DECOIT

CeBIT 2014

CeBIT cebit.com HANNOVER 10.-14. MÄRZ 2014

Effektive Virtualisierung von Serversystemen und Netztopologien durch Virtual Security Appliances (VSA)

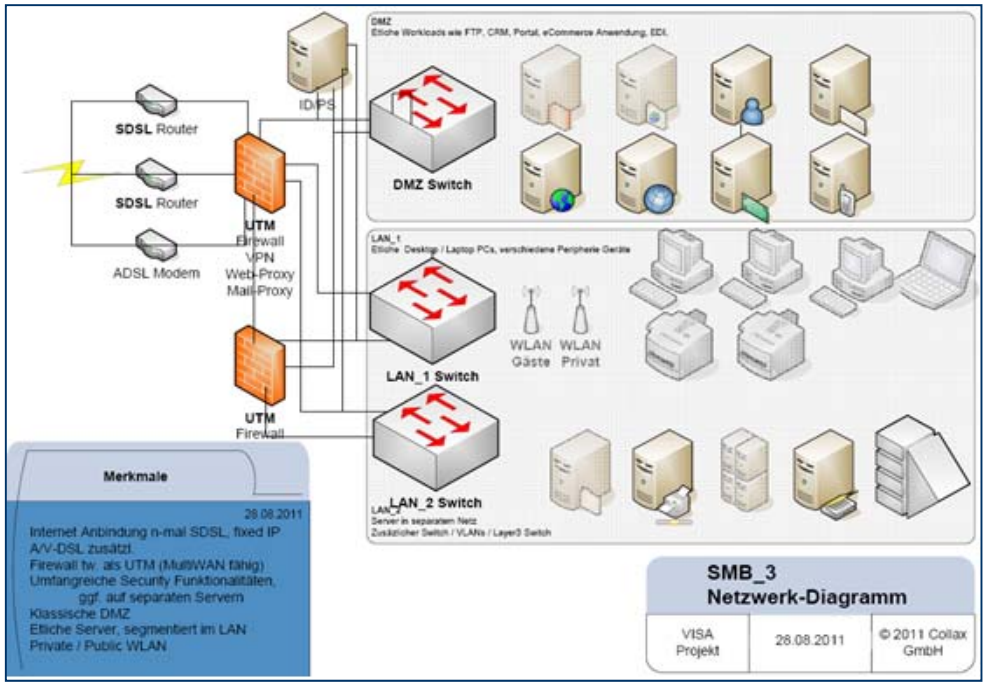
Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
detken@decoit.de

Ausgangslage

- IT-Infrastrukturen sind mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) relativ komplex
- Die Auswirkungen von Änderungen sind oft erst im Realbetrieb zu erkennen
- Zusätzlich müssen auch BSI IT-Grundschutzanforderungen heute umgesetzt werden
- Die Virtualisierung hat zunehmend Einzug gehalten und wird die Komplexität noch erweitern
- Daher sollte der Umgang mit IT-Infrastrukturen vereinfacht werden, um
  - Konfigurationsfehler zu minimieren
  - Hohe Verfügbarkeit zu erreichen
  - Das IT-Sicherheitsniveau hoch zu halten
- Dies könnte man auf Basis sog. Virtual Security Appliances (VSA) schaffen

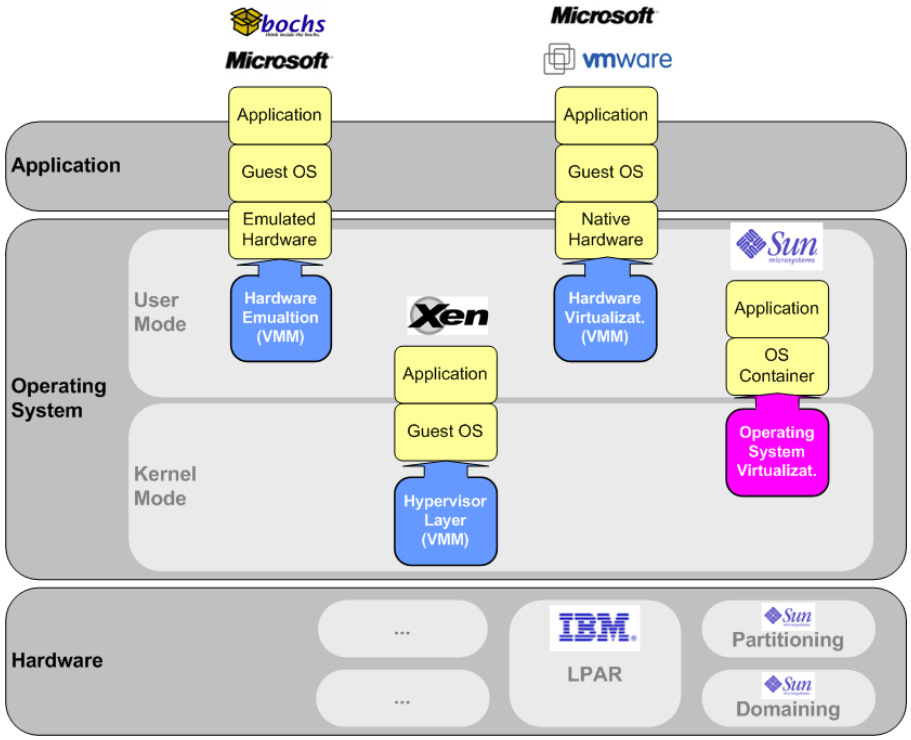
KMU-Infrastruktur

- Die IT-Infrastruktur eines KMU
  - DMZ
  - Firewall
  - IDS
  - Switches
  - Remote-Zugänge
  - E-Mail-Server
  - FTP-Server



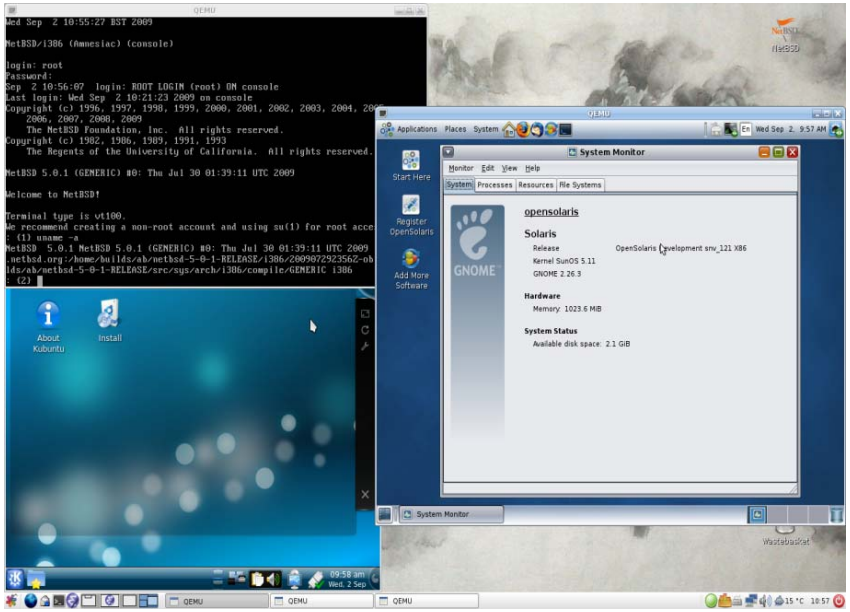
Virtualisierungslösungen

- Diverse Hypervisor-basierte Systeme:
  - VMWare ESX/ESXi
  - VMWare Workstation
  - VMWare Fusion
  - VirtualBox
  - Windows Virtual PC
  - QEMU
  - Xen
  - KVM



DECOIT

Kernel-based Virtual Machine (KVM)



- Die DECOIT GmbH hat sich auf KVM festgelegt:
  - Einzige (wirklich) freie Lösung am Markt
  - Breite Unterstützung
  - Hohe Performance (Hardware-basiert)
  - Fester Bestandteil des Linux-Kernels
  - Keine Lizenzkosten (GNU GPL)

DECOIT

Bestandteile von KVM

- Die Bestandteile von KVM sind Open-Source-Software und stehen unter verschiedenen Varianten der GPL-Lizenz zur Verfügung:
  - KVM-Kernel-Modul: GPL v2
  - KVM-Benutzer-Modul: LGPL v2
  - QEMU Systememulation (für x86: PC-Emulator): GPL v2
  - Linux-Usermode von QEMU: GPL v2
  - BIOS-Dateien (bios.bin, vgabios.bin und vgabios-cirrus.bin): LGPL v2 oder neuer

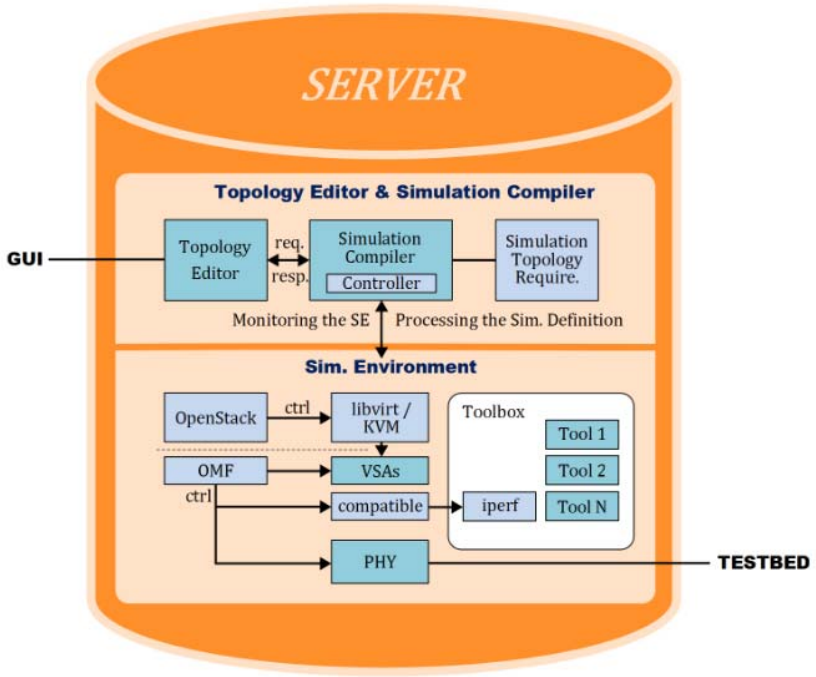
DECOIT

Definition Virtual Security Appliance

- Virtual Appliance (VA):
  - Als VA wird das Image einer Virtuellen Maschine (VM) bezeichnet, welches ein installiertes und vorkonfiguriertes Softwaresystem enthält
  - Hierbei beinhaltet dieses Image auch schon das Betriebssystem selbst.
- Virtual Security Appliance (VSA):
  - Als VSA werden verschiedene Virtual Appliances bezeichnet, die vorrangig der Sicherheit dienen
  - Von der Netzwerksicherheit (Layer 2) bis zur Anwendungssicherheit (Layer 7)
  - Mit Hilfe von VSAs wird versucht, IT-Hard- und Software zu virtualisieren

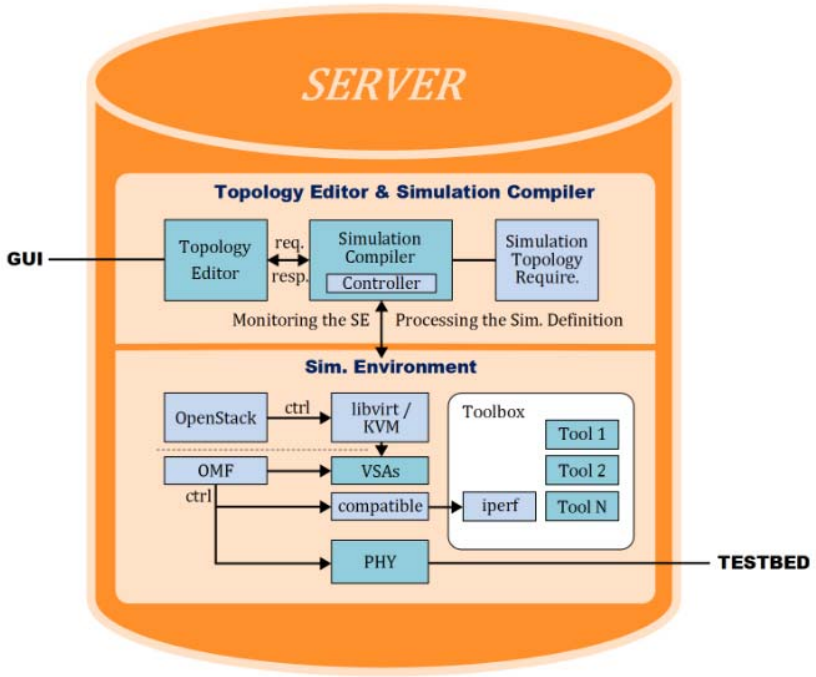
OpenStack-Simulationsarchitektur

- Durch Systemsimulationen und Funktionstests können neue Konfigurationen sicher in das Produktivnetz eingebettet werden
- Die VISA-Simulationsplattform besteht aus:
  - VISA Topologie Editor (V-TE)
  - Simulation Compiler (SC)
  - Simulation Environment (SE)



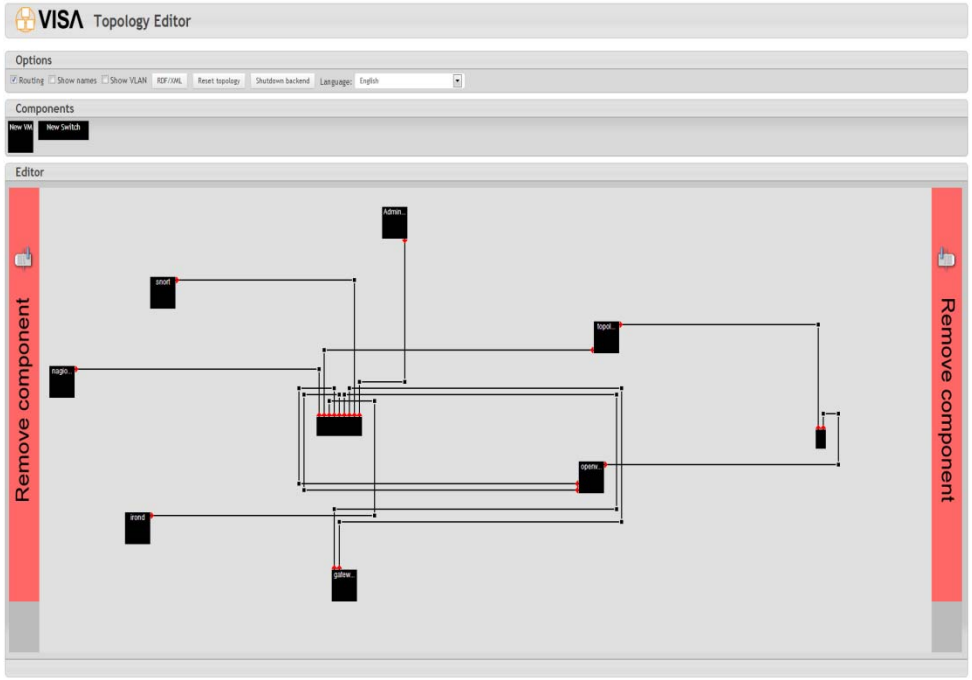
Zusammenspiel V-TE, SC und SE

- Der V-TE ermöglicht die Definition von Modellen, die das reale Netz repräsentieren
- Durch den V-TE kann ein virtuelles IT-System, basierend auf Server, Clients und Netzwerkkomponenten erstellt werden
- Nach der Definition der Randbedingungen kann die Netzbeschreibung an den SC weitergegeben werden
- Das SE ist in der Lage, die Topologie-Definition bzgl. der IT-Sicherheitsanforderungen zu überprüfen
- Das SE ist in der Lage VSAs zu laden, zu konfigurieren und Messdaten zu sammeln



VISA Topologie Editor (V-TE)

- Der V-TE bietet die Möglichkeit Netzmodelle des Produktivsystems nachzubilden
- Es ist ein grafisches Tool, dass folgende Funktionalität anbietet:
  - Abbildung des bestehenden Netzes in virtueller Umgebung
  - Neudefinition von virtuellen Umgebungen
  - Starten von Simulationen
  - Automatisches Routing der Verkabelung
  - Übergabe der Netztopologie an den Simulation Compiler (SC)

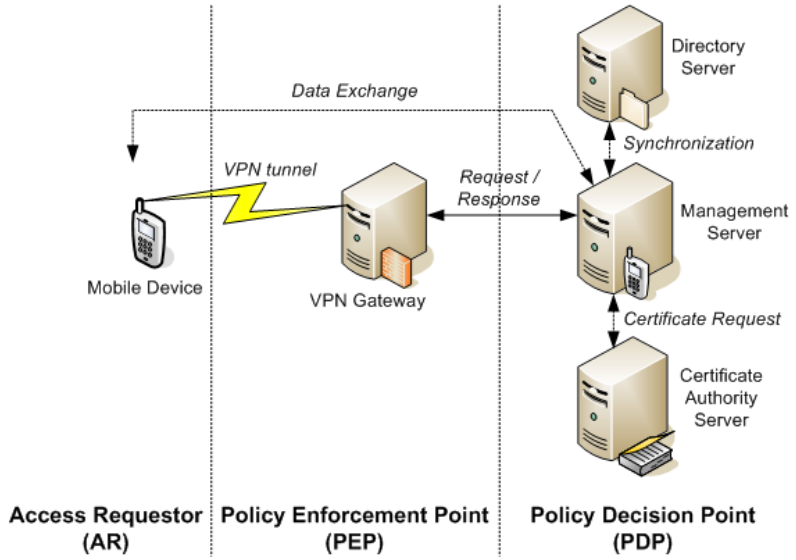


VSA-Beispiele

- VSA-SRA: ermöglicht Android Smartphone-Endgeräten sicher auf verschiedene IT-Systeme zuzugreifen, durch Trusted Computing (TC) Mechanismen
- VSA-MAC: nutzt das IF-MAP-Protokoll der Trusted Computing Group (TCG), um Informationen verschiedener Sicherheitskomponenten zentral auszuwerten

VSA „Secure Remote Access"

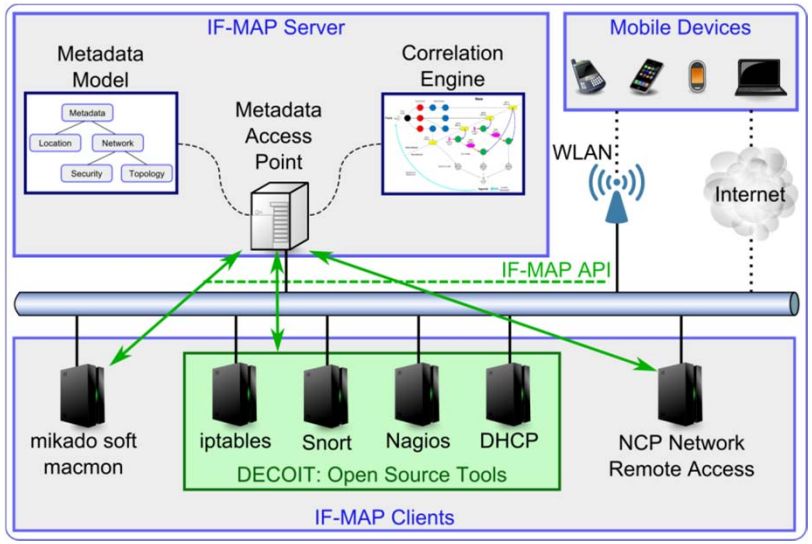
- Die VSA-SRA ermöglicht das sichere Einwählen in ein Firmennetz mittels eines Android-Smartphones
- Dies beinhaltet die Komponenten Android-Client, FreeRADIUS-Server, TNC-Server und VPN-Gateway
- Das Smartphone verbindet sich durch das VPN-Gateway mit dem Unternehmensnetz
- Dadurch ist aber noch nicht sichergestellt, ob das Smartphone als vertrauenswürdig eingestuft werden kann, da nur die Teilnehmerdaten abgefragt werden
- TPM-Chip in den Smartphones wäre zur absolut sicheren Einwahl notwendig, um zusätzlich abzufragen:
  - Applikationsbasis
  - Versionsnummer
  - Sicherheitsrichtlinien



INNOVATIONSPREIS-IT
BEST OF 2012
initiative mittelstand
TK / VOIP

VSA „Metadata Access Control"

- Die VSA-MAC besteht hingegen aus den Komponenten IF-MAP-Server und den IF-MAP-Clients für Android, Snort, iptables, FreeRADIUS und Nagios
- Bei IF-MAP handelt es sich um ein offenes, herstellerunabhängiges Client-Server-Netzprotokoll zum Austausch von beliebigen, in XML codierten Metadaten
- Dabei stellt der IF-MAP-Server die zentrale Komponente dar, indem die Daten von allen IF-MAP-Clients gesammelt und durch einen Graphen zur Verfügung gestellt werden
- Weiterhin stellt er die gesammelten Daten auch den IF-MAP-Komponenten zur Verfügung



DECOIT

Zusammenfassung

- KVM führt bislang noch ein Nischendasein(!)
- Der freie Hypervisor wurde jedoch mit Kernelversion 2.6.20 in den Linux-Kernel fest integriert und wird so mit jeder aktuellen Version mitgeliefert
- Im Mai 2011 gründeten u.a. HP, IBM, Intel, Red Hat und SUSE die Open Virtualization Alliance (OVA) um KVM für Virtualisierung und cloud-basierte Lösungen auf den Markt zu etablieren. Mittlerweile gehören über 200 Mitglieder zur OVA
- Mit dem V-TE und den VSA-Bausteinen der DECOIT lässt sich auf Basis von OpenStack/KVM eine gesamte IT-Infrastruktur abbilden
- Es lassen sich bestehende Infrastrukturen simulieren und/oder virtuelle Infrastrukturen in die Produktivumgebung einbetten
- Bereits in der Basis lassen sich IT-Compliance-Anforderungen erfüllen
- Dadurch kann ein höheres Maß an IT-Sicherheit erreicht werden

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09