Virtualization Raises New Cyber-Security Questions for Government

Hilton Collins | August 18, 2008

Virtualization can work wonders for an IT environment. Virtualization lets one computer do the job of many consuming less floor space, energy and operational costs than installing more hardware. These virtual machines can be managed remotely, and can store critical data and applications for disaster recovery purposes.

But virtualization comes with a potential drawback. Specifically it introduces a new layer of software on top of the host machine or system, which creates additional infrastructure to manage and secure.

Despite security concerns, however, virtualization's here to stay. According to survey results Microsoft released in April, 71 percent of U.S. retailers use virtual tools to cut costs and gain greater infrastructure control. Experts agree other sectors, including government, will ride the virtual wave for the foreseeable future.

As virtualization becomes common, security must adapt and evolve. IT professionals should ensure they don't scale their virtual environments up higher than they can control. To obtain a manageable virtual environment, it should be built with clearly defined goals, architecture and set policies to gauge performance.

Steps to Security

Mark Ramsey, manager of IT operations for Charlotte County, Fla., said shutting down unnecessary services in the virtualized environment can help decrease cyber-attacks.

"It's probably more important in a virtualized environment, because of performance, that you eliminate unnecessary services from your servers," he said. "If you don't need Internet information services for some specific purpose on one of your servers, don't install it."

There will be less activity to protect and monitor if IT managers shut off unneeded activities. Another benefit is the network will likely run better because it will take up less processing power.

But securing a virtual network takes more than the efficient use of resources.

There are three areas that are different between virtualized and nonvirtualized environments, according to David Greschler, director of integrated virtualization strategy for Microsoft. "First, customers need to secure the virtualization layer by ensuring they are running virtualized applications on a trusted platform," he said. In other words, secure physical resources before running virtual systems on them.

Second, IT staff should isolate virtual machines, Greschler said. One way is to segment virtual machines into groups - one set running on one piece of hardware and another set running on a different piece - based on function and level of importance. This way, if one operating system inside a virtual machine is compromised, it's harder for viruses to infect systems running on other hardware.

"Third, customers must monitor virtual machine-to-virtual machine traffic so that the only communications through the network [are] where policies can be enforced and traffic analyzed," Greschler said.

Sometimes it's hard for people to track virtual machine activity. If they deploy additional virtual machines, they create another layer of machines to manage on top of the ones in their physical environment. This added virtual traffic can lead to security lapses and "blind spots" - areas people can't see in the infrastructure. It's not unusual for networks to be so vast that people lose track of which virtual machine runs what application.

This problem can be solved, but at times, it may not be that pressing of an issue.

"There are very rare cases where customers need full visibility of every sort of piece of traffic going between machines," said Nand Mulchandani, VMware's senior director of product management and marketing. In normal physical data centers, no one views traffic because it's not cost effective. "So when you move to a virtual environment, the loss of that visibility is actually not that big a deal," Mulchandani said.

Security and Management

Suppose you're an IT manager who wants to see what happens in a section of your network. Virtual machine No. 20 is communicating

with virtual machines No. 21 and No. 22, and you want to see what packets - formatted data blocks - are being exchanged. The solution is to find an application that lets you monitor traffic and provides the visibility you need.

"There are a couple of folks, and VMware's one of them, that have built net flow interfaces, which give you the ability to view what traffic is moving between all the different virtual machines within a specific hardware enclosure," said Mike Rothman, president and principal analyst of Security Incite, an independent information security firm.

Other vendors, including Microsoft, Blue Lane Technologies and Altor Networks, also have applications designed to monitor virtual traffic. These applications let people block, stop or analyze traffic. However, with so many vendors selling security-monitoring products, it's not easy to pin down an industry leader or select a solution.

"Right now, no one vendor can solve all the virtualization issues on [the] security side," said Stefan Nguyen, a consultant for the Florida Department of Transportation who works on servers that support the central department office. Though these vendors' software solutions all promise to monitor security, they don't all do it the same way. "Each piece of software plays a [certain] role, so you can't combine everybody. That's why you have to use your own best practices."

Best practices are helpful, but sometimes customers are so in love with virtualization's benefits - cost savings and energy reduction - that best practices become afterthoughts.

"There [are] a lot of industry guidelines and platform providers' suggestions, best practices, for securing virtualized environments," said Christopher Hoff, chief security architect at Unisys. "It's amazing how many people don't do them."

Managing virtual networks is similar to managing physical ones. In fact, a good first step to securing a virtual infrastructure is securing the software that runs it. A properly configured physical network lays the foundation for a safe, properly configured virtualized one.

"I don't differentiate between my virtual and physical infrastructure," said Ramsey, who recently received certified chief information officer accreditation though the University of Florida. In Charlotte County, Fla., he has eight physical servers that run 109 virtual machines. "You apply all the same methodologies and checks and balances that you would whether you're dealing with a virtualized server or a physical server," he said.

As a beginning point, Mulchandani recommends securing the software that runs the virtualization platform.

"When you move your machine from a physical machine - say you run on a Windows server or a desktop - and you [create] a virtual machine out of it, the security products and security of your machine are unchanged," Mulchandani explained. "Meaning, if you were running antivirus software on your physical machine, it actually continues to run unchanged in your virtual machine."

Virtual World Attackers

Software that manages virtual machines is called the "hypervisor." When installed on a host machine or operating system, the hypervisor sorts the host system's processing power and other resources to support the various virtual machines. Some experts wonder if it's a prime target for malicious programmers to corrupt or penetrate to gain access or control of scores of virtual machines.

"The probability is high that we will see exploits targeting the hypervisors," Unisys' Hoff said. "The possibility really depends upon how well these vendors do in securing the underlying hypervisors themselves."

Hoff said inevitably hackers will target virtual environments specifically, but vendors have done a decent job of securing hypervisors' underlying code.

"There haven't been any attacks against the hypervisor, so all of this talk and discussion is theoretical," Mulchandani said. "What makes it hard to attack the hypervisor is the fact that the hypervisor is actually a very small piece of code. It has few interfaces to the outside world and does not communicate or have users checking e-mail and browsing the Web on it."

But just how do you secure the hypervisor? There are applications that reduce its attack surface, and methods include embedding the hypervisor deeper within the network or limiting the number of network channels.

Attacking the hypervisor may be worth the trouble for only the most sophisticated hacker. After all, if you're going to burglarize a house, why smash through the concrete foundation when you could break open the door or a window?

"A Windows machine running on your Dell box in your physical data center and a virtual machine look identical because they have an IP address," said Mulchandani. Consequently most hackers won't care much about the hypervisor when they can use their regular tricks to attack the machines directly.

Hoff feels the same way. "Attackers are lazy. They go after the low-hanging fruit," he said. "Why would I bother deploying virtualized rootkits when I can just essentially exploit a poorly configured server?" This takes the same amount of effort it would take to infect a system with malware once someone clicks on a link they shouldn't.

http://www.govtech.com/security/Virtualization-Raises-New-Cyber-Security-Questions-for.html