CAW Mai 2021

Windows 10 Supportende

Windows 10 Version schnell herausfinden, 21H1 steht zur Verfügung

Die 10 raffiniertesten Hacker Tricks

WLAN Verschlüsselung im Router

Aktuelle Browserversionen (Stand 19.05.2021)

- Chrome : Version 90.0.4430.212
- Firefox : Version 88.0.1
- Edge : Version 90.0.818.62

Windows 10

WINDOWS 10 SUPPORT-ZEITRÄUME

Windows 10 Version	Support-Ende für Privatnutzer	Support-Ende für Unternehmen
Windows 10 20H2	10. Mai 2022	9. Mai 2023
Windows 10 2004	14. Dezember 2021	14. Dezember 2021
Windows 10 1909	11. Mai 2021	10. Mai 2022
Windows 10 1903	8. Dezember 2020	8. Dezember 2020
Windows 10 1809	10. November 2020	11. Mai 2021
Windows 10 1803	12. November 2019	11. Mai 2021

Eine Versorgung mit Sicherheitsupdates erfolgt normalerweise etwa 18 Monate

Windows 10

Nicht jeder weiß, welche Windows-Version auf seinem System läuft.
Man kann es aber ganz einfach herausfinden.

Windows-Taste drücken, danach der Befehl "winver" tippen und per Enter-Taste bestätigen.

Im dann erscheinenden Fenster wird die Version incl. des aktuellen Build angezeigt.

Alternative:

Windows-Taste – Einstellungen – System - Info

Hacker Trick 1

Altes Windows angreifen

Gefährliche Sicherheitslücken in Windows XP und Windows 7.
Mehr als 1 Million Rechner laufen noch mit diesem Betriebssystem.
Hacker suchen gezielt nach Rechnern mit alten Windows Versionen um die Sicherheitslücken auszunutzen.

Lösung:

Halten Sie ihr Windows System (aber auch alle Mobilgeräte) stets aktuell.

Betreiben Sie vorhandene Rechner mit Windows XP oder 7 nur **OFFLINE**.

Hacker Trick 2

Software als Einfallstor

Auch Programme und Treiber haben durchaus Schwachstellen.
Kritisch sind vor allem die Browser sowie darin enthaltene ADD-Ons.
Unbedingt deinstallieren sollten Sie den Adobe Flash Player dessen Support am 31.12.2020 beendet wurde.

Lösung:

Halten Sie alle installierte Software auf dem aktuellen Stand.

Installieren Sie nur Software aus unbedenklichen Quellen.

Hacker Trick 3

Remote Software

wie z.B. Teamviewer, sind ein gefährliches Einfallstor für Hacker.
Mit erbeuteten Zugangsdaten kann auf fremde PCs zugegriffen werden.

Lösung:

Schalten Sie die Remote Software aus, wenn sie nicht benötigt wird.
Nutzen Sie ein sicheres Passwort.

Hacker Trick 4

Social Hacking

Arglose Menschen werden per Telefon, E-Mail oder fingierten Sicherheitsmeldungen auf Webseiten kontaktiert und zur Herausgabe von Zugangsdaten oder Überweisung von Geldbeträgen genötigt.

Lösung:

Nie Zugangsdaten preisgeben.

Reagieren Sie nie vorschnell auf eine E-Mail.

Microsoft, Apple, Ihre Bank, etc. wird Sie nie per Mail nach den Zugangsdaten fragen.

Hacker Trick 5

Passwort-Leaks

Im Darknet können ganze Datenbanken mit Zugangsdaten gekauft werden.
Da viele Anwender immer dieselben Passwörter verwenden, ist es für Hacker sehr einfach, gestohlene Zugangsdaten zu missbrauchen.

Lösung:

Passwortverwalter wie z.B. **Dashlane** prüfen automatisch, und melden sich wenn Ihre Zugangsdaten entdeckt wurden.

Auf der Webseite : https://haveibeenpwned.com können Sie prüfen ob Ihre Zugangsdaten geleakt wurden.

vertrauliche Informationen (zumeist mithilfe einer Enthüllungsplattform im Internet) der Öffentlichkeit (widerrechtlich) zugänglich machen.

Hacker Trick 6

Gefakter WLAN-Hotspot

Wer steckt hinter einem kostenlosen WLAN-Hotspot?

Lösung:

Nutzen Sie keine kostenlosen (öffentlichen) WLAN-Hotspots für sensible Daten.

Beschränken Sie sich auf Internetseiten mit HTTPS (also verschlüsselt)

Hypertext Transfer Protocol Secure

Hacker Trick 7

Neugier ausnutzen

Sie finden eine USB-Stick (präpariert). Aus Neugier wird er in den Rechner gesteckt. Dann könnten Hacker in ihr Netzwerk eindringen, da die Controller Firmware des Stick so manipuliert wurde, dass er als USB Tastatur erkannt wird, und damit nicht vom Virenscanner untersucht wird.

Lösung:

Nutzen Sie keine USB Sticks unbekannter Herkunft. Stellen Sie den Virenscanner so ein, dass er alle Wechselmedien beim Einstecken untersucht.

Hacker Trick 8

Gefälschte Software

Immer wieder wird im Internet teure Software zu Dumpingpreisen angeboten.
Die Installation kann schlimme Folgen haben, da der Quellcode womöglich mit einer Schadkomponente versehen wurde.

Lösung:

Laden und installieren Sie Software nur aus vertrauenswürdigen Quellen.
Lassen Sie den Virenscanner immer aktiv, selbst wenn eine Software während der Installation zum Abschalten auffordert.

Hacker Trick 9

Offene Ports und Freigaben finden

Um Einfallstüren am PC und im Netzwerk zu finden, wird mit entsprechenden Tools nach offenen Ports gesucht.
Diese dienen dazu, Dienste und Programme aus dem Internet erreichbar zu machen.

Lösung:

Unterbinden Sie in den Routereinstellungen, dass der Router selbstständig Portfreigaben einrichten kann.
In der Fritzbox kann der „Stealth Mode“ eingeschaltet werden, das erschwert die Identifikation Ihrer Box gegenüber Portscans.

Internet – Filter – Listen -Globale Filtereinstellungen

Definitionen

Ports

Bei Computern bezeichnet der Begriff Port allgemein eine Schnittstelle, über die sie sich mit einem anderen Gerät über eine Buchse oder einen Stecker physikalisch verbinden lassen.

Hacker Trick 10

Ungeschützte WLAN aufspüren

Bei WLAN ohne Verschlüsselung erhalten Angreifer Zugriff auf den Router und damit auf Ihre verbundenen Geräte. Auch eine veraltete Firmware kann ein Angriffspunkt sein.

Lösung:

WLAN-Router per Firmware-Update immer aktuell halten.
„Unknackbare“ Netzwerkschlüssel vergeben.
Falls der Router es bereits unterstützt wechseln Sie zum WPA Modus WPA2+WPA3

Router: Angriff prüfen

Router

- WLAN
- Funknetz
- Erfolglose Anmeldeversuche zeigen

Ergebnis:

Liste aller MAC Adressen der Geräte die erfolglos versucht haben sich ins WLAN einzuwählen.

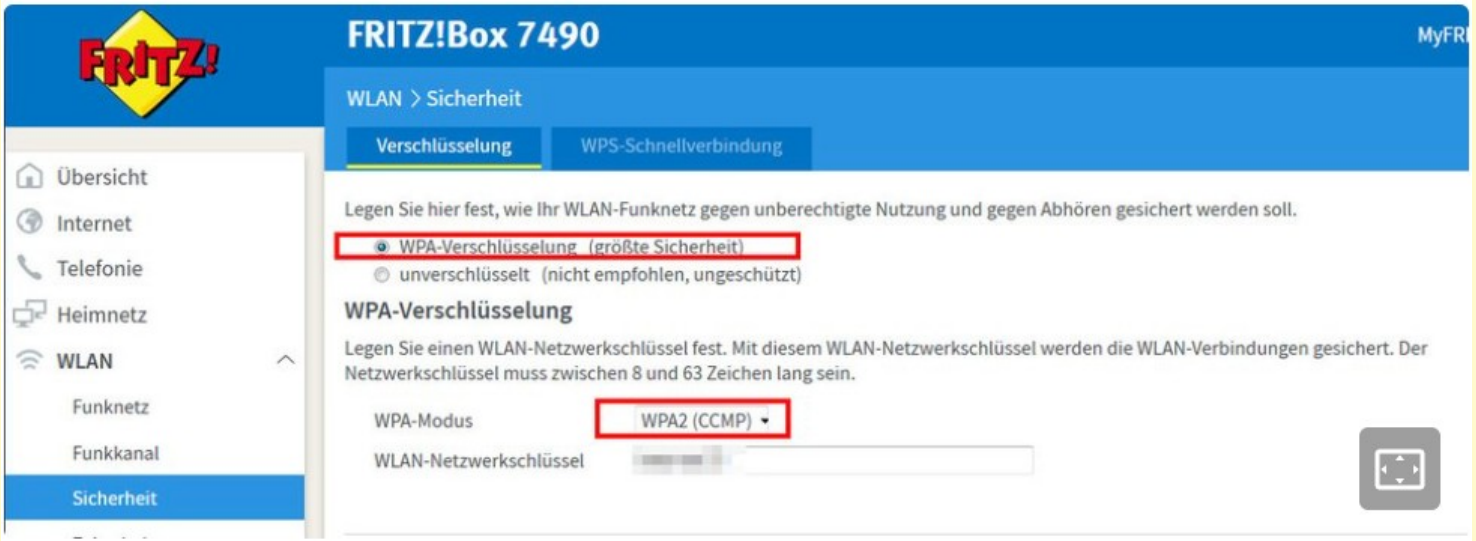
WLAN Verschlüsselung 1

Verschlüsselung	Sicherheit	Erklärung
WPA2 (CCMP)	Hoch	Grundsätzlich solltet ihr immer diesen Modus nutzen als Verschlüsselung, da er am neuesten und sichersten ist. Wenn einige WLAN-Geräte damit nicht funktionieren, bleibt noch der nächste Modus.
WPA + WPA2	Hoch	Diesen Modus solltet ihr auswählen, wenn eure WLAN-Geräte nur WPA (TKIP) unterstützen. Dann wird der Router für diese Geräte WPA nutzen und für alle anderen das bessere WPA2.

WLAN Verschlüsselung 2

WPA (TKIP)	Hoch	Dies ist ein veralteter Verschlüsselungsmodus, den ihr auch nutzen könnt. Ihr solltet ihn mit einem sicheren und nicht zu kurzen WLAN-Passwort nutzen.
WEP	Gering	Dies ist eine sehr unsichere und bereits gehackte Methode. Sie wird in vielen Routern daher gar nicht mehr angezeigt.
Unverschlüsselt	Keine	Ihr solltet immer eine Verschlüsselung des WLAN-Netzwerks einstellen und keinesfalls „unverschlüsselt“ nutzen.

Einstellungen Router



Diese Einstellungen sind am sichersten für euer WLAN.

Abkürzungen erklärt

WEP:	Wired Equivalent Privacy
WPA:	Wi-Fi Protected Access
WPA2:	Wi-Fi Protected Access 2
TKIP:	Temporal Key Integrity Protocol
AES:	Advanced Encryption Standard
CCMP:	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

Frage 1 (I.Koch)

Zum 15.06.2021 wird der Microsoft Servicevertrag geändert.

Welche Änderungen sind für mich wichtig?

Schließen des Kontos: Wartefrist 30 / 60 Tage, wenn Anmeldung innerhalb der Frist wird Konto wieder aktiv.

Dienstverfügbarkeit: (Internet- / Netzwerkverbindung) wurde an die europäische Richtlinie (EECC) angepasst.

Zahlungsbestimmungen: Die Stornierungsrichtlinien wurden angepasst.

Microsoft Teams wurde eingefügt.

Defender müllt Windows 10 zu

https://www.pcwelt.de/news/Bug-Windows-Defender-muellt-Windows-10-zu-so-loesen-Sie-das-Problem-11024473.html

Ein kurioser Fehler führt seit kurzer Zeit dazu, dass der Windows Defender auf Windows-10-Rechnern Tausende Dateien anlegt, die überhaupt keinen Sinn haben und jeweils nur 1 oder 2 KB klein sind. Das kann dazu führen, dass auf den Windows-PCs der Speicherplatz knapp wird.

Das Problem tritt bei solchen PCs auf, die den Windows-10-eigenen Windows Defender mit der Engineversion **1.1.18100. 5** als Standardsicherheitslösung verwenden.

Defender müllt Windows 10 zu

- Einstellungen

- Update & Sicherheit

- Windows Sicherheit

- Windows Sicherheit öffnen

- unter Einstellungen – Info steht die aktuelle Engine-version **(1.1.18100.6)**

Der erzeugte Datenmüll landet in folgendem Verzeichnis:

C:\ProgramData\Microsoft\WindowsDefender\Scans\History\Store\