网管实战宝典

网管实战宝典

专业网管笔记　成就资深网管

网络安全大全

胡文启　徐军　张伍荣◎主编

PROFESSIONAL NETWORK MANAGEMENT
SENIOR NOTES ACHIEVEMENTS

清华大学出版社

网管实战宝典

网管实战宝典

专业网管笔记　成就资深网管

网络安全大全

胡文启　徐　军　张伍荣　◎主编

清华大学出版社
北　京

内 容 简 介

本书以“应用实例导航”为主线，由浅入深、系统全面地介绍了网络安全中所遇到的一些问题和常用的网络安全设备的使用方法。

本书以企业网络应用的安全需求作为出发点，以实例的形式陈述攻击行为，然后对攻击原理进行分析，并通过部署相应的设备防止攻击再次发生来介绍网络安全。本书结构清晰，易教易学，实例丰富，可操作性强，注重能力的提高，既可作为大中专院校的教材，也可作为各类培训班的培训教材。此外，本书也可作为各类企业网络管理员及各类网络爱好者、企业IT经理以及网络安全工程师的参考用书。

图书在版编目(CIP)数据

网络安全大全/胡文启，徐军，张伍荣主编. —北京：清华大学出版社，2008.10
(网管实战宝典)
ISBN 978-7-302-18619-9

Ⅰ. 网…　Ⅱ. ①胡…　②徐…　③张…　Ⅲ. 计算机网络—安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 144785 号

责任编辑：章忆文　宣　颖
封面设计：柏拉图＋创意机构
版式设计：北京东方人华科技有限公司
责任校对：李凤茹
责任印制：孟凡玉
出版发行：清华大学出版社　　地　　址：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　邮　　编：100084
社　总　机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　印　张：26.25　字　数：620 千字
版　　次：2008 年 10 月第 1 版　　印　　次：2008 年 10 月第1 次印刷
印　　数：1～4000
定　　价：39.80 元

丛 书 序

他山之石，可以攻玉。——《诗经》
你应该了解真相，真相会使你自由。——《圣经》
我之所以成功，是因为站在巨人的肩膀上。——牛顿

策划初衷

网管员(Network Administrator)是国家劳动和社会保障部近年颁布的第四批国家职业标准中明确规定的一个新兴职业。网管员职业要求从业者具备一系列专业、高端的计算机及网络操作技能。

为了给广大网管员提供一套标准实用的高效实战教材，清华大学出版社在广泛调研与充分论证的基础上，聘请了国内著名院校资深学者和实战经验丰富的网管专家，历时 18 个月精心打造了这套《网管实战宝典》。本丛书由网管员的职业应用切入，根据网管员的行业内容细划科目，以实际工作的项目案例为主线，解决实际应用中可能出现的问题，是目前市面上唯一从“网管员职业应用案例实战”角度切入的精品丛书。本套丛书全面介绍网络管理、设计与维护的热点应用案例，剖析透彻，确保技术的先进性、实用性和深入性，是网络管理员必备的实践读物。

首推书目

《网管实战宝典》系列首批推出 9 本，书目如下。

1.《中型局域网组建一本通》
2.《网络规划、设计与配置》
3.《Windows Server 2003 配置与管理》
4.《Windows Server 2003 服务器架设与管理》
5.《网络管理工具使用大全》
6.《网络安全大全》
7.《Linux 服务器架设与管理》
8.《网络故障排除与维护技巧》(Windows 版)
9.《网络故障排除与维护技巧》(Linux 版)

丛书特色

本丛书具有以下主要特色。

1. 针对性

从网管员职业应用切入，以网管员的行业内容细划科目，所介绍的内容紧紧围绕网管员必备的知识与技能展开，从而突出针对性。

2. 实用性

以实际的项目案例为主线，解决实际应用中可能出现的问题，而不仅仅是理论上的介绍。这些应用案例是广大专业人士多年的网管实战经验总结，对读者朋友有最直接、最宝贵的指导意义。

3. 可操作性

本丛书在介绍各种实际应用配置方案时，都以图解、截屏等方式与清晰的步骤相结合，避免泛泛而谈，并且着重强调了各步配置细节，方便读者按步骤操作，快速掌握案例操作过程。

4. 先进性

本丛书所介绍的各种网络技术和方案均是当前最主流，甚至最新的，读者通过阅读本丛书即可了解当前最主流，甚至最新的网络技术与应用方案。

5. 深入性

丛书中的应用案例讲解细致入微，分析透彻，过程完整，从而确保读者能够完全理解与掌握，以便在实际工作中应用与借鉴。

6. 精彩点拨

丛书以大量点评与拓展、注意、提示等特色段落为辅线，帮助读者理解与加深关键技术，使读者学得轻松，记得深刻，用得灵活。

读者对象

1. 从事网管员职业的人员。
2. 有志于网络管理员职业的读者。
3. 大专院校计算机相关专业师生，以及网络培训班学员。

创作团队

我们一直深信一流的团队，奉献一流的作品，成就一流的读者。本丛书创作团队来源

于著名院校资深学者、实战经验丰富的网管专家，他们长期工作于网管一线，有多年的网络管理与设计经历，经验丰富，实力雄厚。

互动交流

读者的进步，是我们的心愿。本丛书愿为读者提供全面的技术支持，服务方式包括：

(1) 技术讲座。将在适当的时间组织专家进行技术巡讲，介绍最新的技术并当面解答读者的疑问。

(2) 版本升级。本丛书将跟踪最新网络技术发展动态，及时更新版本，为读者提供最新的网络技术。

(3) 问题解答。如果您阅读本丛书的过程中，发现任何问题或疑问，或者有什么意见或建议，请发邮件至我们的答疑信箱 Book21Press@126.com，我们将及时为您提供解决方案。

特别致谢

在此，我们对丛书所选用的参考文献的著作者，以及丛书所引用网站及其他相关著作者表示真诚的感谢。感谢为本丛书出版提供帮助的各界人士。

知识是一个宝库，实践是打开这个宝库的钥匙。
借助于别人成功的实践经验，便是捷径。
我们乐意与您一同分享成功的网管实践经验。

——编委会

前　言

随着网络和信息技术的快速发展和日益普及，信息化成为现代企业生存的必要条件。随着企业内部信息化程度逐渐加深，网络管理员这一职业应运而生。能否管理好企业的网络事关企业的成败。

清华大学出版社策划出版了网管实战宝典系列丛书，本书是该系列教材之一。

1. 关于网络安全

网络安全实现通常很难，而且实现的成本很高，在电子通信成为无处不在的通信手段的今天，电子商务等商业实践在企业网络基础设施上逐渐展开，各个企业都试图了解和控制与之相关的风险。企业网络安全变得越来越流行，同时也使得人们感到有些担忧。绝对安全的网络是不存在的，任何设备都有配置错误或者缺陷。因此网络安全是一个长期的过程，并且需要进行日常的风险审计和风险消除。本书就是基于这样的原则，以企业网络应用的安全需求作为出发点，以实例的形式陈述攻击行为，然后对攻击原理进行分析，并通过部署相应的设备防止攻击再次发生来介绍网络安全。同时也介绍了日常安全审计的要点，从而可有效地防止网络风险。

2. 本书阅读指南

本书由浅入深、系统全面地介绍了网络安全中所遇到的一些常见问题和常用的网络安全设备使用方法。全书共分 13 章。

第 1 章主要介绍网络安全的基本原理。通过分析攻击事件的来源描述了网络安全的关键要素以及用户应具备的网络安全意识。同时讲述了一些常见的攻击实例，并对其进行了风险分析。

第 2 章主要介绍了防范常见网络攻击事件的一些方法和解决方案，并简要介绍了路由器、防火墙、VPN、IPS 等各种网络安全设备的使用。

第 3 章从几个不同的方面讨论网络设备的安全。首先是网络设备的物理安全，其中包括供电安全、环境安全等，然后介绍了各种网络设备的访问权限及相应的漏洞攻击和防范方法等；最后详细介绍了网络冗余的一些协议和实施方案。

第 4 章主要介绍路由器及路由协议安全，通过配置安全的路由协议和访问控制使得路由器更加安全。

第 5 章主要介绍交换网络安全，并介绍了处理广播攻击、MAC 攻击、VLAN 欺骗、ARP 病毒等二层攻击的方法。

第 6 章主要介绍 AAA 体系结构以及基于 Radius 的身份认证体系，同时也介绍了 Windows 电子证书服务及 PKI 证书体系。

第 7 章主要介绍网络安全接入以及终端安全，同时介绍了部署 802.1x、Cisco NAC 以及

WSUS 自动更新服务的配置方式。同时还介绍了基于终端的安全防护产品 CSA/CSA-MC。

第 8 章主要介绍防火墙的工作原理，同时介绍了 Cisco PIX/ASA 防火墙、微软 ISA 防火墙以及 Linux 防火墙的配置方式。

第 9 章主要介绍入侵检测系统和入侵防御系统的配置方式，并讲述了常见 IPS/IDS 系统及 IDS 的部署，最后介绍了基于 Cisco 的 DDoS 防御技术。

第 10 章主要介绍远程访问的知识，并且介绍了 IPSec VPN、SSL VPN、ISA Server VPN 和 Linux VPN 的配置方式，同时还介绍了常见的 VPDN 远程接入配置。

第 11 章主要介绍网络管理软件，如何通过对日志进行统一管理获得较快的攻击响应速度。

第 12 章主要介绍基于 EFS 的文件加密系统和 RMS 文件权限控制系统等。

第 13 章根据各种企业规模进行了网络安全方案设计，并根据企业的规模和资金状况设计了多种网络安全升级方案。

3. 本书特色与优点

(1) 系统地讲述了局域网面临的安全问题及防范措施。本书对局域网络中的关键软硬件设备，如操作系统、服务器、客户机、路由器、交换机和防火墙的安全性进行了分析，并针对这些设备的安全隐患指出了加固的方法，其目的是从整体上提高局域网络的安全防御能力。

(2) 重视实用性和可操作性。本书偏重于实际操作方法的讲述，目的是为那些从事网络管理及网络安全规划与设计的从业人员提供一定的安全操作参考。另外，对网络安全感兴趣的读者也可以从本书中学习到网络防御的基本知识和技巧。

(3) 以“应用实例导航”为牵引。本书在介绍各种网络入侵手段与应对措施时，都通过一个应用实例导航进行导入，这些应用实例大多数是作者在实际工作中遇到的问题，旨在为读者解决大型网络安全问题提供思路和借鉴。

(4) 网络安全产品选择具有代表性。目前，网络安全产品众多，使用与配置方法各不相同，但原理基本相同。由于 Cisco 和 Microsoft 所生产的网络安全产品在局域网使用广泛，技术先进，本书就以 Cisco 和 Microsoft 的网络安全产品为例，介绍如何实施和管理网络安全。

4. 本书读者

本书既可作为大中专院校的教材，也可作为各类培训班的培训教程。此外，本书也可作为企业网络管理员及网络爱好者、企业 IT 经理以及网络安全工程师的参考用书。

本书由胡文启、徐军、张伍荣编写，全书框架结构由何光明拟定。另外，许勇、吴婷、陈玉旺、许娟、吴蕾、姜萍萍、赵传申、杨明、杨萍、陈芳、范荣钢、钱阳勇、陈智、张凌云、王国全、丁善祥等同志对本书出版亦作出了重要贡献，在此一并感谢。

限于作者水平，书中难免存在不当之处，恳请广大读者批评指正。

编　者

目　录

第 1 章　网络安全基础

随着 Internet 的迅猛发展以及电子交易的逐渐增多，基于网络的应用程序和服务使所有公司信息资源的安全风险增加。在资产评估方面，信息资产将成为一种非常重要的受保护资产。如果没有充分的保护，个人、企业和政府将面临巨大的资产流失风险。

网络安全主要是保护数字资产的机密性和完整性，以及确保这些数字资产的可用性。根据这个原则，本章将介绍如何应对多种网络威胁。通常，这些威胁源于不同种类的攻击行为，或者来自一些软硬件的错误配置以及最终用户的疏忽等。有一点是值得我们注意的，我们无法完全消除网络威胁，但我们可以对网络进行有效的安全评估和风险管理，从而使网络威胁降到最低。

通过本章的学习，读者应掌握以下主要内容：

- ✧ 网络安全的基本原理
- ✧ 攻击事件的来源
- ✧ 网络安全的关键要素
- ✧ 如何提高用户安全意识
- ✧ 如何进行网络安全分析

1.1　网络安全的基本原理

1.1.1　网络发展及需求

传统的网络安全观点认为，封闭式的网络具有较高的安全性，而且当时的运营商受技术限制，远程接入的封闭式网络通常仅能使用调制解调器拨号的方式，如图 1-1 所示。

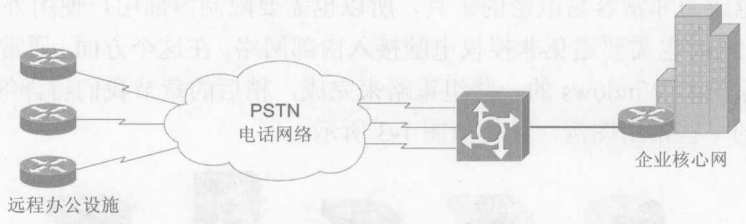

图 1-1　封闭式网络

但随着 Internet 的发展，各种新技术不断涌现，网络交流更加顺畅，企业办公也逐渐转移到 Internet 这样开放式的网络上。这就带来一个矛与盾的问题：一方面需要将自己公司的信息公布于众，另一方面又需要将敏感数据仅供授权用户访问。

大量的安全风险是由局域网和个人电脑接入 Internet 而产生的。特别是对于公司，它的一些公共接口的服务器和电脑成为泄密的最大来源。而这些供访客和公众使用的设备，通常没有专人维护，导致系统和应用软件补丁更新不及时，从而非常容易受到攻击。通常我们把这种攻击叫做“0 day”入侵，因为这些入侵借鉴已有的漏洞报告，仅需要 0 天的时间就能完成攻击。

我们对于这种攻击的解决办法是采用深度的防御模型，也就是说，使用防火墙将公共领域的服务器和接入的计算机与核心工作区域隔离。在防火墙的产品定义中，通常借鉴军事上的定义方式，将与公众接触的计算机定义为非军事化区域(Demilitarized Zone，DMZ)，简称 DMZ 区域。例如 Web 服务器、邮件服务器、DNS 服务器、前台查询计算机等。而内部的文件服务器、数据库服务器等关键应用都放置在军事化区域中，受到良好的保护，如图 1-2 所示。即便 DMZ 区域的设备因某些“0 day”攻击而导致瘫痪，黑客也会因受到防火墙的隔离而无法访问内部网络。

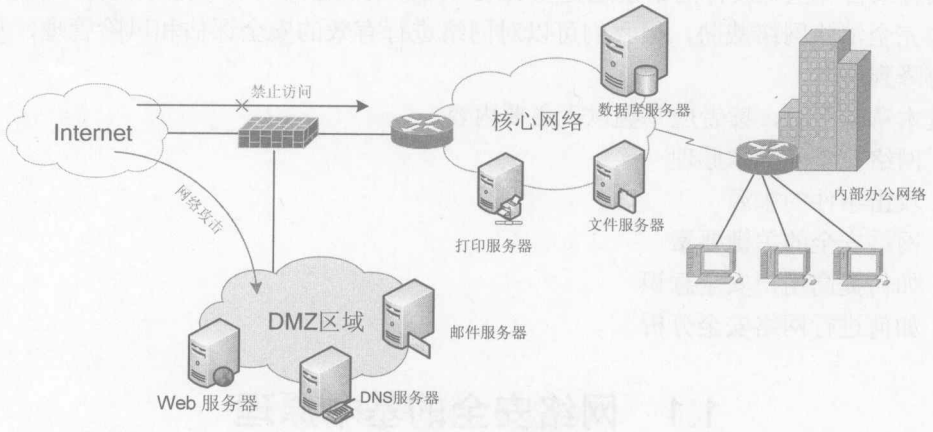

图 1-2　DMZ 区域

在此，虽然我们抵御了来自外部的攻击，但有一个因素我们必须考虑，来自内部的威胁通常更大。最近的统计数据表明，80%的网络安全问题来自网络内部。所以我们需要采取一些措施来降低内部的威胁。首先需要限制内部用户的访问权限，使得只有授权用户能够连接到数据库服务器、文件服务器、打印服务器等关键应用服务器。随着技术的发展，U 盘、移动硬盘也成为非常容易泄密的工具，所以也需要限制内部用户使用外接硬件的权利，避免数据被窃；同时也需要避免非授权电脑接入内部网络。在这个方面，通常使用的是 NAC 接入访问控制系统和 Windows 的一些组策略来完成，稍后的章节我们将详细介绍。

本书使用的一些常用图例，具体如图 1-3 所示。

图 1-3　图例

1.1.2　攻击事件的来源

除了少部分黑客基于研究目的带来的攻击外，大多数的网络攻击出于一些特定的目的。根据《2006 年度中国网络安全报告》的结论，截止到 2006 年 12 月 25 日，据不完全统计，中国网络发生的网络攻击事件中，脚本入侵比例为 53%，拒绝服务攻击比例为 26%，漏洞利用比例为 13%，暴力猜解比例为 8%，社会工程学比例为 5%，其他方法为 1%。但与 2005 年同期相比，2006 年度的网络攻击事件要多出 1 倍之多。据不完全统计，自 2006 年 1 月 1 日起，截至 2006 年 12 月 25 日，中国网站被篡改的数量达 25 820 个。其中政府类网站有 3661 个；企业类网站为 11 828 个(其中博客运营类被攻击数量达 1683 个)；教育\培训类被攻击网站数量达 2216 个，其中：中、职专及中小学网站占 73.5%(1628 个)，大学网站的二级网站占 18.0%(398 个)，培训类机构为 127 个，大学一级域名站点为 63 个。

下面是 2006 年出现在我国几个著名的攻击的事件。

- ✧ 2006 年 5 月 27 日，某市的区政府服务器被入侵并植入香港汇丰银行的假冒网站。2006 年 4 月，国外多家媒体以《中国的银行网站被利用作 Phishing》为题，报道了中国某银行网站被植入假冒 Paypal 网站的事件。
- ✧ 2006 年 6 月 19 日，D 市某区政府网站邮件服务器被入侵并植入电子港湾(eBay)的假冒网站。
- ✧ 2006 年 9 月 12 日，著名搜索引擎百度遭受有史以来最大规模的不明身份黑客攻击，导致百度搜索服务在全国各地出现了近 30 分钟的故障。
- ✧ 2006 年 9 月 21 日，某域名服务商“新网”域名解析服务器发生故障，造成超过 30%在其上注册的网站无法访问长达 20 小时。“新网”官方确认此次断网事件是黑客所为。此事件被称为中国互联网的“9 • 21 事件”。

在具体的攻击手法上也有变化，猜测口令、物理入侵、安装键盘记录设备以及盗窃笔记本电脑等传统方式的攻击成功率逐渐下降，而 SQL 注入、钓鱼、拒绝服务攻击以及各类木马病毒等攻击频率急剧上升。更值得关注的是，内部人员滥用网络、盗窃关键数据的事件也在上升。随着无线网络的使用，无线网络入侵也成为一个非常值得关注的焦点。

1.1.3　网络安全的关键要素

虽然 Internet 的成功带来了全球信息化的一次巨大飞跃，但是它必须以保护有价值数据和网络资源免受篡改和入侵为基石。

1. 网络安全目标

M. Fites、P. Kratz 等在《Control and Security of Computer Information Systems》中提出了一个被广泛采用的网络安全性设计建议。该建议包括以下内容。

- ✧ 确定要保护什么。
- ✧ 确定尽力保护它免于什么威胁。
- ✧ 确定威胁的可能性。
- ✧ 以一种相对廉价的方法来实现资产保护的目的。

✧ 不断地检查这些步骤，发现弱点就进行改进。

2. 资产评估

资产评估用于实现网络安全目标的第一步，需要确定保护什么。通常的资产评估仅对网络设备(例如交换机、路由器、防火墙、电脑)等实物以及关键数据进行评估，而忽视了这些设备上的配置信息、用户访问权利，随着 DDoS 攻击的增加，可用带宽和访问速率也成为资产评估一个不可缺少的部分。当然资产评估随着需要保护的资产数量增长还会出现变化，下面列举了一些重要的网络资产。

✧ 网络设备：路由器、交换机、防火墙、入侵检测设备。
✧ 网络数据：数据服务器、邮件服务器、Web 服务器等。
✧ 网络带宽：链接网络的链路带宽和速度，以及冗余备份线路。
✧ 个人电脑：个人电脑是否携带关键数据以及个人电脑安全防护。
✧ 任意时刻通过网络的消息是否安全。
✧ 网络身份识别是否有效。

3. 威胁评估

根据网络安全目标，完成资产评估后需要对威胁进行评估。通常的攻击手段主要有 3 种类型。

✧ 未授权的网络资源访问。
✧ 未授权的网络数据修改和操作。
✧ 拒绝服务。

授权是网络威胁的一个重要环节，给用户授权通常可以使用很多方式，最常见的身份认证协议是 RADIUS (Remote Access Dial-In User Service，远程访问拨入用户服务)、TACACS+ (Terminal Access Controller Access Control System，终端访问控制器访问控制系统 Plus)、Kerberos 等。当然，还有新兴的数字证书、智能卡、生物界定和目录服务等。

4. 网络安全策略

当完成对威胁的评估后，就需要进行相应安全策略的指定工作了。按照 RFC-2196 站点安全手册的建议，可以从如下几个方面入手指定相应的安全策略。

1) 提供服务和保证安全

每个提供给用户的服务都会带来安全上的风险。对于有的风险高于受益的服务，管理员可能宁愿选择取消它而不去再试图保护。

2) 易用性和安全性

使用起来最简单的系统是允许任意用户不使用密码就可以访问的系统，也就意味着没有任何安全性。要求密码使得系统有些不方便，但是却更安全了。需要设备产生的一次性密码使得系统更不方便了，但是要安全得多。

3) 保障安全的开销和发生损失的风险

保障安全的开销有许多种：金钱(购买像防火墙和一次性密码生产器这样的安全设备和软件的花销)、性能(加密和解密要花费时间)和易用性。发生损失的风险也有许多级别：泄密(信息被未授权的个人所阅读)、数据丢失(信息错误或消除)和服务损失(填充数据存储空间、占用运算资源和拒绝网络服务)。每种开销都要和每种损失作权衡。

RFC-2196 中规定了一个好的网络安全策略应包括如下几个方面。

- ✧ 计算机技术购买的指导方针。它指出什么是必需的或首选的，指出安全的特征，这些对于已存在的购买的政策和指导方针将是补充。
- ✧ 隐秘政策。它规定了对隐秘的合理期望，比如怎么对待电子邮件的监视、按键记录和用户文件访问。
- ✧ 访问政策。它通过列举用户、操作人员、管理者允许使用的功能，规定了存取访问的权利和特权，从而保护资产不损失或泄密。它会在外部的连接、数据交流、网络连接装置和给系统添加新的软件等情况下，提供指导方针。它同时也要列出需要声明的信息(例如，连接信息应该提供关于授权使用和线上监视的警告，而不是仅仅简单地显示“欢迎”)。
- ✧ 责任政策。它规定了用户、操作人员、管理者的责任。它应该明确谁有审查的能力，并提供突发事件的处理方针(就是如果发现可能被入侵了要做什么和联系谁)。
- ✧ 认证政策。它通过有效的密码政策建立信任，使用对远程身份认证设置指导方针的方法或使用认证设备(这里指一次性密码和产生一次性密码的设备)。
- ✧ 可用说明。它预计了用户可以使用的资源。它应该考虑到冗余和恢复的情况、特殊的工作时间和停机维护的时期。它应该也包括系统和网络失败报告的连接信息。
- ✧ 信息技术系统和网络维护政策。它描述了人们被允许怎样运用技术手段进行内部和外部的维护。这里要考虑的一个重要话题是是否允许远程维护，这种访问怎么控制。这里要考虑的另一个问题是外购和怎么管理它。
- ✧ 侵害报告政策。它指出哪种侵害(秘密还是安全，内部还是外部)必须报告，报告给谁。无危险的气氛和匿名报告将会导致被发现的侵害都更可能报告上来。
- ✧ 支持信息。它向用户、职员和经理提供每种侵害的联系信息；怎么处理外部的关于安全事件的询问或什么可以当做秘密私有的指导方针；安全程序和相关信息的交叉参照，例如公司政策和政府的法律规章。

对有些安全政策(如在线监控)可能需要一些调整，安全政策的创建者在产生政策的时候应该考虑寻求法律援助，至少这些政策必须让法律顾问过目一下。一旦安全政策已经建立，应该清楚地与用户、职员和经理进行交流，让所有人都写下一句话表明他们已经阅读过，并且同意遵守这个政策。最后，安全政策应该被当做一个正式的基本政策进行重新检查，看看它是否成功地支持了安全需求。

1.1.4　用户安全意识

正如前述，现在较多的安全漏洞都是由用户不经意间的一些操作引起的，每个公司有必要为员工提供足够的训练来教育他们如何安全地使用这些设备。这种训练需要所有设计、实现和维护网络的人员参与。同时除了技术类的培训外，还应该加强内部控制等。负责网络安全的人员应该对安全技术、威胁评估、标准威胁处理流程及系统补丁及时升级等进行进一步的练习。而作为账号管理员，或者密码分发人员，需要在职员提供完全真实的信息后才能进行相关口令的处理，但很多时候口令的泄露是因为没有被要求出示足够详细的证件。

在终端安全方面通常可以采用安全代理工具来完成一些安全性检查，同时，还可以通过 NAC 网络接入控制来限制未授权的电脑接入网络。

1.2 网络安全实例分析

应用实例导航：A 大学网络安全风险评估

※场景呈现

A 大学是一所历史悠久的全国重点高校，校园网络相当复杂，同时它又是某国家网络的骨干结点，所以网络安全是一个非常重要的环节。众多的服务器和接入计算机使得网络维护难度相当大，因此需要对整个网络进行相应的安全评估和风险分析，然后做出适当的安全升级方案。

※技术要领

(1) 资产评估；
(2) 风险分析；
(3) 制定安全策略。

1.2.1 资产评估

首先要做的仍旧是资产评估，通过资产评估来确定网络需要保护什么。A 大学的资产如下所示。

- ✧ 接入用户。学生宿舍网络用户约 4 万人，办公区各院系共有近 3000 台计算机接入网络。
- ✧ DNS 服务器、邮件服务器、教学视频等点播服务器、BBS 服务器、数据库服务器、存储服务器、学生选课系统服务器及财务和在线办公室服务器等。
- ✧ 链接各校区骨干网链路为 10Gbps 以太网。
- ✧ 链接 ISP 为教育网 3Gbps，中国电信 2Gbps，中国网通链路 1Gbps，中国移动链路 1Gbps。
- ✧ 教育网某骨干结点，其中运营商级路由器 10 台。
- ✧ 交换机、路由器等设备来自 Cisco、Extreme、Foundry、实达、华为等多个厂商。
- ✧ 用户接入采用 IP-MAC 绑定策略。
- ✧ 简单的流量监控系统。
- ✧ 网络管理员较少，并且各信息系统开发独立。
- ✧ 仅有简单的网络安全监控设备。

以上是 A 大学所有与网络有关的硬件资产分析，这些网络设备是要保护的资产，当然资产中最重要的并不是这些硬件资产，而是各个数据库中的数据。从后面的实例我们将逐渐看到数据的价值远远高于这些硬件产品。