Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung

Prof. Dr. Kai-Oliver Detken[1] · Prof. Dr. Evren Eren[2] · Marion Steiner[3]

[1]DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen
detken@decoit.de

[2]Fachhochschule Dortmund, Emil-Figge-Str. 42, D-44227 Dortmund
evren.eren@fh-dortmund.de

[3]IT-Security@Work GmbH, Robert-Koch-Straße 41, D-55129 Mainz
marion.steiner@isw-online.de

Zusammenfassung

IT-Infrastrukturen können mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) komplex werden. Neben verschiedenen Typen von Rechnern, Peripherie und funktionalen Netzwerkkomponenten wächst die Komplexität durch unterschiedliche Sicherheitskomponenten an verschiedenen Punkten im Netzwerk. Die Auswirkungen von Änderungen an solchen Infrastrukturen sind oft erst im Echtbetrieb zu erkennen und der Einsatz neuer Sicherheitskomponenten erfordert oft die Integration neuer Hardware und den Umbau der Netztopologie. Darüber hinaus ist das Absichern von Einzelkomponenten, insbesondere im Verbund mit anderen Komponenten, für die Integration in der Unternehmenstopologie nach BSI IT-Grundschutz sowie ISO 27001, nach denen ein ISMS (Informations-Sicherheits-Management-System) aufgebaut und betrieben werden kann, kein einfaches Unterfangen. Da immer mehr KMU ein profundes IT-Risikomanagement vorweisen müssen, muss nachweisbar sein, dass die IT-Infrastruktur über ausreichende Schutzmechanismen verfügt. Vor diesem Hintergrund muss für KMU der Umgang mit IT-Infrastrukturen vereinfacht werden, da diese wenig Personalressourcen und Know-how für das operative IT-Management vorhalten können. Um eine höhere Autonomie in der Konfiguration sowie im Betrieb ihrer IT-Infrastruktur zu erhalten, sind modulare, erprobte Lösungen und Systeme essentiell. Mittlerweile kann und wird die höhere Flexibilität durch Virtualisierung von Rechnern und Diensten erreicht. Jedoch existieren keine Lösungen, die auch Teile oder ganze Netztopologien und Infrastrukturen für Unternehmen virtualisiert abbilden. Dies will das vom BMBF geförderte Forschungsprojekt VISA ändern.

1 Einleitung

Die Virtualisierung von Betriebssystemen hat sich etabliert und hat den wesentlichen Vorteil, dass prototypische Implementierungen und Tests von Soft- und Hardware viel schneller und kostengünstiger realisiert werden können. Dies beinhaltet ebenfalls die Kontrolle und Überwachung einzelner Komponenten, wie auch eine dynamische Veränderung der Netzwerktopo-

P. Schartner · J. Taeger (Hrsg.) · DACH Security 2012 · syssec (2012) pp-pp.

logie im laufenden Betrieb. Darüber hinaus ermöglichen Virtualisierungstools wie VMWare, Xen Source und KVM (Kernel Based Virtual Machine) die Simulation/Emulation von IT-Komponenten und sogar komplexen IT-Infrastrukturen (Subnetze, Router, Switches, Firewalls, DMZ etc.). Mittlerweile ist sogar die Emulation von Kabeln beispielsweise mittels VDE (Virtual Distributed Ethernet) und OpenVSwitch möglich [EREN10]. Diese Technologien und Lösungen lassen sich im Prinzip zur Konzeption und Provisionierung von IT-Sicherheitsarchitekturen und Infrastrukturen nutzen, denn einzelne virtualisierte Sicherheitskomponenten wie Firewalls, Authentisierungsserver, Intrusion Detection/Prevention etc. könnten mittels KVM, VDE und OpenVSwitch flexibel und modular zu komplexen und autarken Systemen zusammengefasst werden.

Damit können nicht nur sog. Virtual Security Appliances (VSA) erstellt, sondern auch die gesamte IT-Infrastruktur eines Unternehmens abgebildet werden, in der dann sehr flexibel und realitätsnah gearbeitet, getestet und optimiert werden kann. Dies war bislang nicht möglich, da bislang nur Virtual Appliances (VA) bzw. Virtual Machines (VM) existieren, die punktuell spezifische Anwendungen oder Dienste bereitstellen. Eine Kombination von verschiedenen Sicherheitsfunktionen und Diensten wird hierbei jedoch nicht angeboten.

2 Virtualisierungstechniken

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.

Die im Kontext wichtigste Technik ist die *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. Der Gast wird aus Sicht des Basis-Betriebssystems (Host oder Wirt) von der Hardware abgekoppelt und kann somit wie ein Softwareobjekt flexibel und unabhängig von der darunterliegenden Hardware behandelt werden. Produkte zur Server-Virtualisierung sind primär auf Skalierbarkeit, Geschwindigkeit und Flexibilität ausgelegt. Die meisten Serversysteme kommen ohne graphische Desktopumgebungen aus und werden meist über Systemkonsolen administriert. Die Virtualisierungskomponente übernimmt die Aufgabe, die Ressourcen des Hostsystems in einzelne VMs aufzuteilen, so dass diese nicht das Gesamtsystem, sondern nur einen Ausschnitt als ihre eigene Umgebung wahrnehmen. Sie stellt weiterhin sicher, dass die virtuellen Maschinen voneinander isoliert und unabhängig auf dem Hostsystem laufen.

Das Verfahren der *Hardware-basierten Virtualisierung* kombiniert Techniken der Voll- und Para-Virtualisierung, wobei die Virtualisierungsfunktionalität in die Prozessorhardware integriert wird. Man bezeichnet es auch als Hardware Virtual Machine (HVM) und native Virtualisierung. Ziel der Hardware-basierten Virtualisierung ist es, die Vorteile der Vollvirtualisierung zu erreichen und gleichzeitig deren Performance-Nachteile zu eliminieren. Durch die immer stärkere Verbreitung der x86-Architektur in den vergangenen zwanzig Jahren, traten die Schwächen in Bezug auf Virtualisierbarkeit in den Vordergrund. Der allgemeine Trend

zur Virtualisierung brachte die Hardwarehersteller dazu, ihre neuen x86-Prozessoren um Virtualisierungsfunktionen zu erweitern. Die Grundfunktionalität dieser Erweiterungen besteht darin, zu erkennen, wann kritische Operationen von virtuellen Maschinen ausgeführt werden und diese gesondert zu behandeln. Diese modernen Prozessoren unterstützen die Interaktion zwischen den virtuellen Maschinen und dem *Hypervisor*. Die ersten Prozessoren mit Virtualisierungserweiterungen kamen im Jahr 2005 auf den Markt (Intel VT, AMD-V). Die Implementierungsansätze sind prinzipiell ähnlich, doch sie sind nicht zueinander kompatibel. Virtualisierungssoftware muss eine getrennte Unterstützung sowohl für Intel VT als auch für AMD-V anbieten [HIRS06].

Das Verfahren der Hardware-basierten Virtualisierung unterscheidet sich prinzipiell nicht von dem der *Vollvirtualisierung*. 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 [DETK11].

Der *Hypervisor* ist nach wie vor für die Verwaltung und Kontrolle der virtuellen Maschinen zuständig, verhält sich aber im Gegensatz zur Vollvirtualisierung rein passiv. Durch die neuen zur Verfügung stehenden Befehlssätze können privilegierte Instruktionen regulär und somit sicher ablaufen. Ein Kontextwechsel zum Hypervisor ist nicht jedes Mal notwendig. Der Virtualisierungsprozess wird nicht gestört und der Virtualisierungsoverhead wird sehr stark reduziert. Bei dem Verfahren der hardware-basierten Virtualisierung laufen virtuelle Maschinen auf Grund der erwähnten Vorteile des Verfahrens äußerst leistungsstark [FISC09].

3 Ist-Zustand in KMU

An dieser Stelle soll einmal am Beispiel eines mittelständischen Unternehmens die Komplexität eines Netzes als Diskussionsbasis dargestellt werden. IT-Infrastrukturen in dieser Umgebung können bereits durchaus komplex werden. In der Regel sind, neben einem größeren Netzwerk, welches ebenfalls meistens auf Ethernet und Wireless LAN (WLAN) basiert, diverse Server und Clients im Einsatz. In Einzelfällen ist es trotzdem möglich, dass es keine zentrale Datenspeicherung gibt und damit auch das entsprechende Backup fehlt. Eine UTM-Appliance (Unified Threat Management) ist als Firewall die Regel, ein reiner Proxy-Server eher die Ausnahme. Auf der Appliance werden verschiedene Sicherheitsanwendungen parallel genutzt. In seltenen Fällen wird eine zweite UTM-Appliance vorgehalten, die eine Redundanz oder Load Balancing anbietet. Das WLAN-Netz ist relativ einfach abgesichert und meistens nicht zentral zu verwalten (kein WLAN-Controller). Ein Sicherheitskonzept besteht in den meisten Fällen nicht, da das grundsätzliche Funktionieren der IT einen höheren Stellenwert einnimmt. Das Ethernet-Netzwerk ist ohne Zusatzfunktionen ausgestattet. Obwohl die Switches Monitoring-fähig sind, ist kein Überwachungssystem im Einsatz.

Bei etwas fortgeschrittenen Anwendern sind grundlegende Sicherheitskonzepte vorhanden. Beispielsweise findet man eine Anordnung von zwei Firewalls oder UTM nach BSI-Grundschutz zur Abschottung verschiedener Netzwerksegmente und zum Routing des Netzwerkverkehrs auf wohl definierten und unter Sicherheitsaspekten optimierten Wegen. In der DMZ werden verschiedene Dienste angeboten. E-Mails werden nicht mehr direkt vom Webserver des Providers bezogen, sondern durch den internen eigenen E-Mail- oder Groupware-

Server abgerufen. Intern sind Verzeichnisdienst- und Applikations-Server (wie etwa ERP oder Dokumenten-Management-Systeme) im Einsatz. Weiterhin gibt es eine Vielzahl von Druckern, die mit dem Netzwerk verbunden sind.

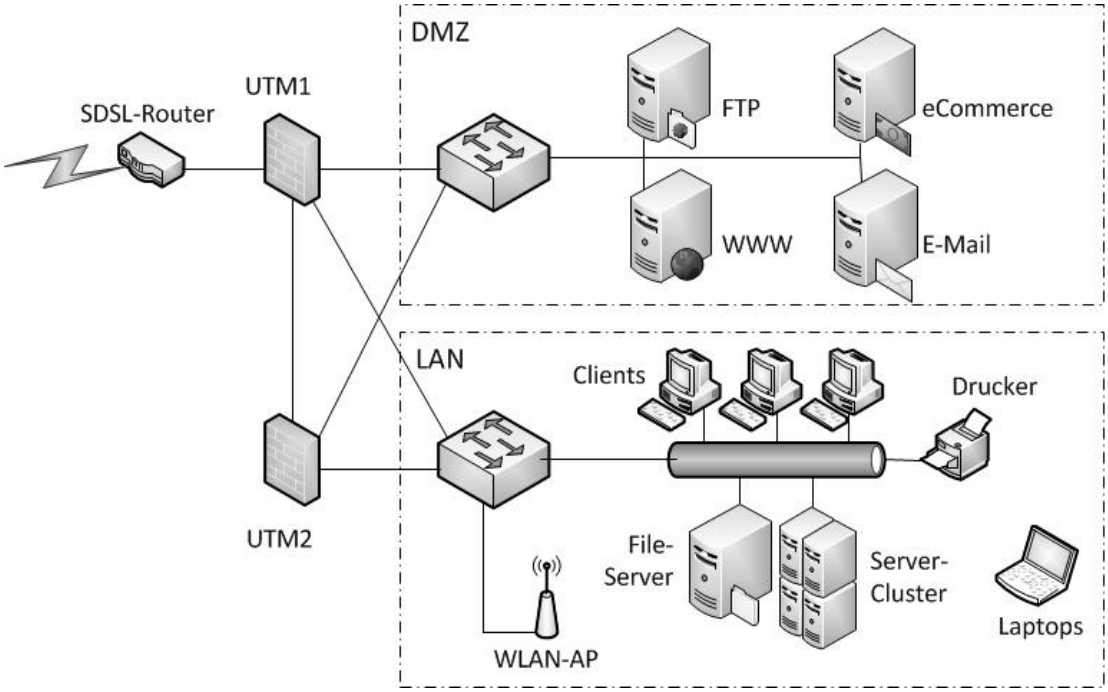

Abb. 1: IT-Infrastrukturbeispiel eines mittelständischen Unternehmens

In gehobenen Mittelstandsszenarien wird die Hardware bereits als Cluster mit einer NAS[1]- oder SAN[2]-Anbindung oder ohne Storage-Lösung umgesetzt. Die Virtuellen Maschinen (VM) können dabei redundant installiert werden. Während im NAS-Konzept die Redundanz nur durch Neustart des Service auf einem anderen VM-Server stattfindet, was auch den Verlust von Daten und Konfigurationen nach sich ziehen kann, ist beim SAN-Konzept ein Umziehen der VMs im Echtbetrieb möglich. Es werden auf logischer Ebene mehrere Server als VMs eingesetzt. Diese werden auch für den Produktivbetrieb genutzt und nicht nur zu Testzwecken.

Bei den mittelständischen Betrieben ist bereits eine kleine IT-Mannschaft im Einsatz, die sich mit allen anfallenden Arbeiten beschäftigt, die im Tagesgeschäft relevant werden könnten. Die Themenspanne reicht hier von Client-Installationen bis zu Netzwerk-Konfigurationen, Serversysteminstallation und -konfiguration, Telefonanlage bis hin zum Support diverser eingesetzter IT-Anwendungen wie z.B. ERP-/FiBu-Systeme. Dafür ist ein rudimentäres Fachwissen vorhanden, was selten in die Tiefe geht und auch nicht ausgebaut wird, da IT-Mitarbeiter im Unternehmen relativ abgeschottet arbeiten. Dadurch werden neue Markttrends nicht erkannt oder verpasst. Aus diesem Grund sind auch Überforderungen vorprogrammiert, wenn z.B. die Geschäftsleitung die Anbindung neuer Smartphones schnellstens fordert, weil diese in anderen Unternehmen bereits erfolgreich eingesetzt werden. Aufgefangen wird dies meistens durch externe IT-Dienstleister, die ggf. auch Projekte in Eigenverantwortung umsetzen.

[1] Network Attached Storage: Speicherlösungen für kleinere und mittlere Umgebungen

[2] Storage Area Network: Speicherlösung mit hoher Performance für mittlere und große Umgebungen

Die IT-Sicherheit kommt in den KMU-Szenarien zu kurz oder wird nur rudimentär behandelt, da auch hier meist kein ausreichendes Know-how besteht und zusätzlich die IT-Mannschaft hierfür keine Ressourcen besitzt. Auch ein IT-Sicherheitsbeauftragter ist meist nicht bestellt oder aber er hat wenig Einfluss auf die konkreten Konfigurationen. Dies wäre aber aus Know-how-Gründen bereits schwierig, da dieser mehr auf konzeptioneller Basis arbeitet. Es wird gerne auf diverse Default-Einstellungen der Hersteller zurückgegriffen (inkl. Beispielpasswörter), um entsprechende Zeit im Tagesgeschäft zu gewinnen. Meistens bleiben die konfigurierten Provisorien nach der Einführung bestehen und werden nicht mehr verändert. WLANs werden oftmals unzureichend abgesichert eingesetzt. Subnetze mit ACLs und VLANs lassen sich zwar zur zusätzlichen Sicherheit auf Netzwerkebene einrichten, sind aber oftmals nicht im Einsatz. Oftmals nimmt die IT-Infrastruktur auch nur eine Nebenrolle ein, so dass auch das entsprechende Budget für Anschaffungen fehlt.

Neben dem fehlenden Bewusstsein für die IT-Sicherheit werden oft auch Compliance-Anforderungen, also die Berücksichtigung gesetzlicher Vorgaben, nicht betrachtet. Sie sind entweder gar nicht bekannt, es gibt keine klaren Richtlinien zur Umsetzung oder sie werden nicht ernst genommen. Dies liegt daran, weil Betriebswünsche nicht hinterfragt bzw. gegen andere Interessen und Anforderungen abgewogen oder die Vorgaben als nicht umsetzbar und behindernd eingestuft werden. Typische Beispiele hierfür sind neben ungeeignet vergebenen Systemberechtigungen beispielsweise auch System- oder Anwendungsprotokolle, die häufig den Datenschutz-Anforderungen widersprechen, das Testen mit Echtdaten oder sogar auf Produktivsystemen, weil keine geeignete Testlandschaft existiert.

Die Umsetzung von Standards hilft IT-Sicherheits- und Compliance-Vorgaben zu erfüllen und Diskussionen um die Angemessenheit einer Umsetzung zu reduzieren. Fehlende Standards führen daher zu Risiken im Unternehmen. Durch diese Risiken können Imageverluste entstehen, es drohen empfindliche Geldstrafen oder sogar der Wegfall der Geschäftsgrundlage. Ursache sind häufig verschiedene IT-Sicherheitsrisiken, durch die das Unternehmen auch auf der IT-Ebene relativ einfach verwundbar ist.

Dabei ist ein Rückgriff auf bewährte Vorgehensweisen aus IT-Sicherheitsstandards sinnvoll. Standards helfen dabei nicht nur, die sicherheitsrelevanten Prozesse zu erkennen und einzuführen, sondern auch die Sicherheitsaspekte in den „normalen“ IT-Prozessen zu berücksichtigen, und sie zum Vorteil des Unternehmens und des Kunden zu bringen. Sie helfen bei der Entwicklung auf Management-Ebene bis hin zur technischen Implementierung durch die Bereitstellung von Methoden und Maßnahmen. Dabei werden Abläufe und Prozesse des Unternehmens transparent und damit das Gesamtrisiko reduziert.

Wesentliche Ziele beim Einsatz von IT-Standards sind unter anderem:

a. **Kostensenkung:** durch Nutzung bewährter Vorgehensmodelle, methodische Vereinheitlichung und Nachvollziehbarkeit.

b. **Wettbewerbsvorteile:** Nachweisbare Sicherheit durch Zertifizierungen und Verbesserung des Unternehmensimage.

c. **Angemessenes Sicherheitsniveau:** Orientierung am Stand der Technik, Aktualität sowie ständige Verbesserung des Sicherheitsniveaus bei Beachtung des Gleichgewichts zwischen Kosten und Nutzen.

Das im Folgenden beschriebene VISA-Projekt hat das Ziel, IT-Infrastrukturen zu vereinfachen und flexibler zu gestalten, unter Berücksichtigung der Compliance-Anforderungen.

4 Das VISA-Projekt

Durch die starke Heterogenität von IT-Infrastrukturen, der relativ begrenzten Ressourcen sowie relativ geringem Know-how muss in Zukunft die Zielgruppe KMU bessere und geeignete Methoden zur flexiblen Konfektionierung, Erprobung und Optimierung ihrer IT-Infrastrukturen bekommen. Dies ist insbesondere für die IT-Sicherheit wichtig. Der Markt für Virtualisierung und IT-Sicherheit adressiert jedoch diese Zielgruppe bis dato zu wenig, so dass meistens keine bedarfsgerechten und dem Budget angepassten Lösungen vorhanden sind. Um eine höhere Autonomie in der Konfiguration sowie im Betrieb ihrer IT-Infrastruktur zu erhalten, sind modulare und erprobte Lösungen und Systeme essentiell. Dies will das VISA-Projekt (http://www.visa-project.de) durch die Entwicklung von sog. Virtual Security Appliances (VSA) sowie Methoden und Tools zur Netzmodellierung und -simulation adressieren.

Nicht nur vor dem Hintergrund der Flexibilität, sondern auch aus Kostengründen (Investition in Hard- und Software) sind VSA auf Basis von Open-Source-Bausteinen (sowohl die Anwendungen als auch die Betriebssysteme) von Bedeutung. Außerdem würde der Einsatz in Unternehmen kein größeres Know-how erfordern, da erprobte State-of-the-Art-Technologien als integrierbare Lösung in die Unternehmens-IT eingebunden werden können. Diese können ein anerkanntes Maß an Sicherheitsmaßnahmen und Standard-Compliance-Anforderungen bereits automatisch umsetzen. Ein weiterer essentieller Aspekt ist die bessere Nachweisbarkeit der Erfüllung von Anforderungen im Sinne von Compliance. Der Aufwand zur Überprüfung von Sicherheitskomponenten bzw. der gesamten IT-Sicherheitsinfrastruktur wird erheblich reduziert, da eine angemessene Dokumentation der Systeme, Security Assessments und Compliance-Tests für VSAs bereits vorliegen können. Trotz steigender Komplexität wird die Überprüfung der Konformität vereinfacht.

Es ist daher das Ziel des Projektes VISA, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen, insbesondere der Sicherheitskomponenten, zu erleichtern und zu unterstützen. Diese Unterstützung basiert auf drei Kernmerkmalen:

a. Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen
b. Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA)
c. Vereinfachung und Nachweisbarkeit der Einhaltung von IT-Standards, IT-Security- und Compliance Anforderungen durch geeignet entwickelte VSAs als fertig verwendbare IT-Bausteine.

Durch das VISA-Rahmenwerk wird der passgenaue und vereinfachte Einsatz von Sicherheitsanwendungen auf Basis von VSAs ermöglicht. Durch die umfassende Emulation der IT-Infrastrukturen können die betriebsrelevanten Parameter und die Integrationspunkte der VSA bereits in der virtuellen Umgebung identifiziert und der Einsatz erprobt werden.

Dadurch ergibt sich ein deutliches Verbesserungspotenzial, um eine hochverfügbare und sichere IT-Infrastruktur für KMU zu schaffen:

1. Die Infrastruktur kann logisch entzerrt werden, und Anwendungen dort im Netzwerk betrieben werden, wo es aus Security-Sicht angemessen ist.
2. Die gesamte Infrastruktur (Server, Firewall, Router, VPN etc.) wird virtuell konzipiert und kann nach erfolgreichen Tests als Live-System direkt übernommen werden. Der

Vorteil liegt in diesem Szenario darin, dass logisch eine komplette Infrastruktur vorgehalten wird.

3. Die Virtualisierung kann gleichzeitig zur Hardware-Konsolidierung genutzt werden, und dadurch einen wesentlichen Beitrag zur Kostenreduktion leisten (Hardware-Bedarf, Strom- und Kühlkosten). Durch die Konsolidierung (Hardware im Allgemein und Security) reduziert sich die Komplexität der gesamten IT-Landschaft nachhaltig, was zur Eingrenzung von Know-how-Bedarf, zur Erhöhung der IT-Sicherheit und ebenfalls zur Reduktion der Kosten beitragen würde.
4. 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.
5. Hiermit steigt auch die Möglichkeit für KMU, die bislang die Aufwände für Zertifizierungen oder ein nachweisbares Sicherheitsniveau nicht leisten konnten, dies zu tun, und sich damit neue Märkte zu erschließen.
6. Durch die Flexibilisierung der Infrastruktur bei gleichzeitiger Komplexitätsreduktion bleibt für die IT-Mitarbeiter mehr Zeit, um sich dem Thema IT-Sicherheit und geordnete Betriebsprozesse pro-aktiv zuwenden zu können.
7. Aufbau von Know-how als auch operativer Umsetzung können gezielt in den notwendigen Themenkomplexen erfolgen, die minimal notwendige Breite wird geringer und so sinkt die Gefahr, sich mit zu vielen Themen gleichzeitig zu beschäftigen.
8. 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. Notwendige Maßnahmen hierfür, wie z.B. die einfache Bereinigung des Systems von Echtdaten, können dabei durch ein geeignetes Konzept der VSA und der Bereitstellung von geeigneten Standardprozessen für ein solches Vorgehen, bereits berücksichtigt werden.
9. Die Standardbausteine können bereits ein geeignetes Maß an Dokumentation und Sicherheitsnachweisen mitbringen, so dass damit Anforderungen ohne großes eigenes Know-how und Aufwände im Unternehmen umgesetzt werden können. Das Unternehmen kann sich auf die Abweichungen vom Standard konzentrieren, bzw. die darüber hinausgehenden Themen. Das Sicherheitsniveau steigt und der Aufwand und das Know-how, um einen sicheren Betrieb aufzubauen, sind geringer
10. Neben dem Konzept für die VSAs kann eine Empfehlung für den Umgang mit der virtuellen Infrastruktur sowie Prozessempfehlungen für das Management der Landschaft gegeben werden. Damit können auch weite Teile der Anforderungen an Betriebsprozesse (z.B. Change-Management) abgedeckt werden.

Um diese Verbesserungspotentiale nutzen zu können, muss bei der Konzeption der Virtualisierungsumgebung und der VSAs auf weitere Rahmenparameter geachtet werden. So dürfen Sicherheitsmaßnahmen auf VSA-Ebene nicht durch die Virtualisierungsschicht hinfällig werden bzw. die Virtualisierungsschicht muss ebenso geeignete Maßnahmen bieten, die wiederum die Sicherheit und Nachvollziehbarkeit in der Landschaft durchgängig ermöglichen.

Ein anschauliches Beispiel hierzu ist z.B. die Nachvollziehbarkeit von Änderungen an Daten oder einem System: in der physischen Welt ist es in der Regel ausreichend, die Änderungen am System selber sowie ggf. noch Recovery-Maßnahmen zu protokollieren, um den Stand eines Systems für jeden Zeitpunkt rekonstruieren zu können. In einer virtuellen Landschaft kommt mit der Verwaltung der VSAs hier eine Schicht hinzu: denn neben den Änderungen (Changes) an der VSA ist ebenso relevant, ob VSA bzw. virtuelle Bausteine zwischenzeitlich ausgetauscht wurden und ggf. die für ein System geltende Change-History nicht für die Landschaft gilt, weil die Maschine teilweise nicht produktiv genutzt wurde.

Für die Nachweisbarkeit der Sicherheit und Compliance muss weiterhin die Übertragbarkeit von Security Assessments oder Tests sowie die übergreifende Effektivität der umgesetzten Maßnahmen in VSAs zwischen verschiedenen Einsatzszenarien sichergestellt werden, bzw. deren Möglichkeiten und Grenzen eindeutig dargelegt werden, um valide Aussagen treffen zu können. Sind diese Voraussetzungen erfüllt, können die durch geeignete Sicherheitsmaßnahmen gemäß existierender Standards gesicherten Infrastrukturbausteine, die virtuellen Systeme der VSAs, wie bisher physische Systeme abgesichert werden. Die Maßnahmenauswahl richtet sich dabei anhand der Funktion der jeweiligen Komponente aus.

5 Bisherige Ergebnisse

Bisher wurden im VISA-Projekt die für KMU identifizierten VSA konzeptioniert, die vorrangig der Sicherheit dienen (von Netzwerksicherheit, Layer 2 bis Anwendungssicherheit, Layer 7). Diese VSA 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 an dieser Stelle kurz vorgestellt, da sie innerhalb des Projektes bereits erarbeitet wurden bzw. den größten Fortschritt beinhalten:

1. **VSA-AAA:** Virtual Security Appliance – Authentication, Authorization, Accounting
2. **VSA-MAC:** Virtual Security Appliance – Metadata Access Control
3. **VSA-SRA:** Virtual Security Appliance – Secure Remote Access

Derzeit wird von dem Projektpartner FH Dortmund (www.fh-dortmund.de) die *VSA-AAA* realisiert, der eine CA/RA (Zertifikatsserver mit Online- bzw. Offline-RA), ein Linux-basierter Domain Controller mit LDAP sowie ein RADIUS-Server beinhaltet. Bei dieser VSA steht das Zusammenspiel von State-of-the-Art Authentisierungs- und Autorisierungs- sowie PKI-Komponenten auf Open-Source-Basis im Vordergrund. Die VSA-AAA soll somit die sichere Einwahl in ein Unternehmensnetz sowie Log-In in Domänen innerhalb des Unternehmensnetzes ermöglichen. Sie wird derzeit auf Basis der Open-Source-Lösung FreeIPA realisiert. FreeIPA ist eine integrierte Sicherheitslösung, was sich aus einem Linux-Grundsystem (Fedora), 389 (ehemals Fedora Directory Server), MIT Kerberos, NTP, DNS und Dogtag-Zertifikatsserver zusammensetzt und diese kombiniert. Zur Konfiguration bietet eine Webschnittstelle und Kommandozeilenbasierte Tools [FRIPA12].

Der Projektpartner DECOIT GmbH (www.decoit.de) arbeitet an den beiden anderen VSA. 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 vertrau-

enswürdig eingestuft werden kann, da nur die Teilnehmerdaten abgefragt werden. Dies wird erst durch das Senden gesammelter Metriken des Android-Smartphones vom TNC[3]-Client an den TNC-Server ermöglicht. Die Metriken enthalten die installierte Applikationsbasis, Versionsnummern und Richtlinien, die für das Smartphone gelten. 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 Quarantänenetz 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 [DDH11].

Die VSA-MAC besteht hingegen aus den Komponenten IF-MAP[4]-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. 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 unter anderem die Blockierung des Datenstroms durch eine Firewall, Sperrung des Zugriffes auf das Unternehmensnetz in Form eines Switches oder eines VPN-Gateways, Isolierung des Endgerätes in eine Quarantänezone etc. Abschließend können auf Grundlage der gesammelten Informationen die unterbundenen Aktivitäten sowie deren Details protokolliert und entsprechende Meldungen an die verantwortlichen Systemadministratoren generiert werden [DDB11].

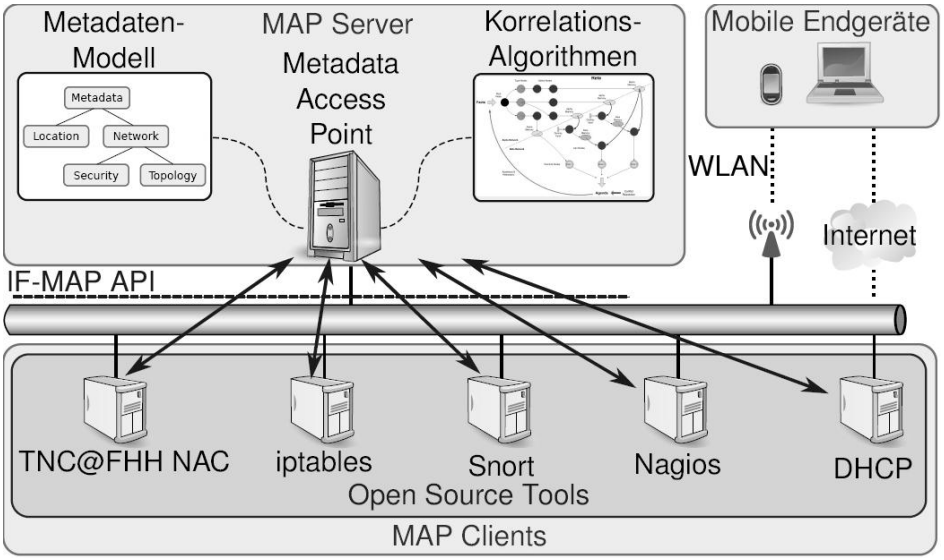

Abb. 2: IF-MAP-Architektur der VSA-MAC [DDB11]

[3] TNC = Trusted Network Connect (Spezifikation der Trusted Computing Group)

[4] IF-MAP = Interface for Metadata Access Point (Spezifikation der Trusted Computing Group)

Als essentieller Bestandteil einer Sicherheits-IT von Unternehmen sollen diese Dienste in der VSA gebündelt werden, jedoch bedarfsweise modular zu- und abschaltbar sein. Derzeit werden noch unterschiedliche Front-Ends hierzu analysiert, die in Frage kommen könnten. Wichtig dabei ist, dass das Zusammenspiel dieser Komponenten funktioniert. Als Basis wird ein gehärtetes VSA-System (Hostsystem und Gastsysteme) eingesetzt.

Essentielle Eigenschaften, der im VISA-Projekt zu entwickelnden VSA, sind:

1. **Integrierbarkeit:** Eine VSA soll als autarke Einheit in bestehende IT-Infrastrukturen integrierbar sein. Die Grundlage für Topologien werden Empfehlungen des BSI sein.
2. **Steuerbarkeit:** Eine VSA soll steuerbar und monitorbar sein, beispielsweise durch Tools wie libvirt oder über eine GUI bzw. andere Schnittstellen wie REST erfolgen.
3. **Konfigurierbarbeit:** Die virtuellen Maschinen der VSA sollen konfigurierbar sein.
4. **Modularität:** VSAs müssen derart modular konzipiert und realisiert werden, dass eine hohe Verzahnung und Kombination dieser zur Erhöhung der Sicherheit bzw. der Flexibilität und Integrierbarkeit ermöglicht wird. Hierzu soll eine Bibliothek von möglichst leicht integrierbaren VMs aufgebaut werden, aus denen VSAs leicht und sicher nach dem Baukastenprinzip konfektioniert werden können.
5. **Vergleichbarkeit:** VSA müssen derart konzipiert und umgesetzt werden, dass hinsichtlich Performance, Verfügbarkeit und Sicherheit keine gravierenden Unterschiede zu physikalischen und konventionellen Infrastrukturkomponenten und Topologien bestehen, sondern dies vergleichbar ist.
6. **Sicherheit:** Die VSA selbst muss sicher sein. Diese wesentliche Anforderung betrifft sowohl die Sicherheit der VMs (Gastsysteme), als auch die des Hostsystems. Eine Härtung des Betriebssystems der VMs und des Hostsystems sowie die Trennung der VMs voneinander durch den Hypervisor oder durch virtuelle Switches mit Authentisierungs- und Autorisierungsfunktionen wie sie beispielsweise durch OpenVSwitch gegeben sind, spielen hierbei eine wichtige Rolle.
7. **Komplementarität:** Ziel ist, VMs mit unterschiedlichen und komplementären Funktionen innerhalb einer VSA zu kombinieren. Dies bedingt auch die Vernetzung der VSAs durch Virtuelle Switches, wie z.B. VDE (Virtual Distributed Environment) oder OpenVSwitch, wobei die letztere sehr viele weitere Funktionalitäten aufweist. Hier werden praktische Erkenntnisse zur Emulation/Virtualisierung von Layer-2 Komponenten einfließen.

Bei der Absicherung von VSAs (einzeln und im Verbund) wurden etablierte Standards zur Absicherung von Komponenten eingesetzt und angewandt. Da dies eine große Zahl von Standards umfasst, können diese an dieser Stelle nicht explizit aufgezählt werden. Sie lassen sich kategorisieren in Protokolle, Verfahren, Algorithmen und fertige Lösungen (kommerzielle und Open Source). Die Absicherung von komplexen VSA, die mehr als eine Funktion bzw. Komponente beinhalten, ist entsprechend aufwändiger. Nicht nur durch die Zahl, sondern auch durch die individuellen und spezifischen Besonderheiten und damit Verwundbarkeiten der Komponenten. Hier kommen etablierte Verfahren zum Tragen kommen, um die VSA zu schützen bzw. abzusichern. Einfachstes Beispiel ist eine Firewall-VSA, die eine spezielle Implementierung einer am Markt verfügbaren Firewall ist (z.B. iptables). Sie muss mindestens

den Sicherheitslevel dieser Implementierungen bzw. Distributionen abbilden und es dürfen keine Sicherheitslücken dazu kommen.

Um in konkreten Anwendungsszenarien effizient Test- und Produktivumgebungen mit VSAs aufbauen zu können, werden von der Virtualisierungsplattform verschiedene Eigenschaften verlangt. *VSA Templating* erlaubt für eine gegebene VSA ein „Muster" anzulegen, das dann mehrfach instanziiert werden kann. Dies ist immer dann sinnvoll, wenn in einem Szenario gleiche oder sehr ähnliche VSAs, die sich nur in Ihrer Konfiguration unterscheiden benötigt werden. *VSA Cloning* erlaubt eine gegebene VSA in ihrer Gesamtheit zu kopieren. Dies ist sinnvoll, um VSAs aus dem Testbetrieb in den Produktivbetrieb zu übernehmen.

Um VSAs auf mehr als einem Virtualisierungshost im Verbund betreiben zu können und dabei die Vorteile der Virtualisierungstechnologie zu bewahren, müssen Netzwerke über Hypervisor-Grenzen hinweg virtualisiert zur Verfügung stehen. Dabei stehen mehrere Design- und Implementierungsmöglichkeiten zur Auswahl (Bridge/Tun-Devices, VDE, OpenVSwitch), die im Projekt untersucht wurden. Aktuell wird der Schwerpunkt auf OpenVSwitch gelegt.

Um VSAs aus dem Testbetrieb in den Produktivbetrieb überführen zu können, wird von der Virtualisierungsplattform *Storage Migration* verlangt. Dies erlaubt einen virtuellen Server in seiner Gesamtheit, also persistente Daten der VSA sowie ihre Laufzeitkonfiguration von einem Virtualisierungsserver (Hypervisor) in der Testumgebung auf einen anderen Virtualisierungshost in der Produktivumgebung zu verschieben. Um hier größtmögliche Offenheit und Flexibilität zu gewährleisten wird zusätzlich die Import- und Exportmöglichkeit für OVF/OVA-Dateien angestrebt, das einen de-facto Standard für den Austausch von virtuellen Servern zwischen verschiedenen Virtualisierungsplattformen darstellt.

Die entwickelten VSAs werden innerhalb des Projektes einzeln und im Verbund anhand verschiedener Parameter evaluiert und durch methodisch fundierte *Security Assessments* nach Sicherheitsstandards (z.B. BSI) bewertet werden. Ebenso sind, wenn die VSAs im Verbund genutzt werden sollen, auch die Management-Verfahren des Virtualisierungsrahmenwerks zu betrachten, z.B. Change-Prozesse der VSAs, Deployment-Methoden und die Verwaltung des Frameworks selber. Das Ziel ist es hierbei, die IT-Konzepte auf Sicherheitsstandards wie ISO 27001 und BSI-Grundschutz überprüfen zu können, ohne dass entsprechendes Wissen bei dem KMU vorgehalten werden muss. Diese Standards werden für Zertifizierungen bzw. zur zertifizierten IT-Sicherheit angewandt. Diese auf Standards und Vorgehensmodelle geprüften VSAs erlauben insbesondere KMU, ein definiertes Sicherheitsniveau mit angemessenem Aufwand und geringen Kosten zu erreichen, indem sie als geprüften Elemente oder Verbünde dann direkt verwendet werden können. Auf technischer Ebene werden die nötigen Sicherheitsvorgaben damit bereits weitestgehend eingehalten.

6 Fazit

Die Virtualisierungstechniken schreiten immer weiter voran und ermöglichen heute nicht nur mehr den reinen Parallelbetrieb unterschiedlicher Betriebssysteme auf einer Hardware. Längst hat die Virtualisierung auch die Produktivumgebung erreicht, da die Server-Hardware-Systeme immer leistungsstärker und ausfallsicherer werden. 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.

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, wie hier aufgezeigt wurde. Nach der erfolgreichen Simulation können dann zwei Möglichkeiten ausgewählt werden: Übernahme der Konfiguration in die bestehende IT-Infrastruktur oder Überführung der Simulation in das Produktivnetz.

Beide Szenarien werden im VISA-Projekt entwickelt, untersucht und bewertet. Wenn alle Ziele des Projektes umgesetzt werden können, wird es in Zukunft in jedem Fall einfacher werden Server, Clients und ganze Netze zu virtualisieren und sicher in die Unternehmensstruktur einzubetten [DETK11].

7 Danksagung

Das VISA-Projekt ist ein gefördertes BMBF-Projekt mit einer Laufzeit von zwei Jahren, das im August 2011 seine Arbeiten begonnen hat. An dem Projekt sind die Firmen DECOIT GmbH (Projektleitung), Collax GmbH, IT-Security@Work GmbH sowie die deutschen Forschungseinrichtungen Fraunhofer SIT und Fachhochschule Dortmund beteiligt. Zusätzlich ist der australische Partner NICTA (National ICT Australia) mit im Konsortium vertreten.

8 Literaturverzeichnis

[DDB11] Detken, Dunekacke, Bente: *Konsolidierung von Metadaten zur Erhöhung der Unternehmenssicherheit*. D.A.CH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Herausgeber: Peter Schartner, syssec Verlag, ISBN 978-3-00-027488-6, Oldenburg 2011

[DDH11] Detken, Diederich, Heuser: *Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC*. D.A.CH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Herausgeber: Peter Schartner, syssec Verlag, ISBN 978-3-00-027488-6, Oldenburg 2011

[DETK11] Detken, Kai-Oliver: *Virtualisierung ganzer Netze – Überprüfung der eigenen Infrastruktur*. NET 12/11, ISSN 0947–4765, NET Verlagsservice GmbH, Woltersdorf 2011

[EREN10] Eren, Evren: *Scheinwelten – Mit Virtualisierungssoftware ganze Infrastrukturen abbilden*. NET 09/10, ISSN 0947–4765, NET Verlagsservice GmbH, Woltersdorf 2011

[FISC09] Fischer, M.: *Xen – Das umfassende Handbuch*. Galileo Press, 2009

[FRIPA12] Open-Source-Projekt-Webseite: http://freeipa.org/page/Main_Page

[HIRS06] Hirschbach, D.: *Vergleich von Virtualisierungstechnologien*. Diplomarbeit an der Universität Trier. Trier 2006