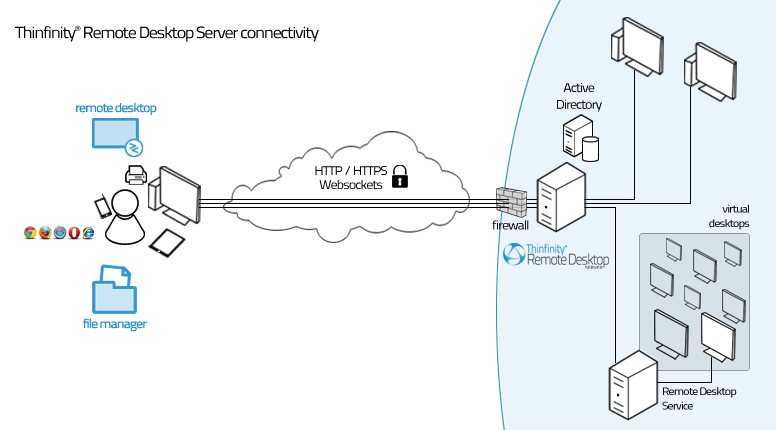
# RDP - Remote Desktop Protokoll

Remote-Desktop bezeichnet den [Fernzugriff](https://de.wikipedia.org/wiki/Fernsteuerung) auf den [Desktop](https://de.wikipedia.org/wiki/Desktop_(grafische_Benutzeroberfläche)) eines Computers. Dabei werden Anwendungsprogramme auf einem Computer (Server) ausgeführt und auf einem anderen Computer (Client) dargestellt und bedient.

Auf einem Windows Server können beliebig viele (je nach vorhandenen Lizenzen) RDP Sessions gleichzeitig ausgeführt werden.

Auf einem Windows Client kann genau 1 RDP Session ausgeführt werden. **Ein lokal angemeldeter Benutzer wird dabei abgemeldet.**

RDP ist bei Windows im Installationsumfang enthalten und bezeichnet eine Software als auch ein Netzwerkprotokoll.



Für die Kommunikation zwischen Client und Server sind spezialisierte Protokolle verantwortlich. So liefert Microsoft mit dem Remote Desktop Protocol (RDP) beispielsweise ein proprietäres Remote-Desktop-Protokoll, mit dem sich Bildschirminhalte entfernter Computer übertragen und steuern lassen. Weitere Vertreter entsprechender Übertragungsverfahren sind Citrix XenApp ICA (Independent Computing Architecture) oder das X Windows System.

## Motivation für den Einsatz von RDP

Sogenannte **Remote Desktop Services** werden nützlich, wenn nur wenige, standardisierbare Anwendungen benötigt werden.

Hier ist es nun möglich, dass alle Mitarbeiter direkt auf dem Server arbeiten. Das bedeutet, man verbindet sich direkt nach dem Starten des eigenen PCs auf dem Remote Desktop Server. Die Programme werden direkt auf dem Server ausgeführt. Dort wird ist eine entsprechende Rechenleistung erforderlich.

Als Workstations können **leistungsschwache PCs, Thin Clients oder Zero Clients** eingesetzt werden.

Durch einen zentralen RDP- oder Terminalserver, auf dem die Anwendungen laufen, müssen Softwareprodukte nur an einem **zentralen Punkt** gepflegt werden.

Da nur die Bildschirminhalte übertragen werden, gibt es eventuell Probleme bei **grafikintensiven Anwendungen**.

Ein RDP Server stellt einen zentralen Punkt für einen Ausfall dar, z.B. durch Hardwaredefekte oder nach Updates (**single point of failure**) --> doppelt auslegen, Virtuelle Maschinen

## Thin Client

Das Konzept von Thin Clients beschreibt Endpunkte, die vordergründig als Benutzerschnittstelle dienen und sich zu großen Teilen auf die Rechenleistung eines Servers verlassen.

Während entsprechend ausgestattete PCs oder Fat Clients auch anspruchsvollere Aufgaben komplett autark abarbeiten, verlassen sich Thin Clients zu großen Teilen auf die Rechenleistung eines per Netzwerk verbundenen Servers. Sind damit mehr Schnittstelle zwischen Anwender und lokaler Peripherie sowie einem entfernten Rechner, der anspruchsvollere Rechenoperationen übernimmt.



Als Vorteil von Thin Clients gilt deren einfacher Betrieb. Auf den Systemen läuft lediglich die Software, die für den Zugriff auf zentral bereitgestellte Apps notwendig ist. Dem entsprechend komfortabel lassen sich einzelne Systeme installieren oder wechseln. Nutzern steht derweil an jedem Arbeitsplatz eine identische Anwendungsumgebung zur Verfügung.

Thin Clients verzichten typischerweise auf **bewegliche Teile wie Lüfter** und sind dadurch **weniger störanfällig**. Weil an lokalen Arbeitsplätzen lediglich eine begrenzte Rechenleistung vonnöten ist, verbrauchen die Systeme in der Regel **weniger Energie** als voll ausgestattete Desktop-PCs und erreichen eine höhere Lebensdauer.

## Zero-Client

Bei Zero Clients, die auch als Ultra Thin Clients bekannt sind, handelt es sich um ein serverbasiertes Computing-Modell, bei dem der Client des Endbenutzers keinen lokalen Speicher hat. Ein Zero-Client kann mit einem Thin Client verglichen werden, der über ein minimales Betriebssystem (eher nur Firmware) verfügt und einen Flash Speicher für lokale Konfigurationen.

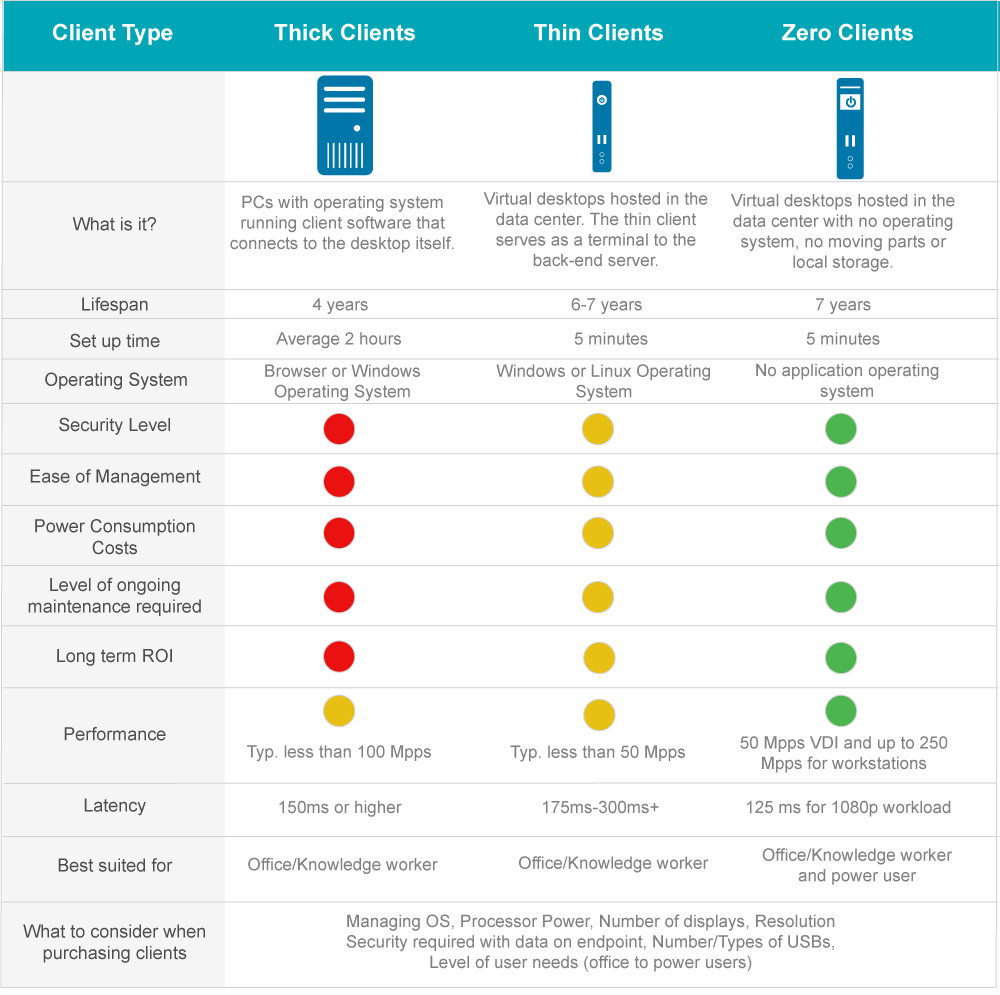
Ein typisches Zero-Client-Produkt ist eine kleine Box, die zum Anschluss einer Tastatur, Maus, Monitor und Ethernet-Verbindung zu einem Remote-Server dient.

Auf den Server wird **neben der Anwendungssoftware auch das Client Betriebssystem** gehostet. Zero-Clients werden oft in einer **VDI-Umgebung (Virtuelle Desktop-Infrastruktur)** verwendet.

Die Vorteile von Zero Clients sind:

* Der Stromverbrauch beträgt nur einen Bruchteil des Verbrauchs von PCs.
* Die Clients sind viel billiger als PCs oder selbst Thin Clients.
* Keine Software und kein OS auf dem Client bedeutet, dass es keine Anfälligkeit für Malware und keine Updates notwendig sind.

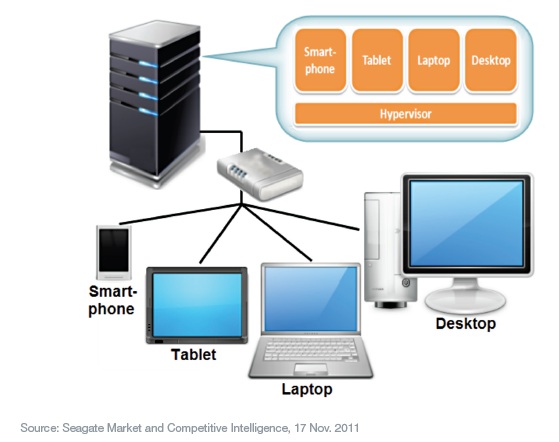




## Virtual Desktop Infrastructure

VDI steht für Virtual Desktop Infrastructure und bezeichnet eine IT-Infrastruktur zur **Virtualisierung und Zentralisierung der Funktionalität von Desktop-Rechnern**. Die Ausstattung des Clients am Arbeitsplatz lässt sich dank VDI reduzieren.

Die Desktop Virtualisierung verfolgt den Ansatz, die Funktionen eines Arbeitsplatz-PCs über einen zentralen Service bereitzustellen. Am Arbeitsplatz benötigt der Anwender nur noch einen [Client](https://www.ip-insider.de/was-ist-ein-client-a-728753/) (z.B. Thin oder Zero Client), mit dem er den virtualisierten PC-Service aufruft. Die Bedienung aller Funktionen per Maus oder Tastatur und die Ausgabe der grafischen Anzeige erfolgt lokal auf dem Client, während **die eigentliche Software und auch das Betriebssystem auf einem Server** ausgeführt wird.



**Vorteile durch den Einsatz VDI**

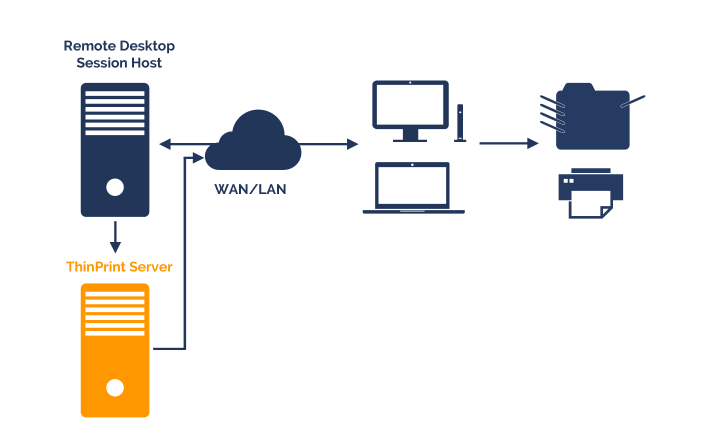
* Dank der zentral bereitgestellten Desktop Services **vereinfacht sich deren Administration**. Updates lassen sich wesentlich schneller und mit weniger Aufwand durchführen. Zudem sind auftretende Probleme oder Inkompatibilitäten nur noch an einer zentralen Stelle zu analysieren und zu lösen.
* Markante Vorteile in einer Virtual Desktop Infrastructure ergeben sich durch die Verwendung von weniger aufwendigen Clients. In der Regel kann auf teure, vollwertige PCs mit Komplettausstattung verzichtet werden. Es lassen sich **günstigere Clients** einsetzen, die geringere CPU-, Grafik- und Speicherleistung besitzen. Die Verflechtung zwischen Hardware und Softwareanwendungen wird aufgehoben und ein eventueller Austausch der PCs aufgrund neuer Softwareanforderungen überflüssig. Die Clients sind dadurch deutlich länger nutzbar.
* Im Fall von Hardwarestörungen muss der Administrator nicht mehr lokal direkt vor Ort beim Anwender tätig werden, sondern kann die **Probleme am zentralen Server lösen**. Auch das Wiederherstellen von Daten durch das Zurückspielen eines Backups erfolgt zentral.
* Da die Serverhardware für einen professionellen Betrieb ausgelegt ist, **erhöht** sich die **Mean Time Between Failure (MTBF)** deutlich und die Verfügbarkeit der virtuellen Desktops ist gegenüber physischen Desktops höher.
* Nicht zu vernachlässigen sind die Vorteile der Virtual Desktop Infrastructure in puncto **Energieeffizienz und Ressourcenschonung**. Einfache Thin oder Zero Clients verbrauchen weniger Energie als vollausgestattete Desktop Rechner und erfordern geringere Ressourcen in ihrer Herstellung oder beim Transport.
* Die Virtual Desktop Infrastructure verhindert e**inen gefährlichen Wildwuchs an lokalen Rechnern mit unterschiedlichen Betriebssystemständen oder Anwendungen**. In der virtualisierten Umgebung befinden sich alle Desktops auf einem einheitlichen Softwarestand und sind leichter vor internen oder externen Gefahren aus dem Internet zu schützen. Sind die Clients soweit reduziert, dass keinerlei Daten lokal gespeichert werden, kann auf lokale Virenscanner oder Firewalls vollständig verzichtet werden.

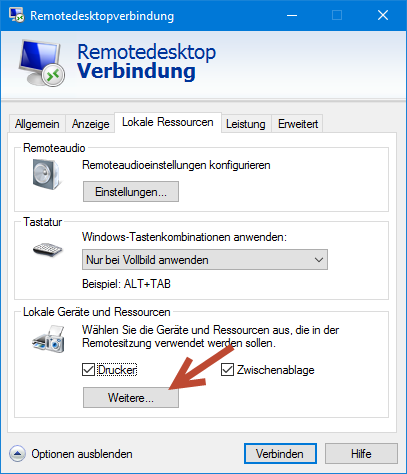
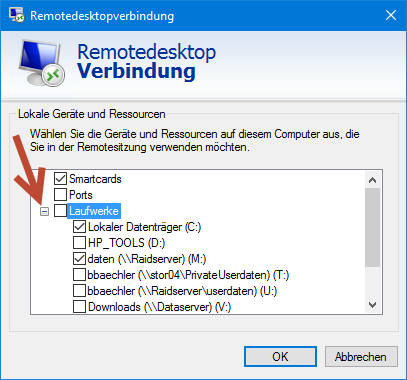
## Drucken und Dateitransfer über RDP

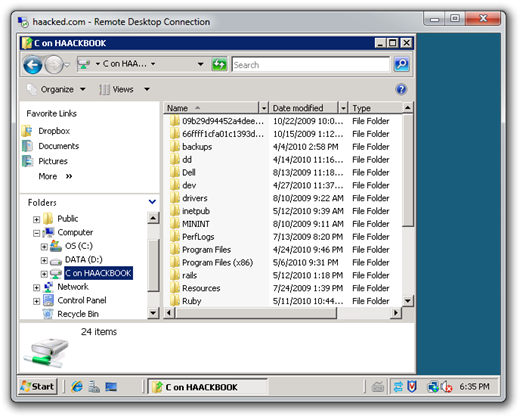
Um bei RDP Verbindungen auf lokale Ressourcen zugreifen zu können (z.B. Drucker, Laufwerke, USB Medien) können lokale Ressourcen vor dem Verbindungsaufbau in die RDP Session eingebunden werden.

Damit sind am Server die lokalen Ressourcen verwendbar. Drucker und Files können dann von dem lokalen Rechner, an dem der Benutzer arbeitet, eingesetzt werden.

Problem: große Datenmenge bei Ausdrucken möglich, Komprimierung notwendig, sehr viele Tools von Zusatzherstellern





## RDP vs. Fernwartung (z.B. TeamViewer, VNC, ...)

RDP:

* Pro Verbindung wird eine eigene Session am Server erstellt, am Server sind die Maus/Tastaturaktionen nicht sichtbar
* Für RDP muss eine direkter Verbindungsaufbau vom Client auf den Server möglich sein, wird es von außen aufgebaut muss durch die Firewall ein port forwarding konfiguriert sein.
* Eine RDP Verbindung läuft direkt vom Client zum Server, wird diese Verbindung entsprechend verschlüsselt ist kein mitlesen möglich.
* Bei RDP werden Objekte des Screens übertragen, was zur Reduktion von Daten führt, z.B. Button, Fenster, usw.

Fernwartung (z.B. Teamviewer):

* Es wird nur der Screen der aktuell angemeldeten Session auf den Client übertragen, am Server sind die Maus/Tastaturaktionen direkt sichtbar
* Bei Fernwartung (z.B. Teamviewer) arbeiten Client und Server über einen Relay Server, d.h. beide Verbindungen werden von innen nach außen durch die Firwewall auf den Relay Server aufgebaut und dann dort „verbunden“
* Bei Fernwartung ist die Verbindung durch den Anbieter am Relay Server mitlesbar.
* Bei Fernwartung wird der Screen als Pixelraster/Bild übertragen

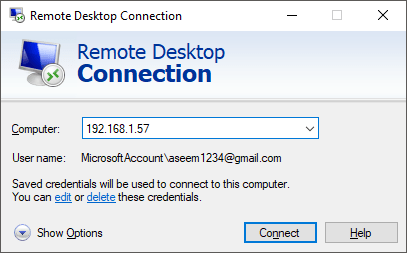
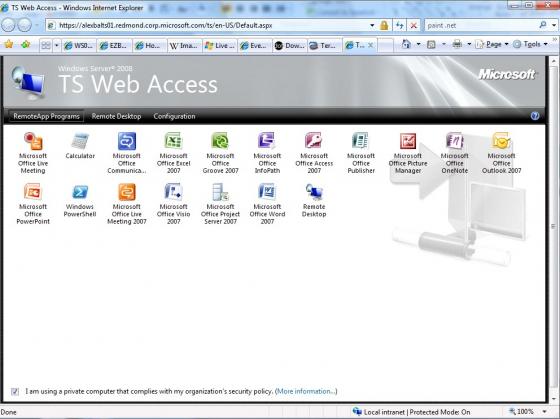
**Terminal Server oder Remote Desktop Service**

Der **Terminalserver** ist eine Software, die in einem Netzwerk auf einem **zentralen Rechner (Host)** installiert ist und **Applikationen über das Netzwerk** mehreren Clients zur Verfügung stellt.

Mit den Windows-Remotedesktopdiensten ist es möglich, Windows-Anwendungen auf allen Arten von Geräten, unabhängig vom Betriebssystem zu starten. Dabei läuft die eigentliche Anwendung auf dem Remotedesktop-Server, während der Benutzer mit einem Client Verbindung zu einer Sitzung auf einem Remotedesktop-Server aufbaut. Auf dem Client werden nur die Bildschirmänderungen angezeigt.

**Remote Desktop Gateway**

Ermöglicht den Zugriff von außerhalb auf einen RDP Server, über HTTPs auf RDP Server von außen zugreifen. Das RD Gateway erlaubt eine Sicherung der RDP Verbindung zwischen nicht vertrauenswürdigen Netzwerken und dem Firmennetzwerk.

Der **integrierte RDP Client** auf Windows Betriebssystemen ist das Programm „**mstsc.exe**“. Mit diesem kann unter Angabe einer IP Adresse oder Hostnamen direkt auf einen RDP eine RDP Verbindung hergestellt werden.

Um den Zugriff zu vereinfachen und auch über Web zu ermöglichen, kann mit Hilfe des RD Gateways der User die Verbindung auch über einen Browser herstellen.

**Sicherheit von RDP**

Das RDP Protokoll selbst hat zwar eine integrierte Verschlüsselung, diese ist allerdings für einen Zugriff über Internet nicht ausreichend. In diesem Fall wird üblicherweise eine VPN Verbindung zum Firmennetzwerk hergestellt über das dann das RDP Protokoll eingesetzt wird.

**Remote Desktop vs. Remote-Apps**

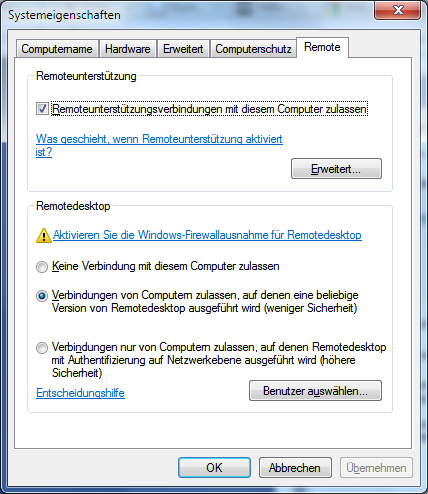
Bei Remote Desktop erhält der **User einen kompletten Desktop** mit allen installierten Anwendungen und Konfigurationsmöglichkeiten des kompletten Rechners. Wird für Benutzer verwendet, die einen vollständigen Arbeitsrechner als Umgebung benötigen.

Bei Remote-Apps können für jeden Benutzer individuelle Anwendungen festgelegt werden, die er auf dem Server ausführen darf. Dabei wird nur das Fenster der Anwendung remote am Rechner des Benutzers angezeigt. Der Benutzer erhält keinen kompletten Desktop.

**Windows Desktop Sharing - Windows Remoteunterstützung**

Remoteunterstützung ist eine mit [Windows XP](https://de.wikipedia.org/wiki/Windows_XP) eingeführte Funktion, die es ermöglicht, einen Windows-Computer über RDP fernzusteuern. Diese Funktion ist für Supportzwecke gedacht.

Im Gegensatz zum Remotedesktop wird mit **der Remoteunterstützung keine neue Sitzung** eröffnet, da die Client-Versionen von Windows grundsätzlich nur einen eingeloggten Benutzer zulassen, sondern der Bildschirm des aktuell eingeloggten Benutzers auf dem fremden System übertragen und bei Bedarf die Möglichkeit eröffnet, das System direkt fernzusteuern.



## Citrix

Citrix = SW-Hersteller von alternativer Remote-Software, Server, Client, Web Clients, ..., sehr weit verbreitet im Business Bereich (Enterprise)

Citrix liefert **eine komplett eigene Umgebung** als auch **Add-On-Produkte** für Remote Desktop. Basis hierfür ist das von Citrix entwickelte **ICA-Protokoll**. ICA (Independent Computing Architecture) ist ein Protokoll für ein Terminalserver-System, das eine Spezifikation festlegt, um Daten zwischen Server und Clients zu übertragen, aber an keine bestimmte Plattform gebunden ist.

## Fragen

* **Wenn du in einem Unternehmen mit 400 Arbeitsplätzen der CTO wärst, würdest du versuchen RDP einzusetzen? Falls Ja/Nein, nenne 4 Gründe.**

Ja

1. RDP könnte das Verwalten erleichtern, vor allem wenn man thin clients verwendet
2. Kleiner Stromverbrauch
3. Verbesserter Virenschutz, da es alles Zentral ist
4. Probleme können sich schneller Beheben und die Downtime zwischen Fehleren ist üblicherweise kleiner.

* **Was ist der Unterschied zwischen Fernwartung und remote arbeiten? Welche Softwarepakete gibt es dafür?**

Fernwartung: Es wird der Bildschirm über ein Relayserver mitgeteilt als Bild.

Remotearbeiten: Es werden die Bildschirmobjekte über eine Direkte Verbindung zum Server geteilet.

Bsp: TeamViewer.

* **Welche Kosten sind in etwa für einen Thin Client zu veranschlagen? (konkretes Produkt + Preis)**

Thin Clients kommen in vielen Preisen. Manche sind um ca. 50 bis 100€ zu kaufen.



Andere kann man um ca. 1000€ finden.

Graphical user interface, application

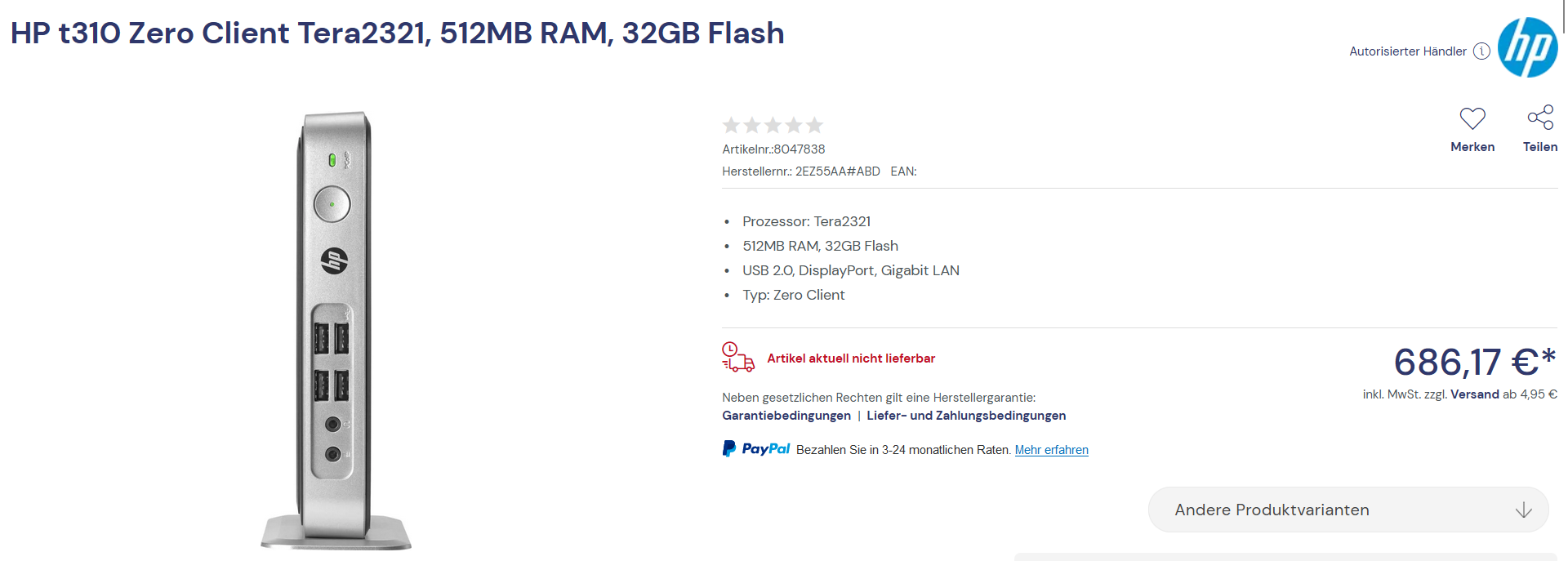
Description automatically generated

* **Welche Kosten sind in etwa für einen Zero Client zu veranschlagen? (konkretes Produkt + Preis)**

Zero Clients varrieren im Preis wie Thin Clients. Anfangen tun sie bei ca. 50€.

Graphical user interface, application

Description automatically generated



* **Wie viele Benutzer können gleichzeitig auf einem Windows Client angemeldet sein?**

Nur 1 Benutzer

* **Wie viele Benutzer können gleichzeitig auf einem Windows Server angemeldet sein?**

Beliebig viele, je nach Lizenz.

* **Was wird unter einer VDI verstanden, wie ist sie aufgebaut?**

Virtual Desktop Interface

Das Betriebsystem und Programme werden auf einem zentralen Server gehosted

* **Wo ist VDI ähnlich / unterschiedlich zu RDP?**

Basically the same?

* **Welche Motivation würde in deinem Unternehmen für den Einsatz einer VDI sprechen?**

Es ist energieeffiezienter sowie einfacher einzurichten

* **Wozu wird die Windows Remoteunterstützung verwendet? Was ist der Unterschied zu RDP?**

Um einen User fern zu helfen. Unterschied: Keine neue Sitzung erstellt

* **Welche Möglichkeiten hat ein User um auf Remote Apps zugreifen zu können? Wenn du CTO wärst, welche Varianten würdest du für welche User anbieten?**

Windows Remote Apps

Web-zugriff

RD-Clients

Start-Menü

* **Würdest du es als CTO erlauben, RDP Verbindungen direkt vom Home Office auf die Server hinter der Firewall zu erlauben?**

Mit geigneter Sicherung mit VPN, ja.

* **Wie wird der externe Zugriff über Remote Desktop Gateway realisiert – Funktionsweise Remote Desktop Gateway?**

Eröglicht die Verbindung zu einem Remote Desktop Server von einem Externen Netz.

Verschlüsselt (https)

* **Citrix vs. RDP**

**Funktionalität, Vor- u. Nachteile**

Performance: Citrix ist Schneller

Scalability: Citrix is besser skalierbar

Citrix ist einfacher für den User.

Citrix kann besser bei schlechter Verbindung verwendet werden.

RDP ist günstiger

* **Welche Citrix Lizenzen sind verfügbar? Geben Sie den dazugehörigen Preisbereich an.**

Citrix Server (SaaS)

Citrix Virtual Apps and Citrix Virtual Apps and Desktops 11 – 21$ / user / Monat

Citrix Hypervisor frei, 1200$ / Jahr / socket, 1800$ / Jahr / socket

* **Wenn du in einem Unternehmen mit 400 Arbeitsplätzen der CTO wärst, würdest du anhand der Lizenzmodelle RDP oder Citrix einsetzen?**

Ich würde Citrix verwenden. Es ist zwar teurer als RDP, aber es ist auch schneller und skalierbarer. Die Experience wird mit Citrix sehr wahrscheinlich besser sein.