安全补丁管理指南

安全补丁管理指南

补丁管理已经困扰企业很多年了，而且还将被继续讨论。随着技术的进步和攻击者对漏洞攻击方法的开发，电脑安全的管理在维护业务架构的完整性上越来越重要了。作为一种提前的主动行为，安全补丁管理是保护企业电脑架构的防御前线。

补丁管理是使电脑和现有的软件产品开发的更新保持一致的人、程序和技术。安全补丁管理是关注减少安全漏洞的补丁管理。

安全补丁管理分步指南：简介

安全补丁部署分步指南

本部分详细分步解释如何配置安全补丁，这个过程包括安全补丁测试阶段、实际补丁部署阶段和配置后的检查阶段。过程中都包括了配置的注意事项以及安全补丁的评级等标准。

- 如何准备安全补丁测试
- 安全补丁的测试和部署
- 安全补丁的审定和核查

安全补丁管理的争论

你有两种基本方法来实现补丁应用的自动化。补丁可以从一台中央服务器发给各个不同的客户机系统，或者由客户机与中央服务器联系并下载补丁。哪一种方法更好?是前者

更有效率还是后者更有效率?补丁的跟踪管理应该使用手动方法呢还是应该选择第三方产品呢？

- 补丁管理之争：主动发布与客户下载
- 补丁跟踪管理：手工还是自动

安全补丁配置方法

安全管理对于中小企业非常重要,然而时下的可以自动操作和管理补丁程序的工具还不足够满足需要，本文介绍一下先进的安全管理配置方法以及在没有活动目录和 SMS 的情况下如何配置补丁。

- 安全配置管理：先进的打补丁法
- 没有活动目录和 SMS 只能手工部置补丁?

安全补丁管理分步指南：简介

补丁管理已经困扰企业很多年了，而且还将被继续讨论。随着技术的进步和攻击者对漏洞攻击方法的开发，电脑安全的管理在维护业务架构的完整性上越来越重要了。作为一种提前的主动行为，安全补丁管理是保护企业电脑架构的防御前线。

补丁管理是使电脑和现有的软件产品开发的更新保持一致的人、程序和技术。安全补丁管理是关注减少安全漏洞的补丁管理。它不是对严重紧急事故作为反应的防御程序。已经发生了这种事件，但是安全补丁管理应该首先是保持环境安全可靠的主动程序。作为一种函数过程，安全补丁管理确保所有验证软件采用了更新，并由此评估环境中的漏洞以及减少电脑被攻击的风险。

这篇指南解释了如何成功的配置安全补丁，包括安全补丁测试阶段、实际补丁部署阶段和配置后的检查阶段。

(作者：Felicia Nicastro 译者：Tina Guo 来源：TechTarget 中国)

如何准备安全补丁测试

为确保成功地对安全补丁进行测试，企业一个组织应首先完成以下骤：

1. 了解安全补丁中的文件、功能函数和操作。为确保所有的用户组（比如服务器组，应用组和桌面组）都充分地理解安装补丁所造成的影响，负责补丁管理的人员应回答以下问题：

- 补丁解决什么问题？
- 会影响哪些系统会造成什么影响？
- 会影响对哪些文件有影响？
- 应用补丁的系统是否需要重启？
- 应用补丁的软件是否需要重新运行？
- 这一补订本是否有卸载功能？
- 如果安装或是卸载补丁的过程失败，如何保恢复系统？

这些问题及其解答，与所计划部署的补丁的细节应记录在案。这将为组织留下了安装补丁的原因、时间、地点的审记记录

2. 根据严重性对补丁进行评级和优先级排序。表 1 显式了如何依据标准则对补丁进行评级，并为每个级别提供了推荐的应对时间和最迟的应对时间。一些组织偏向于用颜色而不是用数字进行标记,。因而,每个等级对应的颜色也列在每一行中。当补丁发布一个补丁后，可用这个表确定它的等优先级。当然，如果组织环境中已经存在被攻击的系统了有了一个与它的环境相符的等级系统时，也不需用这个表就不适用了。

表 1 补丁的评级标准

优先级	表示优先级的颜色	标准	推荐应对时间	最迟的应对时间
1 危急(Emergency)	红色	易受攻击,攻击已出现,其他组织正在受到该问题的影响	6 – 12 小时之内	12 – 18 小间之内
2 关键(Critical)	橙色	易受攻击,但未发现漏洞利用	48 小时之内	2 周之内
3 紧急(Urgent)	黄色	已出现攻击技术,但难以实施	1 周之内	2 周之内
4 严重(Important)	绿色	已出现攻击技术,但难以实施,且危害性很有限或很小	1 个月之内,根据易受攻击的程度,配置新的 service pack 或更新,其中包括对漏洞的修补	2 个月之内进行升级
5 通知(Informational)	蓝色	没有攻击技术	3 个月之内,根据易受攻击的程度,配置新的 service pack 或更新,其中包括对漏洞的修补	5 个月之进行升级,或是不进行任何处理

3.在组织中启动变更控制过程或是流程程序。变更控制程序过程是一组有记录的步骤，以确保所有的变更在安装在系统或和设备上之前都必须通过验证。每个组织都应在事先准备好一个其中的所有用户组都遵守的有文档记录的变更控制流程。变更管理确保系统的修复发生在可控环境中。在收到发布的补丁后即有可能启动变更控制过程的情况下，在测试补丁和准备部署补丁之前完成变更控制过程非常重要。根据补丁的严重等级，启动不同的变更控制过程的执行是依据于补丁的严重等级。比如，如果补丁的严重性等级为危急(Emergency)或是“红色”，应实施与其对应版本的快速的变更控制过程以确保在所要求需的允许时间内完成补丁的安装。

在一个变更控制系统中维护的补丁信息提供了所需的审计记录。当一个补丁通过正在这一流程中时，它也提供了报告这一补丁状态的方法。当完成这些步骤后，就可以进入测试阶段了。

(作者：Felicia Nicastro　译者：Tina Guo 来源：TechTarget 中国)

安全补丁的测试和部署

为测试安全补丁建立与产品环境完全一致的复制环境非常困难，因而测试阶段问题最多。这些问题可以是由经费、环境中的多种多种的操作系统或应用程序引起的。

测试安全补丁

根据安全补丁所要修补的漏洞和补丁中软件功能的不同，它可以影响到系统的很多不同的部分。 因而，部署补丁的过程需要包含测试，且每个计划部署的补丁都要进行测试。测试的目标是确保部署补丁后，系统的操作和应用不受影响，且业务不受干扰。为达到这一目标，在部署之前至少必须满足以下的前提条件，且满足之后将其记录下来：

- 测试环境可以最大程度地模拟目标平台
- 补丁软件成功地传输到目标测试平台上
- 补丁软件安装在目标（测试）平台上，且没有明显问题
- 目标（测试）平台上以往的功能性操作在安装补丁之后照常运行
- 如果出现问题，补丁可以成功删除

如果没有满足任何一个条件，在部署补丁之前都要对易受攻击的系统进行额外的测试。可能需要进行多次重复工作，以确保成功的部署补丁，并降低对受影响的系统带来负面影响的风险。

部署安全补丁

安全补丁成功通过测试之后，就可以进入实际的部署阶段了。部署补丁必须以这样一种方式进行，这一方式必保证部署过程可重复，具有连贯性，可追踪状态，有错误记录。这一过程通常由补丁管理工具实现。现有很多种可选的补丁管理工具，组织应选用最适合其环境的工具。补丁管理工具的管理员、服务器管理员或是桌面用户组，依据他们在补丁

管理流程中所规定的角色和责任进行补丁的部署。每个人在补丁管理中的角色和责任，在部置补丁之前应事先定义好。

一些测试条件受限的组织，在将补丁部署到整个系统之前，先将补丁应用到一个pilot用户组做为试点。如果使用这一方案，补丁程序需要在做为试点的这些系统上运行足够长的时间以确保没有出现任何问题。只有经过了预先规定的考查时间，且这些部署了补丁的试点系统运行良好，显示补丁成功部署之后，补丁在其他设备或是节点上的全面部署才能提到流程中来。

这一试点方案也适用于受影响的服务器。不同的是，应首先在非关键的服务器上打补丁，并试运行。同样，只有经过了预先规定的考查时间之后，才可以在所有受影响的服务器上安装补丁，其中包括最关键的那些服务器。

当所有的系统中都安装了补丁之后，对补丁管理工具负有责任的个人或是用户组需要向他们的团队报告补丁部署的状态。

(作者：Felicia Nicastro 译者：Tina Guo 来源：TechTarget中国)

安全补丁的审定和核查

这一系列文章的最后一部分解释如何完成安全补丁管理过程的核查和检查回顾阶段。这两个阶段与安装补丁的测试和部署阶段同样重要；当然核查和回顾检查主要是由流程驱动的，而不是补丁。

核查补丁的实施

软件安装的复杂性迫使将部署过程和核查过程分离开。部署阶段，根据安全补丁管理工具的反馈信息判断成功和失败。核查阶段涉及到检查相关文件、软件版本和注册表信息与已经起作用的补丁是否相符。补丁的核查必须使用检查补丁特定功能的方法。核查过程主要由工具执行，除非工具无法完成相关任务，那时就需要手动由人工进行检查。

用于部署补丁的补丁管理工具需要具有监测已安装补丁的系统的功能。它也要检查安全补丁是否已正确地安装在系统中，如果工具完不成这样的任务，这个组织需要设计手动一种人工的方法或是一个子程序过程完成这一任务。补丁管理工具需要记录哪些系统已安装补丁，哪些没有。如果一个系统文件或是应用程序的文件被改动，并导致该系统又变得易受攻击，补丁管理工具应标记出这一系统并再一次在该系统上重新安装补丁。

检查顾补丁状态

变更控制过程，可以是一个工具、一份报表或是一个表单，在每一步完成之后都应更新。同样，需要生成一个报告记录每一个补丁的状态。这些报告可以是基于 web 的，并且由补丁管理工具驱动，或是出自于组织中使用的变更控制系统。这一报告用于回顾阶段，并且应发送到相关的人员手中，比如补丁管理团队、IT 人员等。

做为报告的一部分，补丁管理团队需要收到以下信息：

- 成功安装补丁的系统数目

- 补丁安装失败或是补丁安装没有完全成功的系统数目
- 失败原因的总结及后续措施
- 有关重启系统的报告
- 没有参与整个安装补丁过程的系统数目，这一信息通常以异常报告的形式提供
- 介绍这些系统没有安装补丁原因的总结
- 补丁有效性的报告

补丁管理过程需要生成关键性能指标（Key Performance Indicators，KPIs）。KPIs使组织可以衡量补丁管理的成功程度并评估结果。补丁管理的KPIs包括：

指标	描述	原因
没有通过质检测试的补丁数目	在这一测试环境中没有通过质检测试的补丁数目	表示计划可能不充分，或是开发过程中可能存在问题
产生事件报告的补丁数目	没有成功部署补丁，影响了用户操作	表示计划可能不充分，或是测试和质检过程存在问题
成功和未成功实施的补丁数目对比	提供一个表示平均有多少新补丁成功实施的指标	表示计划不可能不充分，或是测试和质检过程存在问题

补丁管理团队或是补丁管理的负责人，需要经常的分析这些报告，并且使用报告中的数据和KPIs回答以下的问题：

- 这一过程的有效性如何？
- 失败率是不是较高，原因何在？
- 可以对补丁管理过程的哪些环节进行改进？

定期地将这些信息用于改进补丁管理过程，以确保这一过程的准确性、有效性和保障组织财产安全的能力。完成整个过程的这一最后阶段确保这一组织的补丁管理具有主动性。

（作者：Felicia Nicastro 译者：Tina Guo 来源：TechTarget中国）

补丁管理之争：主动发布与客户下载

使用补丁修复操作系统和应用软件的漏洞是一件繁重的任务。在 2004 年，平均每一天要出现 100 多个新的安全漏洞，使测试和应用补丁的工作实际上成了一种专职的工作。

补丁管理过程必须说明如何和什么时候获得补丁以及在你的 Windows 环境中使用补丁之前进行哪一种测试。如果这些过程发生交叉，你必须决定如何最有效率和最有效地应用和安装这些补丁。

你有两种基本方法来实现补丁应用的自动化。补丁可以从一台中央服务器发给各个不同的客户机系统，或者由客户机与中央服务器联系并下载补丁。哪一种方法更好?是前者更有效率还是后者更有效率?这个答案根据环境不同而有所不同。

主动发布补丁

根据你的网络配置和你的补丁服务器和网络基础设施的强大程度，你可以从主动发布补丁(Pushing patches)中受益。

支持者:从中央服务器主动发布补丁能够更有效地管理补丁应用的时间安排。这种方式应用补丁在工作时间不会对网络的性能产生影响。而且你能够对企业的不同部门的机器和网络的不同部分采取分部分或者分时间的应用补丁的方式不会使网络带宽或者服务器处理器达到饱和状态。

反对者:要把补丁主动发送给客户机，补丁服务器必须要有最新的补丁储备或者客户机的名单。这个名单中没有记录的新设备或者漏掉的设备可能收不到发来的补丁，即使在补丁应用过程结束之后也仍会存在安全漏洞。要保证这种使用补丁的方法的有效性，需要执行某些程序或者工作流程确保设备一增加到网络中就立即添加到清单中，或者频繁地定期对设备清单进行更新。

下载补丁

对于分布式环境来说，补丁服务器必需同子网连通并且通过防火墙连接到每一台客户机，在这种环境中建立一个客户机能够从服务器下载补丁的应用方法也许更有效。补丁服务器可以放在中央的位置，甚至可以放在所有的客户机都能自由访问的隔离区。客户机可以同补丁服务器联系并且下载他们需要的补丁。

支持者:补丁管理软件和登录脚本可用来启动客户机与补丁服务器之间的通信。注册表和其它按键可用来识别需要补钉的客户机的身份和那些不需要补丁的客户机。对网络进行设置，让客户机自动与补丁服务器联系以便确定它们对补丁的需求，并且给需要补丁的客户机安装补丁。这样可能更有效率，可能比主动发布补丁的效率更高。

反对者:使用登录脚本的不利因素是要保证用户确实根据正常的规则重新启动机器并且登录，以便获得新的补丁。如果所有的用户都在同一时间登录，网络带宽可能由于补丁的安装而达到最大的程度。

主动发布补丁和下载补丁的工具

有些补丁管理应用程序只提供一种方法，或者是这种方法或者是那种方法。而 St. Bernard 公司的 UpdateExpert 或者 Shavlik Technologies 公司的 HFNetChk 等最佳的解决方案能够同时应用这两种方法。你可以根据你的网络的特点考虑补丁应用问题，评估每一种方法的支持意见和反对意见，然后选择一种方法，或者把两种方法结合起来。这将使你网络更有效率。拥有许多漫游用户或者计算机有可能关机的用户的网络选择下载

补丁的方法会更有效，这种解决方案能够保证用户得到他们需要的补丁。

(作者：Tony Bradley 来源：TechTarget 中国)

补丁跟踪管理：手工还是自动

任何管理员的最乏味但是却最重要的任务之一就是跟踪补丁--无情的洪水般涌来的软件升级、安全补丁和修订的操作系统组件。你不仅必须了解都发出了什么补丁，而且还要了解“谁使用了什么补丁”和“谁仍然需要使用补丁”。

一个明智的管理员可以创建一个补丁数据库，跟踪已经使用和需要使用补丁的机器和应用程序。制作这种数据库大体上有三种方法(按效率排序):手工;第三方软件;微软自己的 Windows 管理规范(WMI)和组策略对象(GPO)。

手工补丁跟踪

这是最明显的方法，但是，也是最乏味和最不准确的做法。这项工作无非就是做详细记录，可以在表单上做，也可以在关系数据库中做。但是，这项工作需要严格和耐心。如果你仅处理定制的应用程序和第三方程序，这些程序都没有像 Windows 那样的管理规范，手工跟踪也许是惟一的选择。

如果你选择手工跟踪补丁，详细记录是很重要的。你需要为每一个补丁建立一个清单:

- ✧ 补丁发布的日期
- ✧ 修改的号码
- ✧ 这个补丁解决的安全问题
- ✧ 哪个用户和机器收到了这个补丁
- ✧ 任何已知的或者值得注意的副作用，或者与其它产品的冲突

最后一点是非常重要的。如果你有厂商的文件说明任何已知的副作用，记下来并且保证收到补丁的用户不要受到影响。另一个重要的细节是这个补丁取代或者替换的其它补丁。例如，考虑一下 Windows 服务包相互取代的情况。最后，如果这个补丁很小，并且你

正在使用一个软件能够把这个补丁粘贴为一个文件的附件，你甚至还可以把这个补丁放到文件中保留起来。如果做不到这一点，加上一个内部网的链接或者网站的链接也是很好的。

MyITForum 网站有很多脚本。管理员在做补丁管理的时候可以利用这些脚本。一个快速而有效的脚本是“GetPatchList”。这个脚本能够生成本地或者远程机器的所有补丁的列表，这些机器可通过 WMI 列表显示出来。

用第三方产品进行补丁跟踪

第三方产品减轻了补丁管理的许多痛苦，能够让一个人使用一个工作台对整个机构的计算机使用补丁的状况进行检查。

在这个领域长期保持第一位的产品可能是 Gravity Storm 软件公司的“Service Pack Manager 7.1”。这个软件能够扫描整个网络并且确定哪一台机器需要(或者已经使用了)什么补丁。这个软件还有高级的报告生成功能和规则过滤功能，允许你根据某些配置文件测试你的系统是否需要使用补丁。也就是说，你可以提问，“这个机构的所有的 Windows XP 电脑是否都要使用 SP2?”。这种询问方式更容易处理补丁与软件产品之间的冲突。你可以过滤掉可能存在问题的电脑。这个服务包管理软件还支持微软为 SQL Server 和 Windows 媒体播放器等非操作系统产品提供的补丁。但是，对于非微软产品，这个管理软件还不支持查询的功能。

使用 WMI 和 GPO 跟踪补丁

要保持非微软的软件程序处于最新的更新状态，可考虑使用基于 WMI 和 GPO 处理补丁的其它产品。使用基于 WMI 的产品能够让管理员简单地列出将要发布的补丁列表，确定那些机器需要这些补丁，然后让 GPO 处理其余的机器。不需要扫描或者推动更新，这对于拥有数千台台式电脑的机构来说很有帮助。这是本文介绍的三个解决方案中最畅通无阻的解决方案，不过，这个解决方案需要做更多的工作来提高效率。

DesktopStandard 公司的“PolicyMaker Software Update”就是一个这种软件。这个软件是用一个组策略客户端扩展功能(微软 GPO 的一个标准的附件机制)让系统确定它是否需要更新。有疑问的补丁可能是微软的补丁、拥有自己的元数据的第三方补丁或者你自己制作的不符合特定模式的补丁。这个软件还有一些规则，允许补丁自动地相互替换。这个功能是使用 GPO 跟踪补丁时的做法，手工操作是办不到的。

(作者：Serdar Yegulalp　来源：TechTarget 中国)

安全配置管理：先进的打补丁法

对许多中小企业而言，安全管理就是指设置防火墙并在每个月微软的“Patch Tuesday”补丁日后进行必不可少的修补。时下可以自动操作和管理补丁程序的工具很多，但这些工具还不足够。

保持终端安全并不仅仅涉及到确保充足的打补丁。中小企业的 IT 职业人士们同样需要确保设备中的数据安全受到保护，并且确保与经授权的应用软件相关的组织政策等一致。例如，你可能想关掉 Skype 或者不想让用户在工作或某些特定时间使用网络邮件。

第一代补丁产品并没有提供需用来实施这些方略的间隔尺度水平。它们全部是一些关于扫描电脑、确保采用最新的补丁软件以及电脑正常运行等方面的内容。现在一种叫做安全配置管理(SCM)的工具正在迅速成熟起来并能够处理许多诸如此类的问题。

安全配置管理(SCM)产品可以对台式电脑的整个生命周期进行管理，并且它们集成了许多传统台式电脑的管理功能，比如软件分发、打补丁以及资产管理。

在 SCM 代理器中将会加入更多的其他功能。反病毒以及反间谍软件工作这些新增功能明显提供了更多的杠杆作用，并且为管理那些在典型的设备中运行的其他形形色色的代理器减轻了负担。

最终，你会尝试着增加你的运行环境的安全性并且使管理流线型化。是否听起来就如同你有一块蛋糕并准备吃掉它？ 确实，而且为了该特权你将付出代价——很可能通过你的鼻子。但随着市场的成熟，价格会下降，正如这些经常发生的那样。

因此谁是这个市场中的一些参与者？那些专家和通才照常会是其中的参与者，他们已经在奋力进入该市场了。那些专家包括 BigFix Inc.、配置软件公司(Configuresoft Inc.)、沙利克技术公司以及补丁链公司。其中一些是从做补丁服务开始的并已经增加了

其性能，然而其他的一些公司是从系统管理以及终结安全问题等开始做起的。无论怎样，随着那些Big IT(微软， 惠普公司， IBM， CA)逐渐意识到对把资金拿给那些Big Security(赛门铁克公司以及迈克菲公司.)感到厌烦，这些公司将会很快成长起来。

当谈及Big Security时，两个反病毒了领导者已经收购了一些公司以进军安全配置管理领域。赛门铁克公司已经拥有了许多能够解决部分问题的产品(企业级安全策略管理ESM以及BindView)，并且最近还收购了Altiris公司以增加并加固终端管理容量。迈克菲公司收购了Citadel安全系统公司以及Preventsys公司以把这些公司的性能整合到其全保护(Total Protection suite)中来。

当然，你是明白他们所指的已获技术是什么意思的。除非进行实质性的整合，事实上并非如此奏效。因此我们将继续拭目以待更多与终端安全相关的进展和整合。由于需要八个到十个代理器来做这些工作比较荒谬，因此巩固这些性能就成为必要，而且这些现象正在发生——尽管很慢，但这是肯定的。不管怎么说，安全配置管理已经成为强有力的终端安全平台的又一个特征。

(作者：Mike Rothman 来源：TechTarget中国)

没有活动目录和 SMS 只能手工部置补丁?

问：如果你没有活动目录或 SMS，但需要在一百台以上的台式机上部署微软的补丁，什么是最简单的办法？

答：有几个用于 Windows 的补丁管理工具。这些工具包括 Configuresoft、PatchLink、St. Bernard 软件公司、Ecora、BigFix 和 Shavlik 技术公司的产品。Shavlick 公司开发了微软基线安全分析器中使用的 HFNetChk 扫描引擎。这家公司推出的 HFNetChkPro 补丁管理工具的基础版本主要面向不需要定期扫描和电子邮件支持等高级补丁管理功能的中小企业。

如果你在寻找免费的“Windows Hotfix”补丁工具，你可以看一下由 Michael Dunn 编写的“Windows Hotfix 检查器”(WHC)软件。这个软件是 HFNetChk 扫描引擎的前端软件。WHC 运行 HFNetChk 扫描引擎，捕捉其输出的数据并且创建一个需要安装的热补丁的报告。WHC 能够扫描一台本地计算机、远程计算机或者一个整个的 NT 域。在 Windows 2000 和以后版本中，这个软件还能够扫描一个 IP 地址或者一段 IP 地址。一旦你扫描到必要的热补丁，WHC 还能够从微软下载这个补丁。WHC 详细的热补丁报告还包括指向微软安全公告和每个热补丁的知识库文章的链接，因此找到不能直接下载的正确的热补丁网页是很容易的。最后，一但你下载了必要的热补丁安装程序，WHC 将替你运行这些安装程序。

热门补丁经常是连续性的，也就是说你安装每一个补丁之后不需要重新启动计算机就可以一次安装多个补丁。WHC 使用微软的 QChain 软件支持这个功能。然而，验证你要安装的热补丁是不是连续性的是很重要的，因为这个功能对于不使用“update.exe”作为安装程序的产品更新是不起作用的，如 Windows 2000 和 Windows XP 的 IE 浏览器升级程序。一旦安装了升级程序之后，你可以使用 Qfecheck.exe 工具软件验证你的计算机是否安装了你要安装的全部补丁。

(作者：Michael Cobb 来源：TechTarget 中国)