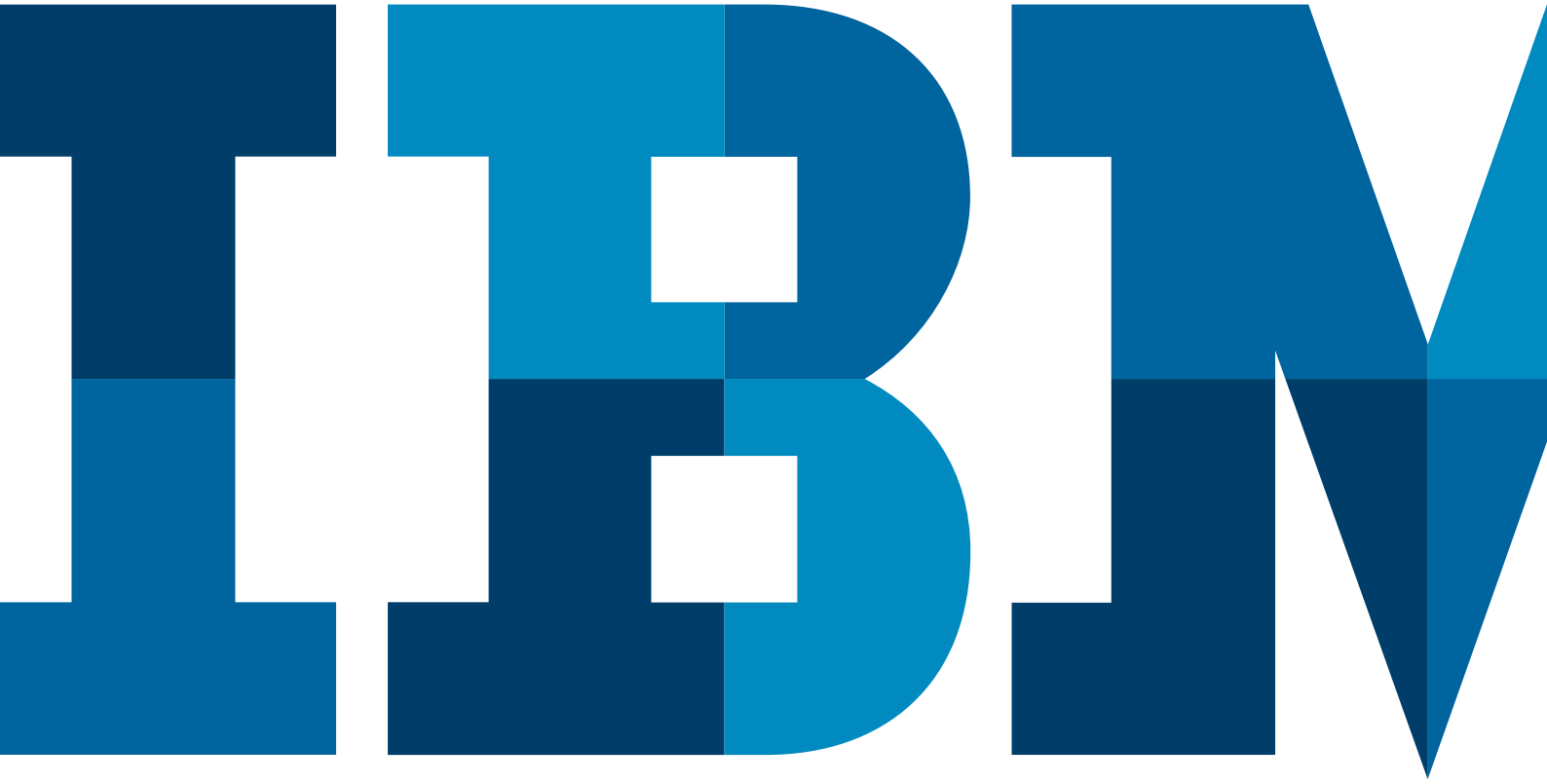
Virtualisierung: eine Technologie voller Chancen & Risiken



Virtualisierung ist die große Chance der Unternehmen, Kosten zu senken und die Flexibilität ihrer IT zu erhöhen. Auch ist Virtualisierung einer der Schritte hin zu Cloud Computing. Selbst wenn Cloud Computing nicht für jeden Kunden und jede Applikation geeignet ist, so ist doch die Vorstufe hierzu eine massive Erleichterung für den IT-Betrieb.

Virtualisierung ja – aber zu welchem Preis?

Die Flexibilität erkauft man sich jedoch mit einem weiteren Sicherheitsproblem. Es gilt nicht nur, die bisherigen Schutzmechanismen einer traditionellen Infrastruktur auch in virtuellen Umgebungen nachzubilden, es müssen darüber hinaus weitere Sicherungsmaßnahmen erfolgen, die auf die Besonderheiten der Virtualisierung eingehen. Das Umziehen ganzer Server von einem Rechenzentrum in ein anderes mit nur einem Mausklick ist eines der Beispiel, die die Besonderheit dieser Technologie aufzeigt.

Virtualisierung ist ohne Frage ein Segen für den kosteneffizienten Betrieb der IT-Infrastruktur. Weniger Server, weniger Netzwerk, bessere Auslastung der Server, geringere Kosten für Kühlung, geringerer Platzbedarf, geringerer Stromverbrauch und das bei mehr Flexibilität. Daraus ist ein „Hype“ entstanden, weil viele IT-Verantwortliche ihr Heil in dieser Technologie suchen. Der permanente Kostendruck lässt auch keine andere Wahl.

Diese Massenbewegung hin zu einer Technologie lockt natürlich auch Hacker an, die sich daran versuchen, Lücken speziell in diesen neuen Technologien zu suchen. Sie forschen nach neuen Angriffswegen, denn die Übernahme einer kompletten virtualisierten Umgebung eröffnet ungeahnte Kontrolle über ein Firmennetzwerk. Die Folgen wären verheerend. Es ist daher dringend nötig, den Schutzbedarf an Virtualisierung anzupassen, frühzeitigen Schutz zu gewährleisten, Transparenz wiederherzustellen und mindestens die gleichen Sicherheitsfunktionen zu etablieren, wie sie in physikalischen Netzstrukturen realisiert sind, plus eine Sicherheitslösung, die mit der Flexibilität von Virtualisierung umgehen kann.

In diesem Zusammenhang sei erwähnt, dass IBM mit seiner Forschungsabteilung X-Force im letzten Jahr 8562 Schwachstellen in Applikationen, Betriebssystemen und Netzwerkkomponenten dokumentiert hat. Das sind mögliche Eintrittspunkte, die teilweise je nach Schweregrad vollen administrativen Zugriff auf den Server ermöglichen können. Kombiniert mit einer sogenannten Hypervisor Escape-Attacke, also dem Bypass des Hypervisors in der Kommunikation zwischen mehreren Virtuellen Maschinen (VM), benötigt man wenig Phantasie, um sich ein Schreckensszenario auszumalen. Ist eine „Cloud Burst Attack“, so nennt sich das oben beschriebene Szenario, nur ein theoretisch möglicher Ansatz verifiziert in den Laboren oder bald schon Realität in Firmennetzen? Die Frage ist nicht leicht zu beantworten, aber hat man Stuxnet vor dem Bekanntwerden für möglich gehalten? Können sich hochqualifizierte Hacker zusammenschließen und den Super-GAU in der IT vorbereiten? Es ist nur eine Frage der Motivation.

Notwendige Gegenmaßnahmen

Was kann ein IT-Leiter in einem vertretbaren Maß an Sicherheitsmaßnahmen ergreifen, wenn Virtualisierung oder gar Cloud Computing nicht der Sicherheit geopfert werden darf?

Die Liste der Maßnahmen ist lang, aber es gibt momentan keinen anderen Weg.

- Netzwerk-Firewall vor dem Virtualisierungscluster
- Netzwerk-Intrusion-Prevention ebenfalls vor dem Cluster
- Patch-Management für Hypervisor und alle VMs
- Virenschutz in den VMs, Virenschutz auf virtueller Netzwerkebene reicht nicht aus!
- Compliance-Management
- Security Configuration-Management
- Vulnerability-Management
- Hyper-Visor Integrity Monitoring
- Root Kit Detection
- Firewall innerhalb der Virtualisierung
- Intrusion Prevention innerhalb der Virtualisierung und/oder den VMs
- File Integrity Monitoring in den VMs für wichtige Applikationen und Daten
- Applikationsüberwachung
- Virtual Network Admission Control

Das sieht zunächst nach einer langen Liste aus, die das Einsparpotenzial von Virtualisierung schnell schrumpfen lässt. Doch sollten sich viele dieser Sicherheitsfunktionen bereits in traditionellen Infrastrukturen auf den Servern und im Netzwerk befinden.

"Wenn man jedoch bereit ist, neue Wege zu gehen, wird man mit einem schnellen Return on Investment und zusätzlich mit einem effektiven Security-Management belohnt."

–Peter Häufel

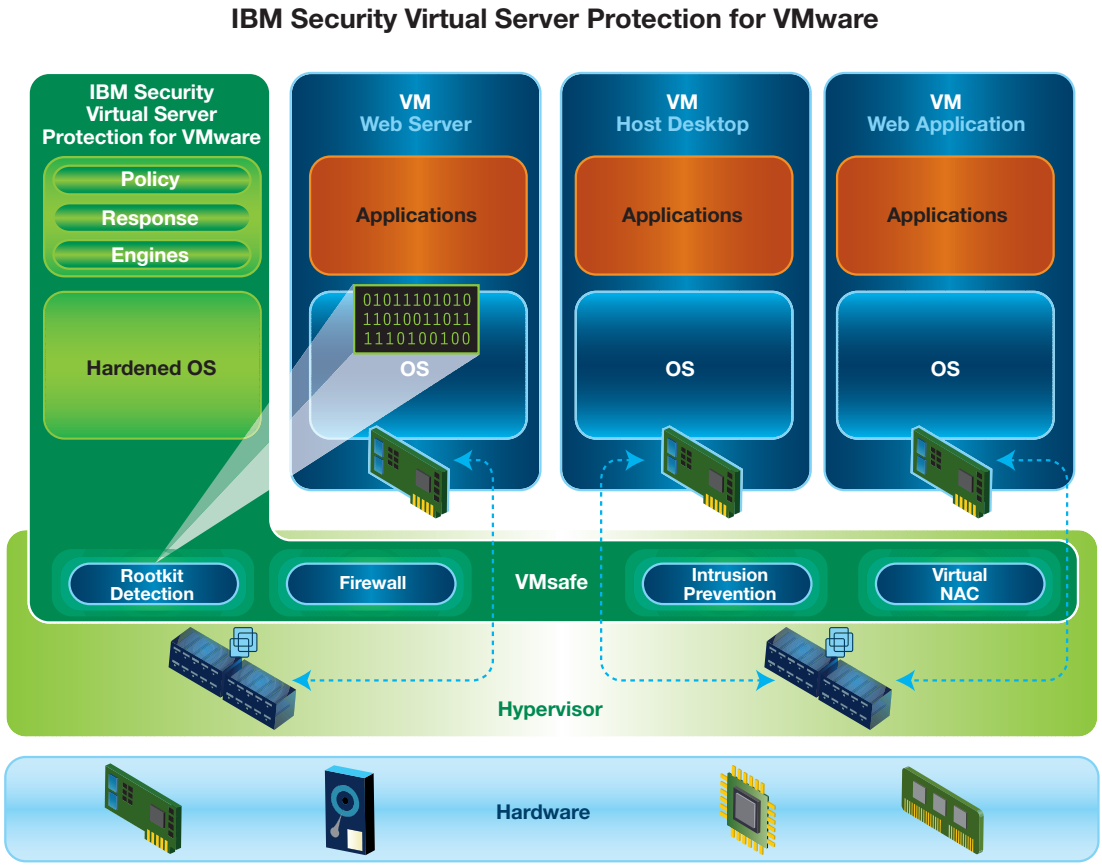


Abbildung 1: Security für Hypervisor und Virtuelle Maschinen

Betriebskosten als möglicher Stolperstein

Zugegeben, wenn man das Thema falsch anpackt, sind die Betriebskosten immens. Das ist auch der Grund, warum viele IT-Leiter vor dieser Investition zurückschrecken. Es sei bisher nichts Nennenswertes passiert, ist selbst in großen Konzernen immer noch eine Antwort, die diesen Investitionsstau begründet. Aufgrund der sich häufenden Vorfälle ist die Begründung allerdings nicht mehr zeitgemäß. Leider starten die Projekte erst, wenn ein Vorfall die Verwundbarkeit aufgedeckt hat oder der Compliance-Verantwortliche die Intransparenz der Virtualisierung als klaren Verstoß gegen die eigenen Richtlinien betrachtet. Dann aber bleibt wenig Zeit, eine gute Lösung zu integrieren. Zeitdruck ist kein guter Ratgeber.

Wie sieht eine Ideallösung auch im Hinblick auf Sicherheit und Betriebskosten aus? Gehen wir davon aus, dass ein Rechenzentrum nicht komplett virtualisiert ist, weil rechenintensive Applikationen und I/O-intensive Transaktionen höchstens in ausgewachsenen UNIX®- und Mainframe-Rechnern virtualisiert werden sollten. Ideal ist demnach eine Security-Lösung, die keinen Unterschied zwischen traditioneller IT-Security und IT-Security in virtualisierten Umgebungen macht, dabei aber auf die Besonderheit der Virtualisierung eingehen kann. Wir benötigen also einen Agenten, der in gleicher Weise auf allen Endpunkten (Server, Desktop, Hypervisor, VMs, mobile Endgeräte) im Unternehmen installiert werden kann, und eine Netzkomponente, die sowohl in virtuellen Netzen wie auch in konventionellen Netzen für die Sicherheit und Transparenz sorgt. Mehr ist nicht erforderlich, wenn wir die Aspekte Datensicherung, Verschlüsselung sowie Identity- und Access-Management in diesem Kontext nicht berücksichtigen.

Effiziente Sicherheit für die Endpunkte

Betrachten wir zuerst den Agenten für alle Endpunkte. Die Vielzahl der notwendigen Funktionen, die in einem einzigen Agenten vereint werden müssen, klingt erst einmal nach einem hohen administrativen Aufwand und nach Performancehunger.

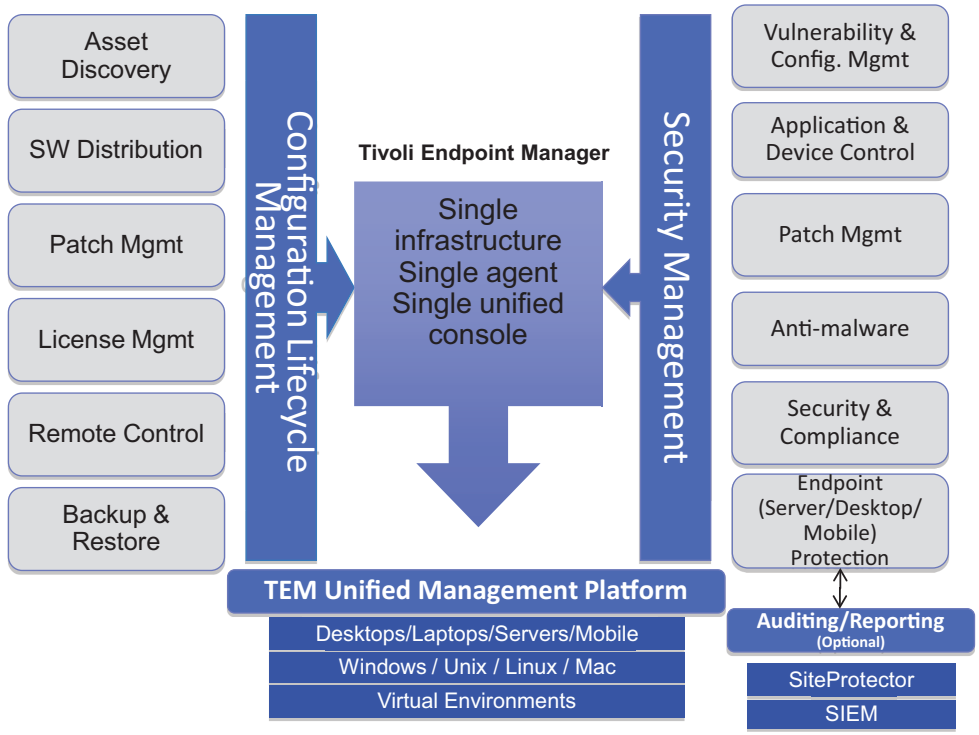


Abbildung 2: IT-Security und Lifecycle Agent

Mit konventionellen Technologien ist diese Herkulesaufgabe nicht angemessen zu bewältigen. Aufgrund der Dynamik, die in virtualisierten Umgebungen zu erwarten ist, muss jeder Endpunkt selbst für seine Sicherheit, Compliance, Aktualität und Funktionsweise verantwortlich sein.

Die Policy hierfür kommt vom zentralen Server, der auch jegliche Änderungen protokolliert, den aktuellen Zustand jedes Endpunktes kennt und nahezu in Echtzeit einen unternehmensweiten Blick auf die Sicherheitslage ermöglicht. IBM selbst hat auf diese Technologie umgestellt, dadurch die Transparenz verbessert und massiv Betriebskosten eingespart. „Better Security @ Lower Cost" ist nicht nur Marketingslogan sondern Realität. Der Agent hat einen extrem kleinen „Footprint", benötigt also nur geringe Systemressourcen, und das bei allen Funktionen, die in Abbildung 2 skizziert sind.

Die Netzkomponente für die Sicherheit in einer Virtualisierungsplattform ist eine Secure Virtual Machine (SVM), in traditionellen Netzen jedoch eine Appliance. Beide werden aus der gleichen Managementkonsole verwaltet, so dass die Konsolidierung und Korrelation der Events schnell und zuverlässig erfolgt. Ein Security-Administrator darf sich nicht die Frage stellen müssen, ob er nun eine Policy für einen virtuellen Server erstellt oder für einen physikalischen. Auch darf kein Unterschied in der Eventbehandlung gemacht werden müssen, denn das kostet Zeit. Im Angriffsfall zählt aber jede Minute; der schnelle Überblick kann viel Schaden abwenden. Aber welche Sicherheitsfunktionen gehören in die Netzkomponente und welche müssen direkt auf dem Endpunkt installiert sein? Je früher ein potenzieller Angriff herausgefiltert werden kann, um so besser. Auf die Netzkomponente gehören also Firewall, Intrusion Prevention, Web Application Security, IP-Reputation, optional Proxy, Virenschutz/Anti-Malware. Da Hacking-Tools mittlerweile schon mit SLAs und 24x7-Support verkauft werden, bieten einige Anbieter an, ihr Hacking-Tool zu aktualisieren, sollte eine Firewall oder eine Anti-Virenlösung den Angriff entdecken. Beides sind Technologien, die weiterhin benötigt werden, aber auf die sich die Hacker schon eingestellt haben. Die Königsdisziplin ist daher, den Datenstrom zu analysieren, den eine Firewall passieren lässt und ein Virenfilter nicht sehen kann.

Sicher und effizient: Intrusion Prevention und virtuelle Patch-Technologie

Intrusion Prevention ist leider ein Begriff, der die Unterschiede der darunterliegenden Architektur nicht beschreibt, aber exakte Erkennung und frühestmöglicher Schutz sind genau die Elemente, die den Wert einer Intrusion Prevention-Lösung ausmachen. Auch muss ein Anbieter einer IPS-Lösung abschätzen, welche Bedrohungen wirklich zu einem Problem werden, denn es gibt weltweit keinen Anbieter, der gegen alle oben bereits genannten 8562 Schwachstellen allein in 2010 einen Schutzmechanismus in seine IPS-Lösung integriert hat. Technisch ist dies zwar zu realisieren, aber der Kunde würde den Preis hierfür nicht bezahlen wollen. Es gilt also eine exakte Abschätzung zu machen. Ein IPS soll gegen alles schützen können, das zu einem Problem werden könnte.

Überflüssige Erkennungsmethoden kosten Entwicklungsaufwand, bringen aber keinen Nutzen. Manche IPS-Hersteller werben mit einer hohen Anzahl von Signaturen. Paradoxerweise ist das ein Hinweis, dass der Anbieter keine hohe Qualität liefert, weil er die Relevanz für Unternehmen nicht einzuschätzen vermag. Masse ist kein Zeichen für Klasse. Umgekehrt ist aber eine kleine Anzahl von Signaturen oder Erkennungsmethoden nicht zwangsläufig ein Gradmesser für hohe Qualität. Ohne massiven Forschungsaufwand, Reverse Engineering, Internetanalyse und einer großen Managed Security Services-Infrastruktur ist diese Aufgabe nicht zu lösen. Das begründet auch, warum hochwertige IPS-Lösungen nicht für wenig Geld zu haben sind.

Der Mehrwert einer Intrusion Prevention-Lösung wird immer deutlicher. Nahezu jeden Tag steht zu lesen, welchen zweifelhaften Erfolg Hacker errungen haben. Ist eine Firma oder eine Sparte erst einmal im Fokus, wird die Lücke schon gefunden. Hacker brauchen Stunden, um aus einer Lücke einen Angriff zu erstellen, aber Firmen brauchen Wochen, um alle ihre Systeme auf den aktuellen Stand zu patchen, falls der Patch überhaupt verfügbar ist. Es braucht also einen virtuellen Patch, der die Lücke so lange verschließt, bis der Herstellerpatch ausgerollt werden kann – im Netzwerk, auf dem Server und auf dem Desktop, ob virtuell oder konventionell. Ein gutes Intrusion Prevention-System sollte dies leisten.

Betriebskosten reduzieren mit einer zentralen Managementkonsole

Bleibt nur noch die Frage nach den Betriebskosten zu klären. In den meisten Organisationen sind die oben beschriebenen Funktionen auf mehrere Managementlösungen verteilt, die jeweils ihre eigene Infrastruktur benötigen.

Patch-Management, Softwareverteilung, Anti-Malware, Compliance-Management, Security Scan, Intrusion Prevention usw. benötigen teilweise je eine eigene Managementkonsole, Relays für größere Installationen und spezialisiertes Betriebspersonal. Der Ressourcenbedarf auf den Endgeräten ist auch nicht zu vernachlässigen. Rechnet man den Aufwand, die Lizenzkosten, die Schulungskosten, das Personal, den Stromverbrauch, den Rechenzentrumsplatz, die Kühlung usw. ein, ist schnell Budget verfügbar, wenn man bereit ist, alte Strukturen aufzubrechen. Der Lohn ist ein einheitliches, zentrales Management, bei stark reduzierten Betriebskosten, einer ungeahnten Transparenz, Compliance Enforcement und natürlich gesteigerter Sicherheit. Einzige Herausforderung bleibt, ein bis zwei Managementkonsolen organisatorisch im Unternehmen zu verankern, die alle relevanten Aufgaben zentral übernehmen können. Aus Kostengründen wird auch diese Hürde fallen, ist aber tatsächlich bei vielen Unternehmen ein nicht zu unterschätzender Faktor.

Fazit – neue Risiken erfordern neue Lösungsansätze

Virtualisierung birgt neben den schon bestehenden Gefahren neues Gefährdungspotenzial. Dieses muss neu bewertet werden. Da der Handel mit Firmengeheimnissen und Kundendaten ein lukratives Geschäft geworden ist, passen sich Hacker diesem Trend an. Eine neue Qualität an Sicherheitsmechanismen ist erforderlich. Wenn man jedoch bereit ist, neue Wege zu gehen, wird man mit einem schnellen Return-on-Investment und zusätzlich mit einem effektiven Security-Management belohnt. Sinnvoll ist, seine Security-Strategie nicht der Virtualisierung anzupassen, sondern in einer geänderten Security-Strategie Virtualisierung mit einzubinden. Das ist ein großer Unterschied.

Weiterführende Informationen

Weitere Informationen finden Sie unter
www-05.ibm.com/de/security/

Über den Autor

Peter Häufel
IBM Deutschland GmbH
Senior Solution Sales Professional, IBM Security Solutions

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

WGW03002-DEDE-00