服务器虚拟化安全注意事项

服务器虚拟化安全注意事项

从现在起，五年以后，几乎没有一家企业会使用“真正的”计算机。虚拟软件将会截取并模拟数据库、网络应用程序或者文件共享所能进行的一切工作，允许一个机架安装服务器起到 10 台服务器的作用。虚拟化是必然的；自 IP 网络以来，它是 IT 业最重要的新势力。对这一趋势带来的影响，安全专家如果有一种挥之不去的恐惧感，他们应该得到原谅。在内部网络中，虚拟化正重新绘制分布图；硬件以及网络过滤曾经将服务器和应用程序分离，虚拟化可以把它们集中到同一个刀片服务器上。影响深远的变化的到来不会没有安全挑战。

不要让你的企业贮存虚拟化安全

虚拟化使企业有了第二次获得 IT 安全主导权的机会。服务器管理员应当对分期、配置和修复虚拟计算机进行规划。网络管理员也应该进行规划，为了保证访问规则的严格性、以及在物理服务器周边和客户操作系统之间的稳定性。

❖ 服务器虚拟化安全注意事项（一）

要在物理 VM 服务器分段

一些客户机需要处理敏感数据，比如信用卡或者受到保护的健康资料。而其它客户机不需要处理这些。千万不要让这两种 VM 共享相同的硬件。

❖ 服务器虚拟化安全注意事项（二）

不要忽视虚拟化附件服务的风险

除了与网络安全和虚拟计算机有关的问题以外，公司还需要考虑虚拟计算机移动的问题。移动特征是首先使企业对虚拟化感兴趣的理念之一，诸如 VMware 的"VMotion"，它允许 VM 从一个硬件平台跳到另一个硬件平台上，而不会造成故障时间。但是它们会对安全造成严重破坏。

另外，也不要忽视了文件备份。

❖ 服务器虚拟化安全注意事项（三）

慎重选择虚拟化安全产品

虚拟化安全产品市场是一个新兴的行业，必须保持关注。网络安全厂商 Sourcefire 的 CTO 兼 Snort 入侵检测程序的创建者 Marty Roesch 说："这是安全界一个引人注目的领域。人们询问我们可以做些什么。"但是，他提出这样的疑问：对于企业而言，这是否是一场正确的战争呢？

❖ 服务器虚拟化安全注意事项（四）

不要因为虚拟化恶意软件而熬夜

这里有一些不是非常清楚可见、引人注目：即虚拟化恶意软件的威胁。什么是虚拟化恶意软件呢？它就是特洛伊木马 rootkit 软件，可以利用管理程序技术将其隐藏于受感染的操作系统"之上"。虚拟化恶意软件的严酷现实就是无法检测到 rootkits 和 botnets。

❖ 服务器虚拟化安全注意事项（五）

服务器虚拟化安全注意事项（一）

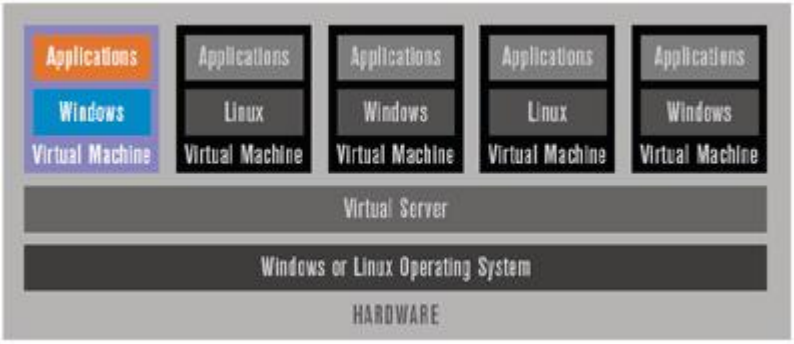
从现在起，五年以后，几乎没有一家企业会使用“真正的”计算机。虚拟软件将会截取并模拟数据库、网络应用程序或者文件共享所能进行的一切工作，允许一个机架安装服务器起到 10 台服务器的作用。

虚拟化是必然的；自 IP 网络以来，它是 IT 业最重要的新势力。

对这一趋势带来的影响，安全专家如果有一种挥之不去的恐惧感，他们应该得到原谅。在内部网络中，虚拟化正重新绘制分布图；硬件以及网络过滤曾经将服务器和应用程序分离，虚拟化可以把它们集中到同一个刀片服务器上。影响深远的变化的到来不会没有安全挑战。我们现在使用的用于促成这些变化的产品，产生还没有十年。

好消息是，虚拟化对于企业安全而言是有利的。修复、分期、配置和变更管理——对于 IT 安全而言，这些是令人感到慢性头痛的工作——在虚拟化的数据中心变得更容易。坏消息是，在虚拟化解决为我们解决这些问题之前，我们还有一些需要克服的挑战。在正常情况下，这里是防止虚拟化隐患的五条注意事项。

不要让你的企业贮存虚拟化安全



企业一般都让 Windows 管理员管理 Windows 安全，Unix 管理员管理 Unix 安全，以及存储器管理员保证 SAN 的锁定状态。如果机构也将从事 VMware ESX 丛集的工作，这种想法是一个致命的错误。

“机构中的虚拟化影响是深远的。”Unisys 的首席安全架构师、虚拟化安全专家 christofer Hoff 说，虚拟化安全把“许多公司搞得措手不及。”他还指出，网络小组正消除配置过程中的拦路虎。只要仅有 VMware 管理员控制管理安全，那么其他任何人都无法参与。给你留下的是一个支离破碎、配置不周的结构体系，其安全仅是事后的想法。

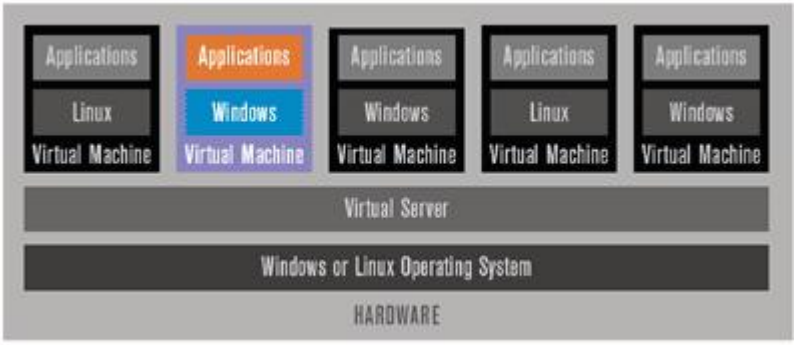
回想 20 世纪 90 年代，那个时候，企业级交换器和虚拟局域网大量涌现。安全方面缺乏合作以及不当的执行计划，给我们今天留下了开放的、毫无控制的网络，这样一旦黑客攻击了服务台的计算机，就会威胁到主机和存储网络。不能让这种情况再次发生了。

虚拟化使企业有了第二次获得 IT 安全主导权的机会。服务器管理员应当对分期、配置和修复虚拟计算机进行规划。网络管理员也应该进行规划，为了保证访问规则的严格性、以及在物理服务器周边和客户操作系统之间的稳定性。安全小组应当有合适的策略，便于审核配置和部署。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）

服务器虚拟化安全注意事项（二）

一定要在物理 VM 服务器分段



一些客户机需要处理敏感数据，比如信用卡或者受到保护的健康资料。而其它客户机不需要处理这些。千万不要让这两种 VM 共享相同的硬件。

为什么分割至关重要，可以询问 Tavis Ormandy。去年夏天，Ormandy 发行一份叫做"iofuzz"的文件，对虚拟化安全进行了深入研究。"iofuzz"是一个工具，可以发现漏洞，尤其是他所测试的虚拟计算机系统管理程序中的漏洞。当谈到虚拟化，他说："x86 很难恢复正常。" 对于 Ormandy 而言，很难把这种观念推广开来：与安全地操作系统内核相比，开发者编写安全的系统管理程序，更为容易一些。这样的话，看起来似乎需要十年多才能锁定 Windows。

系统管理程序漏洞是什么意思呢？其实是这样的：可以访问你的任何一个 VM 的人就可以"越狱"，攻入到主机，并且威胁到其它机算机的安全。这难道不是一个足够充分的理由，让我们务必保证敏感的 VM 与测试 VM 处于分开的硬件上吗？

此外，越狱式漏洞并非问题的终点。考虑一下你为了保护数据中心设置的适当的网络安全机制。或者还是不要，因为当信息流在相同硬件上的客户主机之间的"虚拟交换器"

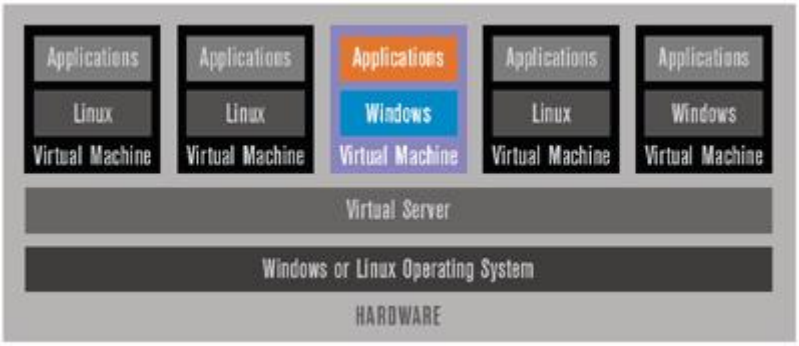
上传输时，所有的网络安全机制均不起作用。Hoff 说：“今天的虚拟交换器尽力复制高可用性的网络安全，确实导致了令人厌烦的性能和实用性问题。”

那您应该做些什么呢？答案从技术上来说是简单的，但是实施起来比较难。企业需要指出其安全域是什么，了解其最敏感的数据是什么。然后，处理这些敏感数据的计算机需要处于隔离的硬件上，不论这样做是不是高效率的。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）

服务器虚拟化安全注意事项（三）

不要忽视虚拟化附件服务的风险



除了与网络安全和虚拟计算机有关的问题以外，公司还需要考虑虚拟计算机移动的问题。移动特征是首先使企业对虚拟化感兴趣的理念之一，诸如 VMware 的"VMotion"，它允许 VM 从一个硬件平台跳到另一个硬件平台上，而不会造成故障时间。但是它们会对安全造成严重破坏。

许多 IT 小组正依赖虚拟计算机，将其作为“虚拟安全装置”，通过虚拟计算机的所有流入和流出应用程序 VM 的信息流都必须指定路由。Hoff 解释说：这就是一个的问题。那些 VM“并不能很好地’被虚拟移动’，因为保护 VM 的程序不能与其一起移动。

这变得越来越复杂。去年，密歇根州大学的一个研究小组在 USENIX 发布了一项报告，演示了对两个最为流行的平台 VMware 和 Xen 中的移动的攻击。其操纵法：当它们经过网络时，立即改写不工作的虚拟计算机。当它们到达其目的服务器时，刚刚还是安全的操作系统就成为秘密的了。

另外，也不要忽视了文件备份。虚拟化软件中的检验点和快速拍照功能促进了生产特殊产品的小型产业的发展，而这些产品可以保证诸如 VMware ESX 系统中流线型文件备份

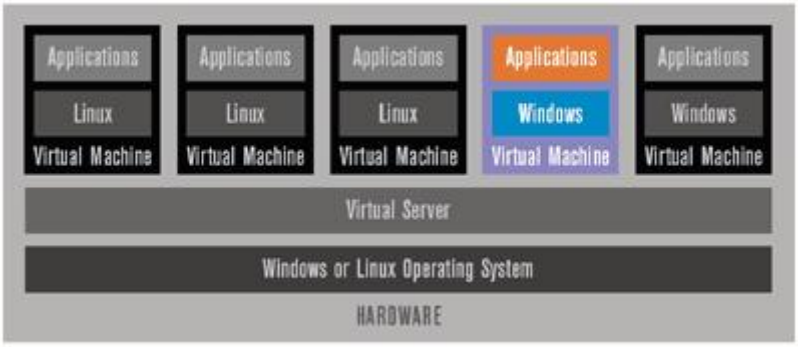
的存储。在 IT 中，再没有比文件备份和灾难恢复更敏感的功能了。它们可以处理大量的受保护信息。确定保你的文件备份厂商懂得这一点。

公司如何才能知道其 VMware 的文件备份是否安全呢？这就应该去问厂商，第三方是否已经测试过了其产品的安全性，如果已经测试过了的话，测试者都发现了些什么？如果厂商跳过了这一步，就会带来灾难性的后果。网络文件备份产品希望得到密钥，登录到你所有的虚拟化服务器中；如果存在缺陷，攻击者可以偷窃到这些密钥，并且有了密钥以后可以进入你公司的每台虚拟主机。买主须自行当心。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）

服务器虚拟化安全注意事项（四）

一定要仔细慎重地考虑选择虚拟化安全产品



虚拟化安全产品市场是一个新兴的行业，必须保持关注。网络安全厂商 Sourcefire 的 CTO 兼 Snort 入侵检测程序的创建者 Marty Roesch 说：“这是安全界一个引人注目的领域。人们询问我们可以做些什么。”但是，他提出这样的疑问：对于企业而言，这是否是一场正确的战争呢？

Roesch 提出疑问：为什么在相同硬件上的客户操作系统之间流动的内部 VM 流量“比交换和访问层中的流量重要的多”？

多少年以来，企业已经尽力在内部网络中设置合适的安全策略。也许，每个虚拟交换器中正确部署安全，这些热心的努力不应该优先于解决实际网络中的安全问题。

Roesch 说：“我不得不问一下，在 200 个服务器刀片中部署安全是否更好一些？或者你的威胁是否来自外部？与在上行线上观测一个相比，传感器单独观测每一个刀片更好一些，好在哪里呢？”

Reflex 安全公司（Reflex Security）是一家虚拟网络安全公司，其工程副总裁 Aaron Bawcom 回答说：由于它更便宜一些，“我们已经了解到客户有许多不同的地址，每

一个都有多个售货点系统，集成到一些处理该地址 IT 基础结构的服务器中。你已经在一千个网页上查看了仅仅配置一个防火墙所需要的费用了吗？”他说，诸如这些配置的花费很高，公司一般会交付信用卡行业审计违规的罚款，而不是重建网络的费用。

Bawcom 希望企业考虑使用虚拟化来巩固分支部门的服务器，而不是为每个分支部门配置硬件。一旦你只管理单一的物理服务器，以及三个虚拟客户机，你就可以通过将网络安全添加到虚拟交换中，来实施网络安全。他说：“有了硬件设备，你不能跨过 ROI 这道障碍。当你将安全虚拟化时，你才可以更多地配置它，即节约了成本，又获得了高质量。”

Roesch 和 Bawcom 达成共识的一方面是安全监测。Roesch 说：“当你在系统管理程序级，配置为虚拟设备时，网络可见性就会增加。因为当你使用工具为你提取信息时，你所获得的信息越多越好。”对于 Bawcom 而言，虚拟化也为管理创造了新的机会，企业可以对其系统有一个全面的了解和认识，并且可以及时返回查看发生了什么变化。

然而，这些优点都不是免费的。Hoff 指出：“虚拟化并不能减少成本，你仍然需要在每个地方配置相同的代理器、相同的入侵防御、相同的防病毒程序。”含义是虚拟环境的灵活性也会受到破坏。他说：“人们要求虚拟安全设备能够屏蔽每一个信息流。仅仅当你认为你已经强制内存和 CPU 消耗完时，十几个 VM 会移动到那个服务器中。很难预测出你需要多少流通量。”

在虚拟安全界，有一个巨头。毫无疑问，最受欢迎的企业虚拟化提供商就是 VMware，而且 VMware 并没有一直处于安全界。VMware 正处于这样的境地：使虚拟化安全成为一个特征，而非一个产品，但是现在，该公司正发出混合的信号。它最近宣布，VMsafe 的最初承诺是为了让第三方经销商更容易地进入到 VMware 管理程序。但是去年，它收购了 Determina，一家很有前途的主机安全公司。现在，VMware 发现自己正在支持一个居支配地位的安全研究小组，这个小组拥有诸如 Alex Sotirov 和 Oded Horovitz 之类的研究成员，这两个人都是漏洞搜索者，而且两人都正忙于从事这项研究工作。

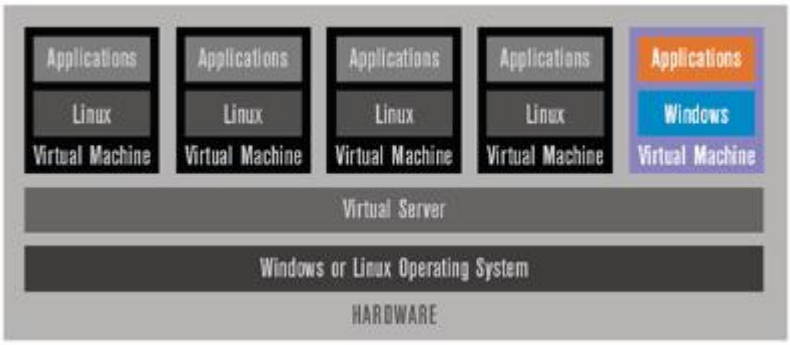
最后，当谈及虚拟化安全产品时，企业需要持有健康的怀疑态度。Ormandy 解释说：“人们仍然相信虚拟化是安全的尚方宝剑，但这并不能反应出当前的实际情况。”虽然虚

拟化安全产品可以为传播更广泛的网络安全领域提供机会，但是企业在实施之前，这些机会应该是清晰可见、引人注目、直接临近的。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）

服务器虚拟化安全注意事项（五）

不要因为虚拟化恶意软件而熬夜



这里有一些不是清楚可见、引人注目、直接临近的：即虚拟化恶意软件的威胁。什么是虚拟化恶意软件呢？它就是特洛伊木马 rootkit 软件，可以利用管理程序技术将其隐藏于受感染的操作系统“之上”。虚拟化恶意软件的严酷现实就是无法检测到 rootkits 和 botnets。

任何谨慎地遵循安全规则的人，可能已经听说了虚拟化 rootkits。正如一个新的故事，它自己表述到：虚拟化现在很流行，并且安全攻击总是可以获得大量的详细信息。但是，在现实的世界中，虚拟化 rootkits 占到问题的多少呢？其问题并不是很多；一般在现实中并不能看到它们。

这样，为什么我们没有看到新一轮的恶意软件利用了虚拟化性能呢？开发概念验证 rootkits 的研究人员可能会辩解：这是由于我们并没有查找它们，或者采用当前的工具，我们是可以找到它们的。但是这可能并非事实。

去年，这个作者与 Root Labs 的 Nate Lawson、以及 Symantec 的 Peter Ferrie，合作共同开发了监测虚拟化 rootkits 的技术。我们发现了如此多的方法可以采用，以至于

我们怀疑追击“无法监测”的虚拟化 rootkits 是最佳策略。该小组的主要研究发现是：在隐藏自己，使得应用程序无法找到方面，虚拟化的确做了大量的工作，并且这足以保证程序正常运行以及精密驱动器持续工作。但是当你仔细观察时，非法的管理程序留下了警告的信号，这种信号很难隐藏。

并非都是好消息。Rootkit 威胁真正存在；它仅仅更可能在应用程序层产生威胁。只有少数几种虚拟化平台可供 rootkit 隐藏；我们可以监测那些平台。但是，有好几万应用程序，每种都可以隐藏 backdoors 和 rootkits。毫无疑问，在虚拟化时代，企业需要保持警惕。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）