

# Von zu Hause aus arbeiten, jetzt und auf lange Sicht.

Vielleicht kann beides gleichzeitig erreicht werden - eine schnelle und langfristig tragfähige Umsetzung.

*Da aufgrund der aktuellen Pandemie immer mehr Mitarbeiter von zu Hause aus arbeiten, stehen IT-Fachleute vor mehreren Herausforderungen. Führen sie eine "quick and dirty"-Lösung ein, um den unmittelbaren Bedarf zu decken? Sollten sie langfristig denken und verstehen, dass die Nutzung von Heimarbeitsplätzen zu einem De-facto-Standard geworden ist und eine professionelle Lösung erforderlich ist?*



Keine zwei Unternehmen haben die gleichen Bedürfnisse in diesem Bereich. Dieses Papier konzentriert sich auf kleine und mittlere Unternehmen (KMUs), bei denen drei wahrscheinliche Szenarien in ihren IT-Strukturen existieren.

- 1. PCs und Server:** Das Unternehmen arbeitet in einer traditionellen Umgebung, in der die meisten Anwendungen lokal auf PCs oder Laptops laufen und einige SaaS-Anwendungen über einen Webbrowser zugänglich sind. Die Daten sind lokal und auf Servern verfügbar.
- 2. Terminal-Dienste:** Das Unternehmen hat die meisten oder alle Anwendungen auf das Server-Backend verlagert und greift mit PCs darauf zu, in der Regel über Microsoft RDS. Eine Mischung aus lokal ausgeführten Anwendungen und Terminaldiensten ist möglich, solange sich die Endbenutzer auf Windows-PCs befinden.
- 3. Virtuelle Desktop-Infrastruktur (VDI):** Das Unternehmen ist vollständig auf eine Desktop-Virtualisierungslösung umgestiegen, wie die von Citrix, VMware oder Microsoft angebotenen Plattformen. Alle Anwendungen laufen im Rechenzentrum oder sind als SaaS zugänglich.

Desktop-Virtualisierung (Nr. 3 oben) ist nach wie vor das beste Szenario für den Einsatz im Heimbüro, da sie Sicherheit, zentrales Management, Datenkonsistenz und eine Backup-Strategie bietet. Diese VDI-Lösungen können jedoch für viele KMUs zu kostenintensiv und zu komplex sein. Für Unternehmen, die Legacy-Szenarien wie 1 oder 2 mit lokalen PCs verwenden, öffnet der Verbleib bei ihnen die Tür zu Sicherheitsrisiken, Datenkorruption und Inkonsistenzen. Einige KMUs sind zu einer Thin Client-Lösung übergegangen. Hier funktioniert ein Endgerät, indem es eine Fernverbindung zu einer serverbasierten Computerumgebung herstellt. Die meisten Anwendungen und alle sensiblen Daten werden auf dem/den Server(n) gespeichert, um sicheres Arbeiten von zu Hause aus zu ermöglichen.

Für KMUs, die noch Szenario 1 oder 2 verwenden, ist der einfachste Weg zur Virtualisierung von Anwendungen wahrscheinlich der Umstieg auf eine Terminaldienstlösung wie Microsoft RDS für alle relevanten Applikationen. Diese Dienste sind Teil bekannter und verstandener Microsoft-Server mit einer unkomplizierten Lernkurve für die IT.

Abhängig von der Arbeitslast und der Anzahl der Heimbüro-Benutzer kann die vorhandene Server-Hardware ausreichend sein, um die zusätzliche Last zu bewältigen. Eine größere Anzahl von Benutzern wird Investitionen in das Server-Backend erfordern, es sei denn, das Unternehmen ist bereit, schnell in eine Cloud-basierte Infrastruktur wie Azure oder AWS umzusteigen.

Der Umstieg auf Cloud-Dienste hat den Vorteil, dass sie schnell übernommen werden und für zukünftige Anforderungen skalierbar sind. Die Kosten für den Datenschutz und die langfristigen Systemkosten werden jedoch den für die interne Server-Infrastruktur erforderlichen CAPEX übersteigen.

Terminaldienste sind eine großartige Möglichkeit zur Virtualisierung von Anwendungen oder sogar von Desktops, auf denen Benutzer eine ähnliche Reihe von Anwendungen nutzen. Wenn Benutzer unterschiedliche Anforderungen haben und verschiedene Anwendungen verwenden, ist eine robustere Desktop-Erfahrung erforderlich. Eine echte VDI-Umgebung wie Citrix oder VMware wäre sinnvoller.

Diese Unternehmen bieten sehr leistungsstarke VDI- sowie Anwendungsvirtualisierungslösungen für eine große Anzahl von Benutzern (bis zu Tausenden) mit Management- und Fernzugriffstechnologien der Unternehmensklasse. Sofern diese nicht bereits vorhanden sind, dauert die Implementierung sehr viel länger und die Lernkurve ist steil.

Sobald die Entscheidung für die Virtualisierung der Umgebung gefallen ist, hat die Suche nach einem sicheren Weg zur Verbindung von Heimarbeitsplätzen mit den Rechenzentren Priorität.

Mehrere Fragen sollten sich stellen:

1. Ist eine zentrale Verwaltung der zu Hause verwendeten Geräte wünschenswert?
2. Wie gut sind die Heimanwender mit der Einrichtung von VPNs und Geräten vertraut?
3. Ist eine Mischung aus persönlicher und geschäftlicher Nutzung und damit eine Kombination aus privaten und geschäftlichen Daten erlaubt?
4. Welche Art von Credential-Management gibt es bereits, und was ist wünschenswert?
5. Wie wichtig ist die Nutzung von Multimedia über das Unternehmensnetzwerk?

Für die meisten Unternehmen wird die Antwort auf die Frage Nr. 3 ein eindeutiges "Nein" sein, d.h. zusätzliche Hardware in Form eines dedizierten Arbeits-PCs, Laptops oder Thin Clients ist notwendig. Obwohl Laptops als die logische Wahl betrachtet werden könnten, sollten ihre Nachteile nicht übersehen werden. Zunächst einmal handelt es sich um vollwertige PCs, die die persönliche Aufmerksamkeit der IT-Abteilung erfordern. Sie sind anfällig für Malware-Angriffe und verfügen über mehr Rechenleistung, als für eine virtualisierte Umgebung erforderlich ist. Außerdem sind sie aufgrund ihres Formfaktors über längere Zeiträume nur schwer zu verwenden, es sei denn, sie werden durch einen größeren Bildschirm, eine externe Tastatur und Maus ergänzt, was diese Lösung ziemlich teuer macht.

Der Einsatz von Thin Clients bietet stattdessen mehrere Vorteile, darunter ein Minimum an Interaktion für das IT-Personal, eine deutlich geringere Anfälligkeit für Malware-Angriffe und eine garantierte Trennung von persönlichen und firmeneigenen Daten und Anwendungen. Thin Clients gibt es in vielen verschiedenen Formen, aber es gibt nur zwei relevante Architekturen:

1. **x86:** Basierend auf der PC-x86-Architektur weisen diese Thin Clients die gleiche Kostenstruktur auf wie ein vollwertiger PC und sind teilweise teurer.
2. **ARM:** Basierend auf Plattformen wie der Raspberry Pi, bieten diese bei ähnlicher Leistung und Leistungsfähigkeit wesentlich niedrigere Hardwarekosten. Sie haben einen kleinen Formfaktor und lassen sich leichter in ein Heim- oder eine entfernten Arbeitstelle integrieren. In einigen Fällen verfügen ARM-basierte Clients möglicherweise nicht über spezifische Gerätetreiber, um alle möglichen Peripheriegeräte zu unterstützen. In einer Heimbüroumgebung ist dies jedoch gewöhnlich nicht relevant.

Thin-Clients werden von Ihrem IT-Team vorkonfiguriert eingesetzt, so dass für den Endbenutzer, der sie anschließen möchte, keine Vor-Ort-Einrichtungs- und Verwaltungskenntnisse erforderlich sind. Wenn sie richtig ausgewählt werden, können sie auch per Fernzugriff verwaltet und unterstützt werden.

Die Verbindung von Clients mit dem hauseigenen oder Cloud-Rechenzentrum kann sicher über integrierte VPN-Clients oder über die von allen großen Anbietern wie Citrix, VMware und Microsoft bereitgestellten Gateways erfolgen.

Zusammenfassend lässt sich sagen, dass dies eine relativ schnelle und einfache Möglichkeit ist, zukunftssichere Heimarbeitsplätze von KMUs bereitzustellen:

- Verschieben Sie alle relevanten Anwendungen auf Anwendungsvirtualisierungslösungen wie Microsoft RDS, entweder lokal oder Cloud-basiert.
- Richten Sie Client-Management-Software als virtuelle Anwendung ein, um eine Fernverwaltung zu ermöglichen.
- Wählen Sie die Verwaltung von Berechtigungsnachweisen (z.B. Yubikey).
- Wählen Sie den preisgünstigsten Thin Client, der einen einfachen Roll-out ermöglicht.

Wenn dies richtig gemacht wird, ist das Ergebnis eine sichere, benutzerfreundliche, standardisierte Home-Office-Lösung, die die Tür zu einer flexibleren, skalierbaren und zukunftssicheren IT-Infrastruktur öffnet.

## Über den Autor:



Jochen Polster ist ein Branchenveteran, der mehr als 25 Jahre im System- und Halbleitervertrieb und -marketing in Europa, den USA und Asien tätig war. Bei NComputing ist er als

Vizepräsident für Vertrieb und Marketing in Europa tätig.

## Über NComputing:

NComputing ist ein führender Anbieter von Desktop-Virtualisierungslösungen für mehr als 70.000 Unternehmen in 140 Ländern. NComputing hat sich auf die Bereitstellung erschwinglicher, einfach zu implementierender, zentral verwalteter und hochleistungsfähiger Thin-Client-Computing-Lösungen auf der Basis von Raspberry Pi spezialisiert. Der RX-RDP Thin Client ist ein Cloud-fähiger Thin Client, der speziell für Microsoft RDS entwickelt und optimiert wurde und auf Raspberry Pi3 basiert. Der RX-RDP bietet ein reichhaltiges PC-ähnliches Erlebnis in einem erschwinglichen, energiesparenden Gerät mit geringem Platzbedarf. Der neue RX420(RDP)-Thin Client bietet erstklassige Leistung und eine native doppelte Anzeige, angetrieben von der neuesten Raspberry Pi4. Beide Thin Client-Lösungen bieten HD-Multimedia-Wiedergabe im Vollbildmodus mit Unterstützung für Microsoft RemoteFX und NComputing vCAST Streaming, WiFi-Konnektivität und integrierte transparente USB-Umleitung, wodurch eine beispiellose Unterstützung von Peripheriegeräten erreicht wird.