

● 王志红

谈图书馆网络安全

摘要 图书馆加强网络安全,首先要制定网络安全管理策略,并构建整体性的多层防护体系(安装防火墙,部署入侵检测系统,安装防毒墙等),要加强日常安全管理。参考文献4。

关键词 图书馆 网络安全 安全策略

分类号 G251

ABSTRACT To improve library network security, we should first draft network security management strategies, construct multi-level protection systems, and then put emphasis on daily security management. 4 refs.

KEY WORDS Library. Network security. Security strategy.

CLASS NUMBER G251

网络环境下,图书馆网站一旦受到黑客攻击,感染病毒,数十万乃至数百万藏书书目信息、流通信息、馆内自建的数据库等数据丢失或被破坏,带来的损失将是灾难性的。图书馆应高度关注网络安全,采取必要措施。

1 制定馆内的网络安全管理策略

管理策略的具体内容大致包括:(1)馆内所有计算机,包括服务器、台式机、笔记本等的管理,明确由谁管理它们、谁使用它们。(2)对密码制定的要求、选择密码的原则,比如定期更换个人和系统密码,禁止使用姓名、生日等作为密码,把密码设置得尽量复杂,禁止使用任何地方的“记住我的密码”选项等。(3)加强电子邮箱管理,尽可能用本馆邮箱。要强化邮件安全意识。(4)要设置每个用户在什么情况下从什么地方可登录及获取什么信息的权限。(5)意外反应机制。即当网络防护发生意外时,谁负责处理,怎样处理等。(6)成立网络安全管理委员会。成员由代表不同用户群的管理人员和技术人员组成,明确各自的安全责任。

2 构建整体性的多层防护体系

通过由外到内、多个层面来对图书馆网络进行保护。单靠某个单一的功能已无法解决实际的网络安全问题,必须要架构整体性的解决方案。

(1)安装防火墙。每一台连接到因特网上的服务器都需要在网络入口处采取一定的安全措施来阻止恶意的通信数据,这就需要考虑安装防火墙。一般来说,防火墙具有以下几种功能:允许网络管理员定

义一个中心点来防止非法用户进入内部网络;可以很方便地监视网络的安全性,并报警;可以作为部署NAT(Network Address Translation,网络地址变换)的地点,利用NAT技术,将有限的IP地址动态或静态地与内部的IP地址对应起来,用来缓解地址空间短缺的问题;可以连接到一个单独的网段上,从物理上和内部网段隔开,并在此部署WWW服务器和FTP服务器,作为向外部发布内部信息的地点。防火墙的这些功能可以很好地帮助抵御黑客的攻击。

(2)部署入侵检测系统。入侵检测是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对它们进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统。一个成功的入侵检测系统不但可使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能给网络安全策略的制定提供指南;而且在发现入侵后,会及时作出响应,包括切断网络连接、记录事件和报警等。入侵检测系统的主要功能有:监测并分析用户和系统的活动;核查系统配置和漏洞;评估系统关键资源和数据文件的完整性;识别已知的攻击行为;统计分析异常行为;操作系统日志管理,并识别违反安全策略的用户活动。入侵检测被认为是防火墙之后的第二道安全闸门,在不影响网络性能的情况下能对网络进行监测,从而提供对内部攻击、外部攻击和误操作的实时保护。

(3)安装防毒墙。目前针对应用层的攻击越来越多,威胁越来越大,只针对网络层以下的安全解决方案已经不足以应付来自应用层的攻击。举个简单

的例子：那些携带着后门程序的蠕虫病毒单靠防火墙便是无法对付的。此外，近两年出现了越来越多依靠操作系统漏洞传播的病毒，这类病毒可以直接绕过杀毒软件来感染系统，使网络版杀毒软件的功效大大减弱。防毒墙则能够提供网关级应用层防护，它将应用层的防护安置在网络的边缘（网关），将防毒操作从各个终端机转移到网关，使病毒在进入内部网络之前即被清除。这种主动防护可将攻击内容完全阻挡在内部网络之外，避免了病毒进入内部网络后再进行查杀的情况发生。防毒墙开创了网络安全防范新概念，将内部网络与病毒隔离开来，使得反病毒的重点从根本上转移到了防的角度上来。它所具有的高度集成化的多种功能较好地满足了人们对网络安全的需要，必将成为网络安全阵线的生力军。

（4）安装网络版杀毒软件或桌面防病毒系统。有了防毒墙，并不表明传统的防护手段就不需要了。边界防毒产品只能说杜绝了病毒从网关向内感染，但病毒还有其他感染途径，如软盘、光盘等移动存储设备等。因此仍然有必要在网络中部署网络版杀毒软件或桌面防病毒软件，在各个层面上封杀病毒。

3 加强日常管理，保证网络安全

（1）强化服务器。“强化”涉及两个简单的实践法则：购买商业软件时，删除不需要的内容，如果不能删除，就把它禁用。一般来说，能够通过强化来删除的对象包括示例文件、使用向导演示、先用后付费的捆绑软件和一些在未来可能不准备使用的高级功能。安装越复杂，越有可能留下安全隐患，应该将安装精简到不能再精简的程度。一些设备和软件通常配置了默认用户名/密码访问、来宾和匿名账户以及默认共享，删除图书馆不需要的，并修改所有身份验证的默认值。

（2）及时为系统打补丁。2001年，当“红色代码”出现的时候，它攻击的便是微软在9个月前就提供了免费补丁的漏洞。但是，这个蠕虫仍然快速和大面积地蔓延，原因就是IT管理员们没有下载和安装补丁。今天，从一个新的漏洞被发现开始，到新的大规模攻击软件问世为止，两者间隔时间已经缩短到了几乎为零。因此，在厂商发布安全补丁的时候，系统管理员就要作出快速响应。访问和安装补丁应该成为系统管理员的工作内容和计划任务的一部分，不要事后才行动。

（3）随时更新防病毒系统。图书馆内可以直接

访问外网的机器最好实施病毒库每日升级，遇重大病毒则随时升级；图书馆局域网内，电脑因不能直接联入外网，其防病毒系统可以一星期升级一次。这项工作看似复杂，其实不然。对那些可直接联入因特网的电脑而言，因为如今各个厂商都提供了杀毒软件自动的升级服务，只要它一直都连在因特网上，它们就能在一个新的安全威胁被发现后的数个小时内下载到计算机上，对防病毒软件进行更新。至于图书馆局域网内的电脑，防病毒软件的更新也比较简单。因为目前许多防病毒软件都支持局域网内的更新，只要抽出一台电脑（暂且将它称为“主机”），使它能够访问外网，及时更新病毒库。病毒库更新后，“主机”便可作为局域网内的病毒库升级服务器，对局域网内其他机器进行升级。以KV2004为例，KV2004在局域网内升级是通过将包含了已更新的病毒库信息的文件夹共享给其他客户机的方式来进行的。更新信息包括在KV2004安装目录下的Update文件夹内，因此，首先就要将这个文件夹设置成为共享。接下来，在客户机上运行KV2004，在菜单栏上依次点击“工具—选项”，切换至“升级”选项卡，选中“局域网升级”选项，将升级的路径指向主机上共享的Update文件夹。由于病毒库经常需要更新，因此人们可以勾选“定时升级”选项，选择一个适当的升级频率，最后单击“确定”即可。这样局域网内的“客户机”就可以在指定的时间连接到“主机”上，自动进行病毒数据库的更新。

（4）必须做好馆内数据的备份工作，馆内文献和流通数据要每天备份，以备不时之需。馆内使用的数据库要定时检测和整理，发现问题及时处理，完毕后，需要写出详细文档并保存，以备查阅。

参考文献

- 1 高嗣昌,姚青.基于网络入侵检测的网络安全监测系统的设计.计算机应用与软件,2004(1)
- 2 赵戈等.用分布式防火墙构造网络安全体系.计算机应用研究,2004(2)
- 3 刘燕妮.信息时代图书馆网络安全与对策.重庆工商大学学报,2004(1)
- 4 孙艳红,熊光明.网络安全技术在高校图书馆的应用.重庆交通学院学报,2004(2)

王志红 河南公安高等专科学校图书馆工作。通信地址：郑州。邮编450002。（来稿时间：2005-05-24）