# Sicheres MultiSeat

Axel Schöner

12. Dezember 2013

**Zusammenfassung**

Der Einsatz von MultiSeat zur Minimierung der Anschaffungs- und Betriebskosten schafft Sicherheitsprobleme. Um einen reibungslosen und sicheren Betrieb zu garantieren gilt es diese zu identifizieren und zu beseitigen. Als geeignetes Mittel hierzu dienen verschiedene Virtualisierungstechniken.

## 1 Einleitung

Einzelplatz-Computersysteme befinden sich weitestgehend im Idle-Zustand. Jedes Computersystem besitzt ein Netzteil mit lastabhängigem Wirkungsgrad, welcher nur unter bestimmten Voraussetzungen optimal ist. Zusätzlich können im Idle-Zustand nicht alle Komponenten des Computersystems ab- oder energiesparend geschaltet werden. Klassisches MultiSeat ermöglicht die Effizienz zu steigern, verringert jedoch die lokale Sicherheit der Benutzer.

## 2 Vor-/Nachteile

### 2.1 Vorteile

Wird ein Computersystem von mehreren Personen gleichzeitig verwendet:

1. sinkt die Anzahl der, außerhalb des Wirkungsgrades betriebenen, Computersysteme
2. erhöht sich die Zeitspanne des optimalen Wirkungsgrades für das verwendete Computersystem
3. verringern sich die Anschaffungskosten pro Arbeitsplatz
4. verringern sich die Wartungskosten pro Arbeitsplatz
5. Serverdienste (zum Beispiel Dateiserver) für Anwender belasten nicht externes Netzwerk

### 2.2 Nachteile

In Bezug auf die Sicherheit entstehen dabei folgende Probleme:

1. Netzwerk-Datenverkehr ist bereits innerhalb des Computersystems nicht mehr privat

2. Wechseldatenträger können von allen Benutzern eingesehen/Manipuliert werden
3. Angriffe gegen lokale Prozesse möglich
4. Umgehung von Authentifizierungsmechanismen
5. Lokale Exploits

# 3 Virtualisierungssoftware

## 3.1 Linux Containers(LXC)

Bei LXC handelt es sich um die Userspace-basierte Komponente zum Betrieb von Linux Containern, welche mittels Kernel-Komponenten den 'virtuellen' Betrieb von Linux-Betriebssystemen ermöglicht. Linux Containers ermöglicht basierend auf Namespaces die Isolierung vorhandener Ressourcen. Durch die Verwendung von CGroups können bestimmte Ressourcen Namespace-basierend freigegeben und limitiert werden. Dies ermöglicht Container gegeneinander abzuschotten, als auch Verklemmungen aufgrund von Überlast einzelner Container zu vermeiden. Im speziellen ermöglicht dies auch den Zugriff auf virtuelle Terminals oder Geräte zum Beispiel zur Ein- und Ausgabe.

## 3.2 QEMU

Bei QEMU handelt es sich um einen Emulator, welcher einzelne Komponenten als auch komplette Computersysteme emulieren kann. Dies ermöglicht den Betrieb jedes Betriebssystems, welches auf einer durch QEMU unterstützten Architektur läuft. Durch die Verwendung von 'KVM-Kernelmodul', 'Virtio' und gegebenenfalls 'VGA Pass-through' wird eine nahezu native Performanz erreicht.

# 4 Konzepte

## 4.1 Container-basierter Desktop

Zum Betrieb eines Linux-Desktop Betriebssystem innerhalb eines Containers sind folgende Vorkehrungen zu treffen:

- Zugriff auf Eingabegeräte über Device-Nodes mittels CGroups erlauben
- Zugriff auf Grafikkarte über Device-Nodes mittels CGroups erlauben
- Laden der Grafikkarten-Treiber im Host-Betriebssystem verhindern
- X-Server innerhalb des Containers auf die speziellen Ein- und Ausgabegeräte konfigurieren

### 4.2 QEMU-basierter Desktop

Zum Betrieb eines Desktop Betriebssystem innerhalb einer emulierten Umgebung sind folgende Vorkehrungen zu treffen:

- X-Server Konfiguration auf die speziellen Ein- und Ausgabegeräte konfigurieren
- Eigene Session für Displaymanager erzeugen, welche die virtuelle Maschine startet

### 4.3 Bereitstellen von Betriebssystemen

Je nachdem welcher Virtualisierungsansatz (LXC/ QEMU) verfolgt wird, kann das Betriebssystem entweder direkt auf Filesystem-Ebene oder in Form einer Image-Datei zur Verfügung gestellt werden. In beiden Fällen kann das Betriebssystem von einem vorher bereitgelegten Verzeichnis abgeleitet werden. Dazu empfiehlt sich ein Snapshot-fähiges Filesystem wie BTRFS als Grundlage zu verwenden.

## 5 Mehrnutzen durch Virtualisierung

Das Aufbauen von VPN-Verbindungen in einer durch Linux-Container oder QEMU bereitgestellten Desktop-Umgebung ist für andere Umgebungen unsichtbar. Die verschiedenen Möglichkeiten der Netzwerkanbindung, welche sowohl für Linux-Container als auch QEMU angeboten werden, gestatten eine flexible Konfiguration je nach Anwendungsfall. Durch den Einsatz temporärer Images, die beim Starten einer virtuellen Maschine von einer zuvor erzeugten Quelle abgeleitet werden, kann jeder Zeit eine saubere Betriebsumgebung bereitgestellt werden. Das Computersystem kann zusätzlich notwendige Serverdienste lokal bereitstellen, sodass zusätzliche Hardware eingespart werden kann.

## 6 Fazit

Durch den gezielten Einsatz von Virtualisierungstechniken lassen sich mehrere sichere Arbeitsplätze über ein einzelnes Computersystem abdecken. Gegenüber dem klassischen MultiSeat bietet dieser Ansatz zusätzlich die Möglichkeit unterschiedliche Betriebssysteme dem Benutzer anzubieten, als auch notwendige Serverdienste isoliert parallel zu betreiben.