

Security pros want strong policy for virtualization

http://searchitchannel.techtarget.com/news/article/0,289142,sid96_gci1357537,00.html#

01 Jun 2009 | SearchITChannel.com

By Heather Clancy, Contributor

Security consultants believe that the ongoing economic malaise is prompting many businesses to rush skunkworks server virtualization projects into production without thoroughly considering how these deployments might affect their overall security posture.

Server virtualization introduces a new layer of complexity to corporate security policy: It isn't enough to protect just the host hardware and its hypervisor layer, security experts say. Businesses should protect not just the hypervisor itself but also each virtual machine, if they hope to keep up with compliance regulations.

The good news is that more companies are raising questions about the security threats introduced in virtual environments, and more mainstream security vendors are beginning to address the problem, said Joe Magee, chief technology officer for Vigilant LLC, a managed security services provider in Jersey City, N.J.

In late April 2009, as an example, Trend Micro Inc. moved to acquire Third Brigade Inc. in a bid to add virtualization security to its product line. This is significant because Third Brigade is the first vendor to support VMware's VMsafe API, which allows third-party security tools to run as protected virtual machines. These tools will be able to watch over virtual machines, applying security within the hypervisor. McAfee Inc. has also introduced enterprise services and tools to protect virtualized environments. Watch for more VMsafe development in the coming months.

"Just three years ago, no one was talking about this. Now, the awareness of this layer and these issues is becoming mainstream," said Gartner Inc. Vice President and Fellow Neil MacDonald. "At the end of the day, you don't necessarily have to go out and buy all new tools. The most important thing to me is that we are having the conversation."

Word to the wise: Think security first

Wolfgang Goerlich, network operations and security manager at a financial services firm in Birmingham, Mich., said security considerations were a critical component of his year-long bakeoff for a server virtualization solution, which has been in production about eight months. VARs and IT managers can no longer think of the operating system layer as the boundary for security policy. Goerlich's focus was on ensuring that the hypervisor layer was as lightweight as possible to reduce the potential for break-ins.

"The inherent risk is that if someone can gain unauthorized access to the host, [then] all of the systems can become vulnerable," notes Yan Kravchenko, security team lead for NetSPI Inc., a security services firm in Minneapolis. "The main reason this issue is surfacing is primarily because people want to apply the virtualization formula to their production environment."

To Kravchenko, there are two inherent threats associated with server virtualization projects: the actual technical threat posed to virtualization environments and the threat caused by potentially sloppy management practices associated with bringing up a low-cost server. One of the biggest benefits associated with virtual servers is the speed with which they can be brought online. However, in their bid to reduce total cost of ownership for their IT infrastructure, some companies may be skimping on the documentation and security policy work they should be applying to these servers, according to Kravchenko.

Gartner's MacDonald also believes businesses should apply the same level of scrutiny and process discipline to their virtual servers as they do with physical ones.

"We have to start treating any virtual environment like a critical platform. It means some of the basic blocking and tackling we do for the operating system, we now need to do for the hypervisor," MacDonald said.

Doug Landoll, chief strategist for Lantego, a security services firm in Austin, Texas, said virtualization projects often expose and exacerbate vulnerabilities in a company's security posture. "If you don't have good configuration management, oversight or review, you are worsening an existing situation," he said.

Virtualization exposes existing IT weaknesses

Virtualization requires companies to adjust core processes, including patch management, change management (such as moves, adds and changes of servers), back-up, performance monitoring, incident response and forensics, network access control and disaster recovery planning, Landoll said.

"When you introduce any new technology, process is the toughest thing," he said. It's what's going to bite you."

Ariel Silverstone, a security consultant in Atlanta, said another step any VAR or IT manager can take is to test virtual machines for superfluous traffic before they are introduced into a production environment.

"You monitor the server to see what traffic it generates. If you don't do this, you aren't doing your due diligence," he said.

Silverstone believes it will be at least two years before there are standard policies and products to automate some of these tasks. Meanwhile, he points security professionals seeking best practice information to two organizations that are working on technologies and data center design approaches relevant for security within a virtualized server environment. They are the Jericho Forum, a group of chief information security officers (CISOs) that are developing best practices for security that steps beyond the bounds of traditional firewalls and intranet environments, and the Cloud Security Alliance, a nonprofit organization formed in November 2008 that seeks to get ahead of the security issues surrounding the ultimate virtualized environment, the cloud.