



## KPMG ANALYSIS

# Virtual Machines Leading to Real Security Concerns

June 6, 2008

By Dave Pelland, Managing Editor, Digital Insider

Security researchers are concerned that so-called "virtual machines" are being deployed rapidly on corporate networks without due consideration of the security threats.

"A lot of companies forget that the same risks are inherent to a virtual host as a physical host because at some point, it's going to be online," says Chris Schwartzbauer, vice president of management software provider Shavlik Technologies.

"If [a virtual machine] has network connectivity, it has all the same capabilities as if it were a physical machine," Schwartzbauer says. "Many organizations don't think of it as the same problem because [the machine] is virtual."

Virtualization, which dates back to the mainframe computing era, uses software to allow a physical server to run several instances of an operating system or application at once. Virtualization allows companies to combine applications on physical servers that are partitioned to act as separate devices.

Virtual machines (VMs) are controlled by "hypervisor" software that runs directly on the physical machine and coordinates the VM operations. If a VM crashes, the hypervisor automatically transfers running applications to another virtual machine, and ensures critical processes continue running.

Companies in numerous industries are using virtual machines to reduce data-center expenses by consolidating physical machines on virtual devices. Part of virtualization's attraction is that virtual machines can be created with just a few keystrokes; however, that advantage can be a potential problem for security pros.

"If a virtual machine on a physical box with 10 other virtual machines gets compromised, it doesn't have to go back out to the corporate firewall or intrusion detection system -- it can just bounce around the 10 machines inside that physical box," says Ryan Malone, vice president of marketing at security software provider Apani Networks.

"The more that people deploy virtualization, the more they start to realize that virtualization is simple to use, but you have to incorporate security into your standard practices," Malone says.

## Old Images, Old Problems

## MORE...

### [IFRS for Technology Companies: Closing the GAAP?](#)

AUGUST 14 A KPMG white paper examines industry-specific issues for technology companies considering a transition to International Financial Reporting Standards.

### [The Consumer Electronics Boom](#)

AUGUST 6 A new KPMG white paper identifies the critical issues inhibiting faster time-to-market for consumer electronics and semiconductor manufacturers.

### [Wireless Carriers Put Money in Mobile Banking](#)

JULY 29 Cell phone carriers are targeting mobile banking applications for growth.

### [Selected Technology Company Earnings](#)

JULY 25 Slowing economic conditions in the United States affected the results of several technology companies in the second quarter.

### [Companies Taking Green-Tinted Look at Data Centers](#)

JULY 18 As corporations become more environmentally aware, they're looking at their data centers and PCs to reduce energy consumption and carbon footprints.

### [Social Media: a New Political Animal](#)

JULY 10 Social media is reaching beyond the traditional corps of political pros and playing a major role in the fall elections.

### [KPMG's Quarterly New and Emerging Markets Magazine](#)

JULY 2 In this issue, KPMG examines how the wireless revolution is shaping everyday life in emerging markets to its logistic systems.

One of the potential problems in virtualization is monitoring VMs added or removed from the network. This ebb and flow of virtual machines can make it difficult for administrators to know how many machines the network is running -- let alone ensure that they have the proper security settings.

"A lot of the problem is not necessarily in the software or the solution, but in enabling the processes that support it properly," says John Pironti, chief information risk strategist for IT service and solution provider Getronics. "Change and service management has become a problem with virtual machines because it's very easy to create another [VM]."

For example, a common issue in virtualized environments is the creation of virtual machines based on disk images that may not include the latest patches. A company may update its network and its devices, but if a new virtual machine is deployed without the most recent updates, vulnerabilities can be re-introduced.

"People might have a false sense of security when their patch management system comes back and says it 'got' 100 percent, but that means it got 100 percent of the known systems," Pironti says. "It's the unknown ones we need to be worried about."

A similar issue exists with virtual machines that are offline when patches are applied, Schwartzbauer says. If those machines are brought back online, whatever vulnerabilities emerged after the patches were deployed could reemerge.

Security executives recommend that policies for creating virtual machines be the same as those for the installation of physical machines. For example, administrators creating virtual machines should make sure the configuration contains the latest patches and meets the applicable security policies.

### **Direct Threats?**

Although companies have not made public news of widespread or severe attacks, researchers are raising concerns that hackers could exploit the hypervisors controlling virtual machines.

"We've seen demonstrations [from researchers] who have made their way through the hypervisor," Pironti says. "We've seen evidence of attackers looking to log in and create rogue servers that act as attack points that nobody knows exists."

Once inside a network, attackers could modify virtual machines to harvest information from corporate databases or to use virtual machines for relaying spam and coordinating bot attacks.

"The virtual server is like a mini-network, so if you compromise that core-level machine, you can go do a bunch of [illegal] stuff," Schwartzbauer says.

Pironti and Schwartzbauer say until a major incident emerges that can be attributed to virtualization, the threat is likely to remain theoretical.

And the tremendous cost savings virtualization can offer through server consolidation means potential security concerns are unlikely to slow companies' enthusiasm for virtual machines.

"The more that people deploy virtualization, the more they start to realize that virtualization is simple to use, but you have to incorporate security into your standard practices," Apani's Malone says. "This is more the normal maturation of a product than a problem with virtualization products."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

**PLEASE RATE THIS ANALYSIS**

**Quality of Analysis**

1  2  3  4  5   
POOR EXCELLENT

**Comments or Questions**

**e-Mail Address** (optional to enable Insiders to reply)

[Submit](#)

© 2008 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

[Privacy](#) | [Legal](#)