IT 安全策略汇总

IT 安全策略汇总手册

随着 2010 年的结束，新的攻击类型已经突破了今天传统的防御措施，这给我们敲响了警钟。因为疏忽，谷歌、Adobe 和 Gawker 在安全方面都打了盹，也都因此付出了代价。在 2011 年，其他企业也将会犯同样的错误，请不要让您的公司成为其中之一。

本文将从三个方面为您提供详细的安全策略，包括：网络安全策略，防范攻击安全策略和系统平台安全策略。

网络安全策略

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。

由此带来的基于网络连接的安全问题也日益突出，如何确保你的网络安全呢？

- 如何通过部署深度防御来规划安全的网络
- 通过 WLAN 测试验证网络的安全性与连接性
- 从路由器入手改善网络的安全性
- Web 安全策略：使用云安全服务

防范攻击安全策略

随着互联网黑客技术的飞速发展，网络世界的安全性不断受到挑战。对于黑客自身来说，要闯入大部分人的电脑实在是太容易了。如果你要上网，就免不了遇到黑客。所以必须知己知彼，才能在网上保持安全。那么如何避免漏洞被利用带来的攻击呢？

- 创建 Java 安全框架 避免 Java 漏洞被利用
- 企业该如何防范攻击者利用多个零日攻击？
- Stuxnet 蠕虫攻击方法简介
- 企业如何避免遭受零日攻击或未知恶意程序攻击？
- 蜜罐技术：如何跟踪攻击者的活动？（上）
- 蜜罐技术：如何跟踪攻击者的活动？（下）

系统平台安全策略

网络操作系统是网络的心脏和灵魂，网络安全性在很大程度上取决于网络操作系统平台的安全性。在网络环境中，网络的安全可信性依赖于网络中各计算机系统的安全可信性，而计算机系统的安全性又依赖于网络操作系统平台的安全性。因此，若没有网络操作系统平台的安全性，就没有各计算机系统的安全性，从而就不可能有网络系统的安全性。系统平台安全在解决网络安全上起着基础性、关键性的作用。

- Linux 服务器系统最佳安全实践
- Windows Server 2008 用户权限管理简介

如何通过部署深度防御来规划安全的网络

深度防御(Defense-in-depth)描述的是利用一系列防御机制来保护计算机网络的理念，这一系列防御机制的组织结构方式是：如果其中某一机制无法正常运行，会有另外一个可正常运行的机制替代它。本文侧重描述一个实用的利用现有技术来部署深度防御的例子，以及探索怎样将它们结合起来，从而构建一个全面、有效的企业网络安全体系。

环境

为了阐述怎样部署深度防御，我们先来考虑下面的一个普通企业信息技术体系方案。许多企业都选择使用第三方作为基础设施托管商，他们这样做是有一些原因的。通过同外部托管商合作，企业可以使传统范围和权力模式（也称为空间出租，colocation）都限制在托管商那里的一个非常安全的平台中，同时还可以自己对系统进行管理，或者从提供商那里购买功能更强大的托管服务，包括网络、系统和安全服务。这种平台通常是为托管一个企业的公共访问系统而设计的，服务范围从企业用户的邮件或文件传输，到企业的电子商务平台。

无论采取配置或托管部署方法，安全性都是这种平台设计中的重要组成部分。典型的为这种平台设计安全体系的方法是从网络开始的，为了便于讨论，我们假设企业将其电子商务平台托管在该工作环境中，该电子商务平台（为了讨论的方面，我们对其进行了高度的简化）包括Web层，它扮演的是各种交易的购物车或是支付途径的角色，这反过来又是通过中间设备（应用服务器）和数据库层来支持的。这种设计需要每个层面都在自己专门网络中进行管理，即虚拟局域网（VLANs），这通常是通过使用类似防火墙一样的过滤设备分割层面来实现的，即将Web服务器设置在低安全接口处，而把中间设备和数据库层设置在高安全接口处，中间设备和数据库层不能从公共网络直接访问。在有些设计方案中，中间设备和数据库层在同样的防火墙接口处，但是在不同VLAN，这种情况下，两个层面之间就不存在网络流量过滤，除非通过开关强制执行。

在这种情况下防火墙可能主要也只是起到对互联网的防御作用。而我们要做的是：利用现有的安全技术，以这种环境平台为基础，实施一个深度防御战略。

实用深度防御

我采取一种"厨房水槽"方式来实施如上所述的环境的安全保障工作，用这种方式，每一部分能够独立于其它部分单独实施，并且能随每个企业的特定具体要求而定。

深度防御刚开始可能面临的难题是由提供商所提供的网络基础设施中的企业平台外部强制引起的。这种技术组件负责保护平台不受分布式拒绝服务（DDoS）攻击，而 DDoS 攻击缓解技术通常由两部分组成：第一部分负责通过监控正常传输流中存在的异样来检测攻击，第二部分负责通过已知的传输行为方式来缓解这种攻击（例如威胁管理系统，即 TMS）。

DDoS 保护是通过近乎即时传输分流来实现的，这种分流采用从核心路由设备到 DDoS 清理中心（TMS）的边界网关协议（BGP）。最有效的 DDoS 攻击缓解方法是通过提供商的基础设备（上游）来实现的，因此链接饱和与增加带宽花费的风险就降低了。

虽然防火墙在防御某些网络威胁时是有效的，但在一些端口对互联网 HTTP（80//TCP）和 HTTPS（443/TCP）开放的托管平台里，防火墙的效果就降低了。在这种平台环境中，再加入一个网络应用防火墙（WAF）以形成一个增强的防火墙体系，这是一个不错的想法。

WAF 主要为保护平台免受一些特定应用型攻击服务，如跨站点脚本（XSS）、结构化查询语言（SQL）注入和参数的篡改。这些设备通常是在托管平台内沿防火墙到核心网关之间的途径配置的，在那里，WAF 起一个桥接设备的作用，具有阻止与已知应用层的攻击媒介相匹配的攻击的能力，同时，它也可以在硬件故障时使打开命令不能执行，这样可以保证传输继续流到网络服务器处。一些 WAF 供应商还提供数据库监控和保护功能，能够处理针对数据库的威胁，保护是通过代理实施，并安装在托管数据库实例的服务器上的。

由于 WAFs 通常侧重于来自应用层的攻击，它们在阻止类似网络蠕虫这样的以网络为中心的攻击时，效率是有限的。WAF 可以用来与入侵防御系统（IPS）配合，这种方式的侧重点是利用基于签名的网络层缓解措施，从而弥补这方面的不足。这些设备可以作为能够与内嵌防火墙集成的模块，在那里即使威胁离开防火墙也能被阻止。

当我们越靠近服务器平台，对深度防御来说，防止恶意威胁与文件系统监控就变得至关重要。这可以通过主流杀毒反恶意软件产品和内容完整性监控系统（CIMS）的结合使用来实现，从而实时跟踪并对文件系统的变化发出警报。

将所有这一系列捆绑起来就形成了一个集中的日志管理系统，除了具有传统的服务器日志功能之外，它还可以储存来自每个安全组件的工作记录。日志管理系统（LMS）除了可以为从各个安全组件查询记录数据提供灵活的搜索界面之外，还可以在预先设定的事件过滤器上产生

实时警报。另外，一系列以日志管理为基础的产品，称为安全信息和事件管理（SIEM）系统，也可以被用在日志管理系统（LMS）上，SIEM 通过提供智能威胁分析和威胁缓解功能而扩展了 LMS 的功能。

组合

正如你所看到的，从提供商的基础设备 DDoS 攻击缓解开始，到防火墙和 IPS 技术对网络的保护，到 WAF 对应用层的保护，再到 CIMS 对文件系统完整性的保护，最后到 LMS 起到储存来自各个安全组件和服务器组件日志信息的作用，我们已经确定了一种具体的、可用于保护企业托管平台每个组件的安全技术。通过实施深度防御，或者只实施其中的部分组件（如 LMS），你的企业将逐步进入一个灵活的、可以提供实时安全威胁监控的安全平台。

（作者：Anand Sastry　译者：Sean　来源：TechTarget 中国）

通过 WLAN 测试验证网络的安全性与连接性

由于 802.11n 技术所实现的速度和可靠性，许多公司正开始使用带宽更大的无线 LAN 来支持新的移动服务。但是这个变化需要进行更复杂和更可靠的 WLAN 测试，以验证网络的安全性、连接性和性能。

公司可以不再需要使用耗费人力的工具来检查信号强度、服务器可访问性和 Wi-Fi 漏洞。测试在地理位置上分散的整个企业网络的成百上千的接入端（AP）和无数的客户端需要使用更高效的自动化工具和方法。

在许多早期的 Wi-Fi 部署中，安全性意味着检查整个建筑物或园区，监听陌生信号，以便发现未授权的恶意 AP。这不仅极为低效，而且经常会"阻碍"许多识别错误的 AP，也会忽视其他的一些威胁，如配置错误和操作不当的客户端。

使用具有无线入侵防御系统的 AP 进行全天监控

随着 Wi-Fi 越来越流行，许多 AP 经过更新后能够监听频道内或频道外的流氓信号。另外专门的 Wireless Intrusion Prevention Systems (WIPS)，也可用于全天监控无线攻击或违规行为，以及响应临时阻挡和发现嫌疑的流氓信号。

然而，这两个方法已经开始融合到一起。许多企业 AP 现在能够在需要时变成专职 WIPS 探测器，而且有几个 AP 供应商也提供了专用的 WIPS 设备。现在争论的重点越来越不在于扫描的频率，24/7 是依赖无线的企业必须要求实现的。相反，合理的安全任务和符合规范要求则占据了核心地位。

集中的 WLAN 评估工具保证了规范性

为了符合像 PCI DSS 或 Federal Information Security Management Act (FISMA) 这样的规范，组织必须证明安全控制的有效性，并记录嫌疑违反规范的情况。现在，许多商业

WIPS 和一些 WLAN 管理器能够根据流行的行业规范产生封闭的规范报告，但是仍然需要持续地评估这些安全性控制和政策。

许多公司都雇佣第三方审计人员到现场执行评估；例如，要在一个商店中验证 PCI DSS 规范。然而，在进行这个审计之前，我们最好先测试一些有问题的地方，然后在它们暴露之前修复 这些问题。理想情况下，这些自我评估应该定期进行，而且不会消耗太多的员工时间，不需要太多的现场调查费用。

这正是集中评估工具发挥作用的地方。例如，AirTight Networks 使用基于云的 WIPS 与上述探测器通信来实现每季度的 PCI 扫描和修复服务。这些探测器会监听邻近的流量，并探测 Cardholder Data Environments (CDEs)的无线漏洞，从而产生 PCI DSS 1.2 规范所要求的月扫描报告（至少）。

对于那些已经部署了 WIPS 的公司而言，像 Motorola AirDefense 提供的无线漏洞评估模块等插件能够将部署的探测器变成远程测试引擎，它们能够周期性地连接 AP，探测暴露的端口和 URL，并生成记录结果的报告。

自动的远程安全性扫描，不管是由本身的 WIPS 执行，或者是云服务实现，都能够实现廉价的常规自我评估。然而，它们并不能替代不定期的人工现场渗透测试。

非自动化 WLAN 测试——渗透测试

查找可能淹没客户端、AP 和 WLAN 管理器的盲点、错误和新攻击是 WLAN 测试的重要组成部分。然而，这种无线测试还没有实现完全的自动化。

例如，MDK3 是一个命令行工具，它可用于猜测隐藏的 SSID 和 MAC ACL，寻找客户端的认证漏洞，并发送 802.11 Beacon、Deauth 和 TKIP MIC DoS 攻击。审计人员可以使用 MDK3 方便地在不同的位置发起这些渗透测试，如办公室内部和外部。然而，诸如 MDK3 等工具绝不应该在工作时间内对生产环境 WLAN 执行测试，因为生产使用需要人工指引和结果解释。

集中的渗透测试工具经常可用于发现影响 WLAN 安全性的较上层的系统漏洞。例如，Metasploit 脚本能够尝试许多不同的有线和无线 LAN 应用程序。如果要对一个大型网络执行更高效的 Metasploit 测试，我们可以考虑 Rapid7 的 Metasploit Pro，它可以从一个中央控制台执行多层次的远程渗透测试。

（作者：Lisa Phifer　译者：曾少宁 陈柳　来源：TechTarget 中国）

从路由器入手改善网络的安全性

路由器往往有不同的角色。例如，一般情况下，一个以太网端口连接到外部网络，四个端口提供到达局域网有线设备的互联网连接，无线发射装置向无线客户端提供访问。无线接口甚至可能提供多种 SSID。

路由器通常都将其特性的诸多方面分离来，但在今年的黑帽大会上，黑客展示了攻击大量路由器的方法及破解路由器的可能性。要理解这个问题，就得从 IP 地址说起。

多数 IP 地址都位于公网，但是有些 IP 地址仅保留给内部网络使用。即，任何人都可在其局域网上使用且仅能用于内部的 IP 地址。这些特定的 IP 地址是不允许用在公网上的。

最常用的内部 IP 地址以 192.168 或 10 开头。例如，一台连接到路由器内部端口的计算机会将路由器的 IP 地址看成是 192.168.0.1。如今，局域网上的大量路由器都可以使用这个 IP 地址，因为它可以保证这个地址不会通过路由器传到互联网上。路由器都有一个默认的内部 IP 地址，路由器的管理员可以将这个地址改为仅能用于内部的任何 IP 地址。

在将路由器用于互联网上的通信时，它还使用另外一个不同的 IP 地址，即公网 IP 地址。路由器的管理员无法控制公网 IP 地址，它是由把路由器连接到互联网的 ISP 提供的。

局域网上的所有计算机看似都拥有同一个 IP 地址。可以认为路由器是所有局域网计算机的"公共发言人"。

这样就出现了安全问题，即路由器无法将公网和私有的特性完全地分离开并保持其独特性。

公网 IP 地址仅能被互联网上的计算机"看见"，而私有 IP 地址仅能被局域网上的计算机看到，无论是有线网，还是无线网都应当如此。

如果这道屏障无法得以维持，那么，互联网上的黑手就有可能登录进入路由器，从而导致整个局域网中的全部设备都遭殃。

为修改路由器的配置，局域网的计算机可以通过 IP 地址来访问。例如，可以键入“http:// 192.168.0.1”，然后键入用户名和口令来访问路由器的配置界面。

通常情况下，仅能根据内部 IP 地址才能访问路由器。这就确保了仅有局域网上的计算机才能更改其配置。

用户访问的每个网站都知道用户路由器的公网 IP 地址。当然，用户的 ISP 也知道。但是，有很多措施可以阻止外部人员登录进入到路由器。

首先，路由器中有一个防火墙，它通常会阻止未经请求的进入通信。此外，路由器有一个远程管理选项，当然，此选项一般是禁用的。

现在，我们就可以理解克雷格.黑夫纳在黑帽大会上所公布的问题了。简言之，他所发现的漏洞准许恶意网页通过公网 IP 地址访问路由器。

应当对基于局域网的计算机进行限制，使其仅能根据内部地址才能访问路由器。由于远程网站可以轻松地知道你的公网 IP 地址，这个漏洞准许恶意的黑客登录到你的路由器。更糟的是，许多人并没有修改其路由器的默认口令。有不少人甚至并不知道路由器还有口令。恶意的黑客随时准备访问路由器的默认口令，并还可以在一定程度上检测你使用的路由器的类型等信息。

在对最初的 30 台路由器的测试中，克雷格.黑夫纳发现有 17 台路由器易遭受这种攻击。

判断自己是否易受攻击

测试自己的路由器是否易受攻击并不麻烦。在此，笔者向您介绍两个网站，用户可以通过 ipchicken.com 或 checkip.dyndns.com 知道自己的 IP 地址。在打开这两个网站后，就会得到一个 IP 地址。如 2.3.4.5，然后再用浏览器打开它，看看有什么发生。如果你得到提示，要求输入用户名和口令，就说明你的路由器易受攻击。如果你得到出现错误的网页，则表明你不易受到这种攻击。

在技术层面上，这种攻击是 DNS 重新绑定问题的新伎俩。它依赖于这样一个事实，即单个网站可以拥有多个 IP 地址。在你第一次访问一个恶意网站时，你的计算机得到了此恶意网站的两个 IP 地址。第一个是合法的，而第二个是非法的，它就是你的公网 IP 地址。此后，通

过高速缓存伎俩和恶意生成的错误，恶意网页会欺骗你的计算机访问恶意网站的可选 IP 地址，实际上就是你的路由器的公网地址。

黑夫纳通过试验进一步得出结论，他认为要让这种攻击成功，并不需要启用远程管理。只要目标网络中的某个用户访问了被恶意控制的网站，这种攻击即可获得成功。这种攻击的发生不依赖于受害者的操作系统，它是针对路由器的。

这种攻击还牵涉到 JavaScript，这种脚本语言通常仅能与其来源网站进行交互。但是，由于有了 DNS 重新绑定伎俩，浏览器会认为用户的路由器是恶意网站的一部分。因而，JavaScript 也就可以操纵路由器了。

捍卫路由器的安全

最简单的防御就是不要使用路由器的默认密码。应当将路由器的密码改为一种难以猜测的序列。

如果用户的路由器易受攻击，应当上网检查，看看制作商是否有了新的固件可以修复这个问题。

任何刚买的新路由器都应当测试一下是否易受攻击，特别是在退货期限内时。

虽然远程管理与此无关，不过，还是建议用户关闭自己路由器上的这个功能。

如果你使用无线网络，不妨检查一下，看看路由器能否限制对有线连接的管理性访问。这条措施可以防止无线用户登录进入路由器。

（作者：茫然　来源：TechTarget 中国）

Web 安全策略：使用云安全服务

如果你从未留意过企业内的 Web 安全策略，那现在就是时候重新审视一番了。可以肯定地说，你的公司有各种部门正在使用 Web 应用和云计算架构或服务，而现在是在他们周围建立安全策略的时候了。

最近的思科系统 2009 年度安全报告指出了做好 2010 年切实计划的必要性。基于云的工具和使用云的生产力软件可能已经在你的公司里应用了，而黑客也已准备好猛扑上去。

传统的 Web 安全主要包括 URL 过滤、HTTP 协议校验和单一登录访问控制。然而，恶意软件作者感染正规网站或者改变域名的速度要超过信誉系统能够适应的速度，这使得 URL 过滤的作用从反恶意软件安全手段变成了保证允许使用策略的强制执行。

协议校验已经被集成进防火墙中，以便在下游系统受到影响之前就在网络边际查出异常流量。而 Web 安全被留给终端，这使更新签名定义和软件功能对 IT 来说代价高昂。

给 IT 的好消息是因特网流量可以通过基于 Web 的安全云重定向，且性能仍可接受。云安全服务可以使处理和管理任务集中化，使得在控制成本的同时将有效的安全扩展到企业更加简单。

入流量可以被检查是否有恶意软件并强制执行经验证的访问控制；出流量可以被检查是否有受限数据以及是否依策略进行了传输加密。从管理上讲，集中的 Web 安全控制可以为新的基于 Web 的应用增加额外的应用层安全，并提高检查能力以达到更好的性能，而不需要把管理的负担大范围分布出去。

Web 安全有多种实现方式，可以将他们混合以适合网络架构的需求。类似微软的 TMG 或者 Check Point 安全公司的 Web 安全软件刀片网关这样的设备很适合支持分公司，或者需要一个专用设备进行高性能过滤的情形。安全云服务，包括趋势科技和 Zscaler 公司等提供

的服务，可以在不需要大规模分发签名来给占用网络带宽的低优先级应用限速的前提下，有效地过滤已知的恶意软件，同时使得所有用户可以立即享有新增的安全功能带来的好处。

企业安全云可以遵循相同的模式。那些希望被阻断的消息和数据存在站内的系统上，而不是在一个安全服务商的数据中心的企业，可能对数据外泄保护功能特别有兴趣。虚拟桌面基础架构项目也给了 IT 一个机会，来以一个独立的安全云的形式来部署安全。IT 团队可以把出去的流量都通过安全产品来路由，以保护业务，而不需要在每个虚拟机或者虚拟的服务器上安装 Web 安全软件。例如，Xceedium 公司允许 IT 对数据中心内的因特网访问进行颗粒状的控制，而 HyTrust 则可以提供对虚拟数据中心内的经授权的用户操作的控制——两者都是将应用和桌面与安全策略执行相分离的重要能力。

在安全团队考虑用 Web 安全云保护业务的可行性的时候，他们也可以考察虚拟化帮助台服务的能力。Citrix 系统公司和 Bomgar 公司这两个公司提供可以轻松从因特网下载的"可降解"的代理软件，使得 IT 可以通过 Web 支持远程用户。这种方式要依靠 Web 安全来降低服务台的运营成本（例如，更少的系统软件更新），并通过更快地解决安全和配置问题来提高用户满意度。在审视将 Web 安全责任赋予安全云的同时，IT 可以通过集中化管理远程支持软件来理顺帮助台运营。

还没有动作的公司应该预留 2010 年的资源来重新审视 Web 安全的趋势、其对业务的影响和满足普遍的 Web 访问安全需求的其它方法。

（作者：Eric Ogren　译者：李博文　来源：TechTarget 中国）

创建 Java 安全框架 避免 Java 漏洞被利用

虽然蠕虫病毒、Zeus 僵尸网络和极光行动是去年的头条新闻，但是据 Krebs On Security 的 Brian Krebs 和微软的 Holly Stewart 最近的报道，针对 Java 的袭击数量一直在稳步上升。正如 Stewart 写道，针对 Java 的攻击和成功攻击的数量快速增加，最近甚至超过了针对 PDF 和其他目标的攻击。

在这篇文章，我们将谈到为什么 Java 容易成为攻击者的目标，以及企业应该如何创建 Java 安全框架，从而成功抵御基于 Java 的漏洞攻击。

Java 的现状

Java 运行时环境（Java Runtime Environment），也称为 JRE 或就简称为 Java，安装在各种不同类型的设备上，包括大多数 PC 机、苹果电脑和 Linux 台式机，以及智能手机和其他嵌入式设备。在这些设备上，PDF 阅读器和 Flash 播放器同 Java 的普及水平相似，但 Java 本身比较特殊，因为它被设计成为可以一次编写、到处运行的环境，包括你可能想不到的嵌入式系统。

Java 既是一种编程语言，也是一种需要安装从而支持 Java 程序运行的软件，它还具有额外的保护（比如说，沙箱（sandboxes）和额外的内存保护），这是其他编程语言没有的，然而最近的攻击却都绕开了这些保护。甲骨文公司凭借收购 Sun 微系统公司从而拥有了 Java，虽然其频繁发布 Java 更新以便控制漏洞，且 Java 本身也包括自动升级功能，但是这个功能并不是那么可靠，无法保证运行的是 JRE 最新版本。另外，苹果公司也发布了自己的 Java 版本，其通常落后于安全修补过程，这就使得 Java 整体的安全问题更加严峻了。

因此，Java JRE 对于攻击者而言，是很有吸引力的目标。Stewart 报告说，在过去一年中，三个 Java 的漏洞累计遭到 350 万次攻击，近 200 万台电脑受到攻击，这使得 Java 成为最易受到攻击的软件之一。

Krebs 报告说，针对 Java 的攻击已经包含到了漏洞利用程序包中，从而允许攻击者可以对该编程语言的攻击进行自动化。另外，使用 PC 机的企业不是唯一应该担心的，最近针对 Java 的攻击有些甚至包括了 Mac 电脑。从事 Mac 安全的 Intego 公司最近报道称，一个恶意的 Java applet 超链接 http://blog.intego.com/2010/10/27/intego-security-memo-trojan-horse-osxkoobface-a-affects-mac-os-x-mac-koobface-variant-spreads-via-facebook-twitter-and-more/被命名为 Koobface，其已经感染了苹果的操作系统。由于缺少 Java 补丁，很多被感染的电脑已经被黑客控制，而最近针对 Flash 或 PDF 的袭击，台式电脑上防恶意软件的安全措施已经不起作用了。不管怎样，要想在网络层上检测 Java 的袭击，对 IPS/IDS 提供商而言已经更加困难了，因为任何潜在的恶意 Java 程序都需要进行运行测试，以检查恶意代码，而这需要耗费大量的计算资源。

企业防御策略

企业可以通过创建一个 Java 的安全框架来减少与 Java 相关的风险。首先，企业应该预判自己是否需要在台式机或者服务器上安装 Java，如果不需要的话，请卸载 Java 或者从一开始就不安装 Java。用户应该只在有应用程序需要时，或台式机需要 Java 程序支持的情况下，才安装 Java。这是基本的建议，因为如果 Java 不存在，它就不可能被黑客进行漏洞利用。

接下来，检查以确保只有最新版本的 Java 安装在客户机上。这些检测可以用企业管理软件、脚本版本检测、或手动访问 Java 下载页面来完成，这将报告已安装的 Java 是哪一版本。以我的经验来看，老版本经常遗留在系统中以保证向后的兼容性，特别是自己编写的应用程序。如果安装了 Java，它可以配置成每天自动检查更新，但是这只对用户可以自己更新软件的家庭电脑有用。企业应该把对 Java 打补丁的优先级同微软或 Adobe 保持一致。对 Java 的一些特定安全选项进行调查也是可取的，用户通过使用 Java 控制面板就可以进行，比如禁止用户给来自不受信任的认证授予访问权限，或检查证书以防止潜在的恶意 Java 程序的运行。你可能还需要启动日志记录，以便发现恶意 Java 程序是否已经运行。如果你的企业使用 Firefox，还可以利用 NoScript 插件的白名单功能来批准 Java 程序，以限制恶意 Java 程序的风险。

结论

过时的 Java 版本所构成的威胁不容低估，Java 补丁应该与微软或 Adobe 更新拥有同样的优先权。甲骨文负责 Java 的更新，如同微软对其产品负责一样，甲骨文应该有同样的标准。所以，如果有可能，你可以向甲骨文公司报告因恶意软件袭击 Java 而引起的任何问题。

企业应该在其客户端系统中增加更新 Java 的优化措施，以防止系统被黑客利用漏洞。他们也应该以此作为警钟，更仔细地评估什么软件应该安装在客户端电脑上，并确保定期更新，防止黑客凭借应用软件来控制系统。虽然这可能还有一场硬仗要打，但这也相应的推动了企业去更好的理解安全，即除了打补丁以外还可以有更多的具有前瞻性的办法，比如使用应用程序白名单功能，从而在第一时间防止恶意软件的运行。

（作者：Nick Lewis　译者：Sean　来源：TechTarget 中国）

企业该如何防范攻击者利用多个零日攻击？

零日攻击：谁容易受到攻击？

鉴于 Stuxnet 如此受人关注，似乎许多系统都被该病毒感染。虽然 10 万个系统不算少，但是与被 Renos 恶意软件感染的百万个系统相比还是小数目。然而，受到感染的系统虽然比较少，但是容易受到利用多个零日漏洞的恶意软件攻击的系统数量却极其巨大（前提是零日攻击的目标为电脑中的多个软件）。

有趣的是，最应该关心多个零日攻击的企业通常是那些已经阻止了其他常见攻击的企业。如果传统攻击技术无效的话，攻击者更可能利用零日技术进行攻击。没有阻止过常见攻击的企业也会受到多个零日技术的攻击，但是他们可能已经被普通的恶意软件入侵过了。

为了确定你的企业是否容易受到此类攻击，请仔细评估现存的安全保护系统，并确定所有的这些保护是否会被最近的零日攻击绕过。企业必须自己进行这些具体的评估，因为它们取决于你系统上的各种保护措施。

注重安全的企业在评估系统和网络时需要了解利用多个零日漏洞的恶意软件，并且要把它们考虑进去。如果系统保护措施相互重叠严重，并且会以同样的方式失败，那么即使安装多层保护也可能无法提供重要的额外安全，反而会增加系统的攻击面，让管理更加困难。

企业对多个零日攻击的防御策略

为了防御多个零日攻击或者有针对性的攻击，企业不仅需要使用杀毒软件、更新补丁、采用基于主机的防火墙等标准措施，还应该考虑部署外围防火墙、基于网络的杀毒监测和阻断、以及入侵监测等，从而防御各种类型的攻击。虽然额外的多层安全在某层失败后可以提供协助保护，但是多层保护并不能真正提供足够的深层次防御。

比如，如果你的企业在台式机、服务器、电子邮件系统以及网络设备中使用相同的杀毒软件引擎，单靠这些杀毒软件监测提供的保护范围可能并不会比只在台式机中安装这种杀毒引擎提供的保护范围大多少。如果不是所有的台式机都安装了杀毒软件，或者不是所有机器中的杀毒引擎都进行了合适的操作，那么使用相同监测引擎的额外层才可能会提供额外的安全保护覆

盖面。在服务器、电子邮件系统以及基于网络的杀毒设备中运行不同的或者额外的杀毒引擎，可以增加额外的零日保护或者恶意软件的监测覆盖面。

如果你的企业担心这类攻击，你可以采取额外的步骤（保护 USB 连接的安全）以防护或者限制攻击。如果不需要 USB 连接，请禁用它们，确保 USB 设备是在安全的配置中使用，确保 USB 设备的自动运行不能攻击系统。禁用 USB 设备之后，请锁定其他的物理安全设置，比如说系统 BIOS。还有，只允许用有效的证书进行软件签名，并与应用程序白名单一起使用，从而防止恶意代码在系统中执行。微软的增强的减灾体验工具包 （EMET）可以为微软软件提供额外的恶意软件保护，防止软件被攻击者进行漏洞利用。只要有可能，企业还应该考虑不要把任务优先的系统连接到通用网络或者互联网上。

总结

Stuxnet 只是使用高级功能和利用多个零日漏洞的恶意软件之一。历史的经验告诉我们，恶意软件和攻击者只需做最少工作的就可以入侵系统，而随着防护水平的提高，攻击者的水平也会相应提高。Stuxnet 以及将来可能利用多个零日漏洞的恶意软件，表明了企业需要仔细评估自己的安全保护措施，并且弄清这些保护是否能够阻断以及如何阻断这种攻击。利用多个零日漏洞的攻击将会更加常见，因为在恶意软件中可以绑定攻击的平台不断涌现，而且在恶意软件中包含新型攻击变得越来越简单了。

（作者：Nick Lewis　译者：Sean　来源：TechTarget 中国）

Stuxnet 蠕虫攻击方法简介

Stuxnet 蠕虫病毒已经引起了媒体的广泛关注，因为这种病毒能够感染多种不同类型的系统。Symantec 公司发布了一篇详细介绍 Stuxnet 的技术文章，并且指出，该病毒已经感染了近 10 万个系统。

Stuxnet 类似于 2009 年 12 月的 Operation Aurora（极光行动）攻击和 Zeus 僵尸病毒，因为它表现出了恶意软件的尖端技术。然而，Stuxnet 更加复杂，主要是因为它能够同时利用多个零日漏洞。虽然通常很难预测未来的恶意软件，但是可以确定的是，Stuxnet 不是最后一种同时利用多个零日漏洞的攻击。在本文中，我们将讨论 Stuxnet 的具体攻击方法，以及企业应该如何防御这种类似的漏洞利用程序。

Stuxnet 是目前世界上最先进的恶意软件之一，因为它含有多种不同的恶意功能。它可以利用四种零日漏洞，其中包括 Windows 打印机后台处理中的一个远程漏洞，以及另外一个具有本地升级权限的漏洞。攻击一个零日漏洞比较普遍，而试图利用多个零日漏洞媒介可以让攻击者更加成功地入侵系统。虽然这是真的，但是对于每个零日漏洞来说可能都存在保护措施，或者系统并不会运行该软件容易受攻击的版本（比如，恶意软件试图攻击 32 位系统，但是最终攻击的却是 64 位 Windows 系统，或者目标系统使用的是另外一种 PDF 阅读器，而不是 Adobe Reader），然而如果恶意软件包括多个零日漏洞攻击，只要其中一个攻击媒介没有受到充分的保护，就为攻击者提供了可乘之机。

攻击零日漏洞的恶意软件并不常见，普通的恶意软件一般针对的是比较老的、没打补丁的常见漏洞以及安全性差的系统，而能同时攻击多个零日漏洞的恶意软件则少之又少。

虽然利用多个零日漏洞可以增加攻击者成功的机会，但是攻击者所带来的破坏跟零日漏洞的数量没有关系。破坏的大小取决于攻击者利用漏洞所获得的访问权限，以及是否能够完全控制整个系统。如果恶意软件能够控制系统，不管它同时利用几个零日漏洞都没关系，因为它只利用一个漏洞入侵系统。一旦攻击者控制了系统，就可以截获数据，使用该系统去攻击其他系统，或者进行该系统可以完成的任何事情。

幸运的是，攻击多个零日漏洞的恶意软件利用了多个攻击媒介，这会增加它被监测到的机会，具体的取决于恶意软件的工作方式。如果多个失败的利用被记录下来，就会引起更多的关

注，因为这可能是一个不寻常的事件。所以，攻击者需要进行权衡，因为他们越是使用多个零日攻击入侵系统，就越有可能被监测到。

（作者：Nick Lewis　译者：Sean　来源：TechTarget中国）

企业如何避免遭受零日攻击或未知恶意程序攻击？

2009年12月，谷歌和其他著名公司受到了未知恶意程序的攻击。这一事件被称为极光行动（Operation Aurora），此次零日攻击是针对当时未发布补丁的IE浏览器漏洞。

极光行动中最严峻的情况是：即使配置了较完善安全资源的组织仍然可能是受害者。如果一些最先进并获得雄厚资金支持的IT安全组织都可以被黑客攻击，那么对那些拥有较少安全资源的小型组织而言，为了保护自身不受这样的攻击，他们的日子将会更加艰难。然而，从极光行动中我们也可以吸取很多重要的教训，在本文中我们将讨论关于该攻击，企业需要了解的信息，以及在今后发生类似的攻击时企业应该采取的预防措施。

极光行动：背景

让我们回顾一下已经报道出来的关于极光攻击以及各个组织应该如何阻止该攻击的一些技术细节。谷歌报告说，它以及至少20家大公司，在2009年12月成为极光行动的攻击目标。谷歌认为这次攻击侵犯了知识产权，其目标针对的是中国人权活跃分子的Gmail账户。

根据极光行动攻击后发布的报告，黑客将IE浏览器零日漏洞及其利用程序与未知的恶意软件绑定在一起发起攻击。某些攻击被黑客认为是成功的，因为被攻击的对象是重要的公司，媒体紧接着就进行了广泛的报道。而高端的黑客技术和比较普通的零日攻击和未知恶意软件结合在一起使用，这一点也被认为是成功的。他们通过在网络通信中使用多层加密，成功地让攻击躲避了安全检测。

极光行动的攻击媒介

虽然IE浏览器零日漏洞及其利用程序本身并不是最高端的攻击，但它可以使攻击者完全控制受害者的电脑系统，这一点已在极光行动中被证明是成功的。然而，如果攻击者想成功做到这一步，还需要提高其登陆帐户的访问权限，或者由攻击者凭借漏洞利用程序去获得较高的访问权限。当已登陆的用户只具有普通用户访问的权限时，一些恶意软件将感染系统，但却不容易接管系统。很多组织不必允许所有用户都具有管理员级别的权限，因为该类权限可以进行应用程序安装、更改配置以及其他一些没有限制的操作。然而，当攻击者找到了可以提高系统

权限的途径，那么就没有办法去阻止黑客滥用这些权限了。而通过只为用户提供必要的访问权限，可以使漏洞更难被成功利用。

过去从未出现过的恶意软件是相当常见的攻击媒介，经常被普通的网络罪犯用来做一些可以马上得利的事情。在这次极光行动攻击中，黑客获得了一些知名度很高的账户。虽然发起极光行动的直接动机尚不清楚，但从长远来看，敏感数据是具有价值的，最起码可以作为一个监视的战术。

预防类似极光行动的攻击

尽管这些攻击方法很令人烦恼，但也有很多方法可以防御它们，以确保类似的攻击不会成功。刚开始的时候，你可以选择使用非 IE 的网页浏览器或者其他操作系统，从而避免 IE 浏览器零日攻击，这依赖于你的环境可承受的危险等级，部署的深度防御安全控制有多少，以及对攻击者的价值。然而，使用非微软的软件可能会让管理更复杂、更耗时（最终产生的费用也相当昂贵），因为它们往往需要依赖于你的环境、应用程序补丁以及基础设施结构，这是一个明显的缺点。

另一种可以抵御攻击的方法是通过确保 DEP 生效，从而使得 IE 运行在被削减的权限之下，尽管这种措施据称也已经被漏洞利用程序绕过了。DEP 是用于阻止来自非可执行存储位置上的可执行代码的攻击，这在理论上会使攻击者更难使用类似极光行动中的攻击来控制系统。另外，IE8 也提供了额外的保护措施去对抗这种类型的攻击。

多层加密或者代理服务器可以用来隐藏被控制电脑的网络通信，并使通信的源头不被检测到。为了能发觉和终止这样的通信，网络连接需要被监控，特别是那些从公司网络向外的连接。但这种监控可能会因为外部连接的多样性而变得没有效率，但是监控从系统流出的特定非正常的大型数据也是可以辨别电脑是否被控制的一种途径。一个经验丰富的组织或许也会想到用防火墙来划分它的网络，从而限制攻击者从一个部分跳到另一个部分。

为了确保类似于极光行动的攻击不再发生，组织应采取一些基础的信息安全措施。公司需要评估他们的网络并确定最高风险在哪，然后运用合适的防御措施去应付这些风险。比如说，在谷歌最初的声明中，该公司推荐企业使用知名的反恶意软件工具，勤打补丁以及定期升级浏览器。

对所有组织而言，本文所谈到的方法并不都是适用的。每个组织在防御攻击之前都需要进行基础的部署。通过深度防御策略，将类似攻击的影响降到最小，从而更好的避免零日攻击完全控制目标电脑，并防止其通过隐藏而免于被检测。

（作者：Nick Lewis　译者：Sean　来源：TechTarget 中国）

蜜罐技术：如何跟踪攻击者的活动？（上）

你们中的许多人可能对专业术语"蜜罐（honeypot）"和"蜜网（honeynets）"比较熟悉。虽然从严格意义上讲，有人可能认为它们是安全研究人员的工具，如果使用得当，它们也可以使企业受益。在本文中，我们所使用的"蜜罐"和"蜜网"表示的是同一个意思，蜜罐一般试图模拟一个更大更多样化的网络，为黑客提供一个更加可信的攻击环境。

蜜罐是一个孤立的系统集合，其首要目的是：利用真实或模拟的漏洞或利用系统配置中的弱点（如一个容易被猜出的密码），引诱攻击者发起攻击。蜜罐吸引攻击者，并能记录攻击者的活动，从而更好地理解击者的攻击。蜜罐一般分为两种类型：高交互蜜罐和低交互蜜罐。

类型和折中

高交互蜜罐是一部装有真正操作系统（非模拟），并可完全被攻破的系统。与攻击者进行交互的是一部包含了完整服务栈（service stack）的真实系统。该系统的设计目的是捕获攻击者在系统中详尽的活动信息。而低交互蜜罐只是模拟出了真正操作系统的一部分（如，网络堆栈、过程和服务），例如模拟某个版本的 FTP（文件传输协议）服务，其中的代码存在漏洞。这可能会吸引蠕虫查找服务脆弱部分的漏洞，由此可以深入观察到蠕虫的行为。

不过，在你使用这两种蜜罐时，需要做出一些折中。用于网络安全的高交互蜜罐提供了真实操作系统的服务和应用程序，使其可以获得关于攻击者更可靠的信息，这是它的优势。它还可以捕获攻击者在被攻破系统上的大量信息。这一点可能会非常有帮助，比如说，在组织想要收集关于攻击者是如何找到攻破特定类型系统的详细真实数据，以便增加适当的防御的时候。另一方面，这些蜜罐系统部署和维护起来十分困难，而且需要承担很高的副作用风险：例如，被攻破的系统可能会被用来攻击互联网上其他的系统。

虽然低交互蜜罐容易建立和维护，且一般对攻击者产生了免疫，但模拟可能不足以吸引攻击者，还可能导致攻击者绕过系统发起攻击，从而使蜜罐在这种情况下失效。到底部署哪种蜜罐取决于你最终的目标是什么：如果目标是捕获攻击者与系统的详细交互情况，那么高交互蜜罐是一个更好的选择；如果目标是捕获针对某个有漏洞的服务版本的恶意软件样本，使用低交互蜜罐就足够了。

在你决定使用哪种蜜罐部署时，另一个需要考虑的重要因素是：蜜罐是安装在物理系统上，还是安装在物理系统的几台虚拟机上。这将直接影响到系统维护的工作量。虽然虚拟系统自身的确有一系列安全问题，但虚拟系统允许快速回复，并能显著缩短部署和重新部署的时间。

（作者：Anand Sastry 译者：Sean 来源：TechTarget 中国）

蜜罐技术：如何跟踪攻击者的活动？（下）

蜜罐部署

无论是高交互蜜罐还是低交互蜜罐，都被设计成在互联网上不进行传统目的活动。换句话说，除操作系统要求的以外，蜜罐系统不运行其他的进程、服务和后台程序。这种思想实际上把所有与蜜罐有关的交互作用都当作具有恶意活动嫌疑的对象，这样一来反而有利于检测攻击活动。在探讨蜜罐部署的最佳做法之前，先让我们来看一下常用的高交互和低交互蜜罐。

通常情况下，高交互蜜罐不需要专用软件就可以进行底层操作系统的安装。一般来说，安装一个 VMware 工作站或者用一个类似 QEMU 的虚拟机，就足以满足蜜罐对操作系统的要求了（典型情况是，主机上的客户操作系统运行虚拟软件）。底层操作系统安装好后，下一步的重点就是进行设置，以对蜜罐（客户操作系统）进行合理的监测。这一设置要分为两部分：监测主机操作系统和监测客户操作系统。主机操作系统应该重点对进出蜜罐的流量进行抓包，这一过程可以利用像 tcpdump 或 Wireshark 之类的程序来完成。同时，如果客户操作系统被感染，恶意带外连接会造成潜在的附加危害，对这一情况用户希望提前被警告，这也被叫做挤压检测（extrusion detection）。这一点可以利用类似 iptables（或者基于主机的防火墙）的本地访问控制列表来完成。执行带内过滤实质上是对蜜罐所受攻击的类型实施部分控制。用户可以把主机操作系统流量过滤和入侵检测系统（例如 Snort）结合起来，从而获得针对已知攻击媒介的附加报警能力（也就是基于签名的报警）。

对客户操作系统，或者是攻击的实际目标进行监测，需要捕捉到攻击者的所有活动，比如跟踪键盘记录活动、记录攻击者所用的工具和记载权限扩大尝试。Sebek 就是一款能够完成上述大规模数据搜集活动的工具。另外一些值得关注的虚拟化高交互蜜罐还有用户模式的 Linux 和 Argos 系统。

与高交互蜜罐不同，低交互蜜罐需要在主机操作系统上安装特殊的软件，另外还要进一步配置，以便有效地模拟有缺陷的服务。较受欢迎的低交互蜜罐技术有 Nepenthes，以及后续产品 Dionaea 和 mwcollectd。

低交互蜜罐创造性地配置了多种检测功能，包括广泛记录功能、恶意软件捕捉功能、实时安全事件通知，以及提交恶意软件活动进行远程分析。它们的功能还可以进一步提高，方法是使用 Nepenthes 中的 log-IRC 附加模块，通过 Dionaea 和 p0f 模块一同使用还可以获得被动识别远程操作系统的能力。Dionaea 同样支持 XMPP（可扩展消息现场协议）模块，该模块可以在企业之间和安全社区中实现恶意软件二进制共享，从而提高用户的安全意识。

笔者接触过一些与高交互蜜罐监测有关的部署最佳实践，这些实践中执行了带内和带外的过滤，以及网络入侵检测。这些功能有待于增强，还需要强化蜜罐和正常网络之间的隔离。理想的情况是，蜜罐环境应该部署在自己专用的互联网入口上，而主机的操作系统管理则放在另一个独立的网络上。另一方面，低交互蜜罐无法被攻击者全部攻破，因此它们的保护工作要简单一些。利用 chroot 之类的程序，可以把低交互蜜罐系统隔离到一个较小的文件系统中。另外，低交互蜜罐系统也要与正常网络彻底隔离，否则低交互蜜罐仍旧会暴露在与高交互蜜罐相同的威胁下。

典型应用

蜜罐的主要用途之一是收集恶意软件样本。这些样本可能利用零日漏洞（zero-day vulnerabilities），或已知的攻击向量。蜜罐可以让研究者对上述攻击有更好的了解。例如，通过监测 IRC 控制通道，蜜罐就可以提供实时攻击流量。它们还具备被动识别攻击者操作系统类型，或存储/重演攻击活动的能力。另外，它们允许研究者共享威胁信息（例如 XMPP），或者把样本提交给在线沙盒和多反病毒扫描工具（如 VirusTotal、Jotti、ThreatExpert 和 CWSandbox）进行进一步分析。

蜜罐收集恶意软件活动的领域可以扩展到僵尸系统（bot）和僵尸网络（botnet）。僵尸网络拥有分布式的特点，依赖于远程命令通道的使用（一般是通过 IRC 和 HTTP），利用的往往是零日攻击或已知攻击向量，这种体系结构使得蜜罐可以很好的对其进行跟踪和分析。

对企业而言，蜜罐的实用性远大于上述情况。然而，蜜罐的有效性很大程度上取决于能否有一个好的设计。任何设计缺陷（比如，不充分的隔离、缺乏监测和实时报警能力）都可能把蜜罐变为严重的负债，而不是可以对危险进行管理的资产。使用蜜罐时，适当的小心和谨慎很必要。如果你没有充足的经验却希望使用蜜罐，那你就需要时常向训练过的专业人士咨询。

（作者：Anand Sastry　译者：Sean　来源：TechTarget 中国）

Linux 服务器系统最佳安全实践

维护一个企业级的安全的计算环境需要设计策略和过程从而使得对系统和数据的未授权访问降至最低。为了保护基于 Linux 的计算机资产免于这些威胁，像许多其它以安全为核心的过程一样，你必须知道你想保护什么以及别人可能会如何尝试获取访问。成功的安全管理是心态。也就是说，像坏孩子那样思考。

在本文中，我们将会讨论基于 Linux 的服务器系统的风险评估。

确保你的 Linux 服务器系统安全的第一步是正确地评估所面临的风险。只有这之后企业才能部署一套有效的防护措施来预防、侦测，并且如果需要的话对于可能发生的违规正确地做出反应。

首先，辨识需要保护的 Linux 资产。资产可能包括硬件、软件、数据或像 email 或 Web 站点主机这样运转的服务。每个资产都具有价值，要么是货币价值要么是未来可能带来收入。

接着，辨识每个资产面临的潜在威胁。威胁可能来自组织的内部或外部。一些内部威胁只不过是偶然的，但是有些可能是恶意的。

对于资产的威胁依赖于攻击的动机和攻击者如何获得对资产的访问。动机可能是纯粹的挑战，伤害资产的拥有者，或是为了谋利。攻击者可能想访问你的数据或只是拒绝合法用户的访问。每个威胁都有被利用的必然的可能性，这通常与资产的价值相关。虽然在组织内广泛地了解和变化会有困难，但是使用一个风险管理框架来给每个辨识的威胁分配一个可能性，会帮助你对缓和这些风险需要采取的行动进行优先级安排。

尽管不可能列出所有潜在的威胁途径，但一份最常见风险的概述能让你开始自己的风险评估。

最棘手的威胁途径是用户。尽管有各种的保护机制，人们仍然会被愚弄或被要挟做出不恰当的行为。用户的意识、培训和访问权限是缓和任何 Linux 风险的重要部分。

密码在任何计算环境中经常代表着最常见的软肋。为了辨识不安全的登录密码，运行如 John the Ripper 这样的密码有效性检查器。应用和数据库的密码也应该检查"可被破解性"或

是进行修改以便满足这样的需求。同时，辨识 Linux 服务器上不需要的访问授权。例如，如果密码文件（/etc/passwd）被远程地分发（通过 rcp/rcopy 程序或 NIS 服务），用户可能会对从未使用的服务器具有登录访问权限，从而创造了毫无好处的潜在的威胁途径。

另外一个主要的威胁途径是网络。任何能访问你的本地网络（物理的或是无线方式）的用户有可能试图连接到网络上任何其它的资产。所有的 Linux 系统运行开放的网络端口，并等待来自网络查询的程序。每个这种服务都代表者一个威胁途径，要么通过欺诈的认证，或是由于软件瑕疵可能错误地允许访问。使用 netstat 命令来找到系统所有的开放端口。

使用 Nmap 工具扫描网络上其它机器的开放端口。每个开放端口代表着一个威胁途径，应该被关闭或是监控非法的访问。不要忽视任何传统的拨号访问点。防火墙是可信网络和不可信网络（如因特网）之间的边界。你的防火墙应该配置只在已知和需要的端口上传输数据。防火墙传输数据的每个端口同样都是一个威胁途径。

除了正常的监控以外，你还应该同时检查日志来关联需要的访问。Lastlog 命令显示用户的登录信息。可以在路径/var/log/messages 下发现各种各样的日志信息。许多应用和数据库也提供记录机制来追溯用户的访问。检查这些日志，你可以观察当前谁在使用和（可能）需要访问特定的资源。

无论什么复杂的软件都是有缺陷的，但是只有当缺陷以不受欢迎的行为表现它们时才会被了解。通常的 bug 只会破坏数据或是引起宕机，但是有一些会造成无法预料的后果，比如允许未授权的访问。这明显地表示为主要的危害。攻击者不断地搜索着这些类型的 bug，而厂商们则在发现这些 bug 时，尽力快速地修补它们和提供软件补丁。你所能做的是确保定期地检查和更新你的操作系统和应用软件。

检查 Linux 服务器上软件更新的过程依赖于应用或是 Linux 版本。例如 Ubuntu 版本的 Linux 提供一个更新管理器（通过菜单"系统>管理>软件源"可以发现），可以配置每天进行检查更新。你越经常性地检查更新，你的漏洞窗口越小。同样对于来自未校验来源或作者的免费程序或软件要小心谨慎。

需要监控和保持更新的最重要的软件是面临外部环境的软件，如 Web 服务器和网络应用（如 VPN 或 SSH）。Web 服务器软件定期地检测糟糕的配置和 bug。Web 应用可能会遇到恶作剧的输入数据来进行不正当的应用。大多数的 Web 应用语言，像 Perl、Python、Ruby 或 PHP 有工具或可用的附件来净化输入数据以及禁止用户输入的代码，如 SQL 或 Java 脚

本。你的 Web 服务器或是其它面临外部环境的应用接收来自用户的数据都意味着可能的威胁。同样，检查这些程序产生的任何日志文件有助于你辨识合法和非法的访问。

(作者：King Ables　译者：Odyssey　来源：TechTarget 中国)

Windows Server 2008 用户权限管理简介

几十年来，大型机和服务器一直使用"超级用户"和"用户"这种用户控制方案。这种方案存在一个明显的安全问题：它需要防止普通用户获取非法访问权限。

在 DOS 电脑以及随后的 Windows 操作系统中，访问控制模式更加复杂。早期的 Windows 操作系统不能在同一台机器上设置不同的用户权限；所有的行动都需要超级用户执行。但是，Windows NT 系统最终定义了管理员角色和用户角色，尽管在实际情况中大多数用户还是需要超级用户的访问权限来执行他们平时的操作。

今天，许多企业的业务模式都要求大范围（地理位置上的）的联合操作，Windows NT 中简单的特权/非特权用户管理功能已经不够用了。意识到这一趋势之后，微软在 2009 年开发了 Windows Server 2008，该系统具有以多级权限属性系统为基础的多层次管理模式。该模式可以限制标准用户，让他们只能用非特权的形式运行应用程序软件，只留给他们操作所需要的最小管理权限，从而改进了微软 Windows 的安全性。比如，服务台用户只能改变其他用户的密码。通过这种方式，大型企业中的用户管理权限可以受到限制，操作中的超级用户数量减少。在本文中，我们将讨论一下如何使用 Windows Server 2008 对权限分配进行控制。

域上的权限管理

在 Windows Server 2008 环境中，有两种政策：活动目录（AD）全局域政策以及本地服务器安全帐户管理器（SAM）注册表政策。AD 利用它的目录架构来控制任何给定 Windows 服务器域（支持通用安全政策的一组服务器）的组权限。这使得 AD 可以对域中的所有用户帐户执行公共帐户权限管理。

当有新的 Windows 服务器添加进来时，他们会连接到活动目录，活动目录会检查所有的组政策对象（Group Policy Objects，GPO）——用户能够执行的应用程序和服务——并把这些权限链接到该目录下的 Active Directory Users and Computers（活动目录用户和计算机）分支中的域根用户。然后 AD 把这些定义的、默认的权限传递到新服务器上，开始管理其用户。AD 目录下的组织单元（Organization Unit，OU）分支也可以定义，人们可以用

OU 为计算机创建本地帐户政策。比如，服务台 OU 可以定义一系列全局政策，帮助服务台人员执行具有公共权限的活动。

Windows Server 2008 的活动目录还引进了一个新的功能，叫做多元密码政策(Fine-Grained Password Policy)，其中包括一个锁定政策。有了这个新功能后，公司可以在同一个域中对不同的用户使用不同的密码和锁定政策。这个功能出现之前，整个域中只有一个政策。为了充分利用这个功能，活动目录管理员必须创建一个新的对象，名为密码设置对象（Password Settings Object，PSO）。他或她可以在 PSO 中设定同样的密码最长期限、复杂度要求、锁定阈值，等等。然后，PSO 会连接到一个活动目录组：组的范围为全局（Global）（不是本地（Local 或者通用（Univeral）），组的类型为安全（Security）（不是分布（Distribution））。所有的组成员都会继承链接到该组的 PSO 中定义的密码和锁定政策。

本地多级控制

域上的全局政策配置完成以后，人们就可以在单独的 Windows Server 2008 系统中通过用户权利分配（User Rights Assignment，URA）功能定义本地权限。用户权利能够控制用户在计算机上执行哪些任务。这些权利包括登录权限和特权。登录权限控制哪些人有权登录到计算机上，以及他们如何登录：通过网络还是本地，作为批处理工作还是作为服务登录。特权则控制计算机和域资源的访问，并可以覆盖特定对象上设定的权限，比如备份文件和目录、创建全局对象、调试程序等等。这些特权由系统 URA 对象下的组政策（Group Policy）进行管理，而且两种用户权利都是由管理员分配到组或者单独用户，作为系统安全设置的一部分。请注意，管理员应该尽可能地通过分组来管理本地权利，确保与企业政策的一致性以及最小化单独系统中权限管理的困难程度。

为了访问本地 URA 对象，添加、删除或者修改权限，管理员必须在 Windows Server 2008 中用 Windows 控制面板打开本地安全设置（Local Security Settings）。他或她可以在左边看见一个树状目录。点击本地政策（Local Policies），然后选择用户权利分配（User Rights Assignment），就能够编辑所有的 39 个登录权利和权限了。

确保适当的权限

Windows Server 2008 中有九个审计政策，分成两个子类，它们可以确保 Windows 管理员正确设置用户权限。安全团队可以在计算机中打开本地安全政策（Local Security

Policy）控制台，进入 Security Settings\Local Policies\Audit Policy 目录，查看系统审计政策设置。下文简要地描述了每个政策，以及它们的用法：

- **审计帐户登录事件**——跟踪所有试图用域用户帐户登录的活动，不管这种尝试源自何处。开启这项政策以后，工作站或者成员服务器会记录所有使用计算机 SAM 中存储的本地帐户的登录尝试。
- **审计帐户管理**——用来监视用户帐户和组的变化，对管理员和服务台工作人员的审计活动有参考价值。该政策记录密码重置、新创建的帐户以及组成员和 Active Directory 控制器的变化。该政策还记录域用户、域分组以及计算机帐户的变化。
- **审计目录服务访问**——提供 Active Directory 中对象变化的低级别审计跟踪。该政策跟踪的活动与审计帐户管理事件中跟踪的相同，但是级别低很多。使用这个政策可以识别用户帐户的哪些领域或者任何其他 Active Directory 对象被访问过。审计帐户管理事件可以提供更好的用户帐户和组的监视维护信息，但是审计目录服务访问是跟踪 OU 和 GPO 变化的唯一途径，这对于变化控制来说很重要。
- **审计登录事件**——记录本地计算机上的登录尝试，无论使用域帐户还是本地帐户登录。在 Active Directory 域控制器中，该政策只记录访问域控制器的尝试。
- **审计对象访问**——处理 Active Directory 之外所有对象的访问审计。该政策可以用来审计任何类型的 Windows 对象访问，包括注册表键值、打印机、以及服务。（注意：如果服务器的对象太多，该政策可能会大大影响该服务器的性能。）
- **审计政策变化**——提供本地系统中重要安全政策的变化通知，比如系统审计政策的变化；当本地系统是一个 Active Directory 域控制器时，该政策会提供信任关系的变化。
- **审计权限使用**---跟踪 Security Settings\Local Policies\User Right Assignment 目录下本地安全政策（Local Security Policy）的用户权利活动
- **审计过程跟踪**——跟踪每一个被执行的程序，不管该程序是由系统还是最终用户执行的。它还可以决定程序运行的时间。结合该政策，加上审计登录事件和审计对象访问事件，以及在这些不同的事件描述中使用 Logon ID, Process ID 和 Handle ID 等，我们就可以详细地描绘出用户活动了。
- **审计系统事件**——与安全相关的系统事件综合，包括系统启动和关闭。Windows 的安全基础设施是模块化设计，可以利用微软和第三方供应商提供的新型、插件安全功能。这些插件可以是认证软件包、合法登录进程或者通知软件包。因为这些插件是值得信赖的扩展操作系统的代码模块，Windows 加载每个插件时都会做记

录，使用从这个分类中的事件。（注意：不推荐在这个层面上管理审计政策，因为这样会产生很多噪声，应该使用子类型。）

即使有些用户偶尔得到了不必要的权限，这些政策也可以让公司的安全人员核实这些用户是否利用管理权限做伤害公司的事情，不管是有意的还是无意的。企业应该尽可能多的启用这些审计政策，但是请记住，加载所有的政策可能会影响 Windows 系统的性能。

当启用这些政策时，企业有多种选择：可以让它们产生成功事件，失败事件或者两者都产生，这取决于公司政策。所有九个审计政策都可以产生成功事件，某些政策可以产生失败事件，作为一种最佳实践，企业不该忽略成功事件（会产生大量的安全日志）而只开启失败事件。一个常见的误解是：只有失败事件审计政策才能警告安全团队注意所有的可疑活动。实际上，安全日志中许多最重要的事件是成功事件，比如关键用户帐户和组的变化、帐户锁定的变化，以及安全设置的变化等等。

总结

随着 Windows Server 2008 的发布，微软最终提供了权限管理功能，能够创建复杂的用户权限分组，却不需要复杂的管理技术。但是复杂的权限分组可能会引起权限的错误配置，不能识别某个人的错误。所以，了解与该功能相关的审计服务同样重要。

归功于适当的考虑和规划，Windows Server 2008 最终赋予企业期待已久的功能：成功地匹配了用户的能力和权限。这不仅满足业务需求和信任要求，而且验证了他们的方法是正确的。

（作者：Randall Gamby 来源：TechTarget 中国）