# Windows

# Windows Server nach Windows Update nicht mehr per RDP erreichbar

Aufgrund eines Updates seitens Microsoft kann es zu einer Sperrung des RDP Ports kommen.

Wir empfehlen hier den RDP Port zu ändern und die Firewall dementsprechend anzupassen. Bitte beachten Sie, dass Sie sich ohne eine Änderung der Firewall komplett aussperren können.

### **Grafische Lösung**

#### **RDP Port anpassen**

Sie können den RDP-Port über die Registry ändern. Hierzu öffnen Sie die Registry über die Suche als Administrator. Hierzu geben Sie in das Suchfeld "regedit" ein. Über einen Rechtsklick können Sie die Registry "als Administrator ausführen".

Z Ausführen					
٨	Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.				
Ö <u>f</u> fnen:	regedit	~			
	OK Abbrechen <u>D</u> urchsuche	n			

Navigieren Sie nun zu: "Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp".

# Windows

Registrierungs-Editor				- 0	×
Datei Bearbeiten Ansicht Favoriten Hilfe					
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Cu	rrentCon	trolSet\Control\Terminal Server\	WinStations\RDP-Tcp		
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Cu Storage StorageManagement StorPort StSec SystemInformation SystemResources StabletPC Terminal Server AddIns ClusterSettings ConnectionHandler ClusterSettings ConnectionHandler SessionArbitrationHelper SysProcs TerminalTypes	rrentCon	trolSet\Control\Terminal Server\ Name MinEncryptionLevel MinEncryptionLevel NWLogonServer OutBufCount OutBufDelay OutBufLength Password PdClass PdClass PdClass PdCLass PdCLL PdFlag PdFlag PdFlag PdFlag PdFlag PdFlag PdFlag PdRame PdName	WinStations\RDP-Tcp Typ REG_DWORD REG_SZ REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_DWORD	Daten 0x00000002 (2) 0x00000006 (6) 0x00000064 (100) 0x0000002 12 (530) 0x00000002 (2) 0x00000000 (11) tdtcp tssecsrv 0x00000004e (78) 0x00000004e (78) 0x00000000 (0) tcp tssecsrv 0x000000d3d (3389)	^
<ul> <li>Utilities</li> <li>VIDEO</li> <li>Wds</li> <li>WinStations</li> <li>Console</li> <li>RDP-Tcp</li> <li>TSMMRemotingAllowedApps</li> </ul>	×	<ul> <li>SecurityLayer</li> <li>SelectNetworkDetect</li> <li>SelectTransport</li> <li>Shadow</li> <li>UserAuthentication</li> <li>Username</li> <li>WdFlag</li> </ul>	REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_DWORD	0x00000002 (2) 0x00000001 (1) 0x00000002 (2) 0x00000001 (1) 0x00000001 (1)	•
<	>	<			>

Über einen Doppelklick auf das Feld "PortNumber" stellen Sie den Eintrag auf "dezimal" um. Im Anschluss können Sie nun den neuen Wert für den RDP-Port einstellen.

DWORD-Wert (32-Bit) bearbeiten			
Wertname:			
PortNumber			
Wert: 3389	Basis Hexadezimal Dezimal		
	OK Abbrechen		

#### Anpassung der Windows Firewall

Navigieren Sie zu "eingehende Regeln". Hier ist ein Eintrag für "Remote Desktop (TCP eingehend)" vorhanden. Hier ist standardmäßig der Port TCP3389 eingestellt und kann, aufgrund der vordefinierten Regel, nicht geändert werden. Um nun eine neue Port-Nummer für den RDP-Port zu Seite 2 / 3

© 2024 myLoc managed IT <faq@myloc.de> | 18.05.2024 11:18

URL: https://faq.myloc.de/index.php?action=faq&cat=25&id=330&artlang=de

## Windows

vergeben, müssen Sie eine neue Regel anlegen. Dazu können Sie über "Neue Regel" eine zusätzliche Regel für TCP anlegen. Hier geben Sie dann Ihre zuvor neu definierte Portnummer ein. Im Anschluss kann die Standard-Regel für den Port 3389 deaktiviert werden, falls Sie diesen Port nicht mehr benötigen.

#### Neustart des Remote Desktop Service

Im Anschluss der Erstellung einer neuen Regel in der Firewall, muss der RDP-Dienst neugestartet werden.

Wichtig: Stoppen Sie nicht den RDP-Dienst, da Sie sich aussperren würden. Sie müssen hier den RDP-Dienst NEUSTARTEN.

Nachdem die Anpassungen vorgenommen wurden und die Standard-Regel für Port 3389 deaktiviert wurde, ist ein Login per RDP nur noch über den zuvor definierten Port möglich. Hierzu geben Sie die die IP-Adresse und den neuen Port bei der Verbindung an:

:Port

### Shell-Lösung

Sie können die Änderungen ebenfalls in der Shell vornehmen. Hierzu öffnen Sie eine Shell als Administrator und geben folgendes ein:

Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "PortNumber" -Value 3390

Setzt den Port auf "3390".

New-NetFirewallRule -DisplayName 'RDP TCP IN' -Profile 'Public' -Direction Inbound -Action Allow -Protocol TCP -LocalPort 3390 New-NetFirewallRule -DisplayName 'RDP UDP IN' -Profile 'Public' -Direction Inbound -Action Allow -Protocol UDP -LocalPort 3390

Setzt die Firewall-Regel.

Im Anschluss wird der RDP-Dienst neugestartet:

restart-service termservice

Eindeutige ID: #1345 Verfasser: Bettina Brauer Letzte Änderung: 2021-04-16 03:13