

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung



Sichere virtuelle Sicherheitskomponenten für KMUs



*Prof. Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH, Fahrenheitstr. 9,
D-28359 Bremen*

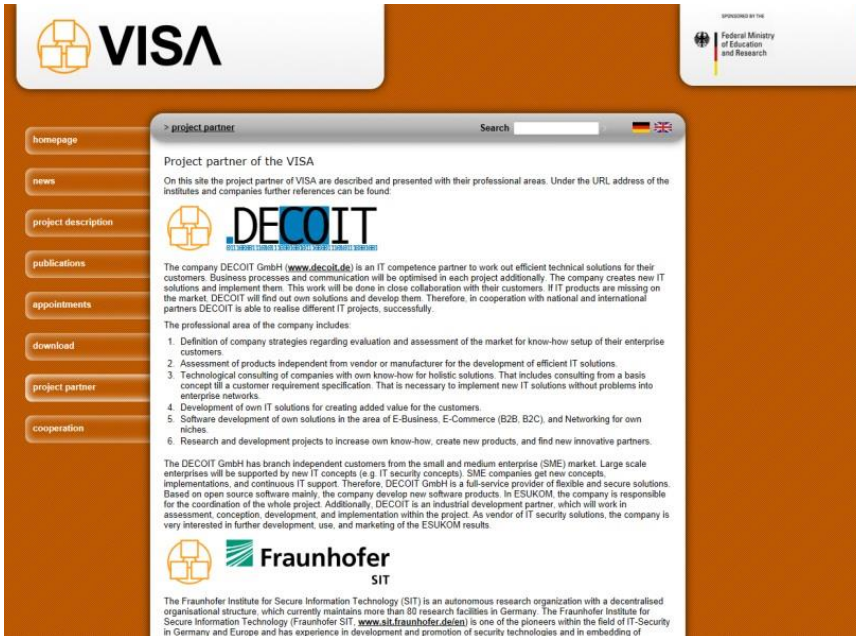


Ausgangslage

- 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
- Um diese Problematik zu lösen wurde das Forschungsprojekt *VISA (Virtual IT Security Architectures)* ins Leben gerufen



VISA-Projekt



VISA

project partner

Project partner of the VISA

On this site the project partner of VISA are described and presented with their professional areas. Under the URL address of the institutes and companies further references can be found.

DECOIT

The company DECOIT GmbH (www.decoit.de) is an IT competence partner to work out efficient technical solutions for their customers. Business processes and communication will be optimised in each project additionally. The company creates new IT solutions and implement them. This work will be done in close collaboration with their customers. If IT products are missing on the market DECOIT will find out own solutions and develop them. Therefore, in cooperation with national and international partners DECOIT is able to realise different IT projects, successfully.

The professional area of the company includes:

1. Definition of company strategies regarding evaluation and assessment of the market for know-how setup of their enterprise customers
2. Assessment of products independent from vendor or manufacturer for the development of efficient IT solutions.
3. Technological consulting of companies with own know-how for holistic solutions. That includes consulting from a basis concept till a customer requirement specification. That is necessary to implement new IT solutions without problems into enterprise networks.
4. Development of own IT solutions for creating added value for the customers.
5. Software development of own solutions in the area of E-Business, E-Commerce (B2B, B2C), and Networking for own niches.
6. Research and development projects to increase own know-how, create new products, and find new innovative partners.

The DECOIT GmbH has branch independent customers from the small and medium enterprise (SME) market. Large scale enterprises will be supported by new IT concepts (e.g. IT security concepts). SME companies get new concepts, implementations, and continuous IT support. Therefore, DECOIT GmbH is a full-service provider of flexible and secure solutions. Based on open source software mainly, the company develop new software products. In ESUKOM, the company is responsible for the coordination of the whole project. Additionally, DECOIT is an industrial development partner, which will work in assessment, conception, development, and implementation within the project. As vendor of IT security solutions, the company is very interested in further development, use, and marketing of the ESUKOM results.

Fraunhofer SIT

The Fraunhofer Institute for Secure Information Technology (SIT) is an autonomous research organization with a decentralised organisational structure which currently maintains more than 80 research facilities in Germany. The Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT, www.sit.fraunhofer.de/en) is one of the pioneers within the field of IT-Security in Germany and Europe and has experience in development and promotion of security technologies and in embedding of

www.visa-project.de

- Das VISA-Projekt ist ein nationales BMBF-Projekt
- Es startete am 01. August 2011 und wird im Juli 2013 enden
- Folgende Partner sind involviert:
 - DECOIT GmbH (Konsortialführer, Bremen)
 - Fraunhofer SIT (Darmstadt)
 - FH Dortmund (Dortmund)
 - Collax GmbH (Ismaning)
 - IT-Security@Work (Mainz)
 - NICTA (Sydney, Australien)
- Es gibt bereits Kooperationen mit anderen F&E-Projekten

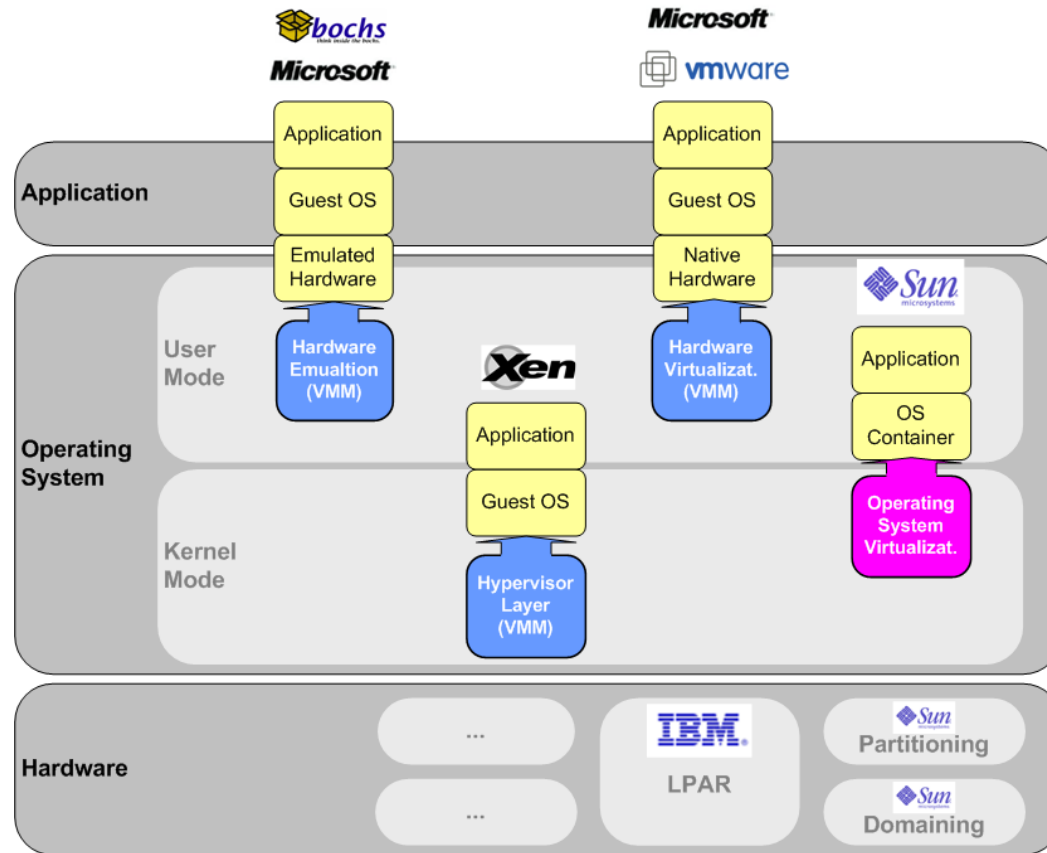


Ziele des VISA-Projektes

- VISA erstellt ein Framework, das das Erproben von VSAs in nachgebildeten, praxisorientierten Szenarien erlaubt. Hierfür sieht das Konsortium folgende technischen Herausforderungen bzw. Ziele:
 - Entwicklung und Paketierung verschiedener *VSA-Module*, die unterschiedliche Bereiche der IT-Sicherheit abdecken
 - Eine automatisierte und dynamische Umgebung, die eine experimentelle Erprobung verschiedener Netztopologien und den Einsatz von VSAs erlaubt
 - Modelle, die die Simulation der Netztopologien steuern
 - Jede VSA muss am Ende als virtuelles Image vorliegen und durch das Deployment-System entsprechend dem zugrunde liegenden Modell konfiguriert werden können
 - Es wird ein Modell bzw. Ausdruckssystem benötigt, um das Deployment zu steuern
 - Eine Bibliothek von virtuellen Images wird benötigt, um die möglichen Wirkszenarien zu bauen



Virtualisierungslösungen



- Das VISA-Projekt hat sich auf *KVM (OpenStack)* als Basis verständigt:
 - Einzige freie Lösung am Markt
 - Breite Unterstützung
 - Hohe Performance (Hardware-basiert)
 - Fester Bestandteil des Linux-Kernels
 - Keine Lizenzkosten (GNU GPL)



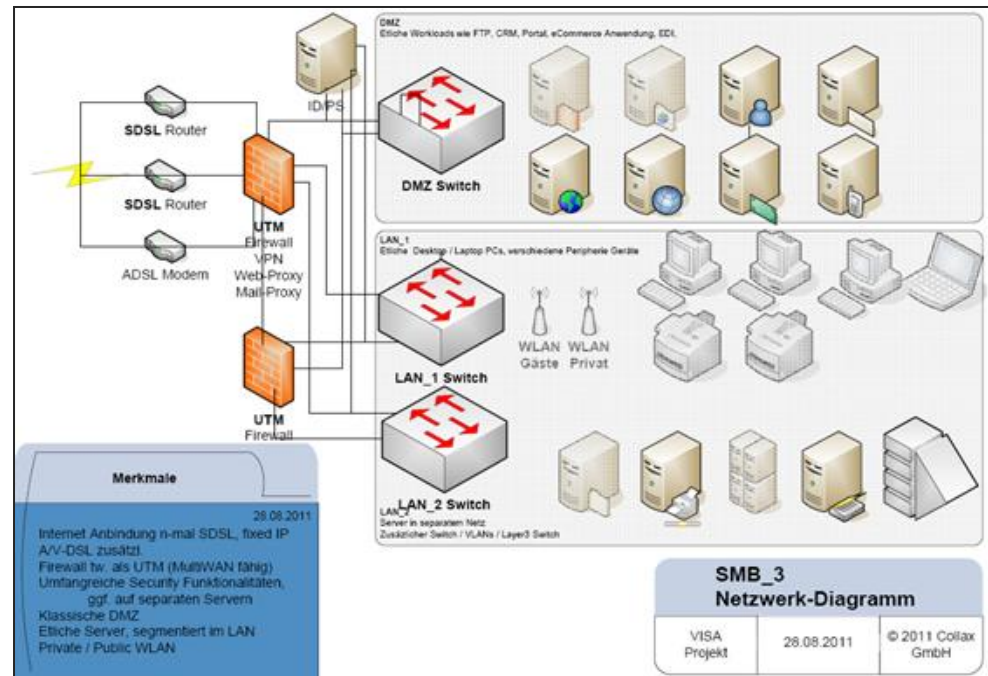
Definition einer Virtual Security Appliance (VSA)

- **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



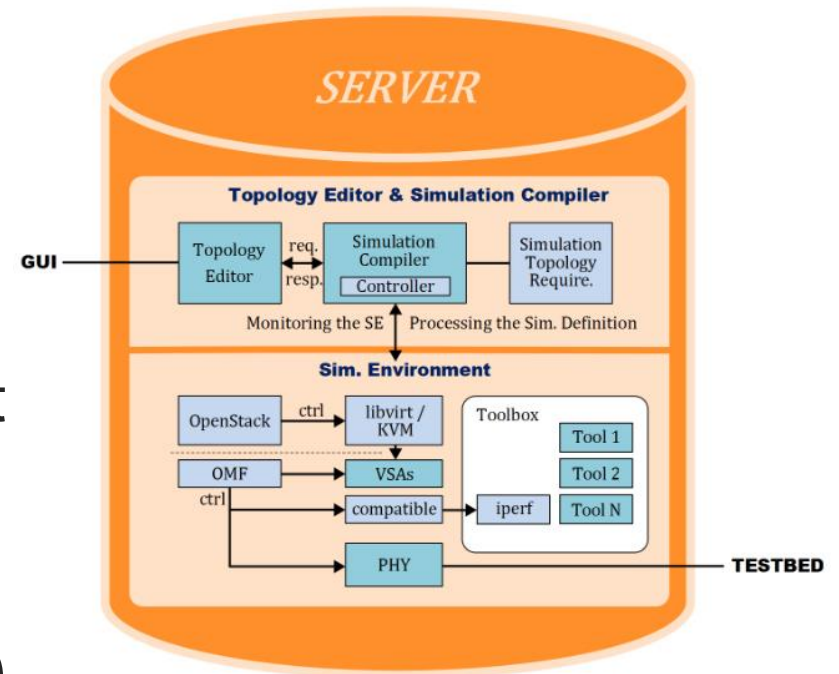
Was soll abgebildet werden mit einer VSA?

- Die IT-Infrastruktur eines KMU
 - DMZ
 - Firewall
 - IDS
 - Switches
 - Remote-Zugänge
 - E-Mail-Server
 - FTP-Server
- Dazu wurden verschiedene KMU-Szenarien untersucht und beschrieben
- IT-Sicherheitsniveau und Verbesserungen durch die VSA wurden ebenfalls untersucht u. beschrieben



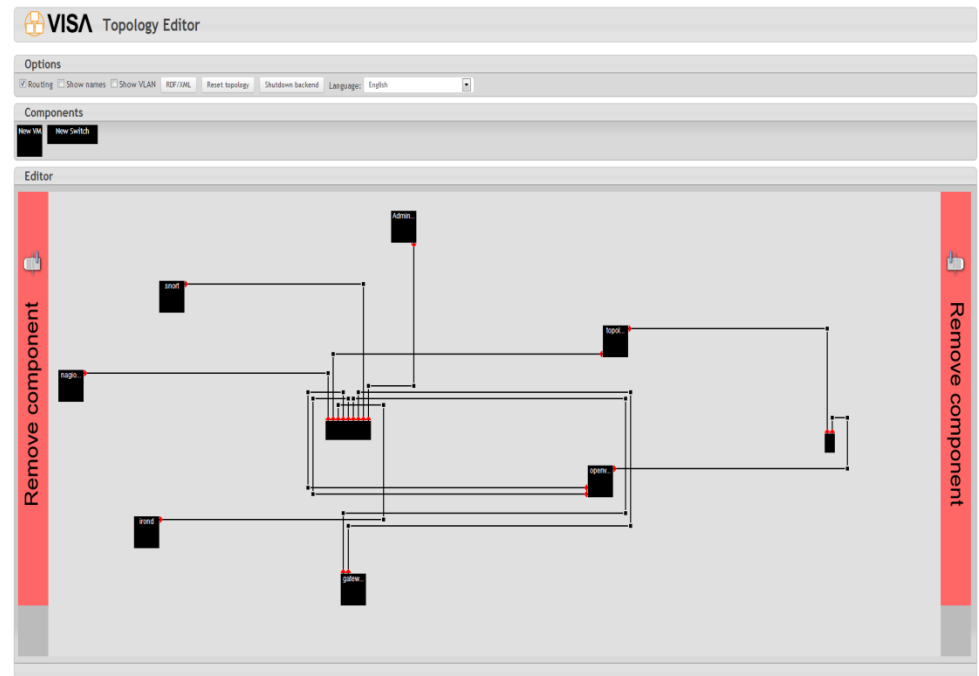
VISA-Architektur

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



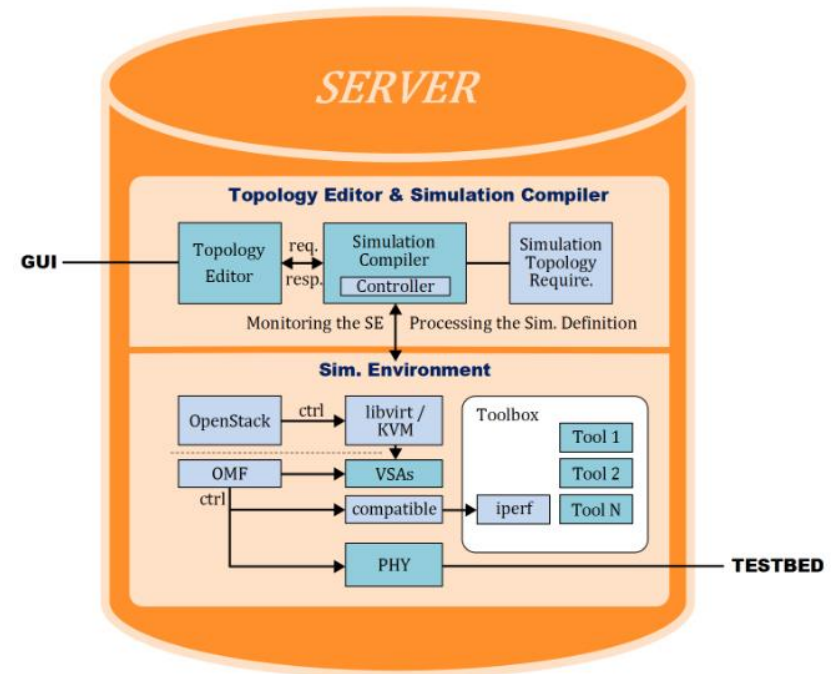
Topologie Editor (TE)

- Der *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 *SC*



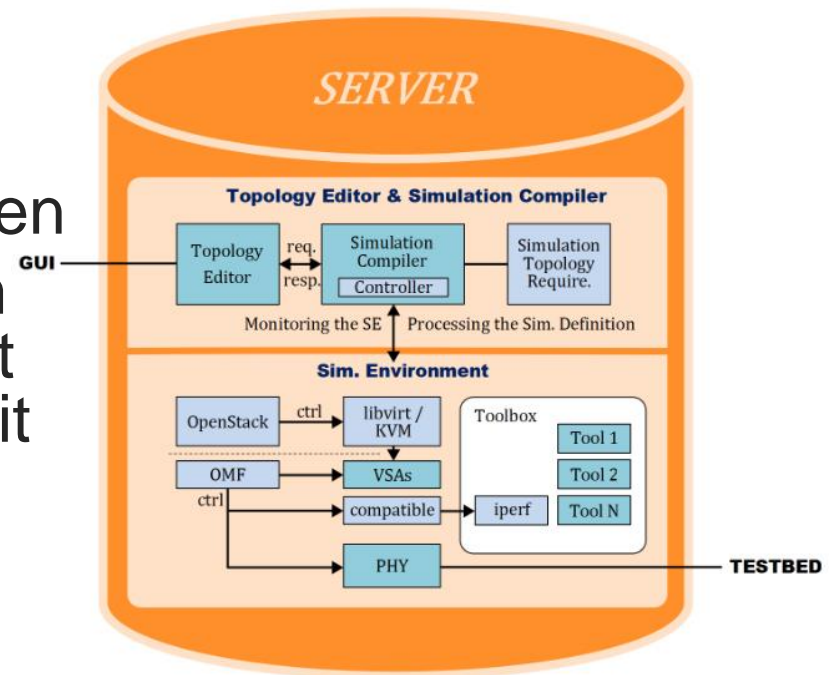
Simulation Compiler (SC)

- Der *Simulation Compiler (SC)* übersetzt die *TE-Parameter* in die Simulationsdefinition
- Die Simulationsdefinition beinhaltet
 - Ausführen automatisierter Tests
 - Erstellen virtueller Images
- Eine bestehende Netztopologie kann erfasst werden
- Die Simulation wird durch das *OMF-Framework* realisiert
- *OMF* kann als Simulationsumgebung und -verteilung genutzt werden
- *OMF* beinhaltet verschiedene Netzanalysetools
- Es werden die Resultate vom *OMF Framework* grafisch dargestellt



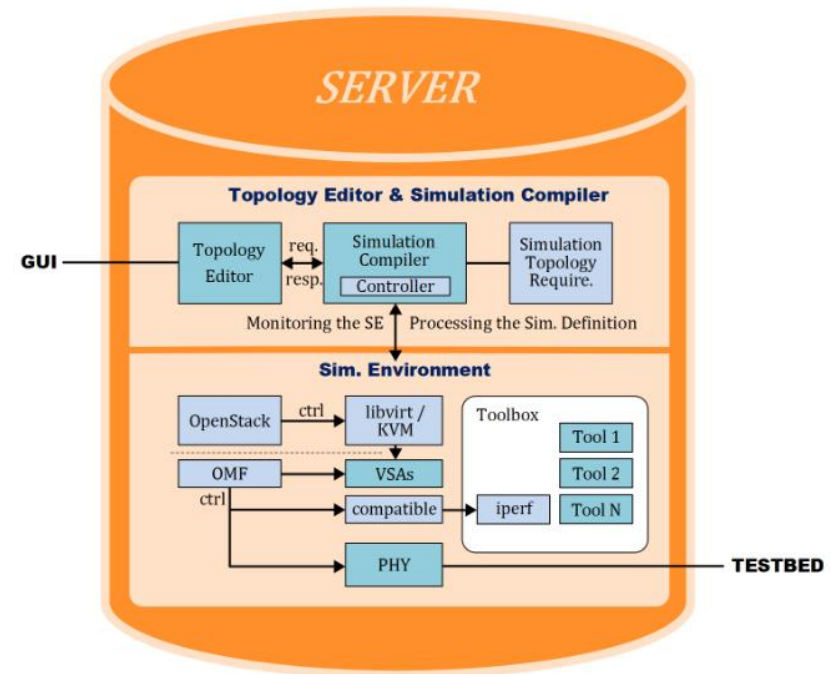
Simulation Environment (SE)

- Das *Simulation Environment (SE)* führt die OMF-kontrollierte Simulation aus
- Das *SE* ermöglicht die Definition beliebiger Szenarien
- Die Messungen können zum Test der Systemfunktionalität bezogen auf die IT-Sicherheit verwendet werden
- Die Simulation nutzt VM-Images auf Basis von OpenStack (KVM)
- Verschiedene Netzanalysetools sind im Einsatz (u.a. iperf, nmap)



Zusammenspiel zwischen TE, SC und SE

- Der *TE* ermöglicht die Definition von Modellen, die das reale Netz repräsentieren
- Durch den *TE* kann ein virtuelles IT-System, basierend auf Server, Clients und Netzwerk-komponenten 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

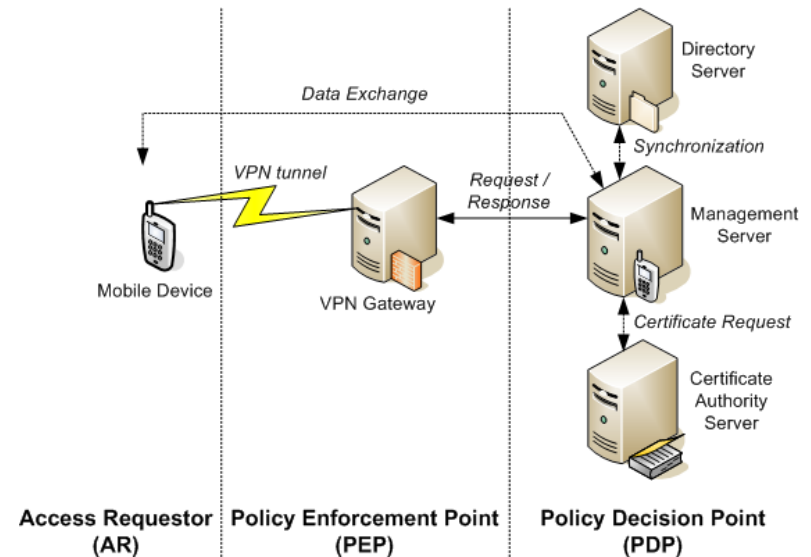


- Das VISA-Projekt hat verschiedene VSA-Bausteine definiert
- Zwei Beispiele sind:
 - **VSA-SRA**: ermöglicht Android-Endgeräten sicher auf verschiedene IT-Systeme zuzugreifen durch Trusted Computing (TC)
 - **VSA-MAC**: nutzt das IF-MAP-Protokoll der TCG, um Informationen verschiedener Sicherheitskomponenten zentral auszuwerten



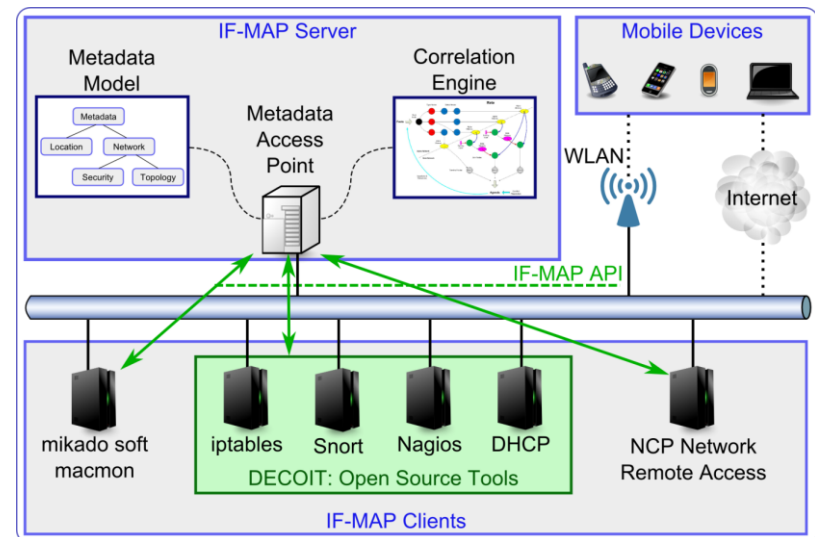
Beispiel: VSA „Secure Remote Access“ (1)

- 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
- TPM-Chip in den Smartphones wäre zur absolut sicheren Einwahl notwendig, um zusätzlich abzufragen:
 - Applikationsbasis
 - Versionsnummer
 - Sicherheitsrichtlinien



Beispiel: VSA „Metadata Access Control“ (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



Verbesserungsmöglichkeiten durch VSAs

- Die gesamte sicherheitsrelevante IT-Infrastruktur könnte durch VISA virtuell konzipiert und getestet werden
- Anschließend könnte man, nach erfolgreichen Tests, die Konfiguration oder die gesamte virtuelle Umgebung übernehmen
- Alle Dienste und Server könnten redundant ausgelegt werden, um eine 100%ige Verfügbarkeit zu erhalten
- Die komplette IT-Infrastruktur könnte komplett virtuell vorgehalten werden. Dadurch lassen sich auch Redundanzen (wie Firewall oder Router) einfacher aufbauen, um neben der IT-Sicherheit auch die Verfügbarkeit zu gewährleisten
- Durch die Flexibilisierung der Infrastruktur bei gleichzeitiger Komplexitätsreduktion bleibt für die IT-Mitarbeiter mehr Zeit, um sich dem Thema IT-Sicherheit pro-aktiv zuwenden zu können



Fazit

- 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
- VISA erhöht die IT-Sicherheit durch zwei Maßnahmen, nach erfolgreicher Simulation:
 - Übernahme der Konfiguration in die bestehende IT-Infrastruktur oder
 - Überführung der Simulation (virtuellen Umgebung) in das Produktivnetz





Vielen Dank

***Besuchen Sie uns auf der CeBIT:
DECOIT GmbH: Halle 6, Stand E16***



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.

Die in dieser Publikation enthaltenen Informationen stehen im Eigentum der folgenden Projektpartner des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „VISA“: DECOIT GmbH, Collax GmbH, IT-Security@Work GmbH, FH Dortmund, Fraunhofer SIT und NICTA. Für in diesem Dokument enthaltenen Information wird keine Garantie oder Gewährleistung dafür übernommen, dass die Informationen für einen bestimmten Zweck geeignet sind. Die genannten Projektpartner übernehmen keinerlei Haftung für Schäden jedweder Art, dies beinhaltet, ist jedoch nicht begrenzt auf direkte, indirekte, konkrete oder Folgeschäden, die aus dem Gebrauch dieser Materialien entstehen können und soweit dies nach anwendbarem Recht möglich ist.

