GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung

Prof. Dr. Kai-Oliver Detken,
DECOIT GmbH

VISA

Agenda

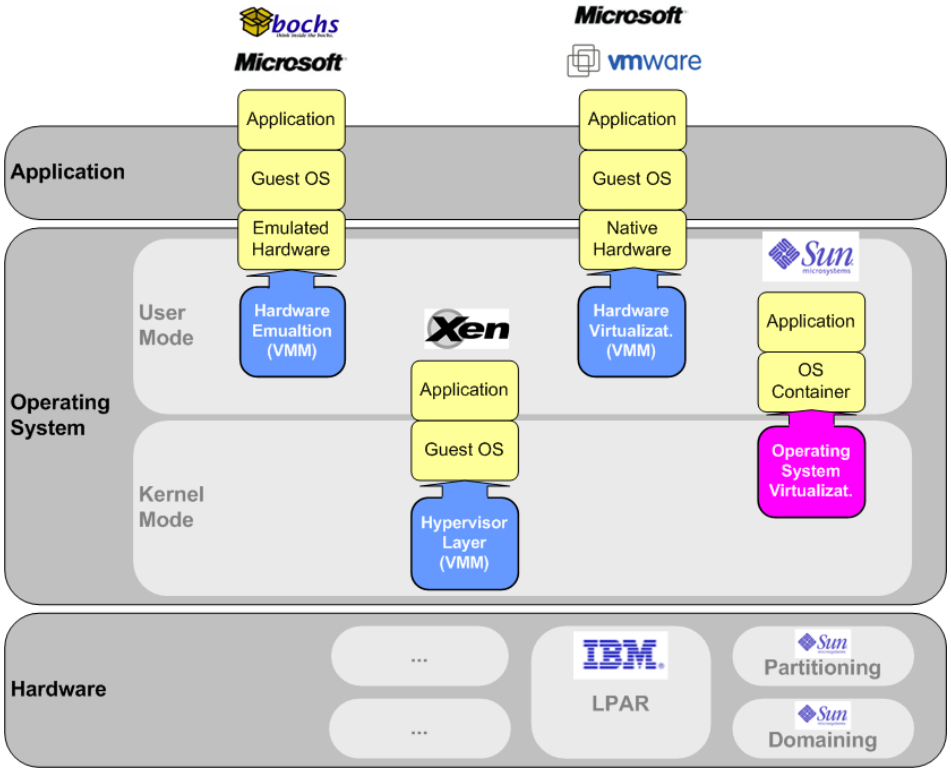
- Virtualisierungstechniken
- Ist-Zustand in KMU
- Das VISA-Projekt
- Virtual Security Appliances (VSA)
- Zusammenfassung und Ausblick

Virtualisierungstechniken

VISA

Definition der Virtualisierung

- Der Begriff *Virtualisierung* muss differenziert betrachtet werden, da er in verschiedenen Kontexten benutzt wird
- Es ist essentiell, die unterschiedlichen Konzepte sowie Verfahren klar voneinander zu trennen
- Die diversen Virtualisierungstechniken haben aber eines gemein: sie trennen die Abhängigkeit zwischen Soft- und Hardware
- Die Erschaffung dieser Abstraktion führt dazu, dass vorhandene IT-Ressourcen flexibel genutzt werden können und eine höhere Auslastung erzielt werden kann



Quelle: Diplomarbeit „Vergleich von Virtualisierungstechnologien“ von Daniel Hirschbach, 31.08.2006, Lizenz: Creative Commons Namensnennung 2.0

Virtualisierungsarten (1)

- Server-Virtualisierung
  - Sie bezeichnet Software- oder Hardware-Techniken, die dazu dienen, mehrere Instanzen eines oder verschiedener Betriebssysteme auf einem einzigen Rechner gleichzeitig nebeneinander zu betreiben
  - Die einzelnen Instanzen werden als virtuelle Maschinen (VM) oder Gast bezeichnet und verhalten sich in der virtuellen Umgebung identisch zum „normalen“ Betrieb direkt auf der Hardware
  - Produkte zur Server-Virtualisierung sind primär auf Skalierbarkeit, Geschwindigkeit und Flexibilität ausgelegt

Virtualisierungsarten (2)

- Hardware-basierte Virtualisierung
  - Das Verfahren kombiniert Techniken der Voll- und Para-Virtualisierung, wobei die Virtualisierungs-funktionalität in die Prozessorhardware integriert wird
  - Ziel der Hardware-basierten Virtualisierung ist es, die Vorteile der Vollvirtualisierung zu erreichen und gleichzeitig deren Performance-Nachteile zu eliminieren
  - Der allgemeine Trend zur Virtualisierung brachte die Hardwarehersteller dazu, ihre neuen x86-Prozessoren um Virtualisierungsfunktionen zu erweitern
  - Diese modernen Prozessoren unterstützen die Interaktion zwischen den virtuellen Maschinen und dem *Hypervisor*

Virtualisierungsarten (3)

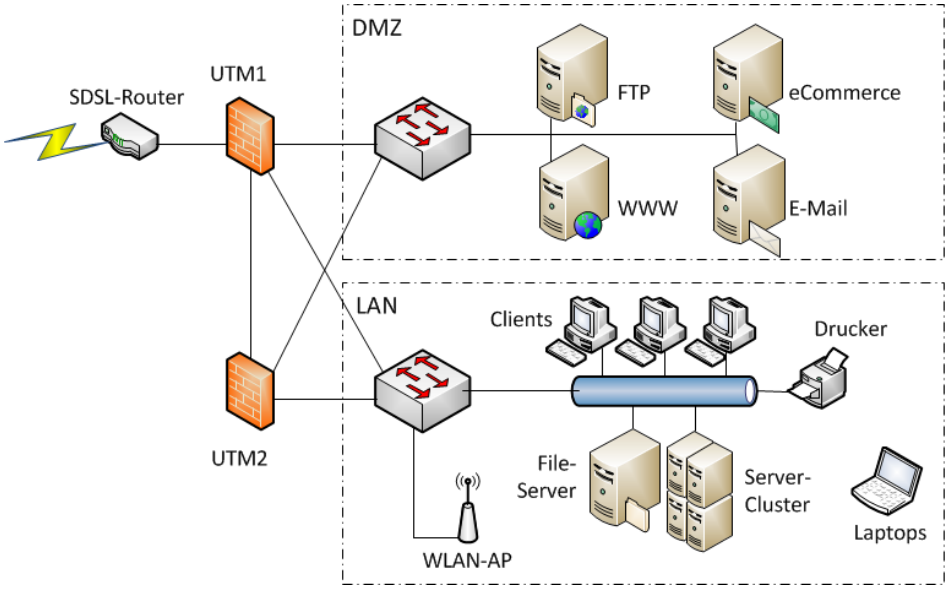
- Vollvirtualisierung
  - Das Verfahren ist mit der Hardware-basierten Virtualisierung gleichzusetzen
  - Ein entscheidender Unterschied liegt allerdings darin, dass das Privilegien-System der neuen Prozessoren erweitert wurde, die Gastsysteme müssen nicht mehr in nicht-privilegierten Ringen betrieben werden, sondern deren Kernel kann direkt in Ring 0 gestartet werden
  - Die Gastsysteme können somit unangepasst bleiben, da sie sich in ihrer gewohnten Umgebung befinden
  - Virtualisierungslösungen, die das Verfahren der Hardware-basierten Virtualisierung einsetzen, sind beispielsweise Xen oder KVM

Ist-Zustand in KMU

VISA

Beispiel eines mittelständisches Unternehmens

- IT-Infrastrukturen in dieser Umgebung können bereits durchaus komplex werden
- Größeres Netzwerk, inkl. WLAN-Anbindung
- Diverse Sicherheitskomponenten
  - DMZ
  - UTM Firewalls
  - Anti-Virensysteme
- NAS/SAN-Storage-Lösungen
- VM-Server



IT-Sicherheitsniveau

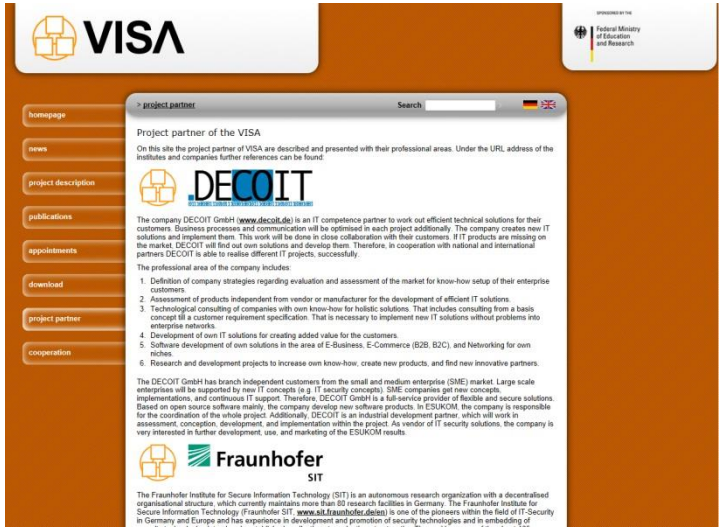
- Themenspanne bei KMUs reicht von Client-Installationen bis zu Netzwerk-Konfigurationen, Serversystem-installation und -konfiguration, Telefonanlage bis hin zum Support diverser eingesetzter IT-Anwendungen wie z.B. ERP-/FiBu-Systeme
- Es ist aber meist nur ein rudimentäres Fachwissen über diese Themen in den IT-Abteilungen vorhanden
- Bei Anbindung neuer Techniken, wie z.B. Smartphones, steht die Funktionalität im Vordergrund und nicht die IT-Sicherheit
- Ein IT-Sicherheitsbeauftragter ist meist nicht bestellt
- Gesetzliche Vorgaben (Compliance-Anforderungen) sind daher unbekannt oder werden kaum beachtet

Das VISA-Projekt

VISA

Überblick über das Projekt

- Gefördert durch das BMBF
- VISA startete im August 2011 und wird im Juli 2013 enden
- Das Gesamtbudget beträgt: 1,7 Mio. € (geförderter Anteil: 1,0 Mio. €)
- Partners des Projektes sind:
  - DECOIT GmbH (Projektleiter)
  - Fraunhofer SIT
  - University of Applied Sciences Dortmund
  - Collax GmbH
  - IT-Security@Work GmbH
  - National ICT Australia Limited



www.visa-project.de

Projektziele

- Es das Ziel des Projektes VISA, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen, insbesondere der Sicherheits-komponenten, zu erleichtern und zu unterstützen
- Diese Unterstützung basiert auf drei Kernmerkmalen:
  - Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen
  - Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA)
  - Vereinfachung und Nachweisbarkeit der Einhaltung von IT-Standards, IT-Security- und Compliance-Anforderungen durch geeignet entwickelte VSAs als fertig verwendbare IT-Bausteine

Verbesserungspotenziale

- Die Infrastruktur kann logisch entzerrt werden, und Anwendungen dort im Netzwerk betrieben werden, wo es aus Security-Sicht angemessen ist
- Die gesamte Infrastruktur (Server, Firewall, Router, VPN etc.) wird virtuell konzipiert und kann nach erfolgreichen Tests als Live-System direkt übernommen werden
- Die Virtualisierung kann gleichzeitig zur Hardware-Konsolidierung genutzt werden, und dadurch einen wesentlichen Beitrag zur Kostenreduktion leisten (Hardware-Bedarf, Strom- und Kühlkosten)
- Es lassen sich Redundanzen (wie Firewall oder Router) einfacher aufbauen, um neben der IT-Sicherheit auch die Verfügbarkeit zu gewährleisten
- Der Aufbau von Testumgebungen und damit die Abschätzung von Auswirkungen von Änderungen an der IT-Umgebung eines Unternehmens wird vereinfacht, da die Bausteine aus der Produktion nahezu identisch im Rahmen einer Testumgebung eingesetzt werden können

Virtual Security Appliances (VSA)

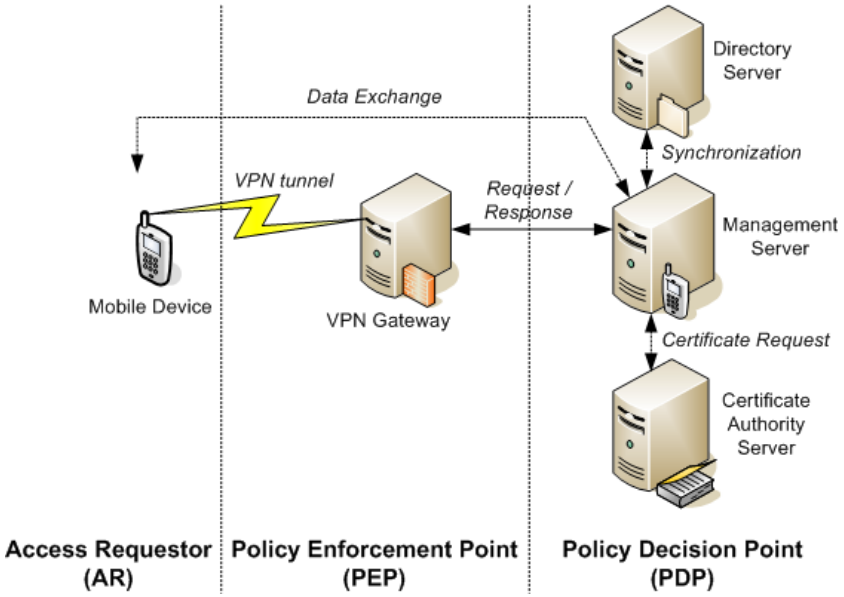
VISA

VSA-Entwicklung

- Bisher wurden im VISA-Projekt die für KMU identifizierten VSAs konzeptioniert, die vorrangig der Sicherheit dienen (von Netzwerksicherheit, Layer 2 bis Anwendungssicherheit, Layer 7)
- Diese VSAs bestehen im Wesentlichen aus virtualisierten IT-Security-Bausteinen (Modulen) und Services
- Sie haben das Ziel, unterschiedliche Bereiche der IT-Sicherheit in typischen KMU-Topologien abzudecken
- Folgende VSAs werden im VISA-Projekt gerade umgesetzt:
  - VSA-AAA
  - VSA-SRC
  - VSA-MAC

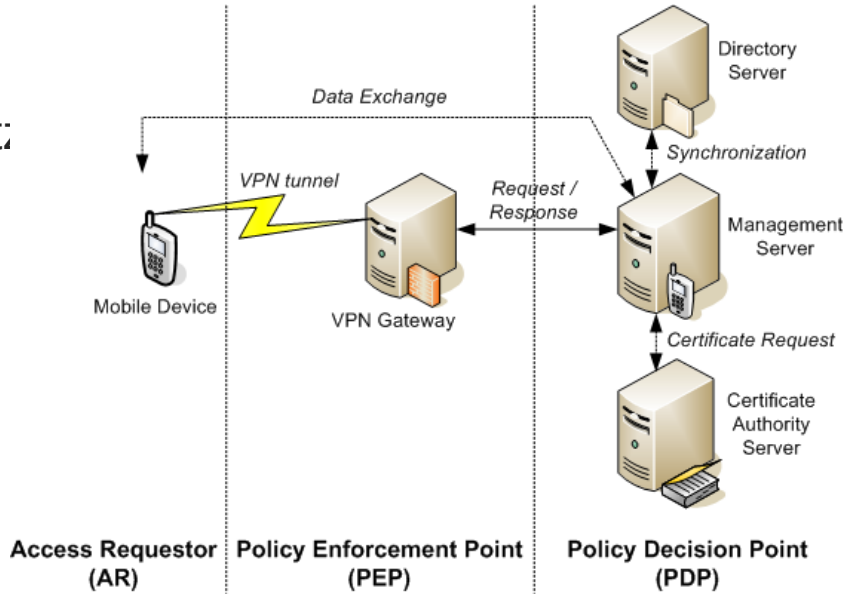
VSA-SRA (1)

- 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
- Dies wird erst durch das Senden gesammelter Metriken des Android-Smartphones vom TNC-Client an den TNC-Server ermöglicht
- Die Metriken enthalten die installierte Applikationsbasis, Versionsnummern und Richtlinien, die für das Smartphone gelten



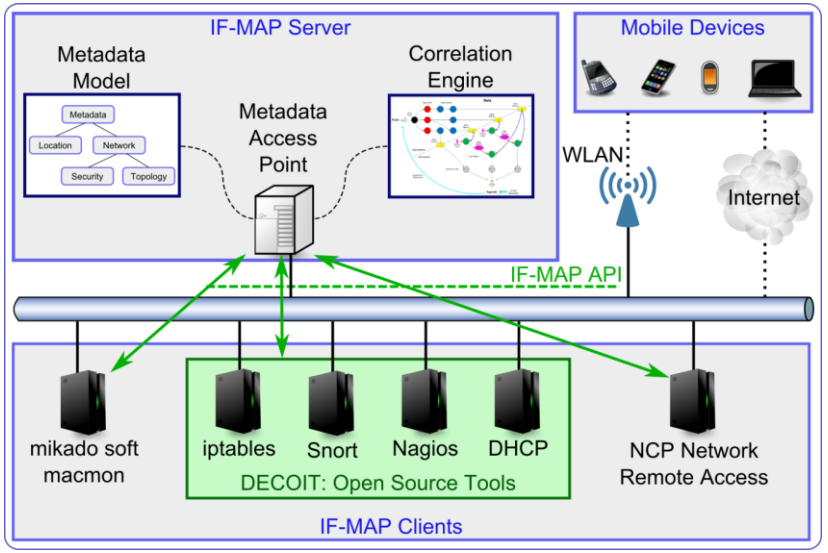
VSA-SRA (2)

- Der TNC-Server vergleicht anschließend die gesendeten Metriken mit denen in seiner Datenbank
- Sind Applikationen installiert, die er nicht kennt oder die auf seiner Blacklist enthalten sind, wird dem Smartphone der Zugang verweigert bzw. das Smartphone wird in ein Quarantänenet: isoliert
- Innerhalb des Quarantänenetzes kann das Endgerät mithilfe einer Softwareverteilungslösung auf den geforderten aktuellen Stand gebracht werden
- Anschließend kann das Gerät gemäß den TNC-Spezifikationen eine erneute Attestierung anfordern
- Sind alle Voraussetzungen erfüllt, erhält der Teilnehmer des mobilen Endgeräts Zugriff auf die gewünschte Zielapplikation und somit auf die gewünschten Zielressourcen



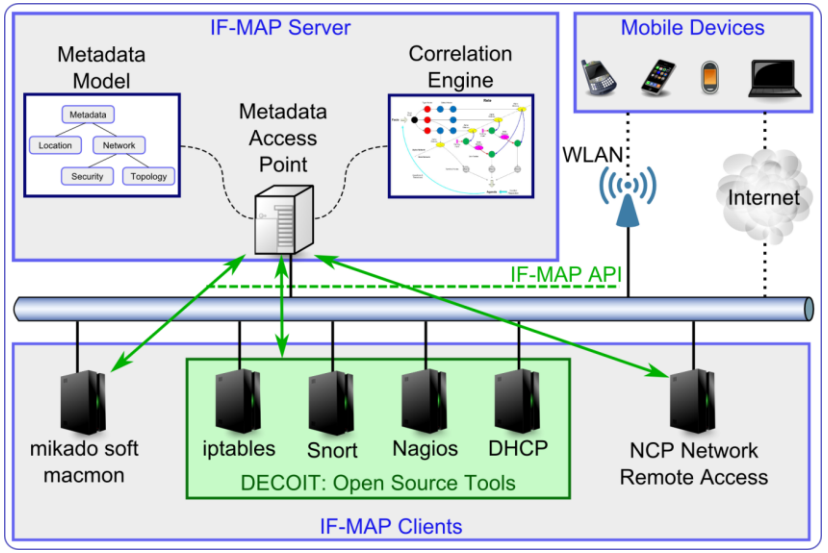
VSA-MAC (1)

- 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



VSA-MAC (2)

- Die Stärke von IF-MAP gegenüber einer reinen IDS-basierten Anomalie-Erkennung liegt dabei in der Diversität der Daten
- Durch die gesammelte Datenbasis lassen sich Korrelationen durchführen und Anomalien leichter erkennen bzw. Angriffen entgegenwirken
- Beispiele hierfür sind u.a. die Blockierung des Datenstroms durch eine Firewall, Sperren des Zugriffes in Form eines Switches oder eines VPN-Gateways, Isolierung des Endgerätes in eine Quarantänezone etc.
- Auf Grundlage der gesammelten Informationen können die Details protokolliert und entsprechende Meldungen an die verantwortlichen Systemadministratoren generiert werden



Zusammenfassung und Ausblick

VISA

Zusammenfassung

- Die Virtualisierungstechniken schreiten immer weiter voran und ermöglichen heute die Abbildung der Produktivumgebung
- Damit kann letztendlich die gesamte IT-Infrastruktur nachgebildet werden, also auch das Netz zwischen Client und Server
- Die Übersichtlichkeit geht allerdings durch diverse Virtualisierungstechniken verloren
- Dadurch können zusätzliche Fehler und Sicherheitslücken entstehen, die das Unternehmensnetz vor neue Herausforderungen stellen

Fazit

- Das Projekt VISA hat sich daher einerseits zum Ziel gesetzt, die Komplexität virtueller Umgebungen zu verringern, indem die Handhabung solcher Lösungen verbessert werden soll
- Anderseits will man aber auch eine Möglichkeit schaffen, bestehende IT-Infrastrukturen vorab simulieren zu können, um Fehlkonfigurationen zu vermeiden
- Das ist nicht nur aus Sicherheitsgründen wichtig, sondern auch aus Sicht der Compliance und Verfügbarkeit relevant
- Nach der erfolgreichen Simulation können dann zwei Möglichkeiten ausgewählt werden:
  - Übernahme der Konfiguration in die bestehende IT-Infrastruktur
  - Überführung der Simulation in das Produktivnetz

Vielen Dank!

…für die Aufmerksamkeit

Copyright 2011-2013

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1160“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.