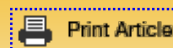


COMPUTERWORLD



Print Article

 Close Window

The scary side of virtualization

IT execs are starting to get spooked about the security risks of virtual servers.

Robert L. Mitchell

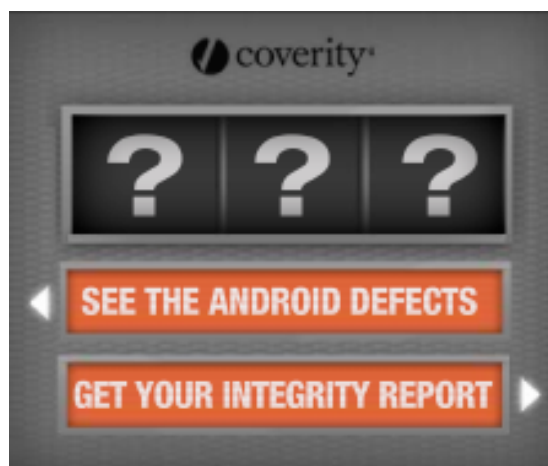
November 8, 2010 ([Computerworld](#))

At the *Computerworld* Premier 100 IT Leaders conference in March, one CIO stood up to express his unease about the security of a virtual infrastructure that has subsumed more than half of his company's production servers. Two other IT executives chimed in with their own nagging worries.

None of the executives in that room wanted to admit on the record that they feel vulnerable, but Jai Chanani, senior director of technical services and architecture at Rent-A-Center Inc., feels their pain. "One of my biggest fears is the ability to steal [virtual servers]," he says.

Chanani's team has about 200 virtual servers operating as file, print and, in some cases, application servers. But, for security reasons, his shop doesn't use [virtualization](#) for the company's ERP system, databases or e-mail.

Michael Israel, CIO at amusement park operator Six Flags Inc., voices a different concern. For him, the most unnerving scenario is a rogue administrator moving [virtual servers](#) from a secure network segment onto physical hosts in



Getting Worried

How concerned is your organization with the issue of security in a virtualized environment?

- Very or extremely: **32.7%**
- Somewhat: **36%**
- Minimally: **23.7%**
- Not at all: **7.6%**

Source: TheInfoPro survey of 214 IT security professionals, November 2010

an unsecured segment, or creating new, undocumented, unlicensed and unpatched virtual servers. "The last thing I want is 25 servers out there that I don't know exist," he says.

John Kindervag, an analyst at Forrester Research Inc., says he's heard stories from clients who have had VMware's vCenter management console compromised, enabling the attacker to copy a virtual machine that can then be run to access data. "When you steal a VM, it's like you broke into the data

center and stole a piece of hardware. It's potentially devastating," he says.

"We worked for many years with customers on best practices that make this a complete nonissue,"

says Venu Aravamudan, senior director of product marketing at VMware Inc. He says most users address such risks by following best practices such as creating an isolated network segment for managing the resources, and creating role-based access controls.

The migration onto virtual servers has saved businesses huge sums of money as a result of consolidation and improved efficiency, but as virtualization gobbles up more and more production servers, some IT executives are getting indigestion. Has anything been overlooked? Could a catastrophic breach bring down critical applications -- or perhaps an entire data center?

"Customers wake up one day, realize that 50% of their business-critical apps reside on virtual infrastructure and say, 'Gee, is that secure?' That's very common," says Kris Lovejoy, vice president of strategy at IBM Security Solutions, a security consultancy.

"There are some huge, well-known corporate names around the globe that you'd think would have this stuff pretty much beat. That couldn't be further from the truth," says Andrew Mulé, a senior security consultant in EMC Corp.'s RSA unit.

The problem isn't that a virtual infrastructure is difficult to secure per se, but that many companies still haven't adapted their best practices (if they have them) to the new environment.

Virtual Headaches

Virtualization introduces technologies -- including a new software layer, the hypervisor -- that must be managed. Also new: virtual switching, which routes network traffic between virtual servers in ways that aren't always visible to tools designed to monitor traffic on the physical network.

Moreover, virtualization breaks down the traditional separation of duties within IT by allowing a single administrator to generate new virtual servers en masse at the push of a button, without approval from purchasing or input from the network, storage, business continuity or IT security groups (see "[Beware the All-Powerful Admin](#)," below).

Meanwhile, virtualization-aware security technologies and best practices are still evolving. The market has emerged so quickly that customers haven't been able to keep up from a best-practices standpoint, says Lovejoy. There's a lack of knowledge on the subject and a lack of skills in the field.

"The questions about security in a virtual environment are centered around lack of visibility, lack of control, and fear of the unknown," says Bill Trussell, managing director of security research at TheInfoPro, an IT market research firm in New York. Could someone hijack a hypervisor within a business's virtual infrastructure and use it to compromise all of the virtual servers residing on top of it -- as one CIO feared? Could an attacker breach one virtual server and use it as a platform to attack another virtual server, such as a payment-card processing application residing on the same hardware, without the administrator ever knowing about it?

Concerns about scary scenarios like those persist despite the fact that there have been no known attacks against virtual infrastructures, says Eric Baize, RSA's senior director for secure infrastructure.

When TheInfoPro surveyed 214 IT security professionals earlier this year, it found that one-third were "very or extremely" concerned about security in a virtualized environment.

Worries about an attack that could compromise a hypervisor rose after [Joanna Rutkowska's "Blue Pill" hypervisor malware rootkit](#) at a Black Hat conference in 2006.

Since then, however, the industry has moved forward with hardware technologies to ensure the integrity of hypervisors, such as Intel's Virtualization Technology for Directed I/O (known as VT-d). "Today, most of [Intel's] Core i5 and i7 processors have those technologies," and virtualization software providers have moved to support those features, says Rutkowska, founder and CEO of

Invisible Things Lab, an IT security research firm.

Rutkowska herself doubts that anyone will actually use a Blue Pill-type rootkit to compromise virtual machines. "The bad guys don't really have any incentive to use such sophisticated rootkits," she says, especially since better-known rootkit technology from the '90s still works well for attacking traditional operating systems.

"People are wringing their hands over theoretical scenarios rather than ones that have been documented to be a problem," Trussell says.

But virtualization does involve risks if best practices aren't followed and adapted to a virtual infrastructure. For example, the hypervisor must be patched just like any other operating system, says KC Condit, senior director of information security at Rent-A-Center.

Security consultants say they've noticed a wide variety of security problems at customer sites.

Lovejoy is seeing malware and cross-site scripting issues that result from poorly constructed virtual machine images, for example. "Commonly, that image will contain malware or have vulnerabilities that can be exploited very easily," she says. "It used to happen once. Now these images are being deployed without end, creating massive headaches for people."

"We're seeing a lot of misconfigured hypervisors," adds RSA's Mulé. He says he often sees poor patch-management practices for virtual machines and the use of easily guessed or default usernames and passwords for virtual machine manager programs that have full access to the hypervisor. In addition, he says, "we sporadically see virtual machine management tools on the wrong side of the firewall."

Using default passwords when creating new virtual servers is very common, says Harold Moss, CTO of cloud security strategy at IBM Security Solutions, and people responsible for administering the new machines don't always change them either. Would-be thieves could dial into a machine, guess the password and have complete control, he explains.

In addition, because virtual machine images are data -- program code stored on a hard disk drive somewhere -- those files must be protected. "You don't want someone walking away with an entire server on a USB drive," says Vauda Jordan, senior security engineer for the Phoenix city government. She says the city uses a combination of physical security, network storage access controls and file integrity monitoring to protect virtual machine images.

The traffic flowing between virtual machines is another area of concern, since firewalls, intrusion-detection and -prevention systems, and other monitoring tools can't tell if the virtual machines are running on the same hardware.

"I've put packet sniffers on virtual servers, and nothing is going in and out of the physical network interface. So, how are those communications happening? And are they over secure channels?" asks Jordan. While the city has a significant investment in virtual infrastructure, Jordan won't even talk about the technology or its scope, citing security concerns.

With VMware's ESX Server and the other major virtualization platforms, the data that passes between virtual machines is unencrypted. Aravamudan says encryption is being "actively considered" at VMware, but he declined to say when it might be added to the company's products.

Systems like VMware's vShield and other third-party tools can create virtual firewalls that segment



Customers wake up one day, realize that 50% of their business-critical apps reside on virtual infrastructure and say, 'Gee, is that secure?'

Kris Lovejoy, Vice President, IBM Security Solutions

VMware, XenServer, Hyper-V and other virtual machines into different security zones, but not all organizations have implemented them. For example, the creation of secure zones hasn't been a big focus at Rent-A-Center. But as the virtual infrastructure scales up, that's becoming a necessity, says Condit.

Some existing firewall tools have visibility into virtual server traffic, but in other cases IT needs to add another set of virtualization-specific tools, and that adds to management complexity.

It's better to have a tool set that spans both the physical and virtual environments, says Neil MacDonald, an analyst at Gartner Inc. Until the traditional security tool vendors catch up, however, IT may need to bring in tools from lesser-known vendors like Altor Networks, Catbird Networks and HyTrust that have been tailored specifically to virtual machines.

More important, the core network architectures need to change to accommodate virtualization, says RSA's Mulé. "Networks that work correctly with physical servers don't necessarily work well with virtual machines. Security would be improved if proper routing and subnets and virtual LANs were implemented," he says. Most business continuity failures in virtualized settings can be attributed to network design flaws, he contends.

Matthew Nowell, senior systems engineer at Six Flags, uses virtual LANs to segregate virtual servers. "Depending on how we set up routing rules, they may or may not be able to talk to each other," he says.

But MacDonald cautions that "VLANs and router-based access controls alone are not sufficient for security separation." The research firm's guidelines call for the deployment of some sort of virtualization-aware firewall.

At the Phoenix city government, Jordan insists that systems administrators isolate each virtual server within its own security zone. "I had to fight with server admins who swear up and down that the hypervisor can do that. But I trust firewalls more than I trust hypervisors," she says.

Security From the Start

Securing a virtual infrastructure isn't about buying more tools, says RSA's Baize. "There's a lot available today in terms of controls for virtual infrastructure. What is lacking is the understanding of what the controls are for and when they should be applied," he says.

The best way to create a secure virtual infrastructure is to get security experts involved early. Gartner estimates that as many as 40% of IT shops don't seek IT security's input on a virtual deployment until after the system is already built and online.

The problem becomes more evident as mission-critical applications move into virtual machines. "When you start looking at virtualizing SharePoint or Exchange or ERP, you really are running into sensitive data. That forces the issue," MacDonald says.

By then, organizations are trying to bolt on security that should have been designed in from the beginning. That kind of after-the-fact redesign work can get expensive. "CIOs should make sure

Related Reading

The Virtual Enforcer

Third-party vendors such as Trend Micro Inc. are offering add-on software to beef up the security of the hypervisor layer. But some experts worry that as the layer gets more crowded and complex, it becomes a bigger target for security attacks. For more on this topic, see our story "[Hypervisor as Virtualization's Enforcer?](#)"

they have their top people in the loop when designing this type of architecture," MacDonald says. It all comes down to policy, contends Condit. "If you don't have a strong security policy in place, a virtual infrastructure is going to show up those weaknesses much more quickly because things happen more rapidly," he says, referring to how quickly virtual servers can be created and then moved around between physical host servers.

CIOs are right to worry. Says Condit, "A certain healthy level of paranoia is always a good thing."

Staffing Advice

Beware the All-Powerful Admin

In an unchecked, unmonitored virtual environment, administrators are all-powerful -- and that's not a good thing, consultants and IT executives agree. "This gives server admins the keys to the kingdom, and most of the time they don't understand the security risks," says Vauda Jordan, senior security engineer for the Phoenix city government.

For example, administrators may create a virtual FTP server that compromises security. Or they may inadvertently use a virtual-machine migration tool to move a server onto different hardware for maintenance reasons, without realizing that the new host is on an untrusted network segment.

Failure to implement best practices, or to establish a clear [separation of duties](#) in virtual infrastructure, is an all-too-common problem, says Andrew Mulé, a senior security consultant at RSA. "Folks still today don't like to practice segregation of duties. They give the crown jewels to a small number of people," Mulé says. He recommends developing a strong change-management process that includes issuing change management tickets.

KC Condit, senior director of information security at Rent-A-Center, agrees. "In the virtual world, there is no inherent separation of duties, so you have to build that in," he says. Change management, configuration management and access control are vital to securing the virtual infrastructure.

Compliance is another concern. As director of systems engineering at the Council of Europe Development Bank, Jean-Louis Nguyen needs to monitor activity to ensure that the administrators of 140 virtual machines comply with regulations and management requirements. The bank tried using VMware's logging capabilities but needed a better way to consolidate the information. "Getting at those logs was nontrivial," he says. He ended up using a dedicated tool from HyTrust that provides a central log of all activity.

The bank also used HyTrust to set up a completely segregated virtual environment for the chief security officer, who can monitor the entire physical and virtual server infrastructure.

"The key is to assure your management that there's no administrator abuse," Nguyen says. "We needed to be certain that we're administering systems and not peeking into the data."

This version of this story was originally published in Computerworld's print edition. It was adapted from [an article](#) that appeared earlier on Computerworld.com.