

Virtualisierung von Laptops unserer Kunden

- Ausgangslage
- Ziele
 - Zugriff aus Standardumgebung
 - Ständige Verfügbarkeit
 - Leichtere Bedienbarkeit
 - Sicherheit gewährleisten
- Technische Ausführung
 - Virtualisierung
 - Abschottung der Virtuellen Maschine
 - Anschluß ans Kundennetzwerk
 - Benötigte Berechtigungen

Ausgangslage

Ich bekomme von Kunden Laptops übergeben, um mit dem für mich im Kundennetzwerk eingerichteten Benutzerprofil für Support- und Projektleistungen auf die Daten und Geräte des Kundennetzwerkes aus der standardisierten Umgebung des Kunden heraus zugreifen zu können. Da ich viel unterwegs bin und nicht ständig alle Laptops mit mir führen kann, ist es notwendig, eine Lösung zu finden, die Funktionen dieser Laptops ständig verfügbar zu machen.

Ziele

Zugriff aus Standardumgebung

Es soll nur aus der standardisierten Umgebung des Kunden auf dessen Netzwerk zugegriffen werden, egal, ob remote via VPN oder lokal am Netzwerk. Auf keinen Fall soll ein Fremdgerät an das Netzwerk angeschlossen werden oder der Zugriff von einem Fremdgerät aus erfolgen. Die Daten sollen nur innerhalb der Standardumgebung gespeichert werden und verfügbar sein.

Ständige Verfügbarkeit

Die Standardumgebung soll ständig verfügbar sein, wenn ich mein primäres Arbeitsgerät "MacBook Pro" mit mir führe, so daß ich jederzeit Support leisten kann.

Leichtere Bedienbarkeit

Alle meine Arbeitsprozesse und Peripheriegeräte sind auf mein MacBook Pro und dessen Bedienung ausgerichtet: Trackpad, Trackball, Monitore. Es erleichtert mir die Bedienung erheblich, wenn ich die Bedienung der Standardumgebung auch damit durchführen kann und z.B. auch von der höheren Bildschirmauflösung meines MacBook Pro am 27" Monitor im Büro profitiere.

Sicherheit gewährleisten

Mein MacBook Pro verfügt über eine vollständige Festplattenverschlüsselung und ein sicheres Kennwort. Es ist somit gewährleistet, daß nicht unberechtigt auf die Standardumgebung (die ja nochmal durch ein extra Kennwort gesichert ist) zugegriffen werden kann.

Technische Ausführung

Virtualisierung

Auf dem betriebsfähigen Laptop des Kunden wird Acronis True Image installiert und aus diesem ein (dann unverschlüsseltes) Image auf meinen Server (temporär) gespeichert. Es wird in Parallels Desktop auf meinem MacBook Pro eine virtuelle Maschine erzeugt und das Windows aus dem Image auf meinem Server mittels Acronis Boot Stick zurückgespeichert. Es werden danach alle spezifischen Hardwaretreiber des Laptop entfernt und die Parallels Utilities und Treiber installiert.

Abschottung der Virtuellen Maschine

Die virtuelle Maschine wird vom Hostsystem (MacOS meines MacBook Pro) abgeschottet, so daß kein gegenseitiger Festplattenzugriff möglich ist. Einzig die Zwischenablage wird freigegeben, so daß Text und Bilder hin- und her kopiert werden können. Es ist ferner möglich, Screenshots des virtualisierten Laptops auf meinem MacBook Pro anzufertigen (was für meine Dokumentationen notwendig ist).

Anschluß ans Kundennetzwerk

Normalerweise greife ich aus dem virtualisierten Laptop per VPN auf Ihr Netzwerk zu. Wenn ich vor Ort bin, verwende ich einen Netzwerkadapter "Belkin USB-C", dessen MacAdresse in der Access Control des Kundennetzwerkes registriert ist. Auf diesen Netzwerkadapter darf in meinem MacBook Pro nur die virtuelle Maschine zugreifen, ein Zugriff von anderen virtuellen Maschinen, wie auch vom MacOS selbst aus ist nicht möglich.

Benötigte Berechtigungen

Für die Virtualisierung ist eine Anmeldung mit administrativen Rechten (zumindest temporär) erforderlich. Ferner ist notwendig, daß der Startprozeß / die Festplattenverschlüsselung nicht mit Hardware des Laptop zwingend abgesichert ist.