谁来填补虚拟机的安全漏洞

■ 本报记者 郭涛

Gartner的分析师Neil MacDonald在一份研究报告中指出，60%的虚拟化服务器的安全性低于物理服务器，这种状况将持续到2012年。如今，虚拟化技术的普及率越来越高。Gartner预计，2012年全球将有超过一半的工作负载被虚拟化。如果不能有效解决虚拟机的安全性问题，那么安全性问题很可能成为虚拟化应用最大的绊脚石。

VMware公司大中华区技术总监张振伦：通过制定严格的安全指导方针和相关的规范性指南，VMwar可以帮助客户设计、部署和操作安全虚拟化环境。VMware虚拟化技术可以被用于隔离不同信任级别的虚拟机。

戴尔大中华区大型企业事业部首席架构顾问陈进坤：为解决虚拟机泛滥及相关的安全问题，用户应设定虚拟机创建限制条件，部署正规流程，设置记录功能，改变原有的控制策略和流程，制定用于虚拟机创建和更换的授权、测试、通信及恢复的规范。

万国数据服务有限公司(GDS)副总裁张权：虚拟化技术可以促进安全技术多样化的发展。虚拟化技术使得有安全问题的系统恢复到安全状态变得更简单，隔离和屏蔽不稳定或具有安全隐患的应用程序相对轻松……

安全漏洞并不可怕

虚拟机的安全漏洞到底有多大？McAfee Avert Labs的David Marcus表示："如果你有能力攻击一个虚拟机，并且能够进入虚拟机之外的主操作系统，那么就完全可以控制服务器中的全部虚拟机。"

2009年5月，网络上曾经曝光，VMware虚拟化软件的Mac版本Fusion中存在一个严重的安全漏洞。别有用心的人可以利用该漏洞，通过Windows虚拟机在Mac主机上执行恶意代码。幸好，VMware很快就发布了Fusion 2.0.4，修复了该漏洞。虚拟机生命周期管理方案提供商Embotics的营销副总裁David Lynch曾表示："在虚拟机的安全性方面，黑客肯定是有机可乘的。如果你参加过像黑帽大会这样的技术安全大会，就会发现虚拟化技术已经成为热议的话题。很多人在关注这个领域。"

2010年3月，据国外网站报道，核心安全科技公司（Core Security Technologies）发出警告，微软Virtual PC中存在一个未被修复的安全漏洞。黑客通过该漏洞可以成功绕过数据执行保护(DEP)、地址空间随机化布局(ASLD)等安全机制，对虚拟机发起攻击。此安全漏洞涉及微软Windows Virtual PC、Virtual PC 2007和Virtual Server 2005，所幸Hyper-V不受影响。

从目前情况看，针对虚拟机的攻击已经不再是纸上谈兵，而是确确实实发生了。一些虚拟化方案提供商、安全厂商反馈，虚拟环境的安全问题确实存在，而且针对虚拟机的攻击和安全漏洞不断涌现。企业用户必须对那些针对虚拟机的安全威胁提高警惕。

让人担心的是，越来越多针对虚拟机的安全威胁并没有引起广大企业管理者足够的重视。很多人在部署虚拟化技术的时候，将主要精力放在提高设备利用率、降低成本等方面，而忽视了安全问题。

"与其他软件一样，x86虚拟化平台软件不可能没有安全漏洞。VMware、Citrix和微软等虚拟化平台软件厂商在近几年都发现了各自平台的漏洞。"戴尔大中华区大型企业事业部首席架构顾问陈进坤表示，"发现安全漏洞后，只要及时打补丁和升级，用户的主机就不会受到攻击。举例来说，ESX等系统管理程序已经通过加拿大通信安全部(CSEC)通用标准评估与认证方案(CCS)的验证，获得了EAL4+级通用标准认证。EAL4+级是《共同准则互认协定(CCRA)》认可的最高安全级别。"

趋势科技认为，虚拟机确实存在安全漏洞。但是，用户只要及时做好针对虚拟机的补丁管理工作，就不会有太大问题。

惠普公司认为，既然虚拟机是被打包好的文件系统，并且基于标准的平台，那么安全漏洞就是不可避免的。但是，用户如果能扬长避短，充分发挥虚拟服务器的灵活性、可靠性和共享性，那么就能获得事半功倍的效果。这也是虚拟化技术如今能够成为市场主流的重要原因。

在记者采访的多家虚拟化软件厂商、安全厂商和服务商中，万国数据服务有限公司（GDS）副总裁张权的观点颇具代表性。他认为："安全问题是IT业界长期存在的一个问题。它不取决于架构是物理的还是虚拟的，平台是x86的还是Unix的，或者应用以何种形式存在。虚拟化技术的出现具有划时代的意义。它能够降低成本，节能增效，提高资源利用水平和资源配置的灵活性，提升业务连续性水平。作为一种新出现的技术，虚拟机面临着与传统物理服务器架构一样的安全问题，如网络、访问控制、数据加密、操作系统和应用等方面的问题。"

解决虚拟机的安全性问题，不能仅依靠虚拟化软件厂商，而是需要操作系统、应用、网络、安全等厂商共同努力。IT管理者还要提高安全防范意识。

事在人为

Gartner的研究报告指出，虚拟机的安全性低并不是因为虚拟化技术本身不安全，而是因为缺乏相关的管理工具，应用流程不成熟，企业员工和经销商缺乏有效的培训等。

VMware公司大中华区技术总监张振伦指出，实际上，多数的安全风险来自于实际使用的过程中，而并非虚拟化技术本身的问题。经过专门的审计和管理控制，完全可以避免虚拟机的安全风险。AstroArch咨询公司创始人Haletky认为："与虚拟化相关的最大安全问题是，很多用户不知道自己在做什么。为了有效解决虚拟机的安全性问题，虚拟化应用管理员必须学习更多的知识。"

张振伦归纳出虚拟机面临的主要安全风险：第一，虚拟化层的妥协可能导致所有托管工作负载的标准降低；第二，内部虚拟网络上的虚拟机之间的通信缺乏可见性和控制力，使得当前的安全策略增强机制丧失效力；第三，在没有被充分隔离的情况下，不同信任级别的工作负载被整合到一个单独的物理服务器上；第四，Hypervisor/VMM层和可管理工具的访问管理缺乏可控性；第五，网络和安全控制职责的隔离存在不足。

其实，技术的问题只是一方面，为了保护虚拟机的安全，更重要的是在人和应用方面下功夫。Gartner研究发现，40%的虚拟化应用在最初的规划和设计阶段，根本没有考虑安全因素。Gartner建议，安全管理流程应扩展到虚拟化管理程序和虚拟机监视器等方面。

许多系统管理员缺乏有效保护虚拟化环境的专业知识。虚拟化技术的出现模糊了IT人员的角色与职责。例如，在虚拟机泛滥而管理员又不知情的情况下，后端存储的性能很容易出现瓶颈。

"虚拟化正在改变传统的服务器配置流程。用户需要建立一个全新的框架，避免出现虚拟机泛滥等问题，进而解决隐藏的安全问题。许多早期部署的虚拟基础设施，并没有采用最佳的基础设施架构部署策略。"陈进坤表示，"用户应该避免为虚拟化而虚拟化的思维定式，将注意力放在人员、流程和技术的无缝整合上，进而创造一个高效、高安全性的企业基础架构平台。"

"无论是物理环境还是虚拟环境，出现安全问题的原因都一样，即技术和管理方面的问题。"张权认为，虚拟化应用成功的关键是三分技术、七分管理，"仅仅依靠技术手段，只能治标不能治本，只有结合安全的运维管理，才可以做到标本兼治。"

张权归纳出虚拟机在管理方面存在的主要问题：第一，安全组织设置和岗位职责不明确；第二，安全风险管控不到位；第三，日常安全运行与维护缺乏有效性；第四，应用系统安全管理有疏漏；第五，灾备管理不专业；第六，企业缺乏内部与针对第三方人员的安全管理规范；第七，企业没有进行必要的安全教育培训。

惠普认为，安全问题在每个环节都有可能发生，关键在于如何创建有效的流程，通过高效的软件工具监控虚拟机的运营，从而避免问题出现。

随着业务的不断增长，企业用户如果不对虚拟环境进行合理控制和管理，很容易出现虚拟机泛滥的情况。虚拟机的泛滥不仅增加了管理的负担，而且造成了现有资源的浪费。惠普融合基础设计架构不仅能通过统一、高效的管理，合理分配现有资源，回收数据中心空闲容量，而且能帮助用户将孤岛式的IT架构转变成池化的，从而实现资源的共享，在提高资源利用率的同时大幅提高IT部门的生产力，使IT部门成为驱动业务发展的核心动力。

更多内容，详见http://blog.cio360.net/b/6_2637_5204.html