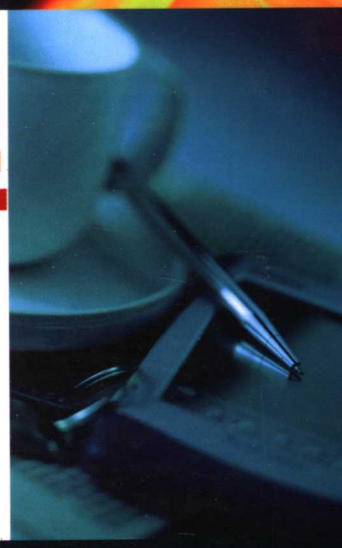
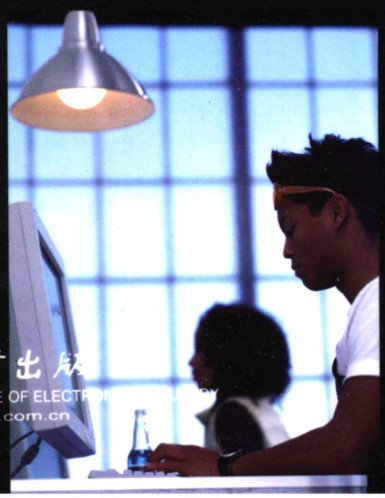
计算机信息安全管理

COMPUTER INFORMATION SECURITY MANAGE



徐超汉　编著

COMPUTER INFORMATION SECURITY MANAGE



電子工業出版
PUBLISHING HOUSE OF ELECTRONICS
http://www.phei.com.cn

计算机信息安全管理

徐超汉　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书在编写的过程中，遵照信息安全管理国际标准 ISO/IEC17799 的精神和原则，对信息安全的风险管理、信息安全策略、信息安全教育、信息安全的组织管理，以及在信息安全管理中常用的安全技术作了详细的介绍。

信息安全不是一个纯粹的技术问题，信息安全重在管理。因此，本书除了适用于计算机系统管理员、网络管理员和信息工程系统集成工程师外，也适用于有关主管领导和计算机网络系统资源的所有使用者。

图书在版编目(CIP)数据

计算机信息安全管理/徐超汉编著. —北京：电子工业出版社，2006.4
ISBN 7-121-02426-8

Ⅰ.计… Ⅱ.徐… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2006）第 024819 号

责任编辑：龚立堇
印　　刷：北京市天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：13　字数：331.2 千字
印　　次：2006 年 4 月第 1 次印刷
印　　数：5 000 册　　定价：22.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着各种计算机应用系统在各行业中的普及，各种安全事件时有发生，加上计算机病毒的广泛传播，使计算机信息安全引起了人们的高度关注。

所谓的信息安全是指对信息的保密￥性、信息的完整性、信息的可用性的保护。

信息安全不是一个纯粹的技术问题，不可能只依赖于大量的人力、物力和财力，在计算机信息网络系统的周边，用信息安全产品建造信息安全的“长城”，来应对迅速发生变化的各种安全威胁和攻击。信息安全重在管理，信息安全保护工作，七分在于管理，三分在于技术支撑和保障。

本书在编写的过程中，遵照信息安全管理国际标准 ISO/IEC17799 的精神和原则，对信息安全的风险管理、信息安全策略、信息安全教育、信息安全的组织管理，以及在信息安全管理中常用的安全技术作了详细的介绍。

本书共分 15 章。第 1 章综合性地对信息安全管理作了概念性的介绍。第 2 章介绍安全风险管理，并探讨了风险的定性和定量分析、风险评估的模型，以及风险评估与安全评估的关系等。第 3 章到第 12 章，对信息系统的物理层、运行、访问控制、应用系统、操作系统等的安全策略与管理，以及数据保密性、完整性、有效性等各方面的管理措施作了全面、详细的论述。第 13 章描述了信息安全教育的内容、目的，以及信息安全教育的策略。第 14 章介绍了信息安全的组织管理所涉及的信息安全团队的构建与管理。第 15 章简单介绍了信息系统常用的安全技术，包括防火墙、入侵检测系统、安全扫描系统，以及反垃圾邮件技术。

信息安全管理是一个全新的课题，理论知识和实践经验的不足在情理之中，又由于作者的水平有限，时间仓促，在编写之中难免有不妥之处，衷心希望广大读者批评指正。

作　者

2006 年元月于广州

目　录

第1章　信息安全管理概述

计算机信息安全问题属于信息技术或相关技术部门的管理范围。很长一段时间以来，信息安全被误认为仅仅是一个安全技术问题。因此，安全措施较为被动，只针对发生的事件进行反应处理，很少考虑从管理层有计划地主动检查是否存在安全隐患，以达到预防安全问题发生的目的。其实，信息安全除了需要先进的安全技术（设备）之外，还需要有安全的技术管理，以及安全的组织行政管理等。

被动的在需要时才去寻找信息或信息系统安全的解决方案已经不适应当前的信息安全的需要，只有通过了解信息安全管理的本质，制定相应的信息安全管理方法，完善信息安全管理机制，才能在不影响整体系统正常运作的前提下，达到信息高度安全性的目的。

1.1　基 本 概 念

计算机信息安全管理是信息安全的核心。本节介绍几个有关计算机信息安全的基本概念。

1.1.1　数据的保密性

所谓的数据保密性是指防止信息被未经授权者访问和防止信息在传递过程中被截获并解密的性能。

数据保密性可分为静态信息保密性和动态信息保密性。静态信息保密性的特征表现为数据存储保密性，而动态信息保密性表现为信息在网络传输过程中的保密性。

数据存储保密性通常可以通过访问控制来实现，具体表现为根据不同访问者可访问的数据不同，把数据分为敏感、机密、私用、共用等级别。这种访问控制可以通过网络操作系统所提供的功能予以实现。此外，需谨防存储数据的介质被人窃走。因此，必须加强相关部门的安全保卫，建立物理安全访问机制。

动态数据保密性的解决方法是对传输的数据进行加密处理。

常用数据保密技术有：

- 防侦收，即使第三者收不到有用的信息；
- 防辐射，即防止有用信息以电磁波的形式辐射出去；
- 信息加密，即使用加密算法对信息进行加密处理，使第三者即使得到了加密的信息也因没有密钥而无法读其含义；
- 物理保密，即用物理方法，如限制、隔离、掩蔽和控制等措施保护信息不被泄露。

1.1.2 数据的完整性

数据的完整性是指信息未经授权不能进行改变的特性，即信息在存储或传输中保持不被删除、修改、插入、伪造、重新排序等破坏和丢失的特性。换言之，数据的完整性要求保持数据的原样，即数据的正确生成、正确存储和传输。

影响数据完整性的主要因素有：设备故障、误码、操作失误、计算机病毒，以及黑客的攻击等。

确保数据的完整性、正确性的方法有：

- 纠错编码方法，最常用的纠错编码方法是奇偶检验法；
- 密码检验和方法，它是抗篡改和检验传输失败的主要手段；
- 数字签名，保障信息的真实性；
- 协议，通过各种安全协议可有效检测被复制的信息、被删除的字段、失效的字段和被修改的字段。

1.1.3 数据的可用性

数据的可用性是保证经授权的用户可以访问到所需的信息。这里所指的信息是指存放在主机中的静态信息。

数据的可用性是信息系统面向用户的性能。当信息系统向用户提供信息服务时，允许授权用户或实体使用的特性，即使在系统部分受损或需要降级使用时，仍然能为授权用户提供有效的服务。

数据的有效性是有条件的，其基本条件包括：身份确认、访问控制、业务流程控制，利用负载均衡的方法，防止业务流量的过度集中而导致网络的阻塞、路由选择、审计跟踪等。

1.1.4 信息安全

计算机信息安全是指对信息的如下三个方面的保护：

- 保密性，即确保信息只能由授权的用户或实体访问；
- 完整性，即保证信息的正确性和完整性，以及对信息的处理方法；
- 可用性，即保证授权的用户可以访问正常的信息。

信息安全是一个动态发展的过程，它不仅仅是一个纯粹的技术问题，只依赖于网络信息安全产品的堆积来应对迅速发展变化的各种威胁和攻击是不能持续有效的。信息安全重在管理，信息安全保护工作七分在于管理，三分在于技术支撑和保障。

信息安全可以通过实施一整套控制管理措施才能达到。这些措施包括：安全风险管理、安全策略、安全教育、行政组织管理，以及软件功能等。对一个企业或一个机构来说，要达到信息安全的目的，建立这些控制与管理措施是必要的。

1.1.5 信息安全风险评估

信息安全风险评估是对信息系统的威胁、影响、脆弱性三者发生的可能性评估。这是

确认安全风险及其大小的过程，它通过利用适当的风险评估工具，包括定性和定量的方法，确定信息资产的风险等级和优化控制的顺序。

信息安全风险评估是应用广泛的一种安全评估方法，是信息系统风险管理的前期活动。根据风险评估实施方法的不同可分为自评估和他评估服务两类。自评估是信息系统所有者对自己系统所进行的安全风险评估，而他评估是包括第二方商业机构或第三方中立机构所提供的安全风险服务。该方法采用定性或定量的方法对信息系统存在的安全风险进行分析和度量。不过，该方法得出的结果——风险值的高低并不直接等同于系统安全程度的高低。而且，风险分析方法及活动还得依赖于经验、数据和评估人员或专家的实际经验。

由于自评估是自我的安全评估，因此，在涉及到一些重大问题时，其客观性、有效性和公正性难以保证。而第二方的安全风险评估大多只是适用于商业性系统，对于涉及国家机密、国家国计民生及重要基础设备等关键信息系统，特别是大的信息系统，则不适宜采用第二方商业性质的安全风险评估。第三方的安全风险评估由于其中立性、公正、公平、科学、客观，而且通常具有政府背景和权威性，因此，其应用范围最为广阔。

1.1.6 信息安全策略

信息安全策略是一种处理信息安全问题的管理策略，它为信息安全提供安全管理和支持。信息安全策略涉及到信息系统的硬件、软件、访问、连接、网络、通信、用户及实施等各个方面。

信息安全策略应该简明，在生产效率和安全性之间应该有一个好的平衡点，易于实现，易于理解。信息安全策略必须遵循确保数据的保密性、完整性和有效性三个基本原则。

信息安全策略为一个信息系统的总体安全提供一份计划，使应用者能按照定义的方式来确保信息的安全，其主要特点：

- 有效的安全策略应能支持绝大部分的需求，同时，能保护好企业的利益；
- 安全策略的制订需由一名负责系统安全领域的高层领导，有法律、相关技术部和用户代表组成制订的草案，需进行审查和评估；
- 安全策略应清晰，具有可操作性；
- 安全策略应提供框架结构说明和一些目标要求，必须进行用户培训，引导受训人员明确构建信息安全系统环境的重要性。

1.2 信息安全的隐患

计算机信息系统不安全的因素来自两个方面：一方面是信息网络本身存在的安全缺陷；另一方面是人为因素和自然因素。自然因素是一些意外事故，如发生地震毁坏信息系统，这种因素并不可怕，可怕的是人为因素，即人为的入侵和破坏。

由信息系统自身存在的安全隐患导致信息系统不安全的主要因素有：网络操作系统的脆弱性、TCP/IP 协议的安全性缺陷、数据库管理系统安全的脆弱性、系统资源共享、数据通信、计算机病毒等。

1.2.1 网络操作系统的脆弱性

网络操作系统是计算机信息系统最基本的软件，无论哪一种操作系统其体系结构本身就是一种不安全的因素。由于操作系统是可以动态连接的，包括 I/O 驱动程序和系统服务都可以用打补丁的办法进行升级和动态连接，这种打补丁的方法正是计算机病毒产生的温床。由于操作系统使用的程序动态连接和数据动态交换是现代系统集成和系统扩展的必备功能，所以，操作系统的这种安全性弱点是无法避免的。

操作系统不安全的另一个原因在于它可以创建进程，即使在网络结点上，同样也可以进行远程的创建和激活。更令人不安的是被创建的进程具有可以继续创建进程的权利，这一点再加上操作系统能支持网上传输文件，能加载程序，二者结合起来构成了可以在远端服务器上安装“间谍”软件的条件。如果把这种“间谍”软件以打补丁的方式“打”入合法用户，尤其是“打”入特权用户，那么，系统进程与作业监视程序根本监视不到“间谍”的存在。

在 UNIX 与 Windows 中的 Daemon 软件实际上是一些系统进程，它们通常总是在等待一些条件的出现，一旦满足要求的条件出现，程序将继续运行下去。这类软件正是被“黑客”所看中利用的。更令人担忧的是 Daemon 软件具有与操作系统核心层软件同等的权力。

网络操作系统提供的远程过程应用（RPC）服务，以及它所安排的无口令入口也是黑客攻击信息系统的通道。

凡此种种，充分暴露了操作系统在安全方面的脆弱性对信息系统的安全已构成了严重的威胁！

1.2.2 TCP/IP 协议的安全隐患

因特网的基础是 TCP/IP 协议，该协议实现上力求简单高效，而没有考虑安全因素。第一，TCP/IP 是以明文（未加密）数据包的方式传递的，电子邮件口令、文件的传输都很容易被监听和窃取，而且可用的实现监听和窃取行为的工具还不少，在网上又是免费提供的；第二，基于 TPC/IP 的应用服务都不同程度存在安全上的隐患；第三，TCP/IP 在流程设计上也存在安全缺陷，缺乏安全策略；第四，访问控制的配置十分复杂，易被错误配置，从而给黑客以可乘之机。

1.2.3 数据库管理系统安全的脆弱性

数据库管理系统（DBMS）对数据库的管理是建立在分级管理的概念上的，因此，数据库管理系统的这种多级管理的安全是可想而知的。另外，数据库管理系统与网络操作系统之间存在不少接口，它的安全必须与操作系统的安全配套，这无疑是一个先天性的不足之处。由于数据库管理系统是在操作系统上运行的，因此，这种安全上的弱点是无法克服的。

1.2.4 网络资源共享

计算机信息系统的最大优点是系统资源的共享，包括硬件资源、软件资源、数据资源等的共享。各终端用户可以访问服务器的资源，各终端用户之间也可以相互共享资源，这种资源的共享为异地用户提供了巨大的方便，同时，也为非法用户窃取信息、破坏信息创造了条件。非法用户可以通过终端或结点进行非法浏览、非法修改。此外，系统的硬件或软件的故障也可能引起信息的泄密。由于大多数共享的资源，同许多使用者之间往往有相当一段距离（如网络打印机），这样就给窃取信息者在时间和空间创造了许多便利的条件。

1.2.5 数据通信

计算机信息系统需要通过数据通信来交换信息，这些被交换的信息是通过物理线路或无线电波，以及电子设备进行传播的，这样在通信中传输的信息极易遭到窃取和破坏，如网络侦听、搭线窃取、电磁窃取、网络线路的辐射泄密等。

1.2.6 网络结点存在的隐患

计算机信息系统可以从各个结点接受信息，因而极易感染到计算机病毒。病毒一旦侵入网络系统，再按指数增长进行复制和传染，很快就会遍及网络系统的各结点，在短时间内可以造成网络等无法正常工作，甚至于瘫痪。

1.2.7 系统管理造成的隐患

计算机信息系统的正常运作离不开系统管理员对信息系统的管理。对系统的管理措施不当或监管不严都可能影响系统的正常运作，甚至造成硬件资源的损坏及敏感信息的泄露。

1.3 信息系统面临的威胁

计算机信息网络系统所面临的威胁可分为两大类：一是对系统中信息的威胁；二是对系统中的硬件资源的威胁。下面仅对影响信息的威胁进行讨论。

1.3.1 非法授权访问

所谓的非法授权访问是指事先未经同意或委托授权，擅自扩大权限、越权对系统信息进行访问。非法授权访问的表现形式有：假冒，非法对信息网络系统进行违法操作，合作用户未经授权进行操作，以及身份攻击等。

1.3.2 信息泄露或丢失

信息泄露或丢失是指信息在有意或无意（如误操作等）中被泄露出去或丢失了。信息泄露或丢失通常发生在信息传输过程或在介质中。在传输过程中，黑客们可利用电磁泄露