Sykasoft Firewall Server konfigurieren

In dieser Anleitung zeigen wir Ihnen Schritt für Schritt, wie Sie die **Windows Defender Firewall** so konfigurieren, dass Ihre Arbeitsplatzrechner reibungslos eine Verbindung zu einem zentralen Server herstellen können. Dabei gehen wir besonders auf die Freigabe bestimmter Programme und Dienste ein, die für den Zugriff auf einen Microsoft SQL Server erforderlich sind.

Die Windows Defender Firewall ist ein integraler Bestandteil des Windows-Betriebssystems und dient in erster Linie dem Schutz vor unbefugtem Zugriff von außen. Sie filtert Datenverkehr basierend auf vordefinierten Regeln und kann so gefährliche oder unerwünschte Verbindungen blockieren. Eine falsch konfigurierte Firewall kann jedoch auch berechtigte interne Verbindungen verhindern – beispielsweise von einem Arbeitsplatz zu einem Server im selben Netzwerk.

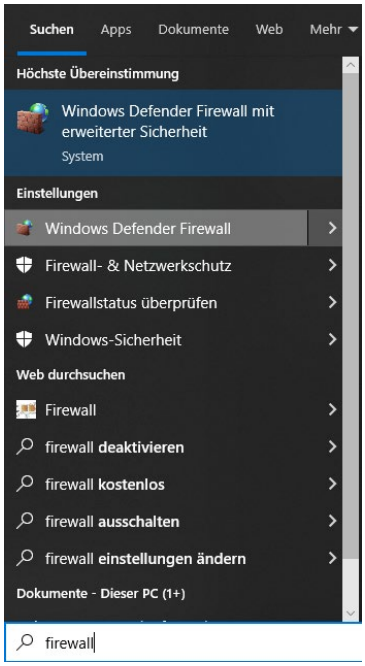
sykasoft GmbH
Schleehofstraße 16, D-97209 Veitshöchheim
Telefon +49 93129914-0
Telefax +49 93129914-30
info@sykasoft.de, www.sykasoft.de

Schritt 1: Öffnen der Windows Defender Firewall

Zunächst öffnen Sie die Windows Defender Firewall. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie unten links auf das **Suchfeld** in der Taskleiste (alternativ drücken Sie die **Windows-Taste** auf Ihrer Tastatur).
2. Geben Sie dort **„Windows Defender Firewall“** ein.
3. Wählen Sie anschließend den Eintrag **„Windows Defender Firewall“** aus den Suchergebnissen aus, um die Anwendung zu starten.

Sobald sich das Fenster geöffnet hat, können Sie mit den weiteren Schritten zur Einrichtung der Firewall-Regeln fortfahren, um den Zugriff Ihrer Arbeitsstationen auf den Server zu ermöglichen.



Schritt 2: Zulassen von Anwendungen durch die Windows Defender Firewall

Nachdem Sie die Windows Defender Firewall geöffnet haben, navigieren Sie nun zu den Einstellungen, mit denen Sie festlegen können, welche Programme und Dienste durch die Firewall kommunizieren dürfen.

Gehen Sie dabei wie folgt vor:

1. Klicken Sie im linken Menü des Firewall-Fensters auf den Punkt **„Eine App oder ein Feature durch die Windows Defender Firewall zulassen“**.
   – Dieser Menüpunkt befindet sich in der Regel im linken Bereich des Fensters unterhalb der allgemeinen Firewall-Übersicht.

2. Es öffnet sich nun ein neues Fenster mit dem Titel **„Zugelassene Apps“**.
   – Hier sehen Sie eine Liste aller Programme und Dienste, die bereits für die Kommunikation durch die Firewall freigegeben wurden.
   – In dieser Liste können Sie sowohl private als auch öffentliche Netzwerkzugriffe einzeln konfigurieren.

3. Um Änderungen vornehmen zu können, klicken Sie zunächst oben rechts auf die Schaltfläche **„Einstellungen ändern“**.
   – Möglicherweise erscheint eine Sicherheitsabfrage der Benutzerkontensteuerung, die Sie mit **„Ja“** bestätigen müssen.

Schritt 3: Anwendungen und Dienste für die Kommunikation durch die Firewall freigeben

In diesem Bereich haben Sie nun die Möglichkeit, gezielt festzulegen, welche Anwendungen und Dienste durch die Windows Defender Firewall kommunizieren dürfen. Dies ist besonders wichtig, wenn bestimmte Programme oder Serverdienste von anderen Rechnern im Netzwerk – in diesem Fall von den Arbeitsplätzen – erreichbar sein müssen.

Gerade in einer Server-Client-Umgebung, in der beispielsweise ein SQL-Server auf dem Server läuft, ist es unerlässlich, die dazugehörigen Dienste freizugeben. Andernfalls kann keine Verbindung vom Arbeitsplatzrechner zum Server hergestellt werden, da die Firewall den Datenverkehr blockiert.

Vorgehensweise:

1. **Anwendung in der Liste suchen:**
   Überprüfen Sie zunächst, ob die benötigten Anwendungen bereits in der Liste der zugelassenen Programme vorhanden sind. Sollte dies nicht der Fall sein, können Sie sie manuell hinzufügen.

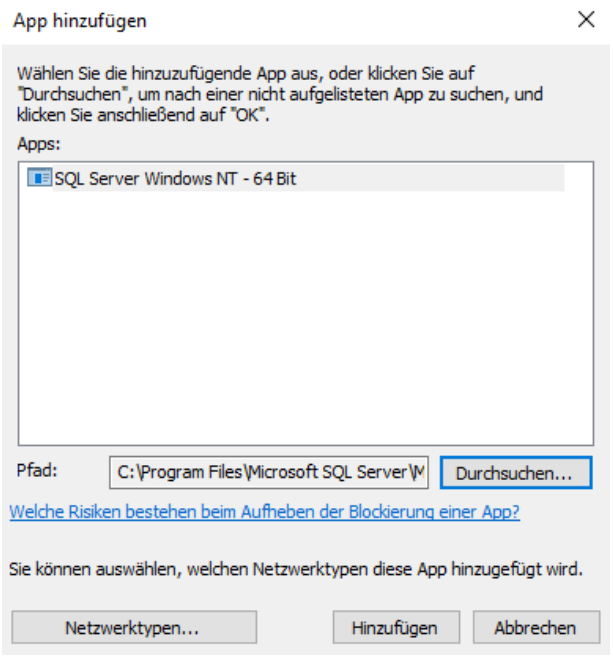
2. **Anwendung manuell hinzufügen:**

    a. Klicken Sie auf **„Andere App zulassen …“** (unten im Fenster).

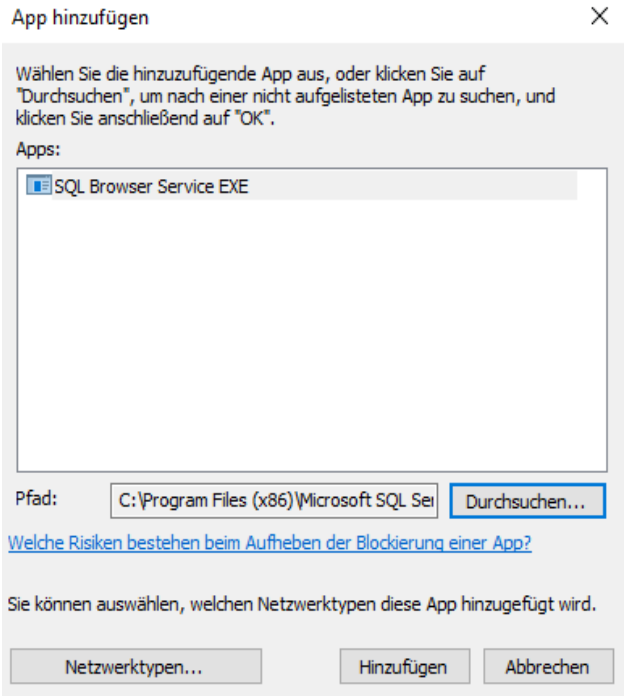
    b. Wählen Sie anschließend den Button **„Durchsuchen …“**, um zur entsprechenden Datei zu navigieren.

3. **Folgende Dienste müssen freigegeben werden:**
   Damit die Arbeitsplätze eine Verbindung zur SQL Server-Datenbank auf dem Server herstellen können, müssen Sie die folgenden ausführbaren Dateien manuell hinzufügen und sowohl für **private** als auch **öffentliche Netzwerke** freigeben:

    a. **SQL Server-Dienst:**
    C:\Program Files\Microsoft SQL Server\MSSQL12.SYKA2014\MSSQL\Binn\sqlservr.exe
    – Dies ist die zentrale Dienstdatei für die SQL Server-Instanz, die für den Datenbankbetrieb zuständig ist.



b. **SQL Server Browser-Dienst:**
C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe – Dieser Dienst ermöglicht es Client-Rechnern, die verfügbare(n) SQL Server-Instanz(en) im Netzwerk zu erkennen und sich mit ihnen zu verbinden.



4. **Nach dem Hinzufügen:**

   a. Stellen Sie sicher, dass beide Programme in der Liste aktiviert sind.

   b. Setzen Sie sowohl das Häkchen für das **private** als auch für das **öffentliche Netzwerk**, falls Ihre Umgebung dies erfordert (z. B. in gemischten Netzwerken oder bei wechselnden Verbindungen).

   c. Klicken Sie abschließend auf **„OK“**, um die Änderungen zu übernehmen.