

Virtualization Security

Even the latest network technologies can introduce security holes.

By Nicole Lewis, ITsecurity.com, June 17, 2008

<http://www.itsecurity.com/features/virtualization-security-061708/>

More security attacks against virtualization software may be coming, according to IT security expert Ed Skoudis. He urges [IT managers](#) to make security a higher priority as server and desktop virtualization continue to carpet IT networks.

In an interview with ITSecurity.com, Skoudis, founder and senior security consultant with [Intelguardians Inc.](#), said IT managers charged with implementing virtualization projects should adopt a strategy that includes configuring their networks in a way that will mitigate against virtualization vulnerabilities. He also noted that IT managers should expect more [attacks](#) to occur as virtualization adoption increases.

“My expectation is that there will be a steady discovery and release of more vulnerabilities of virtualization products of various kinds. That will happen and we’ll probably see two or three big ones per year coming out of the research space,” Skoudis said. “The question is will the bad guys start doing them in the real world. So far they have not but I do think that they will, especially as virtualization is more widely deployed.”

Turning to Virtualization

Undoubtedly, IT managers are turning to virtualization to cut costs and better control information in their [datacenters](#). The continued adoption of server virtualization — which allows a server administrator to divide one physical server into multiple isolated virtual environments — and desktop virtualization — which gives users a chance to access servers that host an entire desktop environment specific to each — means more security considerations.

In its "State of the Data Center Report, 2007," [Symantec Corp.](#) found that server virtualization and consolidation are considered top cost containment strategies for the majority of the 800 respondents. Research results also showed that 90 percent of those surveyed are at least discussing server virtualization, 50 percent are implementing virtualization strategies and 75 percent are considering storage virtualization as a potential solution.

Virtualization Vulnerabilities

As the rush toward virtualization continues, however, there have been a number of reported vulnerabilities discovered particularly in PC and server-virtualization software. For example, last February [Core Security Technologies](#), a Boston-based company that develops IT-security strategies for businesses, [discovered](#) vulnerabilities in VMware Workstation, VMware Player and VMware ACE virtualization software. According to Skoudis, Core’s findings were similar to Intelguardians's demonstration of conducting an escape attack against VMware Workstation.

Last October, [Secunia](#), a Copenhagen-based company that provides software-vulnerability intelligence, [uncovered](#) vulnerabilities in open-source Xen hypervisor, which can be exploited by malicious, local users to bypass certain security restrictions or gain unauthorized privileges. [Microsoft Corp.'s](#) virtualization software was also caught with flaws last year when it was reported that vulnerabilities were [found](#) in Microsoft Virtual PC and Microsoft Virtual Server, which could allow a guest operating system user to run code on the host or another guest operating system.

Still No Attacks

Over at [VMware Inc.](#), executives are quick to note that while there is an excitement in the security industry about finding vulnerabilities in VMware's virtualization products, thus far there have been no reported attacks on VMware's ESX virtualization product, which is used for mission-critical systems at high-security federal agencies. "These examples are all workstation vulnerabilities and server vulnerabilities, and while they are important to us and we fix them very quickly and patch them, these aren't actually very critical to the real enterprises running mission critical data," said Nand Mulchandani, senior director of products at VMware.

According to Mulchandani, the real concern is that IT security managers don't understand the different types of virtualization products on the market and the different use cases. "All of these different types of virtualization products require a very different set of security technologies, a different set of security operation procedures and they have different threat models," Mulchandani said.

Furthermore, IT managers should incorporate security considerations earlier in the process of conducting virtualization projects, said Brian Hernacki, architect in the office of the CTO at Symantec Corp. Another consideration is to organize and classify data, which virtualization should force IT managers to do.

"The first and foremost thing to consider at the design time of a virtualization project, is to look at what data you are going to be storing and what the implications are. What are the access control implications, what are the compliance implications, or the audit implications, how sensitive is that data and what do you need to do with that in terms of security," Hernacki added.

Improving Defenses

To help strengthen security in virtualization products, Microsoft, VMware and other vendors are working on [patches](#), publishing best-practices [white papers](#) and working with IT-security organizations as they develop new products and strategies to confront security weaknesses. According to Skoudis, these companies develop a patching process that gets solutions to customers quickly. "Patches can be rolled out to customers who can get the latest software with the fixes because vulnerabilities will be discovered," he said.