论图书馆网络安全策略

摘要：

由于互联网的发展，已经暴露出不可避免的缺点——易被攻击。网络用户的好奇和技术恐怖主义使金融机构、企业、学校等单位很难幸免。作为**农业大学“教学科研的保障基地，科技创新的支撑平台，信息服务的重要窗口”的图书馆，由于其网络系统的多样性、复杂性、开放性、终端分布的不均匀性，极易遭黑客、恶性软件或非法授权的入侵与攻击，如遇恶性病毒，就会出现多处计算机告急，网络管理人员就像消防队员一样这里打补丁、哪里安装杀毒软件，这里拔网线，那里搞个 24 小时定时重启服务器。这种疲于奔命现象天天再我馆上演。由于不了解工作情况，读者批评、同事埋怨事件也时有发生，在图书馆论坛的留言本上，“这个破网”，“什么网速”，“服务器能不能稳定点啊”，这类词语几乎是个个星期都有。如何保障图书馆网络的安全，如何有效抑制黑客和病毒，及时采取网络应急策略及措施高效率地处理问题，怎样有层次有重点地保障网络的畅通是图书馆网络管理人员不可回避的一个紧迫问题。

全文：

2006 年 7 月起，我开始负责**农业大学的图书馆网络的管理，以及整个图书馆系统的维护工作。**农业大学是国家不多的 211 大学之一，其图书馆负责全国农业书籍编目工作，是 CALIS 重要的成员之一。**农业大学依托**农业大学图书馆自动化、数字化项目，每 5 年投资 2000 万用于图书馆的电子资源采购、信息化建设、机房建设、服务器采购。我为该项目的总负责。

**农业大学图书馆计算机管理系统复杂多样，有服务器、工作用机、电子阅览室用机和免费检索机。由于服务内容的多样化，图书馆服务器台数逐年增加，且 7×24 对外服务，它们具有单独的 IP 地址，如配置不当，极易成为病毒和黑客的试验基地；工作用机因工作人员的职能不同，机器配置、系统安装也不尽相同；电子阅览室是学生学习、娱乐的场所，也是病毒横行的地方。为便于管理，一般将这些机器划分不同的网段。这种情况下要求所有的

终端系统实施统一的安全策略（比如安装防病毒软件、设置可靠的口令）是非常困难的。计算机入网后感染病毒已司空见惯，反过来这些病毒又影响了局域网的运行。

现在攻击的手段越来越多，复杂度越来越高，可是，对黑客技术要求反而越来越低，大多数黑客操作都是对安全问题并不熟悉的网民，从网上下载一些黑客工具添上地址运行，就形成整个网上攻击的蔓延，这种情况给网络安全带来了很严重的破坏。另外安全漏洞被利用周期越来越短，以前可能长达 1 年多，现在最快的从公布后 48 小时内就出现对这个安全漏洞的利用。

本校学生通常是最活跃的网络用户相互间喜欢切磋技艺，对网络新技术充满好奇，勇于尝试。如果没有意识到后果的严重性，有些学生会尝试使用网上学到的甚至自己研究的各种攻击技术，可能会对网络造成一定的影响和破坏。

另外，图书馆中精通网络管理的专业人员很少，网络整体运行效能、网络架构调整不尽人意。盗版资源的泛滥下载的资源占用大量的带宽，而且很有可能附上很多木马，后门等恶意代码，许多系统因此被攻击者侵人和利用。

针对网络中存在的各种问题，可以通过建立较完善的安全策略来最大限度地保障网络安全。但是 Bug 是不可能完全解决的，因为 Bug 不可能全部在被发现和被利用之前得到弥补。网络安全策略主要包括两方面：访问控制策略和信息加密策略只有各种安全策略相互配合才能营造一个安全而高效的网络环境。

1．登录控制

对于能够登录到服务器、交换机和路由器等网络设备的用户应进行身份认证，并控制登录时间、地点，用户名或用户账号是计算机系统中最基本的安全形式，在管理账号时，应当遵循以下规则：安装后及时修改操作系统内部账号的缺省配置；对新建账号必须强制修改口令的时间间隔、口令的惟一性、最小用户名及口令长度等等，口令设置宜大小写字符并与数字结合、口令长度不应过短。建立账号锁定机制，同一账号密码校验错误若干次即锁定账号；在通过网络验证口令过程中不得以明文方式传输避免监听等等。

2．代理服务器控制

代理服务器是运行特定服务程序的计算机，是连接内网与外网的通道，能为图书馆网络提供 Internet 共享服务，代理服务器的优点能控制上网的 IP 范围，对于存在问题的网站，

图书馆网络管理员可以实行屏蔽，有问题时，切断通道，禁止不良信息与网络病毒的侵犯。

3．VLAN 安全控制

VLAN 是控制网络内广播风暴的重要手段，也是保护网络安全的重要措施，VLAN 可以实现子网间的相互隔离，防止非法访问，图书馆可根据计算机使用职能，划分多个 VLAN 区，如服务器、工作人员用机、电子阅览室用机、读者免费信息查询计算机，有些计算机可采用虚拟地址，有些为外部实地址，制定适当的访问控制列表（ACL），实现 VLAN 间的安全访问。

4．服务器安全控制

服务器的默认安装是允许管理员远程登录操作，远程修改注册表。如通过 Telnet 远程连接能够对服务器进行设置操作，虽然为服务器管理提供了一定的便利，但是也造成了非法用户的访问，因此必须加强服务器的安全控制图书馆服务器主要是数据信息，一般情况下，应禁止远程登录与注册表操作，如遇特殊情况，应限制远程登录用户源 IP 地址设定登录时间，防止非法用户登录修改删除重要信息和重要数据。

5．防火墙控制

防火墙是在内网和外网之间构筑一道隔离墙障，用于保护内部网中信息资源不受来自外网，尤其是 Internet 中非法用户的侵犯。它根据用户安全策略控制出入内部网的信息流，检查和控制进出内部网的信息，决定是否允许用户的服务请求，从而阻止对内部网信息资源的非法访问和非授权用户的进入。防火墙对于非法访问具有很好的预防作用利用防火墙的地址转换技术，隐蔽网络内部的真实 IP 地址，避免黑客通过 IP 欺骗等方法突破路由进人局域网，限制外部网络用户对内部主机的访问。通过对发到内部网的数据包过滤、指定 IP 地址段，匹配安全规则等将一些非法访问阻挡在防火墙之外，开放有限端口，如仅打开 80，25，110 端口，只允许外部用户或主机访问防火墙内的 WWW 服务和 EMAIL 服务;限制内部用户对 Internet 的访问。采用 IP/MAC 地址绑定技术，只有被允许的硬件地址才能出访外部网。并限制其对 Internet 的服务，如只能使用 WWW 和 FTP 服务。对内外之间的通讯进行监控，记录下所有通信的内容，从而防止内部用户使用不合适的 Internet 服务。

6. 漏洞补丁检测控制

任何操作系统都有漏洞，网络管理员应及时跟踪软件厂商的最新公告，跟踪国内外网络

安全站点对安全漏洞和安全工具的公告，及时更新操作系统，防止 Bug 带来的安全漏洞。许多防病毒软件如瑞星、江民、诺顿等都提供漏洞检测程序，用户可及时上网更新系统文件，防止病毒侵犯。现在我们设立了自己的 WSUS 服务器，用户通过设置自动更新配置，不用出国就能及时获得最新的 Windows 系统和相关软件的补丁程序。

7．硬盘保护卡控制

硬盘保护卡控制是一种行之有效的最佳保护模式，如果系统感染了病毒，重启计算机则可。这对于系统文件相对稳定，不需要经常安装新软件的计算机十分合适，如图书馆电子阅览室用机广泛采用硬盘保护卡模式，极大减轻了网络管理员的劳动强度。

8．安全管理维护机制

我们把安全管理纳入到日常管理日程上来，主动检查网络运行状态和服务器系统安全，每天定时观察系统日志，检测系统是否正常。

8．定期备份数据

我们为确保重要数据不被破坏，除了采用双机备份外，也可通过 FTP 等文件传输程序，把整个图书馆自动化管理系统或重要数据备份到其他安全可靠的计算机硬盘上，这样故障出现后，就能尽快地恢复系统的运行。

我们图书馆网络通过采取上述措施后，安全性大大加强了，用户投诉大大减少了，同时管理员也不用天天为系统这点、那点电脑故障东奔西跑了。不过由于原因，我们仍然遇到一些服务器攻击，有些黑客通过各种手段登录到我馆服务器上，究其原因，主要是管理员疏忽没有及时更新系统和数据库补丁，导致一些黑客提权成功将一些执行文件放入视频点播服务器的启动目录下。由于，我们重要服务器管理比较死，还没有出现提权成功的情况。同时，我们的备份恢复比较及时，未造成过大的影响。