

# IT 环境下企业的网络安全

刘莉莉

(甘肃省中医院,甘肃 兰州 730000)

**摘要:**随着 Internet 的迅速发展,企业 IT 系统规模的扩大和日趋完善、网络环境的日益复杂,信息安全问题面临新的挑战。就日益发展的企业 IT 系统,提出了在此环境下企业网络安全的解决方案。

**关键词:**网络;安全;防范

**中图分类号:**TP393

随着 Internet 的迅速发展,企业 IT 系统规模不断扩大和完善、网络环境日益复杂,信息安全问题面临新的挑战。一个企业的信息系统安全问题已威胁到整个企业系统的安全、稳定、经济、优质运行,影响着“数字化企业”的实现进程。企业系统信息安全已经成为企业生产、经营和管理的重要组成部分。因此,研究企业系统信息安全问题、开发相应的应用系统、制定企业系统信息遭受外部攻击时的防范与系统恢复措施等信息安全战略是当前信息化工作的重要内容。

网络安全是一项动态的、整体的系统工程,从技术上来说,网络安全由安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成。在企业的综合信息管理系统中,必须从网络、操作系统、应用程序和业务需求等各方面来保证系统的安全。

## 1 网络安全的定义

网络技术是从 20 世纪 90 年代中期发展起来的新技术,它把互联网上分散的资源有机整合,实现了资源的全面共享。近年来,伴随着互联网技术的迅猛发展,网络已成为人们生活中不可或缺的一部分。然而人们在享受网络带来的种种便利时,也受到了日益严重的来自网络的安全威胁。

网络安全从本质上讲就是网络上的信息安全,网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。从用户的角度来说,希望涉及到个人隐私和商业利益的信息在网络上传输时,受到机密性、完整性和真实性的保护。

## 2 计算机网络安全面临的问题

### 2.1 计算机病毒

计算机病毒是专门破坏计算机正常工作,具有高级技巧的程序。它并不独立存在,而是寄生在其他程序之中,具有隐蔽性、潜伏性、传染性和极大的破坏性。计算机病毒通过互联网传播,给网络用户带来极大的危害,它可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名 FTP 文件传送、也可以通过邮件和邮件的附加文件传播。随着网络技术的不断发展、网络空间的广泛运用,病毒的种类也在急剧增加。

### 2.2 黑客攻击手段多样

黑客的攻击手段在不断地更新,几乎每天都有不同的系统安全问题出现。然而安全工具的更新速度太慢,绝大多数情况需要人为的参与才能发现以前未知的安全问题,这就使得它们对新出现的安全问题总是反应太慢。当安全工具刚发现并努力更正某方面的安全问题时,其他的安全问题又出现了。因此,黑客总是可以使用先进的、安全工具不知道的手段进行攻击。目前黑客的攻击方法已超过了计算机病毒的种类,而且许多攻击都是致命的,攻击源相对集中,攻击手段更加灵活。

### 2.3 操作系统漏洞及网络设计的问题

目前流行的许多操作系统均存在网络安全漏洞,黑客利用这些操作系统本身所存在的安全漏洞侵入系统。由于设计的网络系统不规范、不合理以及缺乏安全性考虑,使其安全性受到影响。网络安全管理缺少认证,容易被其他人员滥用,人为因素造成网络安全隐患。另外,局域网内网络用户使用盗版软件,随处下载软件与游戏程序,以及网管的疏忽也容易造成网络系统漏洞。

以上只是网络安全所面临的威胁中的一小部分,由此可见,解决网络安全威胁,保证网络安全已迫在眉睫,这需要寻求一个综合性解决方案,以应对日益严重的网络安全危机。

## 3 计算机网络安全防范技术

### 3.1 防火墙技术

防火墙的作用是对网络访问实施访问控制策略。防火墙技术是为了保证网络路由安全性而在内部网和外部网之间的界面上构造一个保护层。所有的内外连接都强制性地经过这一保护层接受检查过滤,只有被授权的通信才允许通过,同时将不允许的通信拒之门外,最大限度地阻止网络中的黑客来访,防止他们随意更改、移动甚至删除网络上的重要信息。它是不同网络或网络安全域之间信息的惟一出入口,能够根据安全政策控制(允许、拒绝、监测)出入网络的信息流,且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施。

### 3.2 网络病毒的防范

在网络环境下,病毒传播扩散快,仅用单机防病毒产品已经很难彻底清除网络病毒,必须有适合于局域网的全方位防病毒产品。这需要一个基于服务器操作系统平台的防病毒软件和针对各种桌面操作系统的防病毒软件。如果与互联网相连,还需要网关的防病毒软件,加强上网计算机的安全性。

### 3.3 加强网络安全管理

加强网络的安全管理、制定有效的规章制度,对于确保网络的安全性与可靠运行,将起到十分有效的作用。加强网络的安全管理包括:确定安全管理等级和安全管理范围;制定相关网络操作使用规程和人员出入机房管理制度;制定网络系统的维护制度和应急措施等。

考察一个内部网是否安全,不仅要看其技术手

段,更重要的是看对该网络采取的综合措施。

### 3.4 提高安全防范意识

只要我们提高安全意识和责任观念,很多网络安全问题也是可以防范的。我们要注意养成良好的上网习惯,不随意打开来历不明的电子邮件及文件,不随便运行陌生人发送的程序;尽量避免下载和安装不知名的软件、游戏程序;不轻易执行附件中的EXE和COM等可执行程序;密码设置尽可能使用字母数字混排;及时下载安装系统补丁程序等。

## 4 结束语

网络安全是一个系统的、全局的管理问题,网络上的任何一个漏洞,都会导致全网的安全问题,我们应该用系统的观点、方法,分析网络的安全及具体措施。安全措施主要包括:行政法律手段、各种管理制度(人员审查、工作流程、维护保障制度等)以及专业措施(识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等)。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络,包括个人、设备、软件、数据等。这些环节在网络中的地位 and 影响作用,也只有从系统综合整体的角度去看待、分析,才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则,根据规定的安全策略制定出合理的网络安全体系结构,这样才能真正做到整个系统的安全。

### 参考文献:

- [1] 石志国. 计算机网络安全教程[J]. 北京:清华大学出版社,2008.
- [2] 周小华. 计算机网络安全技术与解决方案[J]. 杭州:浙江大学出版社,2008.
- [3] 张庆华. 网络安全与黑客攻防宝典[J]. 北京:电子工业出版社,2007.
- [4] 曲德祥. 网络安全技术的发展趋势[J]. 信息技术与信息化,2008(5).