



VMs You Can't See Can Definitely Hurt You

Edward L. Haletky, CIO
From: www.cio.com

June 27, 2008

Recently [Verizon](#) Business released its [2008 Data Breach Security Report](#), summarizing the results of four years of forensic research into more than 500 security incidents. While it doesn't focus on [server virtualization](#) specifically, it does illustrate a lot about virtualization security as well.

Of the attacks in the report, 73 percent came from outside the organization, 18 percent were internal, and 39 percent involved business partners. Another 30 percent involved collusion between multiple parties (hence why the numbers do not add up to 100 percent).

This is ground breaking information; the common wisdom has been that an average of 70 percent of all attacks come from the inside.

This report indicates that may no longer be true. Instead, it shows that the highest risk to the datacenter is from files compromised by business partners, followed closely by the insider with the external source a distant third.

Measures of impact follow the same pattern. Compromised data records can be assigned a value according to how critical their data is to the company; since insiders and partners have most direct and frequent access to the most valuable files, the report finds those two groups also hold the greatest power to cause havoc.

Even more important, however, is what the report finds that the victims hadn't. In a significant number of cases—listed as the 'Unknown Unknowns' category—the victimized organization either didn't know it owned the system that was compromised (7 percent), or did not know the data was stored on the system that was hit (66 percent).

Other attack paths came from unsuspected connections to a system (27 percent), or unknown, inappropriate privileges on the system (10 percent).

So why is this important to virtualization security?

The answer lies in the nature of the virtual infrastructure: It is very easy to create a system (unknown system), on a virtual network that you just created (unknown network),



and place upon that system sensitive data (unknown data), granting rights to that data to anyone (unknown privileges), without much, if any indication that you'd done it.

As a matter of fact all that can happen within 10-30 minutes and the security team would be completely in the dark.

It is very important for security teams to fully understand virtualization, its security, and how to audit the system to catch such actions. At the moment not many tools exist, but simple read-only access to the virtualization management tools can give the security team the ability to run audits. While the tools are cool, the report states that there is nothing like good old fashioned eyeballs.

[VMware](#) has developed the VMware Life Cycle Manager to try to combat the invisible nature of VM sprawl as this is commonly called.

While this helps with a tool, if the security policy, security teams, and Chief Security Officer are not involved with virtualization, the number of unknown unknowns will increase as virtualization use increases.

Virtualization expert Edward L. Haletky is the author of "VMWare ESX Server in the Enterprise: Planning and Securing Virtualization Servers," [Pearson Education](#) (2008.) He recently left [Hewlett-Packard](#), where he worked in the Virtualization, Linux, and High-Performance Technical Computing teams. Haletky owns AstroArch Consulting, providing virtualization, security, and network consulting and development. Haletky is also a champion and moderator for the [VMware discussion forums](#), providing answers to security and configuration questions.

© 2008 CXO Media Inc