国家精品课程配套教材系列

浙江省“十一五”重点建设教材

中小型网络安全管理与维护

主　编　姚奇富　副主编　马华林

中国水利水电出版社
www.waterpub.com.cn

国家精品课程配套教材系列

中小型网络安全管理与维护

主　编　姚奇富

副主编　马华林

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书从网络安全案例引入，以不同规模的网络平台为载体，设计了“桌面主机安全威胁与防护”、“小型网络安全威胁与防护”、“中型网络安全威胁与防护”、“信息安全风险评估”等四篇共10章，主要内容包括网络安全基本理论、ARP欺骗、密码破解和远程控制、缓冲区溢出攻击、蠕虫病毒、防火墙技术、IPsec VPN、Windows Server 2008安全管理与配置、SQL注入攻击、跨站攻击、Web防火墙的部署和管理、SSL VPN、IDS、IPS、存储技术、风险评估的内容和方法以及风险评估的实施流程，每章内容包括本章工作任务、正文、本章小结、本章习题和阅读材料，部分小节中还包括继续训练内容。

本书注重实践，以项目作为知识、技能与素养的载体，将知识融于项目，以项目为导向，书中内容来源于真实工作任务。

本书可作为应用型本科和高职院校计算机专业教材，以及高职院校电子商务和中职院校网络技术等相关专业的网络安全综合训练教材，也可作为网络安全培训教材。

图书在版编目（CIP）数据

中小型网络安全管理与维护 / 姚奇富主编. -- 北京
：中国水利水电出版社，2012.8
国家精品课程配套教材系列
ISBN 978-7-5170-0001-3

Ⅰ. ①中… Ⅱ. ①姚… Ⅲ. ①计算机网络－安全技术
－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第173333号

策划编辑：雷顺加　　责任编辑：李　炎　　封面设计：李　佳

书　　名	国家精品课程配套教材系列 **中小型网络安全管理与维护**
作　　者	主　编　姚奇富　副主编　马华林
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	三河市铭浩彩色印装有限公司
规　　格	184mm×260mm　16开本　15印张　368千字
版　　次	2012年8月第1版　2012年8月第1次印刷
印　　数	0001—4000册
定　　价	28.00元

序

随着互联网迅速发展和网络安全形势的日益严峻，越来越多的企事业单位对网络安全日益重视，真正感受到了网络安全对企业发展的价值。网络安全产品和服务被企事业单位普遍认同，网络安全也逐渐成为IT行业的主流职能，这为网络安全设备提供商、系统集成商提供了发展和壮大的机会。同时，网络安全人才需求也越来越大，令人欣喜的是一些高职院校（如浙江工商职业技术学院）顺势而为，及时地把计算机网络技术专业的方向转向为网络安全管理和维护，为企事业单位培养了急需的网络安全技术人才。

我一直关注技术，尤其是网络安全领域技术的新发展和新趋势，非常高兴看到《中小型网络安全管理与维护》这样一本优秀教材的出版，这本教材覆盖了大部分目前中小型企业中使用的计算机网络安全设备，以项目为导向，用文字和图相结合的方式深入浅出地介绍了计算机网络安全设备的原理和技术，书中部分项目来源于我公司的真实工作任务。

对于广大高职院校来说网络安全是新的发展方向，《中小型网络安全管理与维护》这本教材无疑是广大高职院校计算机网络技术专业开展网络安全技术教学的理想选择，教材的开发基于“中小型网络安全管理与维护”课程开发团队和合作公司工程师多年的教学经验和工程实践的积累，有理由相信这本教材能够为广大教师和学生助一臂之力。

我去过浙江工商职业技术学院好多次，很喜欢和该校的教师和学生交流，感谢他们为社会和信息安全行业培养了优秀的网络安全技术和服务工程师，并衷心希望本书能成为广大高职院校教师和学生喜欢的网络安全技术教材。

中组部“国家千人计划”特聘专家
杭州市政协常委　　范渊
中国计算机学会计算机安全专委会常委
杭州安恒信息技术有限公司总裁

前　言

随着计算机网络技术的成熟和网络应用的不断深入，网络安全直接关系到个人、企业和国家的生存和发展。纵观当今，网络安全事件的频繁发生，病毒木马蠕虫泛滥，黑客攻击手段层出不穷，网络钓鱼事件明显上升，安全漏洞不断增加，网络安全问题已成为政府、民间组织、企业和个人用户面对的巨大挑战，社会各界和各行各业对网络安全技术人员的需求量越来越大，在未来几年都将处于紧缺状态，同时对技术人员的能力要求也越来越高。

本书是国家精品课程“中小型网络安全管理与维护”配套教材和浙江省“十一五”重点建设教材，主要使用对象为高职院校计算机类专业的教师和学生，同时也可作为应用型本科院校计算机类专业和中职院校网络技术专业的网络安全综合训练教材。教师可以从精品课程网站（http://jpkc.zjbti.net.cn/wlaq/）中下载课件，广大读者可借助精品课程网站自学。

本书基于高职计算机类专业毕业生从事中小型网络安全管理与维护工作岗位实际要求编写。在内容选取上，把实践放在首要位置，涵盖了目前业界大部分网络安全设备，如防火墙、IDS、IPS、VPN、存储设备、Web 防火墙等，在网络安全技术和原理介绍中力求“简明扼要”和“必须够用”，尽量用文字和图相结合来描述相关设备和技术的要点。在内容组织上，结合了目前高职院校普遍采用的项目课程和工作过程系统化课程的开发方法，以不同规模的网络平台为载体，设计了“桌面主机安全威胁与防护”、“小型网络安全威胁与防护”、“中型网络安全威胁与防护”等三篇，每一篇与该门课程中的项目或者学习情境相对应。鉴于目前我国正在大力推行信息安全等级保护和 ISO270001 认证，又增加了以高校校园网络为平台的“信息安全风险评估”作为第四篇。

本书涵盖的内容十分广泛，共分为四篇。第 1 篇为“桌面主机安全威胁与防护”，包括第 1 章和第 2 章，第 1 章介绍了网络安全相关的定义、基本功能、常用设备，让读者在总体上对网络安全有一个初步认识，然后介绍了网络安全实验常用的虚拟机技术，第 2 章介绍了黑客针对桌面主机常用的攻击技术，包括 ARP 欺骗、密码破解和远程控制、缓冲区溢出攻击、蠕虫病毒等。第 2 篇为“小型网络安全威胁与防护”，根据小型网络的典型网络结构和设备部署，从第 3 章至第 5 章分别介绍了防火墙、IPsec VPN、服务器和网站运行管理等技术，其中服务器和网站运行管理中包括了 Windows Server 2008 安全管理与配置、SQL 注入攻击、跨站攻击、Web 防火墙的部署和管理等。第 3 篇为“中型网络安全威胁与防护”，根据中型网络的典型网络结构和设备部署，从第 6 章至第 9 章分别介绍了 SSL VPN、IDS、IPS 和存储等技术。第 4 篇为“信息安全风险评估”，介绍了风险评估的内容和方法，同时以高校校园网为平台介绍了风险评估的实施流程。

本书由浙江工商职业技术学院姚奇富教授任主编，马华林高级实验师任副主编，负责全书的统稿、修改、定稿工作。姚奇富、马华林、吕新荣、王奇、朱震等老师参与本书撰著和教学资源的建设与维护，陆世伟、吴冬燕等老师参与本书素材整理、教学资源建设与维护，徐一卓、岑天伟、张田璐、章权等参与了实验环境的搭建和课程网站资料整理工作。由于作者水平有限，疏漏和错误之处难以避免，恳请使用本书的读者提出宝贵意见。

本书为浙江省“十一五”重点建设教材，得到了浙江省教育厅的资助，在此表示感谢。感谢杭州安恒信息技术有限公司在本书编写中的指导和帮助，感谢为本书出版付出辛勤劳动的中国水利水电出版社的各位朋友。

作者

2012 年 5 月

目　录

第 3 篇　中型网络安全威胁与防护

第 4 篇　信息安全风险评估

第 1 篇　桌面主机安全威胁与防护

1．知识目标

- 掌握虚拟机的工作原理
- 掌握 ARP 协议的工作原理
- 了解 ARP 缓存的缺陷
- 掌握网络嗅探的工作原理
- 了解网卡工作原理
- 了解 TCP 三次握手的过程
- 了解主机和端口扫描的工作原理
- 掌握缓冲区溢出、蠕虫病毒、木马等概念

2．能力目标

- 专业能力
  - 能熟练使用虚拟机
  - 能安装并使用新工具
  - 能设计网络安全实验
  - 能使用 Wireshark 进行网络嗅探和协议分析
  - 能检测和防御 ARP 欺骗攻击
  - 能防御密码的暴力破解攻击
  - 能检测和清除木马
  - 能使用工具查杀蠕虫病毒
  - 能鉴别多种网络钓鱼的手段
  - 能设计和实施桌面主机整体防御方案
- 方法能力
  - 能根据任务收集相应的信息
  - 能通过自学快速掌握新的网络安全工具
  - 能书写木马、病毒等攻击的诊断和防御方案
  - 能通过自学认识一种新的网络攻击技术
- 社会能力
  - 能加入一个团队并开展工作
  - 能与相关人员进行良好的沟通
  - 能领导团队开展工作

3．素质目标

- 能遵守国家关于网络安全的相关法律
- 能遵守单位关于网络安全的相关规定
- 能恪守网络安全人员的职业道德

2006 年 3 月 21 日下午 17 时左右，一名毕业不久参加工作的北京学生王某某通过网上银行查询 A 银行账户余额时，发现账户分六次共被转走一万零九百元钱，王某某立即挂失该账户并拨打了 110 报警。不幸的是这不是个案，2006 年 4 月来，北京地区使用 A 银行网上银行的客户陆续遭受账户中的存款被人转移到陌生账号上，被盗金额从几百到一万不等。在 A 银行官方网站论坛上，仅 2006 年 3 月份，发帖称网银账户被盗的用户就高达 21 人。2006 年 3 月 30 日，受害人任先生将自己被盗经历发表到猫扑论坛上，截至 2006 年 4 月 7 日，该帖已有百余条跟帖，不少网友反映有相似被盗经历。任先生是某 IT 公司的技术人员，接受记者采访时说，由于自己是计算机专业人员，一直都有很强的网络安全防范意识，银行密码采用字母和数字的复杂组合，并不容易被破解，但没想到自己的网上银行账户仍然会被盗。

王某某和任先生等人的遭遇给我们敲响了警钟，网络安全问题已经深入到普通百姓的生活中。假设你是网络警察，将怎样处理这件事？然后思考以下几个问题：

1．如果罪犯是受害者的同事，可能有哪些技术获取受害者的银行账号和密码？

2．如果罪犯是一个互联网上的黑客，可能采用哪些技术获取受害者的银行账号和密码？

3．普通百姓可以采用哪些措施保护自己的信息安全？

4．假如你的重要信息资料被人窃取，并有可能造成经济损失，该怎么办？

第 1 章　网络安全基础

- 安装 VMware 软件
- 使用 VMware 虚拟机组建网络

1.1　网络安全概述

随着信息化的推广、计算机网络技术的成熟和网络应用的不断深入，网络已逐渐成为人们日常生活乃至国家事务、经济建设、国防建设、尖端科学技术等重要领域必不可少的组成部分，同时，信息已经成为和物质、能源同等重要的资源，对社会的发展变革起着极为重要的作用。然而，由于我们对网络的依赖与日俱增，网络的安全性问题日益突出，蠕虫、木马、后门、拒绝服务、垃圾邮件、系统漏洞、间谍软件等花样繁多的安全隐患和威胁开始一一呈现在我们面前。

据国家互联网应急中心的统计，2010 年中国大陆有近 3.5 万个网站被黑客篡改，数量较 2009 年下降 21.5%，但其中被篡改的政府网站却高达 4635 个，比 2009 年上升 67.6%。省部级和中央政府网站安全状况明显优于地市及以下级别的政府网站，但仍有约 60%的省部级网站存在不同程度的安全隐患。政府网站安全性不高不仅影响了政府形象和电子政务工作的开展，还给不法分子发布虚假信息或植入网页木马提供可乘之机。网络违法犯罪行为的趋利化特征明显，大型电子商务、金融机构、第三方在线支付网站成为网络钓鱼的主要对象，黑客仿冒上述网站或伪造购物网站诱使用户登录和交易，窃取用户账号密码、造成用户经济损失。2010 年，国家互联网应急中心共接收网络钓鱼事件举报 1597 件，较 2009 年增长 33.1%，“中国反钓鱼网站联盟”处理钓鱼网站事件 20570 起，较 2009 年增长 140%。2010 年，由于扩大了监测范围，国家互联网应急中心全年共发现近 500 万个境内主机 IP 地址感染了木马和僵尸程序，较 2009 年大幅增加。

2010 年，在工业和信息化部的指导下，国家互联网应急中心会同电信运营企业、域名从业机构持续开展木马和僵尸网络专项打击行动，成功处置境内外 5384 个规模较大的木马和僵尸网络控制端和恶意代码传播源。监测结果显示，相对 2009 年数据，远程控制类木马和僵尸网络的受控主机数量下降了 25%，治理工作取得一定成效。然而，黑客也在不断提高技术对抗能力，2010 年截获的恶意代码样本数量特别是木马样本数量，较 2009 年明显增加，木马和僵尸网络治理工作仍任重道远。此外，网络设备、服务器系统、操作系统、数据库软件、应用软件乃至安全防护产品普遍存在安全漏洞，高危漏洞会带来严重的安全隐患。2010 年，国家互联网应急中心发起成立的“国家信息安全漏洞共享平台（CNVD）”共收集整理信息安全漏洞 3447 个，其中高危漏洞 649 个（占 18.8%），典型的高危漏洞有：论坛建站软

件 Discuz!高危漏洞、MySQL yaSSL 库证书解析远程溢出漏洞、Microsoft IE 对象重用远程攻击漏洞、Microsoft Windows 快捷方式‘LNK’文件自动执行漏洞、IBM 公司 Lotus Domino/Notes 群件平台密码散列泄露漏洞、工业自动化控制软件 KingView 6.5.3 缓存区溢出漏洞等。CNVD 2010 年收集整理的漏洞中，应用程序漏洞占 62%，操作系统漏洞占 16%，Web 应用漏洞占 9%，分列前 3 位[1]。

由于我国计算机芯片和关键网络设备等主要依赖进口，操作系统也是以国外生产的为主，因此存在的安全隐患更是不言而喻。系统漏洞和硬件后门是非法入侵的主要途径，网络攻击的威胁不容忽视。目前，我国各类网络系统经常遇到的安全威胁有恶意代码（包括木马、病毒、蠕虫等），拒绝服务攻击（常见的类型有带宽占用、资源消耗、程序和路由缺陷利用以及攻击 DNS 等），内部人员的滥用和蓄意破坏，社会工程学攻击（利用人的本能反应、好奇心、贪便宜等弱点进行欺骗和伤害等），非授权访问（主要是黑客攻击、盗窃和欺诈等）等，这些威胁有的是针对安全技术缺陷，有的是针对安全管理缺失。2010 年 1 月 12 日，百度遭受到了自建立以来时间最长、影响最严重的黑客攻击。2010 年 9 月，伊朗布什尔核电站遭到 Stuxnet 病毒攻击，导致核电设施推迟启用。Stuxnet 病毒是一种蠕虫病毒，利用 Windows 系统漏洞和移动存储介质传播，专门攻击西门子工业控制系统。业界普遍认为，这是第一次从虚拟信息世界对现实物理世界的网络攻击。工业控制系统在我国应用十分广泛，工业控制系统安全值得高度关注[1]。

政府、民间组织、个人用户对网络安全问题越来越重视，网上银行、证券、信贷、国家事务、国防建设、尖端科学技术领域、经济建设、公共信息服务领域等关键性网络系统越来越综合运用虚拟网技术、防火墙技术、入侵检测技术、安全漏洞扫描技术、防病毒技术、加密技术、数字认证技术等多种安全技术措施，信息系统的安全问题得到基本保障。在国家互联网应急中心 2010 年的调查报告中，有 98%的企业网络使用了防火墙，69%的企业网络使用了入侵检测系统（IDS），97%的系统使用了防病毒软件。据 2010 年全国信息网络安全状况与计算机病毒疫情调查报告分析，95%的被调查单位设立了专职或兼职安全管理人员，24%的单位建立了安全组织。64%的被调查单位还采购了信息安全服务，主要采购的服务有系统维护（67%）、安全检测（48%）、容灾备份与恢复（31%）、应急响应（19%）、信息安全咨询（25%）。此外，有 62%的单位进行存储备份，65%的单位进行口令加密和访问控制，43%的单位制定了安全管理规章制度。这些表明，网络用户的安全防范意识在不断增强，安全管理措施逐步得到了落实，网络安全状况逐步得到控制并转好[1]。

1.1.1 什么是网络安全

网络安全是指网络系统中的软、硬件设施及其系统中的数据受到保护，不会由于偶然的或是恶意的原因而遭受到破坏、更改和泄露，系统能够连续、可靠地正常运行，网络服务不被中断。从本质上说，网络安全就是网络上的信息安全，网络安全的特征主要有系统的完整性、可用性、可靠性、保密性、可控性、抗抵赖性等方面[2]。

（1）完整性

---

1 国家互联网应急中心：“2010 年中国互联网网络安全报告”，http://www.cert.org.cn/articles/docs/common/2011042225342.shtml.

2 马民虎．互联网信息内容安全管理教程[M]．北京：中国人民公安大学出版社，2007：37-40.

完整性是指网络信息数据未经授权不能进行改变，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、破坏和丢失。完整性是网络信息安全的最基本特征之一。要求网络传输的信息端到端、点到点是保持不变的，在存储上能够保持信息100%的准确率，即网络信息的正确生成、正确存储和正确传输。

（2）可用性

可用性是指网络信息可被授权实体访问并按需求使用，即网络信息服务在需要时允许授权用户或实体使用，或者是网络部分受损或需要降级使用时仍能为授权用户提供有效服务。可用性是网络信息系统面向用户的安全性能，网络信息系统最基本的功能是向用户提供服务，用户的需求是随机的、多方面的，有时还有时间要求，可用性一般用系统正常使用时间和整个工作时间之比来度量。

（3）可靠性

可靠性是指网络信息系统能够在规定条件和规定时间内完成规定功能。可靠性是网络安全的最基本要求之一，是所有网络信息系统的建设和运行目标。

（4）保密性

保密性是指网络信息不被泄露给非授权的用户、实体或过程，或供其利用，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用。保密性是在可靠性和可用性基础之上保障网络信息安全的重要手段。

（5）可控性

可控性是指网络对其信息的传播内容具有控制能力，不允许不良信息通过公共网络进行传输。

（6）抗抵赖性

抗抵赖性是指在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。数字签名技术是解决不可抵赖性的一种手段。

网络信息的保密性、完整性、可用性、真实性（抗抵赖性）和可控性又被称为网络安全目标，对于任何一个中小型网络系统都应该实现这五个网络安全基本目标，这就需要网络安全架构具备防御、监测、应急、恢复等基本功能[3]。

（1）网络安全防御是指采取各种技术手段和措施，使网络系统具备阻止、抵御各种已知网络威胁的能力。

（2）网络安全监测是指采取各种技术手段和措施，使得系统具备检测、发现各种已知或未知的网络威胁的能力。

（3）网络安全应急指采取各种技术手段和措施，针对网络系统中的突发事件，使得网络具备及时响应、处置网络攻击的能力。

（4）网络安全恢复是指采取各种技术手段和措施，针对已经发生的网络灾害事件，使得网络具备快速恢复网络系统运行的能力。

---

3 蒋建春等．计算机网络信息安全理论与实践教程[M]．西安：西安电子科技大学出版社，2005：192-195.

1.1.2 中小型网络安全面临的主要威胁

1. 自然威胁

自然威胁可能来自于各种自然灾害，如地震、火灾、水灾等。网络设备在恶劣的环境下会对数据的传输造成不小的影响，还有如电磁辐射和干扰、网络设备的自然老化等这些非人为的自然威胁都会直接或间接地影响网络安全。

2. 物理威胁

物理威胁主要体现在物理设备上，物理设备是整个网络及计算机系统的基础，物理设备的安全会直接影响整个网络信息安全，保证所有组成网络信息系统的设备、场地、环境及通信线路的物理安全是整个计算机网络信息安全的前提。如果物理设备安全得不到保证，整个网络信息安全也就不可能实现。

3. 常见的网络安全威胁

（1）黑客攻击

黑客是指利用网络技术中的一些缺陷和漏洞，对计算机系统进行非法入侵的人，黑客攻击的意图是阻碍合法网络用户使用相关服务或破坏正常的商务活动。黑客对网络的攻击方式是千变万化的，黑客的攻击方式一般是利用“操作系统的安全漏洞”、“应用系统的安全漏洞”、“系统配置的缺陷”、“通信协议的安全漏洞”等来实现。到目前为止，已经发现的攻击方式超过 2000 种，对绝大部分黑客攻击手段已经有相应的解决方法。

（2）非授权访问

非授权访问是指未经授权实体的同意获得了该实体对某个对象的服务或资源。非授权访问通常是通过在不安全通道上截获正在传输的信息或者利用服务对象的固有弱点实现的，非授权访问没有预先经过同意就使用网络或计算机资源，或擅自扩大权限和越权访问信息。

（3）计算机病毒、木马与蠕虫

对信息网络安全的一大威胁就是病毒、木马与蠕虫。在今天的网络时代，计算机病毒、木马与蠕虫已经千变万化，而且产生了很多新的形式及特征，对网络的威胁非常大。

1.1.3 打造中小型网络安全架构

打造一个安全的中小型网络架构环境：首先要建立单位自己的网络安全策略；其次根据现有网络环境可能存在的安全隐患进行网络安全风险评估；再次确定单位需要保护的重点信息；最后选择合适的网络安全防护设备。

1. 建立网络安全策略

网络安全的本质就是信息的安全，中小型网络安全的重点应该落实到信息保护上，保护住关键的业务数据才是中小型网络安全的重中之重。一个单位的网络绝不能简单地定为安全或者不安全，每个单位在建立网络安全体系之初，应该将网络内的应用清单罗列出来，再针对不同的应用给予不同的安全等级定义。需要制定科学合理的安全策略及安全方案来确保网络系统的保密性、完整性、可用性、可控性与可审查性，对关键数据的防护要采取“进不来、出不去、读不懂、改不了、走不脱”的五不原则[4]。

---

4 胡道元. 信息网络系统集成技术[M]. 北京：清华大学出版社，1995：26-28.

（1）“进不来”——可用性：授权实体有权访问数据，让非法的用户不能够进入网络。

（2）“出不去”——可控性：控制授权范围内的信息流向及操作方式，让网络内的机密不被泄露。

（3）“读不懂”——保密性：信息不暴露给未授权实体或进程，让未被授权的人拿到信息也看不懂。

（4）“改不了”——完整性：保证数据不被未授权的实体或进程修改。

（5）“走不脱”——可审查性：为出现的安全问题提供侦破手段与法律依据。

2. 信息安全等级划分

根据我国《信息安全等级保护管理办法》，我国所有的企事业单位都必须对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。具体划分情况如下[5]：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

因此，企事业单位在构建网络信息安全架构之前都应该根据《信息安全等级保护管理办法》，经由相关部门确定单位的信息安全等级，并依据界定的信息安全等级对单位可能存在的网络安全问题进行网络安全风险评估。

3. 网络安全风险评估

网络安全风险是指由于网络系统所存在的脆弱性，因人为或自然的威胁导致安全事件发生所造成的可能性影响。网络安全风险评估是指依据有关信息安全技术和管理标准，对网络系统的保密性、完整性、可控性和可用性等安全属性进行科学评价的过程[6]。

网络安全风险评估对中小型网络安全意义重大。首先，网络安全风险评估是网络安全的基础工作，它有利于网络安全规划和设计以及明确网络安全的保障需求；其次，网络安全风险评估有利于网络的安全防护，使得单位能够对自己的网络做到突出防护重点及分级保护。

4. 确定网络内的保护重点

（1）着重保护服务器、存储设备的安全。

一般来说，大量有用的信息都保存在服务器或者存储设备上，在服务器上文件的安全性比单机上要高得多。在实际工作中应该要求员工把相关的资料存储在单位服务器中，因为单位可以对服务器采取统一的安全策略，例如及时对相关信息进行备份、采取统一的访问控制策略、利用服务器访问日志记录服务器的访问信息，还可以通过统一的安全策略限制不同用户登录的

5 中华人民共和国中央人民政府：“关于印发《信息安全等级保护管理办法》的通知”，http://www.gov.cn/gzdt/2007-07/24/content_694380.htm.

6 陈琳羽．浅析信息网络安全威胁[J]．办公自动化．2009，(02).

访问权限等。

（2）边界防护是重点。

边界防护是中小型网络防护的重点。网络边界是单位网络与其他网络的分界线，对网络边界进行安全防护，首先通过网络安全风险评估来确定哪些网络边界需要防护，根据实际业务和信息敏感程度定义信息安全资产；其次对安全资产定义安全策略和安全级别，对于安全策略和安全级别相同的安全资产，可以认为属于同一安全区域。一个典型的中小型网络可以划分为：互联网连接区、广域网连接区、外联数据区、数据中心区、内网办公区、网络管理区等。

（3）“禁区”保护。

对于某些极其重要的部门，将其划为禁区，例如单位内部的一些研发、生产、客户部门，在这些区域可以采用虚拟网技术或者物理隔离技术来保证网络的安全性。

（4）终端计算机的防护。

与服务器、存储和边界防护相比，终端计算机的安全级别相对较低，但中小型网络内的安全事件往往都是从终端计算机发生的。对于终端计算机防护，最基本的病毒防护和策略审计都是必不可少的。

1.1.4 常用网络安全设备与技术

1. 防火墙技术

防火墙技术是目前最为流行也是使用最为广泛的一种网络安全技术，目的是防止未经允许和未被授权的通信出入被保护的内部网络，并且允许某个机构对流入和流出内联网的信息流加强安全策略。防火墙对流经它的网络通信进行扫描，能够过滤掉一些网络攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口，以封锁木马，禁止来自特殊站点的访问，以防止来自不明入侵者的所有通信[7]。目前，防火墙所用的主要技术有数据包过滤、应用级网关和代理服务器等

2. 入侵检测系统（IDS）

入侵检测是指对入侵行为的检测，它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测系统与防火墙不同，防火墙限制网络之间的访问，目的在于防止入侵，但并不对来自网络内部的攻击发出警报信号。但是，IDS 可以在入侵发生时，评估可疑的入侵并发出警告，IDS 还可以观察源自系统内部的攻击。从这个意义上来讲，IDS 安全工作做得更全面。

3. 漏洞扫描系统

漏洞扫描是增强系统安全性的重要措施之一，它能够有效地预先评估和分析系统中的安全问题。漏洞扫描系统按功能可分为：操作系统漏洞扫描、网络漏洞扫描和数据库漏洞扫描。网络漏洞扫描系统是指通过网络远程监测目标网络和主机系统漏洞的程序，它对网络系统和设备进行安全漏洞检测和分析，从而发现可能被入侵者非法利用的漏洞[8]。

安全漏洞主要存在于三个方面：网络中能为非授权机器提供物理接入的网络接口漏洞、

---

7 彭卓峰．防火墙技术应用分析[J]．大众科技．2004，(04)．

8 单蓉胜，王明政等．基于策略的网络安全模型及形式化描述[J]．计算机工程与应用．2005，(19)．