

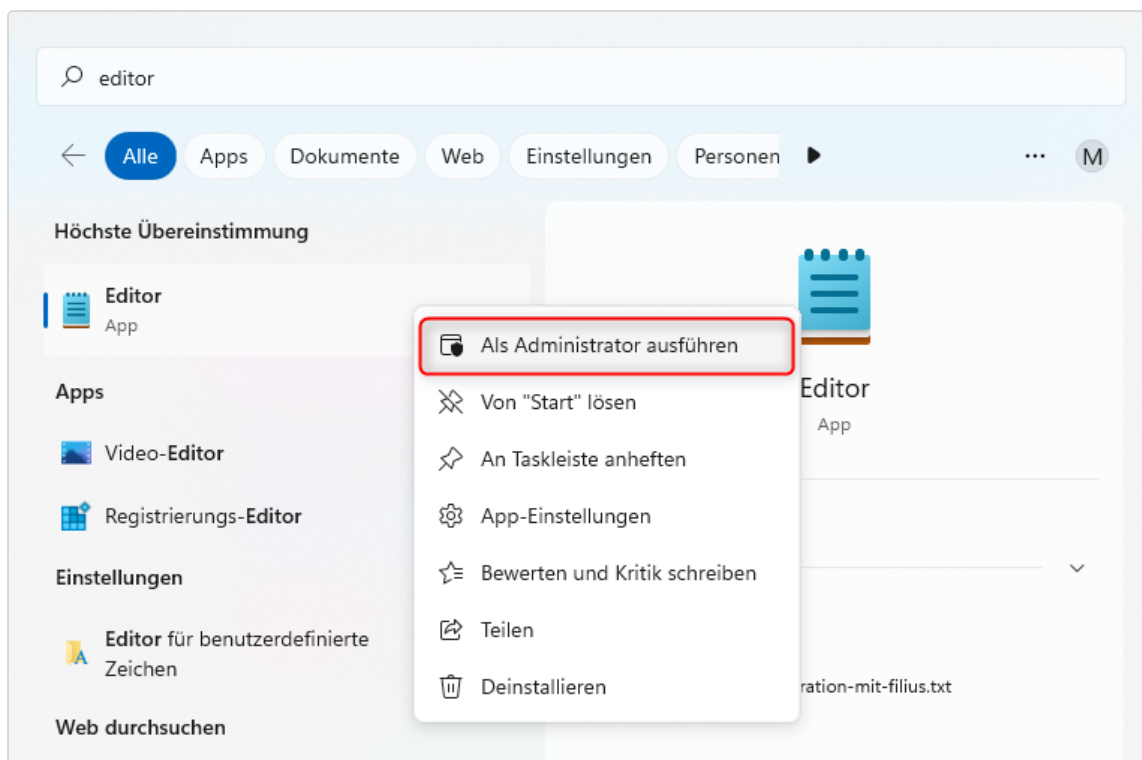
Die Hosts-Datei

Vorbereitung

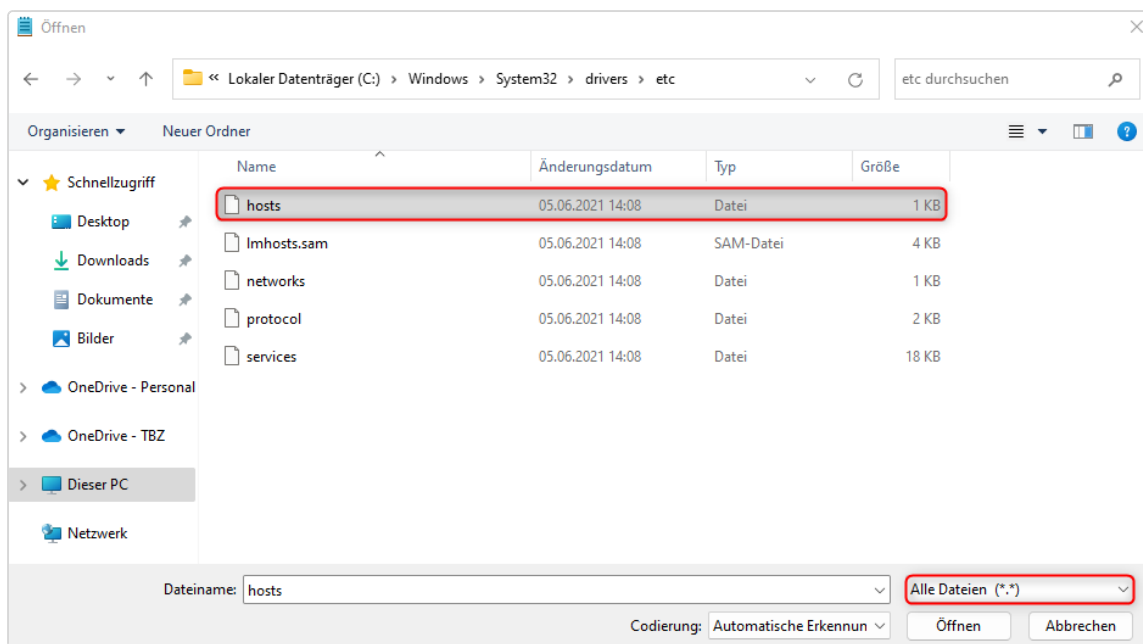
Falls Sie ein MAC-Gerät haben, verwenden Sie folgende Anleitung:

<https://kinsta.com/de/wissensdatenbank/mac-hosts-datei/>

1. Öffnen Sie den Windows-Editor im Administratoren-Modus indem Sie im Windows-Startmenü nach **Editor** suchen und dann auf das Suchresultat einen Rechtsklick machen. Wählen Sie dann die Option **Als Administrator ausführen**. Sie können auch einen anderen Editor Ihrer Wahl nehmen wie z. B. Visual Studio Code oder Notepad++



2. Klicken Sie nun im Editor auf **Datei** um im Menü die Option **Öffnen** auszuwählen.
3. Navigieren Sie in das Verzeichnis **C:\Windows\System32\drivers\etc**
4. Stellen Sie sicher, dass Sie im Date Explorer die Option **Alle Dateien (*.*)** aktiviert haben und öffnen Sie die Datei **hosts**.



5.

Fügen Sie nun folgende Zeile in der Datei hinzu:

```
80.74.136.2 tbz.ch www.tbz.ch
```

6. Speichern Sie die Datei.

Übungen

Rufen Sie nun die Webseite der TBZ auf indem Sie auf folgenden Link klicken oder diesen in Ihrem Browser direkt eintragen:

<http://www.tbz.ch>

Frage: Was sehen Sie, wenn Sie die Webseite aufrufen?

Es erscheint ein Text, dass dies nicht die TBZ-Webseite sei.

Frage: Können Sie sich vorstellen, weshalb es Administratoren-Rechte benötigt, um die betreffende Datei zu bearbeiten:

Die Hosts Datei ist problematisch, da mit Ihrer legitime URL auf fremde Server geleitet werden können. Dadurch ergibt sich ein grosses Missbrauchspotential durch Hacker und Malware. Aus diesem Grund ist die Datei speziell geschützt.

Auftrag: Öffnen Sie eine Kommandozeileingabe (CMD oder Powershell) und setzen Sie eine Ping auf **tbz.ch (ohne www)** ab. Was für eine IP-Adresse wird angepingt?

80.74.136.2

Auftrag: Öffnen Sie nun die Webseite <https://mxtoolbox.com/DNSLookup.aspx> und prüfen Sie, was Sie dort für eine IP-Adresse erhalten für **tbz.ch**.

149.126.4.25

Frage: Können Sie erklären, was die technische Situation sein könnte, dass sich das Resultat der Webseite und Ihrem Windows-Gerät unterscheidet?

Durch den Eintrag in der Hosts-Datei wurde einen manuellen Eintrag gesetzt, welcher das Betriebssystem immer verwendet, wenn es den gesuchten Namen tbz.ch abrufen. Das Betriebssystem fragt somit gar nicht weiter, was die IP-Adresse von tbz.ch ist.

Auftrag: Öffnen Sie nun den Text-Editor erneut und fügen Sie folgende Zeile hinzu:

```
127.0.0.1 instagram.com www.instagram.com
```

Versuchen Sie nun die Seite <https://instagram.com> aufzurufen. Klappt dies?

Nein, die Seite wird nicht geladen.

Frage: Was genau ist die IP-Adresse 127.0.0.1? Recherchieren Sie im Internet zu dieser Adresse.

Die IP-Adresse 127.0.0.1 ist eine sogenannte Loopback-Adresse. Sie verweist auf den eigenen Computer.

Frage: Warum kann nun instagram.com nicht mehr aufgerufen werden, wenn dieser Hostname als Ziel-IP die 127.0.0.1 verwendet?

Der Webbrowser versucht sich nun zur IP-Adresse 127.0.0.1 zu verbinden. Dies ist das lokale Gerät. Da auf diesem Gerät jedoch kein Webserver aktiv ist, kann der Webbrowser keine HTTP Verbindung herstellen.

Auftrag: Kann die Seite <https://help.instagram.com> aufgerufen werden? Wenn ja, warum?

In der Hosts-Datei wird help.instagram.com nicht auf 127.0.0.1 geleitet. Darum wird dieser Hostname ganz normal aufgelöst.

Vergessen Sie nun nicht, die Einträge in der Hosts-Datei wieder zu entfernen.

Frage: Was für Gründe könnte es geben, dass in einem Unternehmen Einträge in der Hosts-Datei durch die Systemadministration erstellt werden?

- Es können URL's auf der Ebene des Betriebssystems blockiert werden. Diese können auch nicht aufgerufen werden, wenn andere Nameserver hinterlegt werden.
- Es können z.B. interne Hostnamen verwendet werden, welche im öffentlichen DNS-Netzwerk gar nicht existieren.

Frage: Nennen Sie die Gründe, warum sich mit der wachsenden Anzahl an Hosts und Hostnamen, eine Bewirtschaftung der Hostnamen in einer lokalen Hosts-Datei nicht mehr möglich war.

- Es gibt zu viele Hosts, die Datei wäre extrem gross und die Abfrage darin langsam.
- Alle Dateien aller Hosts müssten regelmässig aktualisiert werden, wenn es neue Domains und Subdomains gibt.
- Es birgt ein Sicherheitsrisiko, wenn die z. B. der Hostname des Online-Bankings lokal verwaltet wird, wo Malware potentiellen Zugriff hat.

Auftrag: Öffnen Sie nun die Windows Power-Shell (Nicht CMD) und setzen Sie folgenden Befehl ab:

```
ipconfig /displaydns
```

Studieren Sie nun die Daten. Es dürften ziemlich viele sein.

Setzen Sie anschliessend den folgenden Befehl ab:

```
ipconfig /flushdns
```

Zeigen Sie anschliessend die Daten erneut an mit:

```
ipconfig /displaydns
```

Frage: Was hat sich verändert, nachdem Sie /flushdns aufgerufen haben?

Es werden wesentlich weniger DNS-Einträge angezeigt.

Auftrag: Finden Sie heraus, was die Befehle **ipconfig /displaydns** und **ipconfig /flushdns** genau bewirken. Tipp mit **ipconfig /?** können Sie die Hilfeseite vom Programm ipconfig aufrufen.

Mit /displaydns lässt sich der DNS-Auflösungs-Cache anzeigen

Revision #5

Created 5 December 2022 19:07:12 by Admin

Updated 8 December 2022 07:18:42 by Admin