Sicherheit in virtualisierten Betriebssystemumgebungen

Benjamin Vetter, bv@tonim.com

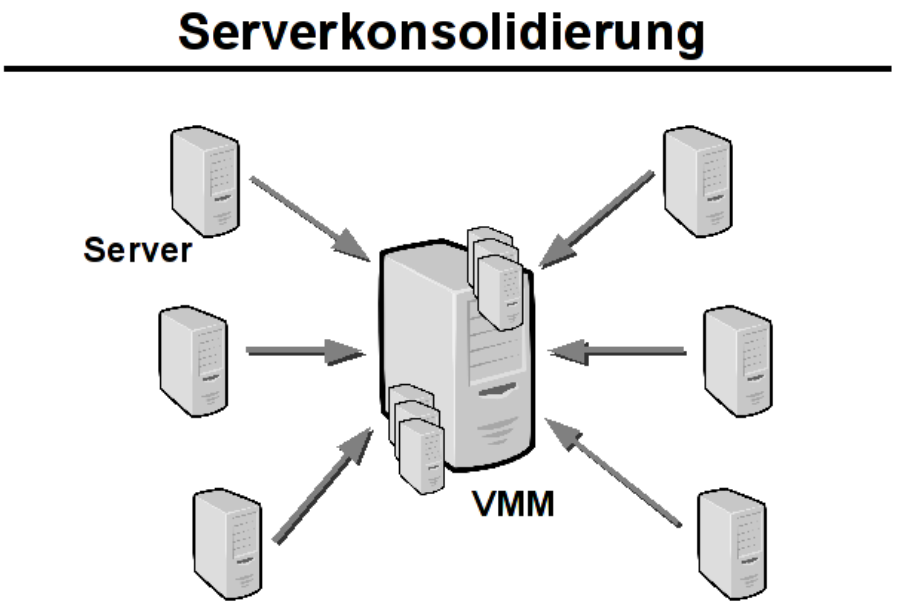
Hochschule für Angewandte Wissenschaften Hamburg
Fakultät Technik und Informatik
Department Informatik

8. Februar 2010

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Gliederung

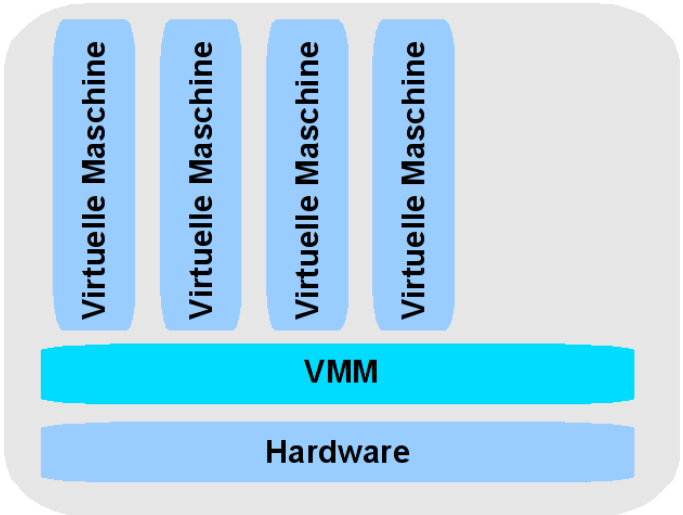
Zweck der Virtualisierung



- Bessere Auslastung der Server
- Kostenersparnis durch Wegfall von Servern
- Höhere Flexibilität beim Umgang mit virtuellen Maschinen

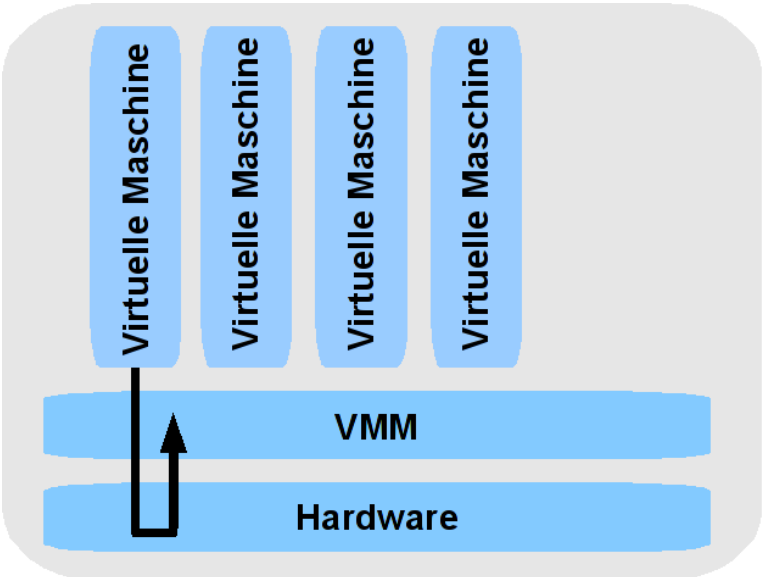
Gliederung

Grundsätzliche Virtualisierungstechniken



- Der Virtual Machine Monitor (VMM) stellt eine Schnittstelle in Software bereit, die von außen der Hardware-Schnittstelle entspricht
- Der Zugriff einer virtuellen Maschine auf die virtuelle Schnittstelle mündet im Zugriff auf die Hardware-Schnittstelle
- Die Koordination der Zugriffe ermöglicht mehrere virtuelle Maschinen auf nur 1 realen Maschine

Grundsätzliche Virtualisierungstechniken

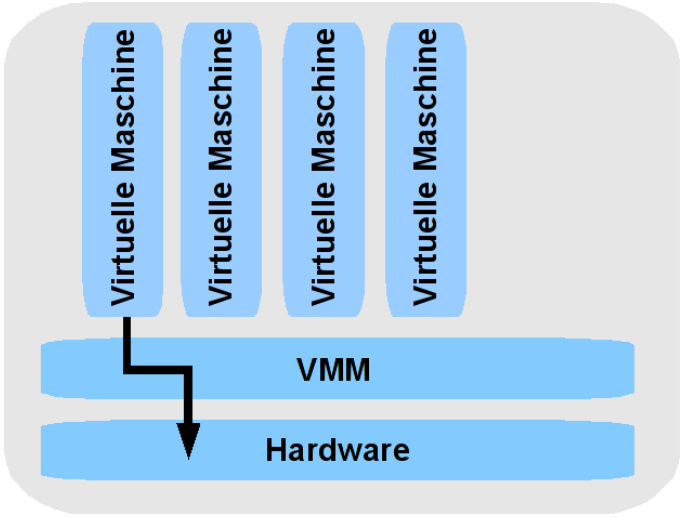


Trap & Emulate:

- Die sensitiven Instruktionen (Zugriff auf sensitive Register oder Arbeitsspeicherbereiche) lösen Traps (Interrupts) aus
- Der VMM erhält die Kontrolle und emuliert das gewünschte Verhalten
- Aber: Die Architektur muss geeignet sein

Grundsätzliche Virtualisierungstechniken

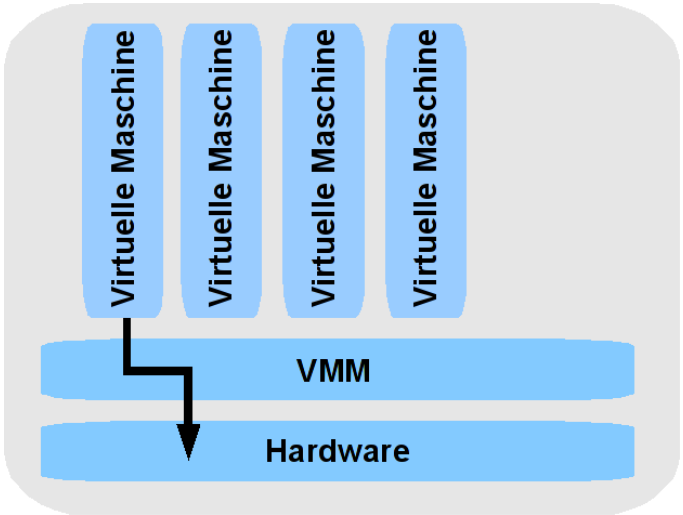
x86-Architektur: Nicht alle sensitiven Instruktionen lösen Traps aus



- Ausweg 1: Binary Translation
  - Den Binärcode vor der Ausführung umschreiben
  - Die Traps manuell einbauen
- Ausweg 2: Paravirtualisierung
  - Die Betriebssysteme arbeiten mit dem VMM zusammen
  - Die Betriebssysteme müssen angepasst werden

Grundsätzliche Virtualisierungstechniken

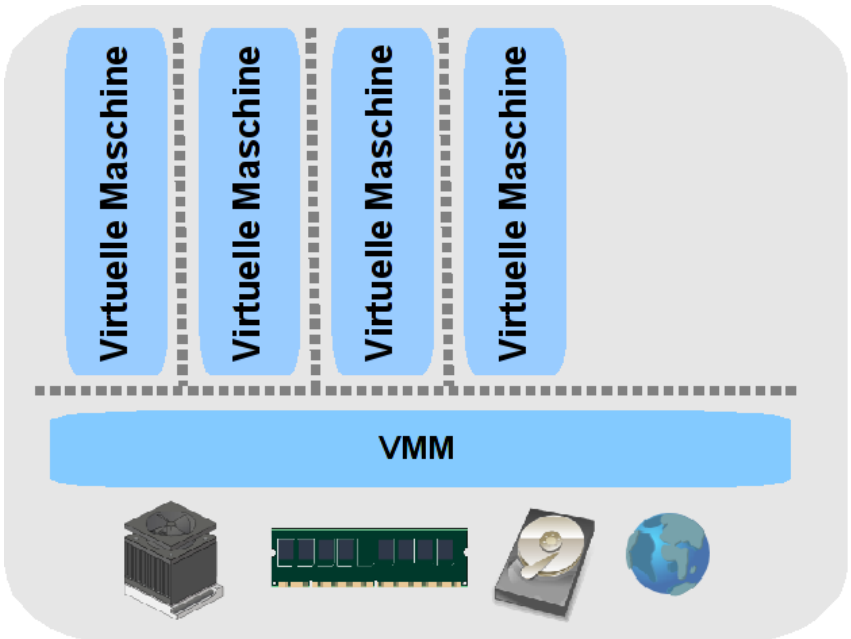
x86-Architektur: Nicht alle sensitiven Instruktionen lösen Traps aus



- Ausweg 1: Binary Translation
  - Den Binärcode vor der Ausführung umschreiben
  - Die Traps manuell einbauen
- Ausweg 2: Paravirtualisierung
  - Die Betriebssysteme arbeiten mit dem VMM zusammen
  - Die Betriebssysteme müssen angepasst werden

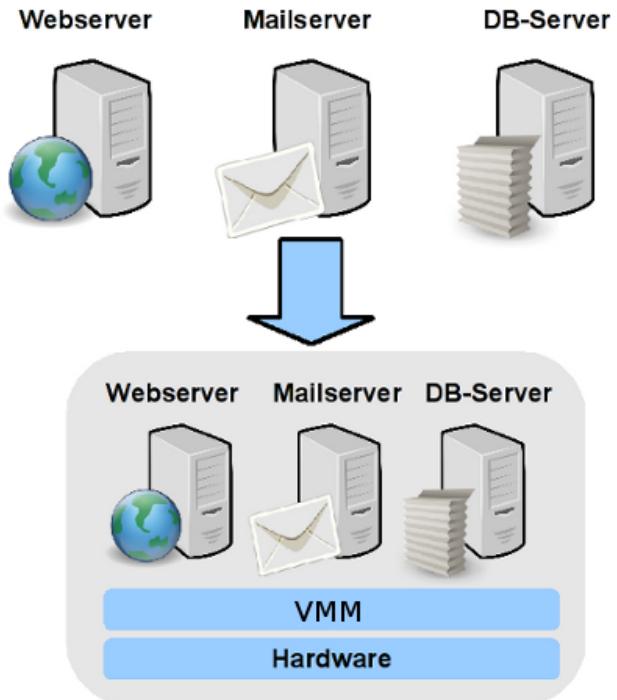
Gliederung

Grundsätzliche Probleme



- Der VMM sorgt für Isolation
- Virtualisierung bedeutet: logische Isolation
- Ein Verlust logischer Isolation bedeutet: Sicherheitsvorfall

Grundsätzliche Probleme



- Normalerweise gilt: 1 Dienst = 1 Betriebssystem = 1 Server
- Jetzt gilt: Die virtuellen Maschinen teilen sich die Hardware
- Physische Isolation ist stärker als logische Isolation
- Die Physische Isolation geht durch Virtualisierung verloren

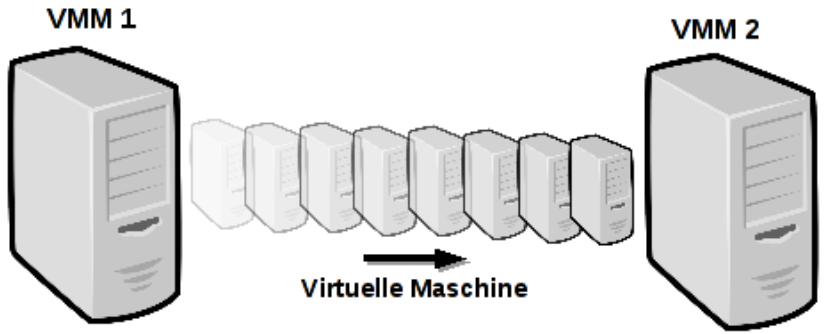
Grundsätzliche Probleme

- Der VMM erhöht die Sicherheit nicht
- Serverkonsolidierung:
  - Die logische Isolation steigt nicht (war schon maximal)
  - Die physische Isolation geht verloren

Das Sicherheitsniveau sinkt bei einer Serverkonsolidierung grundsätzlich

Gliederung

Organisatorische Probleme



- Mobility:
  - Die Trusted Computing Base von virtuellen Maschinen ist ggf. wesentlich größer
  - Statt 1 Host: alle Hosts auf denen die virtuelle Maschine jemals lief

Organisatorische Probleme

- Software-Lifecycle:
  - Rollback und Kopieren von virtuellen Maschinen
  - Widerspruch zu linearer Lebenslinie
  - Sicherheitslücken und gesperrte Accounts werden ggf. wieder geöffnet, Zufallszahlen sind ggf. weniger "frisch"
- Vertrauenswürdigkeit der Administratoren:
  - Ein VMM-Administrator hat ggf. uneingeschränkten Zugriff
  - Probleme bei hoher Mobilität
  - Die Komplexität der Sicherheitsstrategie steigt

Organisatorische Probleme

- Software-Lifecycle:
  - Rollback und Kopieren von virtuellen Maschinen
  - Widerspruch zu linearer Lebenslinie
  - Sicherheitslücken und gesperrte Accounts werden ggf. wieder geöffnet, Zufallszahlen sind ggf. weniger "frisch"
- Vertrauenswürdigkeit der Administratoren:
  - Ein VMM-Administrator hat ggf. uneingeschränkten Zugriff
  - Probleme bei hoher Mobilität
  - Die Komplexität der Sicherheitsstrategie steigt

Gliederung

Komplexität des VMM

Die Sicherheit des VMM ist entscheidend, denn:

- Das Sicherheitsniveau sinkt bei einer Serverkonsolidierung grundsätzlich
- Virtualisierung bereitet organisatorische Probleme
- Der VMM muss die logische Isolation garantieren

Hohe Komplexität (viel Programmcode) des VMM ist schlecht, denn:

- Die Wahrscheinlichkeit von Programmierfehlern steigt
- Die Verifizierbarkeit des VMM sinkt

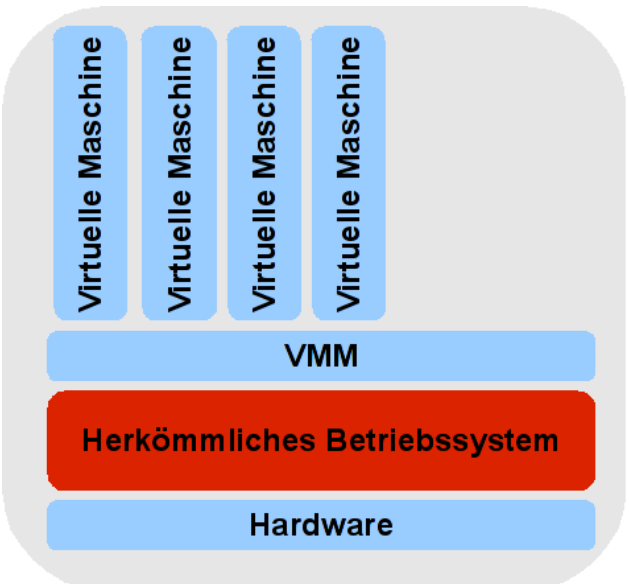
Ein VMM muss möglichst wenig Komplexität (wenig Programmcode) aufweisen um dennoch ein hohes Maß an Sicherheit garantieren zu können!

Komplexität der CPU-Virtualisierung

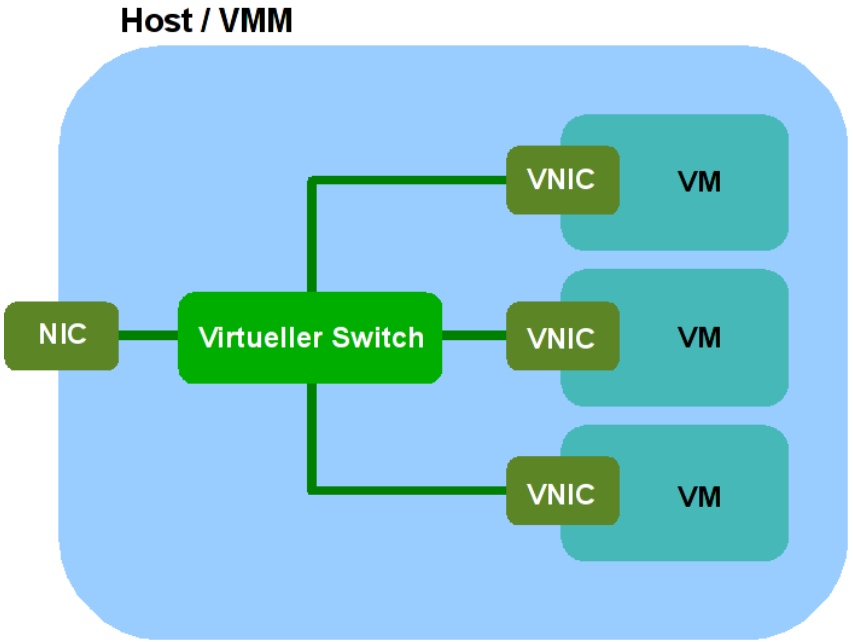
- Trap & Emulate weist geringe Komplexität auf
- Kein Trap & Emulate auf der x86-Architektur möglich
- Binary Translation weist hohe Komplexität auf
- Paravirtualisierung ist besser geeignet, aber bedeutet Portierungsaufwand bzgl. Sicherheitspatches
- Eine CPU-unterstützte Virtualisierung entspricht dem Trap & Emulate

Komplexität der IO-Virtualisierung

- Aufgrund von Direct Memory Access (x86) muss der VMM die vielen Treiber für die x86-IO aufnehmen
- Der VMM muss IO-Komponenten emulieren: fehleranfällig und komplex
- Der VMM setzt ggf. auf einem herkömmlichen OS auf. Die TCB des VMM steigt explosionsartig.



Komplexität der Netzwerk-Virtualisierung



- Ein Netzwerkpaket muss den physischen Host nicht mehr verlassen
- IDS, IPS, Firewalls, etc sehen den Traffic nicht mehr
- Komponenten müssten in den VMM verlagert werden: hohe Komplexität

Gliederung

Resultierende Angriffe

Es resultieren Sicherheitslücken und Angriffe aus den konzeptionellen Bedrohungen:

- VM-Escape (CVE-2007-4993, CVE-2008-0923, CVE-2007-1744, ...)
- Privilege Escalation (CVE-2008-4915, CVE-2008-4279)
- DoS (CVE-2008-4914, CVE-2008-1340, CVE-2007-2491, ...)
- Weitere typische Sicherheitslücken (CVE-2007-1320, CVE-2008-4279, ...)
- Thrashing, Sniffing, Inter-VM-Angriffe

Resultierende Angriffe

Es resultieren Sicherheitslücken und Angriffe aus den konzeptionellen Bedrohungen:

- VM-Escape (CVE-2007-4993, CVE-2008-0923, CVE-2007-1744, ...)
- Privilege Escalation (CVE-2008-4915, CVE-2008-4279)
- DoS (CVE-2008-4914, CVE-2008-1340, CVE-2007-2491, ...)
- Weitere typische Sicherheitslücken (CVE-2007-1320, CVE-2008-4279, ...)
- Thrashing, Sniffing, Inter-VM-Angriffe

Resultierende Angriffe

Es resultieren Sicherheitslücken und Angriffe aus den konzeptionellen Bedrohungen:

- VM-Escape (CVE-2007-4993, CVE-2008-0923, CVE-2007-1744, ...)
- Privilege Escalation (CVE-2008-4915, CVE-2008-4279)
- DoS (CVE-2008-4914, CVE-2008-1340, CVE-2007-2491, ...)
- Weitere typische Sicherheitslücken (CVE-2007-1320, CVE-2008-4279, ...)
- Thrashing, Sniffing, Inter-VM-Angriffe

Resultierende Angriffe

Es resultieren Sicherheitslücken und Angriffe aus den konzeptionellen Bedrohungen:

- VM-Escape (CVE-2007-4993, CVE-2008-0923, CVE-2007-1744, ...)
- Privilege Escalation (CVE-2008-4915, CVE-2008-4279)
- DoS (CVE-2008-4914, CVE-2008-1340, CVE-2007-2491, ...)
- Weitere typische Sicherheitslücken (CVE-2007-1320, CVE-2008-4279, ...)
- Thrashing, Sniffing, Inter-VM-Angriffe

Resultierende Angriffe

Es resultieren Sicherheitslücken und Angriffe aus den konzeptionellen Bedrohungen:

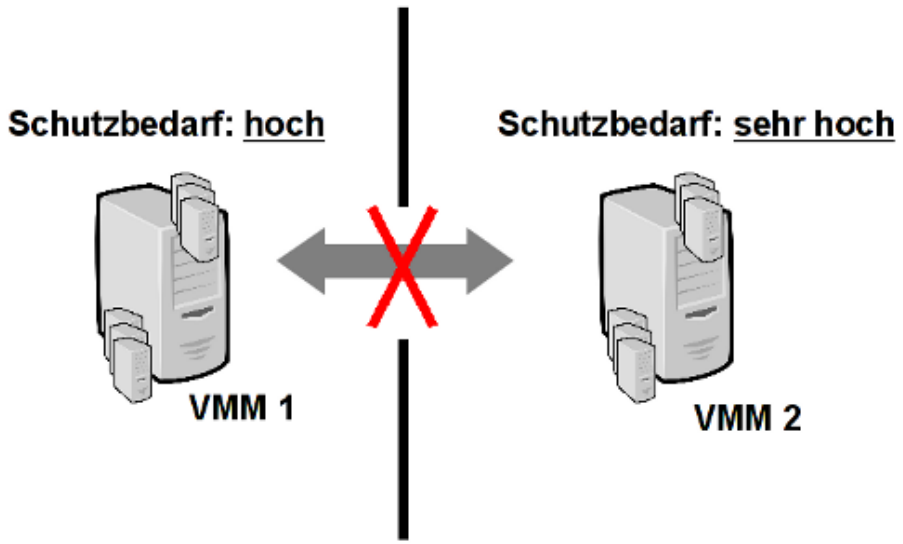
- VM-Escape (CVE-2007-4993, CVE-2008-0923, CVE-2007-1744, ...)
- Privilege Escalation (CVE-2008-4915, CVE-2008-4279)
- DoS (CVE-2008-4914, CVE-2008-1340, CVE-2007-2491, ...)
- Weitere typische Sicherheitslücken (CVE-2007-1320, CVE-2008-4279, ...)
- Thrashing, Sniffing, Inter-VM-Angriffe

Gliederung

Maßnahmen um Risiken der Virtualisierung zu reduzieren

Index	Maßnahme
M.1	VMs mit unterschiedlichem Schutzbedarf nicht oberhalb des gleichen VMM konsolidieren
M.2	Die Komplexität von Virtualisierungstechnologien minimieren
M.3	Das Schutzniveau des VMM bzgl. Angriffen maximieren
M.4	Das Konsolidierungspotential eines VMM einschränken
M.5	Die bestehenden Schutzmaßnahmen aufrecht erhalten
M.6	Den Kreis der Administratoren eines VMM reduzieren
M.7	Die Mobilität von VMs einschränken
M.8	Prozesse für die Inbetriebnahme, den Betrieb und die Wartung von VMs definieren und einrichten

M.1: VMs mit unterschiedlichem Schutzbedarf nicht oberhalb des gleichen VMM konsolidieren



- Die Risiken gelten nur noch innerhalb einer Schutzbedarfskategorie
- Es sind nur noch Systeme des gleichen Schutzbedarfs gefährdet

Reduziert auch die Flexibilität

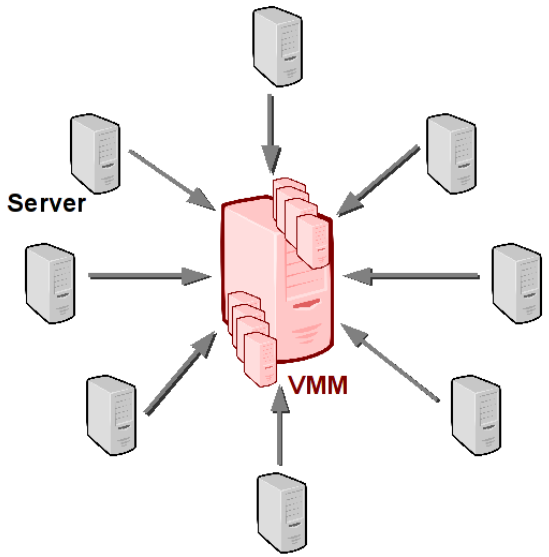
M.2 Die Komplexität von Virtualisierungstechnologien minimieren

Aspekt	Maßnahmen
CPU-Virtualisierung	- CPU-Unterstützte oder Paravirtualisierung - Binary Translation, wenn möglich, vermeiden
Architektur	- Typ-I-VMM (Bare Metal VMM) - Hosted- und Domain-Architektur vermeiden
IO-Virtualisierung	- IOMMU - Auswahl zertifizierter Treiber im VMM - Komplexität der Hardwareemulation vermeiden
Netzwerk-Virtualisierung	- Switching im VMM - auf Routing im VMM verzichten - Rerouting des Netzwerkverkehrs
Ressourcen	- Statische Ressourcenzuweisung durch den VMM

M.3 Das Schutzniveau des VMM bzgl. Angriffen maximieren

- Wer Zugriff auf den VMM besitzt erhält Zugriff auf alle virtuellen Maschinen
- Die Isolation von virtuellen Maschinen und dem VMM ist zu maximieren
- Wenn der VMM auf ein herkömmliches OS aufsetzt: OS gegen Angriffe härten
- Reduziert das Risiko eines Ausbruchs, Privilege Escalation und weiteren offenen Sicherheitslücken

M.4 Das Konsolidierungspotential eines VMM einschränken



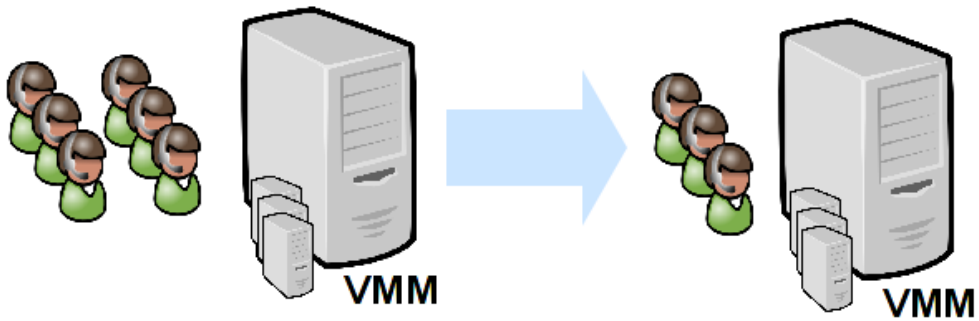
- Verringert das Schadensausmaß bei einem Verlust der Verfügbarkeit
- Ein gleichzeitiger Verlust der Verfügbarkeit wird unwahrscheinlicher

Beschränkt das Konsolidierungspotential auch innerhalb einer Schutzbedarfskategorie

M.5 Die bestehenden Schutzmaßnahmen aufrecht erhalten

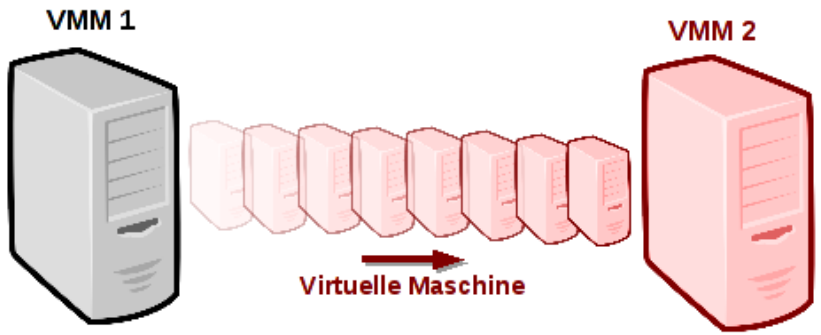
- Virtualisierung beseitigt keine Schwachstellen
- Für Betriebssysteme und Applikationen in virtuellen Maschinen gelten die gleichen Sicherheitslücken
- Patch- und Updatezyklen sind einzuhalten
- Verhindert, dass das Risiko oberhalb des VMM steigt

M.6 Den Kreis der Administratoren eines VMM reduzieren



- Es sollen nur einige Administratoren statisch mit virtuellen Maschinen verknüpft sein
- Vermeidet Inkonsistenzen bei Mobilität von virtuellen Maschinen
- Reduziert das Risiko, das von Insidern ausgeht

M.7 Die Mobilität von virtuellen Maschinen einschränken



- Reduziert das Risiko von Sicherheitsvorfällen
- Vereinfacht die Bereinigung bei Sicherheitsvorfällen
- Vermeidet Inkonistenzen bzgl. der Vertrauenswürdigkeit von VMM-Administratoren

Die Flexibilität sinkt, die Komplexität der Sicherheitsstrategie steigt

M.8 Prozesse für die Inbetriebnahme, den Betrieb und die Wartung von VMs definieren und einrichten

- Zentrale Erfassung aller virtuellen Maschinen
- Verhindert, dass virtuelle Maschinen nur sporadisch, ohne definierte Zuständigkeiten betrieben werden
- Reduziert das Risiko von lange offenen Sicherheitslücken
- Reduziert die Dauer bis zur Entdeckung von Sicherheitsvorfällen

Fazit

- Eine Serverkonsolidierung vermindert die Sicherheit grundsätzlich
- Organisatorische Probleme
- Ein VMM sollte möglichst schmal ausfallen
- Komplexität, Flexibilität und Konsolidierungspotential eines VMM müssen für hochschutzbedürftige Güter eingeschränkt werden
- Flexibilität und Konsolidierungspotential sollten jedoch gerade durch Virtualisierung maximiert werden!

Fazit

- Eine Serverkonsolidierung vermindert die Sicherheit grundsätzlich
- Organisatorische Probleme
- Ein VMM sollte möglichst schmal ausfallen
- Komplexität, Flexibilität und Konsolidierungspotential eines VMM müssen für hochschutzbedürftige Güter eingeschränkt werden
- Flexibilität und Konsolidierungspotential sollten jedoch gerade durch Virtualisierung maximiert werden!

Fazit

- Eine Serverkonsolidierung vermindert die Sicherheit grundsätzlich
- Organisatorische Probleme
- Ein VMM sollte möglichst schmal ausfallen
- Komplexität, Flexibilität und Konsolidierungspotential eines VMM müssen für hochschutzbedürftige Güter eingeschränkt werden
- Flexibilität und Konsolidierungspotential sollten jedoch gerade durch Virtualisierung maximiert werden!

Fazit

- Eine Serverkonsolidierung vermindert die Sicherheit grundsätzlich
- Organisatorische Probleme
- Ein VMM sollte möglichst schmal ausfallen
- Komplexität, Flexibilität und Konsolidierungspotential eines VMM müssen für hochschutzbedürftige Güter eingeschränkt werden
- Flexibilität und Konsolidierungspotential sollten jedoch gerade durch Virtualisierung maximiert werden!

Fazit

- Eine Serverkonsolidierung vermindert die Sicherheit grundsätzlich
- Organisatorische Probleme
- Ein VMM sollte möglichst schmal ausfallen
- Komplexität, Flexibilität und Konsolidierungspotential eines VMM müssen für hochschutzbedürftige Güter eingeschränkt werden
- Flexibilität und Konsolidierungspotential sollten jedoch gerade durch Virtualisierung maximiert werden!