局域网安全与维护

李亭升

成都信息工程大学银杏酒店管理学院　四川 成都　611743

摘　要：计算机技术的发展为计算机网络的广泛应用提供了保障，但是计算机网络并非绝对安全，它一旦发生故障就会给人们造成巨大的不便损失。为了减少计算机网络的故障以及维护计算网络的安全，必要的安全防护策略以及网络维护是应当具备的。

关键词：局域网；维护；安全

1 局域网的维护

1.1 硬件的维护 首先是对联入互联网电脑的网卡、集线器、网线、路由器、交换机等进行检测，其次是查看计算机内存、硬盘和显示器等能够正常工作，如果发现损坏的计算机硬件，应当及时进行更换。网卡的正确安装与配置也是应当检查的内容。总之，我们要保证联入互联网的计算机硬件不会与上网的软件发生冲突，并且能够达到联网的基本要求。

1.2 软件的维护 对软件的维护主要包括以下几个方面：①检查计算机网络设置。②检查网络的畅通性。③检查网络的安全性。

2 局域网的安全

对于单位来说，局域网的安全是非常重要的，单位内部办公自动化网络一般具有开放性，这大大方便了我们的使用。正是由于网络的开放性，系统入侵、病毒入侵等网络安全问题就层出不穷。如果这些网络安全问题解决不了，就很有可能出现各种严重后果，如设备损坏、系统瘫痪、数据丢失、商业秘密泄漏等，对企业的经营活动也会造成极大的影响。

2.1 局域网的现状 关于一些常见的广域网安全问题我们已经有了比较完善的防范措施，如防火墙、漏洞扫描、网络边界、防病毒、IDS 等网关级别方面的防御。对于外部网络的安全威胁，我们常常在网络的入口或者机房安装一些监控设备来防御，这样做的目的就使得外部网络的威胁大大降低。而计算机客户端的安全威胁我们常常没有太过注意，还没有有效的方法进行管理和防范，而这类威胁反而是比较大的。网络用户通常包括授权用户和未授权用户，对于未经授权的网络用户，他们是可以对通过局域网的网络设备进入网络具有任意性和方便性，这对网络安全造成了很大的威胁。在加上局域网系统本身存在一定的弱点，加上系统使用和管理过程中的一些疏忽让安全问题进一步加重。

2.2 局域网安全威胁分析 局域网通常是指在小范围内由服务器和多台电脑组成的工作组互联网络。在局域网内部，我们通常是用交换机和服务器来连接网络内部的电脑，所以在网络内部传输信息通常是比较快的，但是在局域网中我们没有相应的安全措施，加之连接局域网时我们所使用的技术又比较简单，这样病毒就很容易的在这样的局域网中进行传播，让在网络中传播的数据也会遭受到很多威胁。通常局域网的网络安全威胁包括以下几个方面：①使用欺骗性的软件。我们联网的目的主要是进行资源共享，这样就可以从网络中获取我们所需要的资源，而这样的网络数据是对外开放的，换句话说，加入网络的用户都有可能对立面的数据进行删除或者修改，这样让网络中的数据的安全性大大降低。比如我们常见的网络钓鱼攻击，攻击者利用钓鱼工具向用户发送大量的垃圾邮件，而这些邮件的来源通常被伪装成一些知名机构来诱导收信人给出自己的用户名、密码、信用卡信息等，极具有欺骗性。近年来由于大型的网站或者知名机构对于这类问题反应比较迅速，开始不断地增强自己的安全功能，网络钓鱼又开始把目光更多的对准了较小的网站。再加上用户对于数据备份等数据安全方面的知识较为缺乏，信息丢失等现象也就经常性的发生了。②没有独立防护的服务器区域。因为信息在局域网中能够畅通无阻且快速的传播，也给病毒的传播带来了方便，我们必须要把局域网中的服务器区域独立的保护起来，才不会导致其中一台电脑遭受病毒传染以后影响到其他电脑。因为一旦服务器遭受到病毒感染，那么其他在局域网中的电脑只要通过无服务传播信息就有可能被这台感染了病毒的服务器感染。③计算机病毒的威胁。防病毒软件对于我们来说是必不可少的，对操作系统的补丁及时进行安装和更新也是很有必要的，但是对于很多网络用户而言，对于这些问题并不敏感，这样就给病毒的入侵创造了条件。目前很多软件就是在用户电脑上运行，然后趁机修改用户硬盘里的资料，并且向用户硬盘里写入一些恶意的攻击性代码，给用户造成很大的损失。

2.3 局域网安全控制与病毒防治策略 要想对局域网的安全进行控制那就要涉及多个方面，包括技术、管理和应用，并且这也是一个长期的过程。要想从根本上保证信息的安全，这三个方面必须同时进行，并且把每一个方面落实下来。在这个过程中人是主导作用，然而人也是网络安全中最容易犯错的环节，但是如果在这个环节我们做好了，我们也是最容易看到明显效果的。这就对我们提出了更严格的要求，我们应当加强对网络参与人员的管理，对他们定期进行安全问题的培训，提高安全防范意识和管理人员的整体素质也是必不可少的。对工作人员的培训主要从以下几个方面来进行：

我们需要对用户进行授权，对于未经授权的用户，我们要确保网络用户资源、设备、网络管理系统本身不能被他们访问。就目前的网络安全问题而言，客户端安全部分在网络管理工作量中所占的比重是最大的。要想排除网络中的安全隐患，我们就必须得把网络内部的安全问题解决好。我们可以从终端状态、行为、事件三个方面来防御从而对内部网络安全进行管理。

使用防火墙技术。目前防火墙技术已经比较成熟，并且很多计算机基本上都安装了防火墙，这样可以有效的将网络与计算机分离开来，让网络间的相互访问受到限制，从而进一步遏制了非法使用者对于网络内部的威胁，达到保护网络内部资源的目的。

关于用户连接网络的权限方面，我们可以利用桌面管理系统来进行控制，有了桌面管理系统就可以控制恶意用户访问网络资源，这样也就扼守住了网络访问的第一道关口，保障了网络的安全。它是对用户上网的时间、从哪里进入网络以及哪些用户能够登录到服务器并且获取网络的资源的控制。在这个系统中，用户和用户组按照级别事先被给予一定的权限，根据用户的权限我们来设定哪些文件和资源可以被哪些级别的用户访问，并且还规定了这些用户对于文件和资源操作的权限。我们还可以通过密码保护来保障网络安全，对于用户设定的密码我们强制他必须达到一定的安全标准才可以通过，对密码不符合要求的用户在达到一定的警告次数后将其断网。对用户进行非法访问的检测和设定服务器登录的时间也是局域网安全防范中常常采用的办法。

参考文献：

[1]刘建伟.网络安全概论[M].电子工业出版社，2009.

[2]陈应明.计算机网络与应用[M].冶金工业出版社，2005.

[3]谢希仁.计算机网络(第二版)[M].北京：电子工业出版社，2001.

作者简介：李亭升，男，1983 年生，硕士研究生，主要研究方向为电子商务。