Sicherheitsaspekte der Virtualisierung

Das Thema Sicherheit von Virtualisierung wird oft vernachlässigt. Gartner-Experte Neil McDonald warnt, dass die Virtualisierung die Security beeinträchtige. Seine Vorhersage: „2009 werden 60 Prozent aller Virtuellen Systemen unsicherer sein als ihre physischen Gegenstücke.“ Denn Virtuelle Systeme (VMs) als neue Technologie bringen eben auch neue Gefahren mit sich. Zudem wird Virtualisierung aufgrund der Verkaufsargumente wie bessere Ressourcenauslastung und schnelle Bereitstellung oft überstürzt eingeführt, ohne auf Sicherheitsaspekte zu achten. Ganz abgesehen davon, dass Best Practices zum Schutz physischer Server nicht unbedingt eins zu eins auf virtuelle Umgebungen übertragbar sind. Schließlich sind in einigen Bereichen die nötigen Security-Technologien für die Virtualisierung noch unreif oder gar nicht existent.

Gefahren der Virtualisierungskomplexität

Die Vorteile der Virtualisierung, bessere Ressourcenauslastung und schnelle Bereitstellung der notwendigen Dienste, fordern ihren Tribut in Form eines komplexeren Konfigurations-, Release- und Sicherheitsmanagements.

Häufige Fehlerursachen:

1. Viele verschiedene Systeme
2. Einarbeitung in die verschiedenen Systeme
3. Installation, Konfiguration der Virtuellen Maschinen (VM)
4. Provisionierung von Anwendungen in VMs
5. Tendenz zu hoher Anzahl von aktiven VMs
6. Benchmarking bzw. Messung der Auslastung der Ressourcen
7. Konfigurations- und Release-Management erreichen eine neue Komplexitätsebene
8. Virtualisierung erhöht zeitweilig die Komplexität von IT-Infrastrukturen
9. Änderungen aller Arbeitsabläufe der Systemverwaltung und damit auch die Organisation der IT-Abteilungen selbst
10. Etablierte Verfahren zur Verteilung von Softwarepaketen oder Patches sind nicht übertragbar
11. begrenzten Einsicht in die Host-Betriebssysteme und virtuellen Netzwerke
12. Wenn die wenige Hardware ausfällt, dann sind gleich mehrere Funktionen betroffen

Segmentierung auf physischen VM-Server ist geschäftskritisch

Einige virtuelle Server verarbeiten normalerweise geschäftskritische Daten wie Kreditkarten- und Kundeninformationen oder geschützte persönliche Informationen, andere nicht. Auf keinen Fall sollten beide auf einem Server laufen.

Migration

Neben der Netzwerksicherheit virtueller Umgebungen bildet auch die Möglichkeit der Migration von virtuellen Maschinen einen Unsicherheitsfaktor. Unternehmen sind nicht zuletzt deshalb an der Virtualisierung interessiert, weil Tools wie VMwares VMotion es Administratoren ermöglichen, VMs von einer Plattform auf eine andere im laufenden Betrieb zu verschieben. Doch das kann Sicherheitspolicies zerstören.

Virtuelle Switches

Sobald der Verkehr über virtuelle Switches zwischen Gastbetriebssystemen auf einem Server läuft, greifen die existierenden Sicherheitsmechanismen nicht mehr (z. B. IPS-Systeme). „Der Versuch, hochverfügbare Netzwerksicherheit mit heutigen virtuellen Switches zu erzielen, führt vor allem zu Performance- und Verfügbarkeitsproblemen.

Auch das Backup bietet Angriffspunkte

Netzwerkbasierte Backup-Lösungen verlangen Schlüssel, um sich in alle virtuellen Server einloggen zu können. Sind diese Backup-Lösungen nicht sicher, können Angreifer mit einem Schlag alle Schlüssel stehlen und damit Zugriff auf alle Host erhalten.

Folgende Aspekte gilt es zu beachten:

1. Virtualisierungssoftware wie Hypervisor bedeuten eine neue Schicht privilegierter und angreifbarer Software und müssen entsprechend geschützt werden
2. Das Konzept der Rechteteilung für die Administration droht unterlaufen zu werden
3. Patching und sichere Konfigurationsmanagement im VM-Umfeld sind vorab zu klären
4. Für gängige Schutztechnologien wie Intrusion Prevention, Anti-Virus Gateways ist es schwer, den Datenverkehr zwischen VMs zu kontrollieren
5. Feste Regeln und die Einhaltung des Vieraugenprinzips sind angesagt
6. Präzise Workload-Analyse
7. Heterogenität der Plattform berücksichtigen
8. Isolierte Betrachtung der Virtualisierung
9. Sequestrieren von virtuellen Maschinen in Ressource Cluster

10. Virtuelle Maschinen sollten in einem vertrauenswürdigem Netzsegment und Host laufen d. h. virtuelle Maschinen in einer DMZ, von vertrauenswürdige Netzwerken (VMs) physikalisch zu separieren
11. Host muss zusätzlich gesichert sein, da er den „Single Point of Failure“ darstellt.

Virtuelle Bedrohungen sind real

Viele Unternehmen sitzen dem Irrtum auf, ihr Sicherheitsansatz für Betriebssysteme aller Art könne einfach auf die virtuellen Maschinen (VM) übertragen werden. Faktisch kann ein virtueller Server nicht auf die gleiche Weise geschützt werden wie ein physischer.

Der Markt für die notwendigen Sicherheitslösungen steckt noch in den Kinderschuhen, die Bedrohungen tun es nicht.

Virtualisierte Malware

Die Bedrohung durch virtualisierte Malware ist real. Darunter versteht man beispielsweise ein Rootkit (siehe Blue-Pill, SubVir und Vitriol), die die Hypervisortechnologie nutzt, um sich selbst oberhalb des infizierten Betriebssystems zu verstecken. Virtualisierte Malware ist im System sehr schwer nachweisbar.

Proof-of-concept-Attacken:

- Joanna Rutkowska stellte „Blue-Pill“ auf der BlackHat vor (VM-Rootkit auf AMD`s SVM/Pacifica)
- Dino Dai Zovi stellte „Vitriol“ auf der BlueHat vor (VM-Rootkit auf Intels VT-X/Vanderpool)
- Microsoft Research stellt „SubVirt“ vor (VM- Rootkit namens SubVirt installiert sich gewissermaßen unter das vorgefundene Betriebssystem)

Virtualisiertes Rootkit

Die Rootkits "Bluepill", „SubVir“ und "Vitriol“ können im laufenden Betrieb ein System übernehmen und über eine neu gestartete Hypervisor-Schicht die Virtualisierung aktivieren und das ursprüngliche System in eine virtualisierte Umgebung verschieben. Virtualisierungstechniken bergen Neue Gefahren in sich und sind beliebig portierbar auf Linux, Windows oder Unix-Systeme.

Virtualisierte Malware ist praktisch nicht feststellbar

Auf dem kompromittierten System ist dieser Eingriff praktisch nicht feststellbar und sämtliche Benutzeraktionen, also insbesondere auch die Eingabe von PINs und TANs können mitgeschnitten und kompromittiert werden. Das Rootkit ist bei entsprechend implementierten Funktionen mit Betriebssystemmitteln prinzipiell nicht feststellbar und die Erkennung dieser neuen Generation von "Stealth Malware" daher sehr schwierig.

Symptome von Stealth Malware

War Malware früher Softwarespezifisch sprich Betriebssystemabhängig, ermöglicht nun die Virtualisierung auf Hardwareebene eine neue Bedrohung - Stealth Malware. Die Erkennung von virtuellen Rootkits (Stealth Malware) ist beim Arbeiten an derartig infizierten Systemen nicht einfach. Symptome können sein:

1. Ein verlängerter Bootvorgang
2. Hardware ist in einen Suspend-Modus versetzt
3. Veränderte Hardware
4. reduzierte Systemleistung

Aufgrund der schwierigen Erkennung von Stealth Malware, können nur präventive Maßnahmen Schutz bieten:

- ✓ Virtualisierungsfunktionen sollten (sofern Sie nicht genutzt werden) im BIOS deaktiviert werden
- ✓ Werden Virtualisierungsfunktionen genutzt, sollte bereits im laufenden Betrieb die Virtualisierung aktiviert werden

Stichwort Scheinsicherheit

Virtuelle Systeme bieten die normalen Sicherheitslücken die jedes Betriebssysteme/ Software mit sich bringt, hinzu kommen die Sicherheitslücken der Virtualisierungs-software selbst sowie nun die Hardwarespezifische (Virtualisierung) Features der CPU`s (AMD, Intel). Ohne auf die oben erwähnten Probleme, die VM`s mit sich bringen, an dieser Stelle zu wiederholen.

In diesem Kontext überdenken Sie die Aussage von Brian Byun, Vice President Global Partners and Solutions bei VMware: „VM`s sind sicherer als physikalische Umgebungen“.

Fazit

Die schnelle Einführung der Virtualisierungstechnologie ohne das einhergehend Sicherheitstechnologien- und Managementrichtlinien explizit hier für entwickelt wurden, stellt ein weiteres Kapitel dar, wie Features zur Steigerung der Produktivität, durch Angreifer- und Malware missbraucht werden können.

Rösner-IT ♦ Lönsstr. 16 ♦ 48485 Neuenkirchen
Tel: +49 (0) 5973-90 06 52 ♦ Fax: +49 (0) 5973-90 07 98
E-Mail: info@roesner-it.com ♦ Web: www.roesner-it.com