oder die Empfänger bereit und versenden diese:

1. Klicken Sie im **OnionShare-Fenster** auf **Dateien teilen**. Es öffnet sich das gleichnamige Register.

2. Öffnen Sie den **Windows-Explorer** (⊞ + E) und ziehen Sie die Dateien, die Sie übertragen möchten, mit der Maus in das OnionShare-Fenster.

Mein Tipp: Ist Ihnen das Ziehen mit der Maus zu umständlich, klicken Sie im OnionShare-Fenster auf **Hinzufügen** (b) und wählen die gewünschten Dateien über den Explorer aus.

3. Haben Sie alle gewünschten Dateien hinzugefügt, klicken Sie einfach auf die grüne Schaltfläche **Teilen beginnen** (c). Es wird eine Internet-Adresse für das Tor-Netzwerk erzeugt, in diesem Fall die Adresse **http://ciah6eqyq23wbga77hhw2gwr2zpmbzul5p3vn7cttyo6d6tjlvbbp7yd.onion**.

*Nachdem Sie auf **Teilen beginnen** geklickt haben, steht die bereitgestellte Datei zum Abruf bereit.*

4. Damit Sie die Adresse nicht abtippen müssen, klicken Sie auf **Adresse kopieren** und die Adresse wird in die Zwischenablage übernommen.

5. Zusätzlich wird ein privater Schlüssel zur Verbindung mit Ihrem PC benötigt, zum Beispiel: **FKB36ZAKUNEI-5AGYCAD2JAB4RTNLRIDU5W5WFQ7WVUEMY-42RUR7A**. Der Schlüssel wird durch einen Klick auf **Zeigen** sichtbar. Über **QR-Code anzeigen** kann der Schlüssel auch zum Einscannen mit einem Smartphone als Grafik dargestellt werden.

6. Teilen Sie dem gewünschten Empfänger die Adresse und den Schlüssel mit, indem Sie ihm diese zum Beispiel per E-Mail, Kurznachricht oder WhatsApp schicken. Für den Versand fügen Sie die Adresse und den Schlüssel mit der Tastenkombination Strg+V aus der Zwischenablage in Ihre E-Mail oder WhatsApp-Nachricht ein.

7. Lassen Sie Ihren PC eingeschaltet und melden Sie sich nicht ab, solange die Dateien zum Abruf bereitstehen. Hat der Empfänger die Datei heruntergeladen, klicken Sie auf die rote Schaltfläche **Freigabe beenden**. Danach lässt sie sich nicht mehr unter der Adresse herunterladen.

Mein Tipp: Die Adresse Ihrer Dateien wird bei jeder Freigabe neu erzeugt. Stoppen Sie das Teilen und starten Sie es neu, ändert sich die Adresse zum Abruf daher und Sie müssen dem Empfänger die neue Adresse mitteilen.

Empfang Ihrer Daten mit OnionShare/Tor-Browser

Die „.onion"-Adresse zu Ihren Daten ist verschlüsselt und nur der Tor-Browser kann sie entschlüsseln und die Verbindung zu den Dateien herstellen.

Hat der Empfänger den Tor-Browser nicht installiert, lädt er das Installationsprogramm über unsere sichere Service-Webseite herunter und startet es dann. Dann führt ein Assistent ihn durch die Installation, es ist ganz einfach.

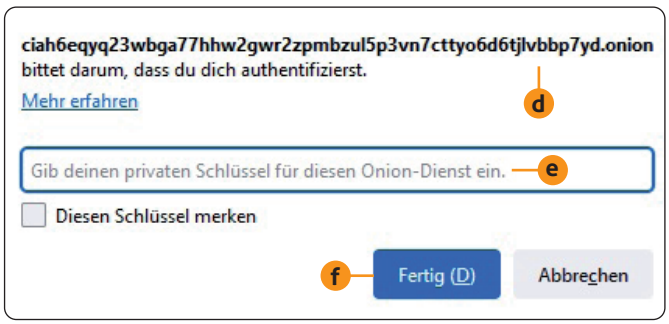
So lädt der Empfänger die Dateien von Ihrem OnionShare-Server herunter

Nachdem der Tor-Browser installiert ist, geht der Abruf der Dateien von Ihrem Server ganz einfach:

1. Der Empfänger startet den Tor-Browser und kopiert die „.onion"-Adresse, die zu Ihren Daten führt, aus Ihrer E-Mail oder WhatsApp-Nachricht in die Zwischenablage. Dazu markiert er die Adresse und drückt die Tastenkombination Strg+C.

2. Dann klickt der Empfänger ins Adressfeld des Tor-Browsers und drückt Strg+V, um die Adresse dort einzufügen. Anschließend drückt er die Eingabetaste ↵.

3. Es erscheint eine Meldung (d) mit der Bitte um Authentifizierung. Darunter gibt der Empfänger den privaten Schlüssel ein (e), indem er ihn kopiert und einfügt. Dann klickt er auf Fertig (f).



Die Meldung enthält die eingegebene „.onion"-Adresse und es wird um die Eingabe des privaten Schlüssels gebeten.

4. Die Dateien aus Ihrem OnionShare-Fenster werden dem Empfänger jetzt angezeigt und er kann diese mit **Download Files** auf seinen PC herunterladen. Sie werden in seinem Download-Ordner gespeichert. Sobald die Dateien vollständig übertragen sind, kann der Empfänger seinen Tor-Browser wieder schließen.

Meine Empfehlung: Dateien lassen sich auch ohne Tor-Browser über OnionShare empfangen. Davon rate ich Ihnen als Privatanwender jedoch ab, denn beim Tor-Browser haben Sie als Empfänger die Kontrolle darüber, wer Ihnen Daten schickt, und kennen die Absender. Diese Sicherheit ist beim Datenempfang über OnionShare nicht gegeben, da dieser für anonyme Datensendungen entwickelt wurde, um Whistleblower, also die (anonymen) Übermittler von brisanten Informationen, zu schützen.

Schützen Sie Ihren PC und Ihre Internet-Konten vor Angriffen durch Betrüger

Checkliste zum Schutz Ihres Windows-PCs und Ihrer Online-Konten im Mai 2022

Der „Welt-Passwort-Tag" ist jedes Jahr am ersten Donnerstag im Mai. Dieses Jahr sollten Sie sich also am 5. Mai die Zeit nehmen und Ihre verwendeten Passwörter auf Sicherheit überprüfen. Dabei gehe ich davon aus, dass Sie als sicherheitsbewusster PC-Anwender keine leicht zu erratenden Passwörter wie „123456" oder gar „Passwort" nutzen und kein Passwort für mehrere Online-Konten verwenden. Doch in den vielen Gesprächen mit Lesern im letzten Jahr habe ich festgestellt, dass sich die Passwort-Sicherheit nahezu immer verbessern lässt. Meist reichen dazu ganz einfache Maßnahmen und wenig Zeit aus. Machen Sie daher bei Ihrem PC meinen Passwort- und Zugangs-Check, damit auch in diesem Jahr kein Hacker unbefugt darauf zugreifen kann.

1. **Haben Sie bei Ihren Konten die 2-Faktor-Verifizierung aktiviert?**
   - ☐ **Ja**
   - ☐ **Nein:** Heute ist kein Konto mehr sicher, bei dem die **2-F**aktor-**V**erifizierung (2FV) nicht aktiviert ist, auch mit einem sicheren Passwort nicht. Daher ist es wichtig, dass Sie bei Ihrem E-Mail-Anbieter sowie allen anderen Online-Konten 2FV aktivieren. Die Anleitung dazu finden Sie in der Hilfe zum jeweiligen Online-Konto.

2. **Sind alle Ihre Passwörter mindestens 16 Zeichen lang?**
   - ☐ **Ja**
   - ☐ **Nein:** Je länger ein Passwort ist, desto besser schützt es. Ändern Sie daher alle Passwörter, die kürzer als 16 Zeichen sind, in längere ab und beachten Sie dabei Frage 3.

3. **Enthalten alle Ihre Passwörter Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen?**
   - ☐ **Ja**
   - ☐ **Nein:** Verwenden Sie sehr lange Passwörter mit 30 Zeichen und mehr, reichen Groß- und Kleinbuchstaben aus (siehe Frage 4). Sind Ihre Passwörter kürzer, sollten sie jedoch auch Ziffern und Sonderzeichen enthalten, je mehr davon, umso sicherer ist Ihr Passwort.

4. **Verwenden Sie über 30 Zeichen lange Passwörter aus mehreren Wörtern?**
   - ☐ **Ja**
   - ☐ **Nein:** Sehr lange Passwörter bieten auch ohne Ziffern und Sonderzeichen guten Schutz. Sind Ihre Passwörter aber kürzer als 30 Zeichen, ergänzen Sie Ziffern und Sonderzeichen.

5. **Nutzen Sie für jeden Zugang ein anderes Passwort?**
   - ☐ **Ja**
   - ☐ **Nein:** Ändern Sie sofort alle Passwörter, die Sie mehrfach verwenden. Denn errät ein Hacker ein solches Passwort, hat er Zugang zu mehreren Ihrer Konten!

6. **Ist Ihr Windows-Zugang über Passwort und optional PIN gesichert?**
   - ☐ **Ja**
   - ☐ **Nein:** Rufen Sie mit der Tastenkombination ⊞+R das **Ausführen**-Fenster auf, geben Sie **netplwiz** ein und drücken Sie die Eingabetaste ↵. Aktivieren Sie per Mausklick die Option **Benutzer müssen Benutzername und Kennwort eingeben** und schließen Sie das Fenster **Benutzerkonten** über das **X**-Symbol wieder.

7. **Ist bei Ihrem Notebook der BIOS-Schutz aktiviert?**
   - ☐ **Ja**
   - ☐ **Nein:** Starten Sie Ihren PC neu und drücken Sie dabei mehrfach die Taste zum Öffnen des BIOS (meist F2, siehe Handbuch zu Ihrem PC). Suchen Sie nach der Option **Supervisor Passwort** oder **User Passwort**. Aktivieren Sie diese Option und geben Sie das gewünschte Passwort ein. Sofern vorhanden, aktivieren Sie zusätzlich die Option **Password Check** oder **Password on boot**. Drücken Sie zum Speichern Ihrer Änderungen die Taste F10. Jetzt kann kein Hacker mehr unbefugt auf Ihre BIOS-Einstellungen zugreifen, um zum Beispiel mit einem Boot-Stick Ihr Windows-Passwort auszuhebeln.

Auswertung: Haben Sie alle Fragen mit **Ja** beantwortet, sind Ihr PC und Ihre Konten gut geschützt. Haben Sie Fragen mit **Nein** beantwortet, beachten Sie bitte meine Empfehlung, damit Ihr PC und Ihre Konten bestmöglich vor Hacker-Angriffen geschützt sind.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Computerwissen, ein Verlagsbereich der VNR Verlag für die Deutsche Wirtschaft AG
Vorstand: Richard Rentrop, Bonn
Redaktionell Verantwortliche: Patricia Sparacio, VNR Verlag für die deutsche Wirtschaft AG, Adresse siehe nebenstehend

Chefredakteur: Michael-Alexander Beisecker
Gutachter: Rudolf Ring, Mülheim; Annika Holtmannspötter, Ochtrup; Ute Samenfink, Freiburg
Druck und Belichtung:
Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Adresse: VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 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.

Lesen macht PC-fit!

Legen Sie ein neues, besonders geschütztes Benutzerkonto an

Die nächste Sicherheitslücke kommt bestimmt: Sichern Sie Ihr Benutzerkonto gegen Hacker-Angriffe

Im Dezember 2021 war es wieder einmal so weit: Ein Sicherheitsforscher meldete eine Riesen-Sicherheitslücke in Windows 10 und 11. Er zeigte, wie er mit Leichtigkeit schützende Gruppenrichtlinien umgehen und nach Belieben Programme ausführen konnte, und zwar mit Administrator-Rechten. Stellen Sie sich vor, ein Hacker macht das bei Ihrem PC! Daher empfehle ich Ihnen das Anlegen eines neuen, besonders geschützten Benutzerkontos. Lassen Sie Gäste immer nur über dieses Benutzerkonto auf Ihren PC zugreifen, dann erleben Sie keine unangenehmen Überraschungen.

Sicherheits-Maßnahme 1: Legen Sie ein neues Benutzerkonto an

Haben Sie bisher nur ein Windows-Benutzerkonto, dann sollten Sie jetzt ein zweites Benutzerkonto anlegen, das Sie anschließend mit Sicherheits-Maßnahme 2 vor Änderungen schützen:

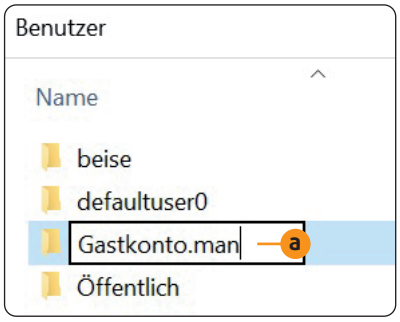
1. Öffnen Sie über die Tastenkombination ⊞+R das **Ausführen**-Fenster.
2. Geben Sie den Befehl **netplwiz** (**net**work **p**olicy **wiz**ard, Assistent für Netzwerkrichtlinien) ein und drücken Sie die Eingabetaste ↵. Das Fenster **Benutzerkonten** öffnet sich.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**, im nächsten Fenster auf **Ohne Microsoft-Konto anmelden (nicht empfohlen)** und dann auf **Lokales Konto**.
4. Geben Sie einen Namen für das neue Konto ein, zum Beispiel **Gastkonto**.
5. Klicken Sie auf **Weiter** und **Fertig stellen**.

Ihr neues Konto ist jetzt angelegt. Es fehlt noch der Schutz, den Sie mit Sicherheits-Maßnahme 2 hinzufügen.

Sicherheits-Maßnahme 2: Melden Sie sich bei Ihrem neuen Konto an

Bevor Sie Ihr neues Konto nutzen können, müssen Sie es einmal aufrufen und den Schutz vor Veränderungen hinzufügen:

1. Öffnen Sie das **Start**-Menü.
2. Klicken Sie auf das Bild zu Ihrem Benutzerkonto und wählen Sie das neu erstellte Benutzerkonto **Gastkonto**.
3. Klicken Sie auf **Anmelden** und folgen Sie dem Assistenten durch die Fragen und Schritte, die bei einem neuen Konto erforderlich sind.
4. Öffnen Sie das **Start**-Menü, klicken Sie das Bild **Gastkonto** an und kehren Sie zu Ihrem vorherigen Benutzerkonto zurück.
5. Starten Sie Ihren PC neu und öffnen Sie anschließend über die Tastenkombination ⊞+R das **Ausführen**-Fenster.
6. Geben Sie zwei Punkte (**..**) ein und drücken Sie die Eingabetaste ↵. Der Windows-Explorer öffnet sich und zeigt Ihnen den Ordner mit den Benutzerkonten an.
7. Klicken Sie Ihr neues Benutzerkonto **Gastkonto** mit der rechten Maustaste an. Wählen Sie **Umbenennen**. Ändern Sie den Namen von Gastkonto in **Gastkonto.man** (a) und drücken Sie die Eingabetaste ↵. Schließen Sie den Windows-Explorer über das **X**-Symbol und Sie sind fertig.



*Nachdem Sie das Gastkonto mit dem Zusatz **.man** versehen haben, ist es „unknackbar“.*

Testen Sie jetzt, ob der neue Schutz funktioniert

1. Melden Sie sich beim **Gastkonto** an.
2. Klicken Sie mit der rechten Maustaste auf eine leere Stelle des Desktops und wählen Sie **Anpassen**. Die **Hintergrund**-Einstellungen werden geöffnet.
3. Wählen Sie ein anderes Bild für den Desktop-Hintergrund aus und schließen Sie das Fenster **Hintergrund** wieder über das **X**-Symbol.
4. Melden Sie sich beim **Gastkonto** ab und gleich wieder an. Sie werden feststellen, dass wieder der alte Desktop-Hintergrund angezeigt wird.

Ganz gleich, was Sie ändern, alle Ihre Änderungen sind nach dem Abmelden nicht mehr vorhanden. Selbst installierte Programme und heruntergeladene Dateien werden automatisch wieder entfernt. Daher kann auch kein Schadprogramm im Gastkonto überleben.

Meine Empfehlung: Lassen Sie Ihre Gäste nur über Ihr neues, unknackbares Benutzerkonto surfen, denn dann brauchen Sie keine Sorge zu haben, dass Ihre persönlichen Windows-Einstellungen verändert werden.

Vor dem Kauf Anleitung intensiv lesen

Bundesnetzagentur warnt vor Spionage-geräten im Haushalt

Duftspender, Futterautomaten, Rauchmelder, Saugroboter, Smartwatches, Spielzeuge und sogar Taschentuchboxen spionieren ihre Nutzer über versteckt eingebaute Kameras und Mikrofone aus. Davor warnt die Bundesnetzagentur und gibt Tipps, wie Sie sich schützen können.

In Deutschland dürfen keine Geräte verkauft werden, die Sie über versteckte Kameras und Mikrofone abhören. Dennoch hat die Bundesnetzagentur allein im letzten Jahr 4.600 illegale Angebote gefunden und gelöscht, und das ist nur die kleine Spitze des Eisbergs!

Kontrollieren Sie alle Geräte in Ihrem persönlichen Umfeld

Überprüfen Sie bei Ihren Elektrogeräten, ob eine Kamera/ein Mikrofon enthalten ist. Hinweise darauf und auf Datenmissbrauch finden Sie in diesen Quellen:

- **Bedienungsanleitung:** Achten Sie darauf, ob dort eine Kamera oder ein Mikrofon erwähnt ist und ein Fernzugriff per App möglich ist.
- **App zu den Geräten:** Sehen Sie bei der App zur Fernsteuerung des Geräts nach, ob darüber Bild und/oder Ton vom Gerät zu empfangen sind.
- **Datenschutzbestimmungen:** Lesen Sie die Bestimmungen genauestens durch und achten Sie auf Hinweise zu Datenübertragung, Bild- und Tonübertragung.
- **Hinweise der Bundesnetzagentur:** Rufen Sie über unsere sichere Service-Webseite die **Webseite der Bundesnetzagentur mit Hinweisen zu Spionagegeräten** auf: www.pc-sicherheitsberater.de. Schauen Sie nach, ob dort erwähnte Geräte oder Produktkategorien bei Ihnen zu Hause vorhanden sind.

Finden Sie ein Mikrofon oder eine Kamera in einem Ihrer Geräte, dann deaktivieren Sie diese. Das kann über die App zum Gerät erfolgen oder mechanisch durch einen Verschluss oder auch durch Abkleben von Mikro und Kamera.

Meine Empfehlung: Wenden Sie sich bei einem Spionageverdacht an die Bundesnetzagentur. Sie erreichen diese per E-Mail an spionagegeraete@bnetza.de und telefonisch unter 030/22480-500 von montags bis freitags in der Zeit von 9 Uhr bis 12 Uhr.

Klicken Sie nicht auf Links in Kurznachrichten

Kaspersky warnt vor SMS-Angriff und schlimmem Datenklau

Der Smishing-Angriff „Roaming Mantis" (deutsche Übersetzung „umherstreifende Gottesanbeterin") schwappt gerade aus anderen Ländern zu uns nach Deutschland herüber. Die Angreifer infizierten Smartphones mit einem Schadprogramm und stehlen dort Daten. Die Mobiltelefone verschicken Kurznachrichten mit Links zu Betrugsseiten.

Smishing ist ein Betrugsversuch über Kurznachrichten (**SMS**-Ph**ishing**). In diesem Fall enthalten die Nachrichten einen Link zu einer gefälschten Anmeldeseite.

Gefälschte Apple- und Google-Anmeldeseiten

Verwenden Sie ein Android-Smartphone, sieht die Betrugsseite aus wie die Google-Anmeldeseite. Als iPhone-Anwender werden Sie auf eine gefälschte Apple-Seite geleitet. Die Betrüger fordern Sie dort unter einem Vorwand zur Eingabe Ihrer Anmeldedaten auf.

Ihr Schutz: Erhalten Sie eine Kurznachricht mit einem Link, klicken Sie nicht darauf. Dann kann Ihnen nichts passieren. Das gilt für jede Art von Kurznachricht. Links in Kurznachrichten sind immer verdächtig und meist ein Betrugsversuch.

Smartphone vor dem Schadprogramm schützen

Haben Sie ein Android-Smartphone, kann dieses auch mit einem der Schadprogramme SpyAgent (Spionageagent), auch bekannt als Fakecop (falscher Polizist), und Wroba.j, auch bekannt als Funkybot (ausgeflippter Roboter), infiziert werden.

Dann werden von Ihrem Smartphone Kontaktdaten, Bankdaten und Fotos gestohlen. Es besteht die Gefahr, dass die Täter mit den Bankdaten auf Ihre Kosten einkaufen gehen oder das betreffende Konto leer räumen, nicht selten sogar weit überziehen.

Ihr Schutz: Installieren Sie Apps immer nur über den Google Play Store, die offizielle Bezugsquelle für Android-Programme. Verwenden Sie dazu die App auf Ihrem Androiden. Dann können Sie Wroba.j und Co. nicht erwischen.

Meine Empfehlung: Sofern Sie keine Nachricht mit einem Link erwarten, sollten Sie auch keiner Kurznachricht von Bekannten vertrauen. Verwenden Ihre Freunde ein Android-Smartphone, ist es womöglich infiziert und die Nachricht stammt von einem Schadprogramm.