

企业内网计算机终端软件补丁管理系统的研究与设计

蓝海燕

(浙江安远检测技术有限公司 浙江省金华市 321000)

摘要: 本文概述了企业内网计算机终端软件补丁管理的基本流程,分析了企业内网计算机终端软件补丁管理存在的三个问题,分别是补丁方案冗余低效,补丁记录缺失,补丁的实施风险高。最后结合实践探讨了关于企业内网计算机终端软件补丁管理的应用设计方案,patch Manager Plus 可以提供所有的功能用于修补漏洞,ManageEngine 的补丁管理解决以及使用补丁管理软件的最佳实践,以供参考。

关键词: 企业内网; 计算机终端软件; 测试补丁

1 补丁管理的基本流程

企业信息化时代的到来,促使 IT 技术成了企业信息系统应用管理工作中的常客,这也导致各企业在业务经营方面对企业信息系统的依赖度更高。PC 机是信息系统的基础构成,它的作用主要是保证 PC 机能够安全运转成企业网络,另外,病毒和漏洞相互结合的同时,诸如 CoderRed、SALSlammer、Blaster、Nimda 等蠕虫严重威胁到了全球网络安全。而导致出现这种情况的主要原因在于应用了操作系统及应用程序漏洞,与此同时,安装补丁是最终能够消除漏洞的根本办法。

只要能很好地解决补丁问题,基本也就等同于给企业网络安装了一道防火墙,然而对于一家稍具规模的大中型企业来说,由于 PC 机的使用数量多且具体应用到的软件复杂性高的缘故,安装补丁的过程并没有那么容易。那么怎样才能保证补丁安装的有效性,以及如何管理好补丁,也成了各企业在 IT 维管工作中需要面临的首要问题^[1]。

当前在企业管理工作中,甚为流行的企业管理补丁流程为,现状分析→补丁跟踪→补丁分析→部署安装→疑难处理→补丁检查六步,补丁管理的运行周期长且循环往复,所以这六个环节又会促成一个环状的流程,这其中既包含了事件驱动工作,也包含例行工作。在此环节综合虑及补丁工作本身的积极性、持续性、严密性,且又虑及补丁可能影响到业务之处,一般在大规模的企事业单位中营运效果往往也比较好,具体情况如下:

现状分析,在此环节若要在某企业中做好其所对应的补丁管理工作,第一步要先分析信息资产、IT 系统环境和信息资产重要等级及 IT 网络环境,目的就是为了方便下个环节可以针对企业所对应的补丁找到合理的

措施。

IT 环境,与系统管理员及网络管理员进行讨论,最终明确于企业安全策略当中目前用到的操作系统类型或版本,应用软件的类型及版本,网络设备的类型或版本,同时也包括对应的补丁版本,以及从未打的补丁出现的原因和补丁的补救方法。

测试补丁,即便软件开发商发布补丁之前就已经测试过了补丁,但这样的测试往往不够充分,结合实际看来,时下一些软件开发商为克服一些安全问题,基本都会尽最大限度地压制补丁的测试时间,且由于不同企业均具备隶属于自身的特殊性应用环境,所以一般补丁又欠缺稳定性,容易诱发各种未知的问题。对此要求我们一定要结合企业实时应用环境做好补丁测试工作,目的是为了测试补丁处于特定企业环境下的兼容状况^[2]。

测试补丁需要重点考虑到测试环节的广泛性、针对性,这样不仅可以确保在结合实况的条件下充分测试。尽量保证测试环境包含企业各种应用,尤其部分核心应用,便于正确分析出该应用对补丁造成的影响。

进行补丁测试时首先要获取到安全、可靠的补丁软件,一般来说,推荐由软件开发商网站获取,倘使在补丁支持校验的条件下,同样需要对其进行安全校验,目的是为了校验补丁的可靠性,避免一些用户恶意篡改补丁。例如, sun 企业就在 2002 年 5 月份打出了数字签名的补丁。

假如测试环节出现了问题,则必须要认真分析,找到问题发生的具体原因,还要及时解决问题。如果在无法解决问题的状况下则一定要认真记录问题发生的环境,重复验证之后,经确认假如着是测试环节出了问题,则需要及时给厂商反馈。

待提交变更之后, 需要组织领导评审小组(由安全专家、系统管理员组成的组评小组)正确评审具体变更的必要性、补丁推行计划以及风险等。待通过评审之后, 再交由管理员或者业务代表按照不同系统的业务实况商议决定变更的时间, 最终明确各系统的变更计划。待全权明确变更计划之后, 需要交由各系统管理员提交各自的变更请求, 最重完成系统变更, 此间要将变更过程中提交的问题记录下来^[3]。

补丁检查, 为明确实际补丁安装的实况, 要求对安装系统要进行全面检查。假如此过程用到了工具, 则可用工具完成全网检查, 或者采取漏洞扫描的方式同样可以完成检查。另外自行编写脚本或采取人工抽查的方式也可以。按照以往的经验总结, 鉴于服务器大都是由管理员统一进行管理的, 故补丁安装状况较好。而由于桌面系统大都是用户自行维护的。因此时常会遇到各种补丁未打的情况, 致使企业内部问题不断凸显, 蠕虫滋生。

待结束此补丁管理周期之后, 实际工作由于蠕虫爆发的缘故, 往往需要增加一些流程, 并且配合防病毒技术人员以及网络管理人员一并处理。

前述即为企业内网补丁管理的基本流程。

2 企业内网计算机终端软件补丁管理存在的问题

2.1 补丁方案冗余低效

此为大多数企业都要面临的问题, 对于企业而言, 其通常在 IT 架构中储存了大批量源自各厂商的业务系统或软件产品。且在持续发展业务及外部法律条例的过程中, 相继也会部署一系列新的解决方案。针对此类源于各个厂商的业务系统, 很多企业都会采取许多套不同的补丁分发方案。

比如, 对于某中等规模制造企业而言, 已经部署了基于 Red Hat Linux 操作系统的许多台应用服务器, 且该服务器同样是运行在 Java 技术 ERP 系统之上的, 于企业内网应用到了 Microsoft 活动目录及 Windows 操作系统, 另外又部署了一套网络版本的 Symantec 防病毒软件在设计部门的客户端。所以, 为保证可以将补丁程序及时分发至此业务系统上, 一般要求企业 IT 部门要制定多套补丁升级方案: Red Hat Linux 服务器借助由 Red Hat 供给的 RHN 实现补丁升级服务, 然后 ERP 系统又会以开发商现场维护的手段完成实时的补丁升级服

务, 再者设计部门客户端 CAD 系统又借助补丁离线升级的手段, 除此之外, 该企业 IT 部门又于内网中架设了一台 Microsoft WSUS 服务器用于完成所有 Windows 系统的补丁分发工作, 不仅如此, 内网还运行着一台 Symantec 防病毒管理升级服务器。

如前所述, 该企业在运行过程中同时采取了多套补丁分发方案, 虽然足以达到现有的 IT 补丁升级需求, 但在许多套方案同时运行的过程中, 恰恰难以将其整合成为一个统一的企业补丁管理流程, 这就使得企业无法有效提升当前现有的补丁分发方案。就在更多企业相继加入企业 IT 架构的同时, 同时应用多套补丁分发方案, 除了会进一步提高当前补丁分发环境的复杂性和维护难度系数以外, 同样在持续抬高企业用于 IT 架构维护及补丁管理的开支, 从而加重企业 IT 部门的负担。

假如企业可以结合安全策略方面重制定一个崭新的、更全面的且更加便于操作的统一性补丁管理策略, 则如果将多套补丁分发方案合并起来, 往往更有助于减小或者消除某些弊端^[4]。

2.2 补丁记录缺失

如果企业 IT 部门在采取手工或是自动化的补丁分发工具, 在业务系统上安装了补丁程序以后, 大都不会记录下是否安装成功的信息。即便当前大多数 Windows 操作系统自动化补丁分发方案多数都具备了带有补丁安装结果的记录功能, 但综合整体企业来讲, 大部分企业 IT 架构当中的业务系统及软件产品补丁安装记录基本都为零, 仅部分比较核心的服务器及软件产品对少量补丁程序安装做了记录。

事实上, 对于企业 IT 部门来说, 经常会遇到诸如以下案例状况: 虽然企业内网已经提前部署了一套自动化的补丁分发方案 Microsoft WSUS, 但只要一遇到发布一些定期或临时性的补丁程序时, 便会有该补丁分发方案自动由 Microsoft 补丁发布站点补丁, 经分类之后便能够朝企业内网所对应的软件系统推送相应的补丁程序。一般来说, 此补丁流程自部署环节伊始最佳, 一直持续性平稳运行, 并未出现大碍。某日, 企业 IT 部门接到许多来自其余部门用户求助电话, 其内容基本都倾向于自身系统在完成最新补丁的自动安装之后, 便相继出现了系统反应慢、持续性重启、开机无法登入系统等问题。为此, 部门用一段时间给用户现场做技术支持, 但问题

依然未得到解决，直至最后于 WSUS 服务器上禁止使用其补丁的自动分发功能，且在对用户系统产生影响的基础上，将已经安装升级的补丁程序进行了卸载。后来发现，此原因是于两个月前由于某补丁程序出现软件冲突最终未完成安装所致，但当前的补丁程序则要求要在之前补丁系统支持的基础上进行安装，因此现有的补丁程序反复性安装之前补丁程序，用户系统也在这时终止响应。

很明显，假如企业内网 IT 部门能灵活掌握 IT 架构中的系统补丁安装程序装配结果，则基本就可以避免前面案例中出现的问题。

2.3 补丁的实施风险高

对于企业来说，在采取手工或自动化的补丁分发方案时，一般都没有提前测试补丁程序当前的 IT 架构兼容性，所以，在一些核心系统上面安装补丁程序的过程风险性恰恰都很高。

于电商企业而言，IT 架构中最关键的组成内容当属用户和交易数据后台数据库系统的储存，然而此数据库系统服务延时与停机却很大程度上影响到了本企业的业务以及商业信誉。假如在这时此数据库生产系统开发商推出新的补丁程序，则企业 IT 部门是否需要升级该数据库系统？这个问题对于 IT 部门来说，听起来比较有难度——假如及时安装补丁程序，则大概率上可能遭遇软件兼容性问题，最终延长此数据库系统的服务时间，也可能导致停机或丢失很多价值较高的数据；但如果不及时安装补丁程序，又或是禁止安装补丁程序，即便后期企业业务能够持续开展，也会因为受到恶意软件及非法用户使用威胁而带来补丁程序补漏洞侵入风险。所以，经过一番权衡利弊之后，一般企业 IT 部门都会提前安装补丁程序，但是显然，此必然会抬高企业在面对业务高价值数据或补丁安装程序时的风险。

企业 IT 部门分发或安装补丁程序前若能了解既有的补丁程序及当前的 IT 架构兼容性状况，则往核心业务系统上装配补丁程序必然就能排除高风险。然而，或因不同企业 IT 架构的构成或是 IT 部门技术能力存在差异性，因此如果要求企业自行架设测试补丁环境程序往往没有任何现实性可言，此对于企业来说或者也可以于小规模生产环境中尝试使用补丁程序，或者是委托第三

方机构提前测试评估补丁程序的兼容性，以便于更好地把握核心系统上使用新的补丁程序，同时尽可能地降低并消除新的补丁程序及业务数据带来的风险。

3 企业内网计算机终端软件补丁管理应用设计方案

一般不同的管理软件其功能也都不同，而且鉴于各个企业差异化的需求集，对于大部分组织来说均渴望在补丁管理软件当中找到一些共同特性。此要求于各主设备操作系统上使用补丁，其包含 Windows、Linux 及 Max。

3.1 Patch Manager Plus提供

Windows 修补程序管理：Windows 自动化修补程序可以有效降低安全风险，并于短时间内完成漏洞修复。

Mac 补丁管理：自一个控制台出发往各个 Mac 端点完成补丁的部署与管理。

Linux 补丁管理：根据 Linux 关联安全补丁的需求于特定时间内完成补丁的部署。

远程补丁管理：对自家至办公室的远程补丁进行实时管理。

可以对台式机、笔记本、漫游用户、服务器等异构端点用户的软件进行修补。

可以修补第三方应用程序。

具备自动化的补丁管理功能，既省时又省钱。

供给修补程序状态具体信息动态报告。

具备交互、使用便捷且基于网络界面的支持文档，可为用户提供各个环节的修补服务。

前述补丁修复程序方案是一个免费的补丁管理工具，patch Manager Plus 可以提供所有的功能用于修补漏洞，且它可以同时与 Mac、Windows、Linux 兼容，可以同时支持 25 台设备。

3.2 ManageEngine的补丁管理解决方案

ManageEngine 的 Patch Manager Plus 实际补丁管理需要完成六个步骤环节：同步→扫描→下载→测试→部署经批准补丁至各计算机→生成报告。具体情况如下：

同步：自开发商出搜集全所有补丁信息，然后把这些信息输入补丁数据库。接下来该修补程序数据库会同步 patch Manager Plus 服务器。

检测：紧接下来一步是要明确这些亟须修补程序的

计算机。Patch Manager Plus 能自动对网络中的计算机进行扫描, 目的是为检测计算机中的漏洞。

下载: 由开发商处站点下载欠缺的补丁, 其中包含安全更新、非安全更新及服务包或汇总、可选更新及功能包。

测试和批准: 先提前在计算机上测试下载的修补程序; 于特定环境下完成未经测试的修补程序的部署, 此间可能存在风险性, 一些修补程序或经更新之后容易出现经部署后的问题, 例如兼容性问题, 此会提升管理人员的工作难度, 注意要更新或卸载不兼容的修补程序。仅在部署之后无任何问题的情况下, 才能批准 这些修补程序。

部署: 依照多元的部署策略, 除了可以对部署窗口灵活选择以外, 也可以创建起修补策略。对于这样的修补程序管理策略恰恰针对多部署访问权限, 故可以及时完成任何部署修补程序。

报表: 结束部署后便会自动生成报表, 同时还会将信息发送给服务器。此环节可以经自定义生成报表, 以便于筛选出数据, 同时借助不同的格式将结果共享给他人。

3.3 使用补丁管理软件的最佳实践

众所周知, 虽然修补整网的端点能有效防控网络攻击, 但要是能提高针对保护网络的警惕性, 则效果会更好。

为此, 以下提出几个补丁管理最佳实践:

扫描作为补丁管理系统的重要组成, 于 Patch Manager Plus 中, 若在持续更新补丁数据库的过程中往往会完成自动扫描, 此过程可以成功地完成漏洞检测且辅助用户进行系统的正确修补。

定期修补系统。修补频率由发布软件修补程序的关键性来决定。

需要将缺失修补程序部署严重性级别为“严重”、“重要”。比如, 要采用 APD 功能来完成 Windows 安全修补程序的及时部署。即便在短短一周内能够完成严重性“中等”、“低”缺失修补程序的部署, 但还是建议先进行测试, 经批准后于非生产计算机当中完成对这些修补程序的测试, 之后再 用 APD 来完成部署。

每天至少扫描一次防病毒更新, 并定期进行修补。

完成产品主页选项卡当中排列的最新安全新闻提要

的阅读。此环节可以帮我们正确决定应将哪个软件修补程序部署在先。故此举可以避免错过重要补丁。

以修补程序管理的 服务形式供应给托管服务开发商。此不管对于什么样规模的企业来说都能灵活地求助于托管服务供应商匹配的补丁服务。且抛却类似于此核心任务外包更有助于让企业专注于核心业务功能。由此可以断定 Patch Manager Plus 当属由 MSP 供应的最佳补丁管理工具。

结合前述所有的实践之后, 用户可以时刻维持用户系统网络始终处于最新状态, 同时又能避免其遭到恶意软件 的攻击。这样一来, 就能大幅度降低安全漏洞发生的概率, 缩短停机时间^[5]。

4 结束语

综上所述, 信息时代的到来让互联网家喻户晓, 同时它也在很短的时间内成了人们日常工作中的得力助手, 随着互联网的普及, 计算机网络漏洞问题必然成为各企业争相讨论的热点, 因此, 新的企业内网计算机补丁管理方案的提出也必然会受到热捧, 且这也是当前行业进步和发展的一大趋势和动向, 我们不难猜测出, 未来对于企业内网补丁管理提出的设计方案会更先进, 更高效, 也更加实用。

参考文献

- [1] 王懿嘉. 计算机信息系统维护与网络安全漏洞处理策略分析[J]. 无线互联科技, 2020, 17(10): 20-21.
- [2] 于广, 郭浩. 关于计算机信息系统运行维护的浅析[J]. 通讯世界, 2019, 26(1): 35-36.
- [3] 倪沈慧. 计算机技术在现代企业信息化管理中的运用[J]. 市场周刊·理论版, 2019(11): 102-05.
- [4] 郝晶. 计算机维护技术 在企业 发展中的应用[J]. 科学与信息化, 2022(7): 189-191.
- [5] 张亮. 关于计算机系统安全补丁管理问题的探讨认识实践[J]. 计算机产品与流通, 2018(15): 147-149.

作者简介

蓝海燕(1989-), 女, 浙江省金华市人。大学本科学历, 测评师。研究方向为网络安全等级保护测评。