Leibniz Universität IT Services

Leibniz Universität Hannover

Telearbeit: Anleitung RDP-Freischaltung

Robert Euhus

18. Januar 2021

Einzurichten durch: OE-Administratoren
Getestet für: Win10Pro 20H2

1 Überblick Technik-Setup

Die Telearbeitenden greifen von ihrem heimischen Arbeitsplatz aus mittels eines Thin-Clients via Remote-Desktop-Protokoll (RDP) auf Ihren Arbeitsplatz-PC (APC) in der Universität zu.

Dazu muss auf dem Arbeitsplatz-PC im Institut bzw. in der zentralen Einrichtung oder Verwaltung (zusammenfassend kurz OE) der externe Zugriff via Remote-Desktop-Protokoll (RDP) freigeschaltet werden. Der Zugriff per RDP wird aber aus Sicherheits- und Wartungsgründen nicht direkt vom Thin-Client auf den Uni-Desktoprechner erfolgen, vielmehr kommt ein im Rechenzentrum stehender Server als VPN-Endpunkt für die Thin-Clients und Vermittler der RDP-Verbindung zum Einsatz.

Die VPN-IPs der Thinclients liegen in einem LUH-internen privaten 10er-Netz. Der RDP-Zugriff wird jedoch auf dem VPN-Server vpn-tele zu dem jeweiligen Arbeitsplatz-PC umgebogen (Source-NAT). Dieses hat zur Folge, dass der RDP-Zugriff auf den Desktops nur für diesen VNP-Server (vpn-tele.rrzn.uni-hannover.de, IP 130.75.6.31) benötigt wird und aus Sicherheitsgründen auch nur für diesen freigeschaltet werden sollte.

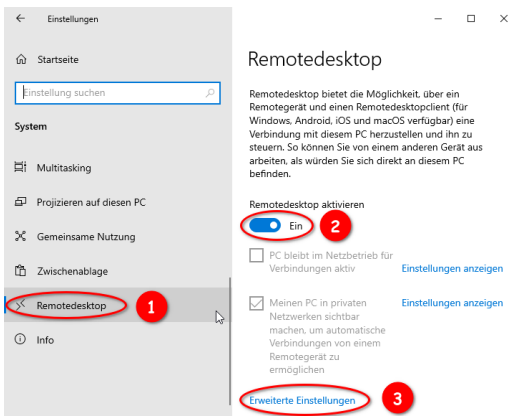
2 Vorzunehmende Konfigurationen

Die Anleitung bezieht sich auf Windows 10 Professional (Win10Pro 20H2). Für das Vornehmen der Einstellungen sind Administrator-Rechte erforderlich.

2.1 RDP Aktivierung

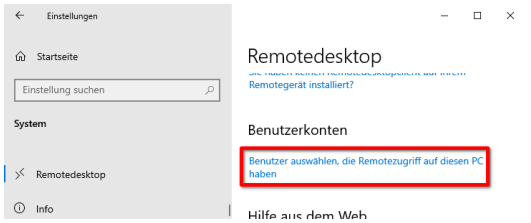
1. Die System-Einstellungen öffnen:
   (1) *Start*-Knopf drücken
   (2) Die *Einstellungen* mit dem Zahnradsymbol öffnen
   (3) Den Bereich *System* auswählen

2. Im Fenster System-*Einstellungen*
   (1) links *Remotedesktop* wählen
   (2) rechts Remotedesktop aktivieren *Ein*schalten
   (3) und *Erweiterte Einstellungen* anklicken



3. Im Menü *Erweiterte Einstellungen* von Remotedesktop Den Haken entfernen:
   Computer müssen für Verbindungen die Authentifizierung auf Netzwerkebene verwenden (empfohlen)

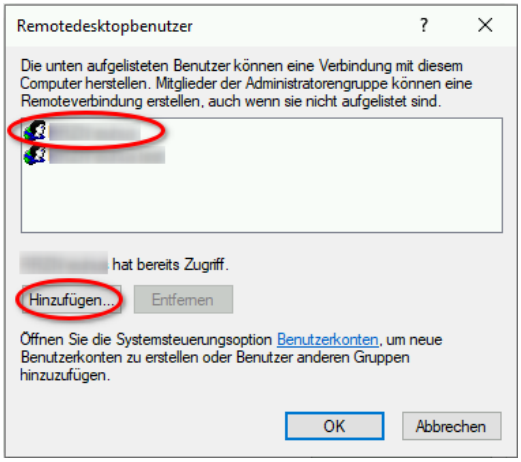
4. Zurück im Fenster *Einstellungen* von Remotedesktop rechts nach unten scrollen bis *Benutzerkonten* und *Benutzerkonten auswählen, die Remotezugriff auf diesen PC haben*



5. *Remotedesktopbenutzer* auswählen:

   - ggF unnötige Nutzer *Entfernen*
   - den Nutzeraccount des zukünftigen Telearbeitenden *Hinzufügen*.

     In einer Domäne muss der Nutzer mit Domänenzusatz (z.B. test@beispiel.intern) angegeben werden.
   - Beachten Sie, dass die Nutzer für einen Remote-Zugriff über gesetzte Kennwörter verfügen müssen (was eigentlich sowieso üblicher Standard in der LUH ist).

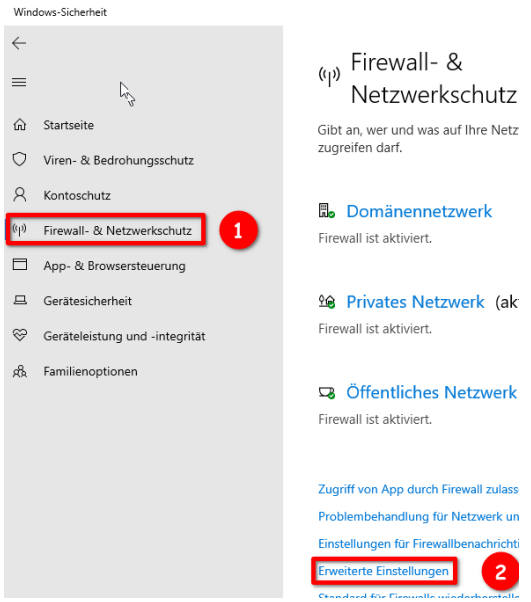


2.2 Einschränkung der Windows-Firewall

1. (0) *Windows-Sicherheit* öffnen:
   Start > *Einstellungen*
   > *Update und Sicherheit*
   > *Windows-Sicherheit*
   > *Windows-Sicherheit öffnen*

   (1) Darin links *Firewall- & Netzwerkschutz* wählen

   (2) *Erweiterte Einstellungen* aufrufen

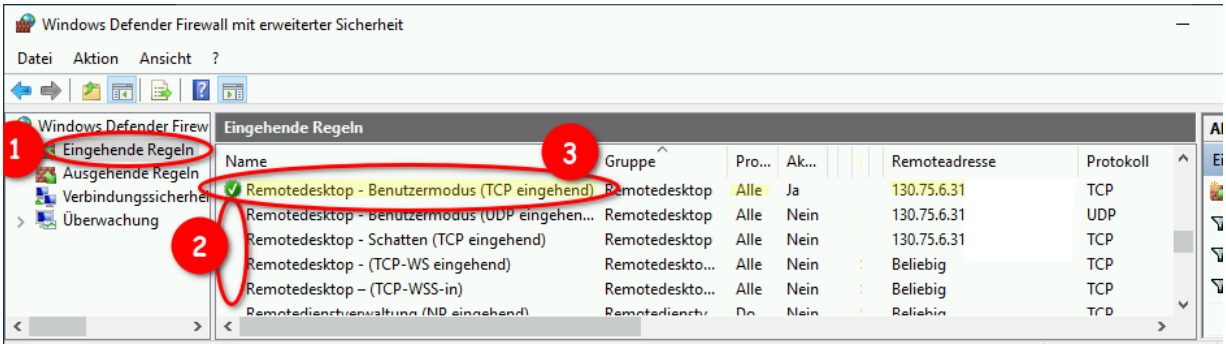


2. Im Fenster *Windows-Firewall mit erweiterter Sicherheit*

   (1) im linken Bereich *Eingehende Regeln* wählen,

   (2) im mittleren Bereich des Fensters nach den Einträgen für die Gruppe *Remotedesktop* suchen und alle bis auf den ersten Eintrag *Remotedesktop - Benutzermodus (TCP eingehend)* deaktivieren. (*Rechtsklick*)

   (3) Nun nach einem *Rechtsklick* auf diesen ersten Eintrag *Eigenschaften* wählen.



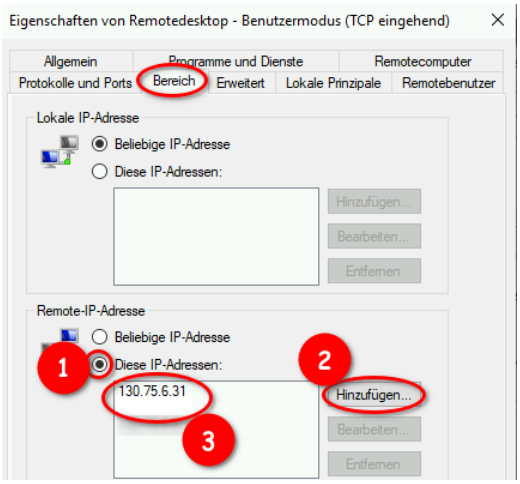
3. Auf der Karteikarte *Bereich*

   (1) im unteren Abschnitt *Remote-IP-Adresse* den Radiobutton *Diese IP-Adressen* wählen.
   Eventuell sind dort schon Einträge vorhanden, die für Fernwartungszwecke eingerichtet wurden.

   (2) Anschließend über den *Hinzufügen*-Knopf die IP *130.75.6.31* hinzufügen.

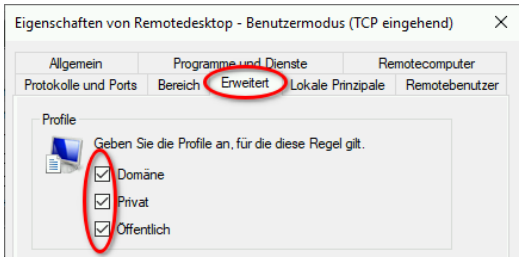
   (3) Am Ende sollte der Eintrag, wie hier gezeigt vorhanden sein.

   (4) *Optional:* Zum Testen, können Sie hier zusätzlich die IP-Adresse eines anderen Rechners im selben Subnetz hinzufügen und von diesem eine Remotedesktopverbindung herstellen. Bitte nach dem Test diesen zusätzlichen Eintrag wieder entfernen!

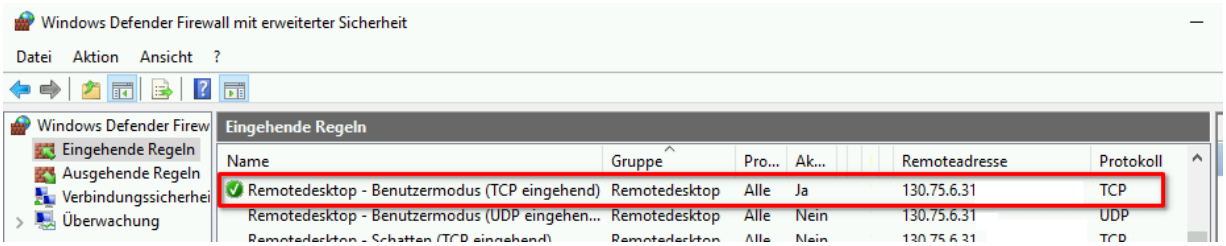


4. Auf der Karteikarte *Erweitert*

   - im Abschnitt *Profile* alle Profile anhaken.



5. Im Fenster *Windows-Firewall mit erweiterter Sicherheit* sollte nun die die aktivierte Regel für Remotedesktop die gezeigten Einträge haben:



2.3 OE-Firewall

Sollte vor dem Subnetz / VLAN der OE eine Hardware-Firewall wie z.B. bei der Teilnahme am LUIS-Netzschutz installiert sein, so ist auch dort eine Öffnung für den Remote-Desktop-Zugriff nötig:

IP-Protokoll	Quell-IP	Quell-Port	Ziel-IP	Ziel-Port
tcp	130.75.6.31	beliebig	IP des Desktop-PCs	3389

Diese Öffnung muss der OE-Administrator vornehmen. Sollte die OE am Netzschutz des LUIS teilnehmen, so sollte dennoch der OE-Administrator die Änderung wie gewohnt bei der Security-Gruppe des LUIS beantragen.

3 Anmerkungen

Für diese Lösung muss der Desktop-PC in der Einrichtung i.Allg. eingeschaltet bleiben. Der Telearbeiter darf nicht beim Verlassen des Uni-Büros den Rechner ausschalten, wenn er am nächsten Tag an seinem häuslichen Arbeitsplatz arbeiten wird.

Als Möglichkeit, versehentliches Ausschalten aufzufangen, oder auch als generelle Lösung, den Stromverbrauch zu senken, bietet sich das automatische Einschalten durch das BIOS an. Dieses ist sehr abhängig von der verwendeten Hardware — sowohl die Art der Aktivierung also auch die Zuverlässigkeit. In jedem Falle darf dabei der Rechner nicht am Netzteil oder über eine Schaltleiste ausgeschaltet werden. Er wird dabei zwar über Windows "'ausgeschaltet"', dieses ist in Wahrheit aber eine Art Standby, wie man sie vom Fernseher kennt. Der Rechner kann aus dieser Art Standby durch gewisse Ereignisse wieder hochgefahren werden, z.B. Anschlag auf der Tastatur oder eben zeitgesteuert.

So ein automatisches Hochfahren sollte unbedingt getestet werden. Zur Sicherheit (egal ob automatisches Hochfahren oder nicht) sollte geklärt werden, wer aus der OE ggf. Zugang zum Büro hat und den Rechner einschalten könnte.

4 Rückmeldung

Wenn Sie die Konfigurationsänderung vorgenommen und die Druckertreiber installiert haben, melden Sie dieses bitte dem Rechenzentrum per Mail an `telearbeit@luis.uni-hannover.de`. Geben Sie dabei unbedingt folgende Informationen an:

- die IP-Adresse des Arbeitsplatz-Rechners,
- ggF. die IP und die Portnummer auf dem NAT-Gateway (falls notwendig),
- den Benutzernamen des Telearbeitenden auf dem APC,
- die Domäne (falls vorhanden).