

<<信息安全管理基础>>

图书基本信息

书名：<<信息安全管理基础>>

13位ISBN编号：9787115176349

10位ISBN编号：7115176345

出版时间：2008-5

出版时间：人民邮电出版社

作者：北京大学电子政务研究院电子政务与信息安全技术实验室

页数：305

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<信息安全管理基础>>

### 内容概要

为了推进我国信息化人才建设，CEAC国家信息化培训认证管理办公室组织IT和培训领域的资深专家精心编写了国家信息化计算机教育认证系列教材。

本书作为国家信息化计算机教育认证项目电子政务与信息安全培训认证专项的教材之一，以国际主流的安全技术为基础，详细介绍了信息安全涉及的安全理论知识与技术。

本书根据企事业单位和信息安全从业人员的实际需求，深入浅出地介绍了信息安全的物理安全、身份鉴别与认证、风险管理、安全管理策略等内容，并详细阐述了用户必须了解的安全法规和标准。

本书结构清晰，讲解详细，并在每章后配有丰富的思考与练习题。

非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导教材，还可供读者自学使用。

## &lt;&lt;信息安全管理基础&gt;&gt;

## 书籍目录

- 第1章 信息安全管理概述 1.1 全球信息安全发展形势 1.1.1 互联网骨干网络面临的安全威胁 1.1.2 根域名服务器面临安全威胁 1.1.3 全球黑客动向 1.2 中国信息安全形势 1.3 信息安全管理基本概念 1.3.1 信息安全及信息安全管理 1.3.2 信息安全管理系统 1.4 我国的信息安全管理 1.4.1 我国的信息安全管理现状 1.4.2 我国信息安全管理存在的问题 本章小结 思考与练习
- 第2章 物理安全 2.1 物理安全威胁与安全需求 2.2 机房与设施安全 2.2.1 机房安全等级 2.2.2 机房场地的环境选择 2.2.3 机房组成及面积 2.2.4 机房的环境条件 2.2.5 电源 2.2.6 围墙和门禁 2.2.7 锁的使用 2.2.8 网络通信线路安全 2.2.9 机房物理基础设施解决方案举例 2.3 技术访问控制 2.3.1 人员控制 2.3.2 检测监视系统 2.3.3 审计访问记录 2.4 防火安全 2.4.1 火灾检测 2.4.2 火灾抑制 2.5 电磁泄漏 2.5.1 计算机设备防泄露措施 2.5.2 计算机设备的电磁辐射标准 2.6 有关物理安全威胁的特殊考虑 本章小结 思考与练习
- 第3章 身份鉴别与认证 3.1 用户标识与鉴别 3.1.1 什么是用户标识 3.1.2 什么是用户鉴别 3.2 用户鉴别的原理 3.2.1 鉴别的分类 3.2.2 实现身份鉴别的途径 3.2.3 Kerberos鉴别系统 3.3 证书授权技术 3.3.1 什么是PKI 3.3.2 什么是数字证书 3.3.3 X.509证书标准 3.3.4 认证中心 3.3.5 数字证书的应用 3.3.6 安全电子邮件 3.4 一次性口令认证 3.4.1 一次性口令 3.4.2 口令安全 本章小结 思考与练习
- 第4章 风险管理 4.1 安全威胁 4.2 风险管理 4.2.1 识别熟悉信息系统 4.2.2 识别检查机构漏洞 4.2.3 所有的利益团体都应负责 4.3 风险识别 4.3.1 资产识别和评估 4.3.2 自动化风险管理工具 4.3.3 风险分类 4.3.4 威胁识别 4.3.5 漏洞识别 4.3.6 正确看待风险识别 4.4 风险评估 4.4.1 风险评估分析策略及实施流程 4.4.2 风险评估种类 4.4.3 风险评估分析方法 4.4.4 风险消减—实施安全计划 4.5 风险控制策略 4.5.1 避免 4.5.2 转移 4.5.3 缓解 4.5.4 承认 4.5.5 风险缓解策略选择 4.5.6 控制的种类 4.6 有关风险管理的特殊考虑 4.6.1 风险可接受性 4.6.2 残留风险 4.6.3 实施风险管理的一些建议 本章小结 思考与练习
- 第5章 安全管理策略 5.1 安全策略 5.1.1 安全策略的建立 5.1.2 安全策略的设计与开发 5.1.3 制定安全策略 5.2 信息安全管理 5.2.1 信息安全 5.2.2 信息载体安全管理 5.2.3 信息密级标签管理 5.2.4 信息存储资源管理 5.2.5 信息访问控制管理 5.2.6 数据备份管理 5.2.7 信息完整性管理 5.2.8 信息可用性管理 5.2.9 可疑信息跟踪审计 5.3 安全应急响应 5.3.1 安全应急响应的概况 5.3.2 安全应急响应管理系统的建立 5.3.3 实施应急措施 5.3.4 安全应急响应管理系统的有效性测试 5.3.5 应急响应的成本分析 5.3.6 安全应急响应流程实例 本章小结 思考与练习
- 第6章 安全法规和标准 6.1 国际信息安全标准组织 6.1.1 国际标准化组织发展概况 6.1.2 国际电工委员会(IEC) 6.1.3 国际电信联盟(ITU) 6.1.4 ISO/IEC JTC1(第一联合技术委员会) 6.1.5 其他信息安全管理标准化组织 6.2 ISO9000族简介 6.2.1 ISO9000族标准的起源与发展 6.2.2 ISO9000族核心标准简介 6.2.3 ISO9000族的新发展 6.2.4 ISO26000 6.3 国外信息安全标准化现状 6.3.1 美国信息安全管理标准体系 6.3.2 英国信息安全管理标准体系 6.3.3 其他国家信息安全标准化现状 6.4 我国信息安全标准化现状 6.5 基础信息安全标准 6.5.1 信息安全标准体系结构 6.5.2 安全框架标准指南 6.5.3 信息安全技术中的安全体制标准 6.6 环境与平台安全标准 6.6.1 电磁泄漏发射技术标准指南 6.6.2 物理环境与保障标准 6.6.3 计算机安全等级标准 6.6.4 网络平台安全标准 6.6.5 应用平台安全标准 6.7 信息安全管理 6.7.1 信息安全管理概念及标准简介 6.7.2 BS7799 6.7.3 ISO/IEC 17799 6.7.4 我国的安全管理工作 本章小结 思考与练习

## 章节摘录

第1章 信息安全管理概述随着信息技术的发展，人们在享受信息技术带来的方便与高效的同时也面临着严重的信息安全的威胁。

怎样保证信息被合法有效的利用，是目前信息安全技术所面临的一大课题。

构建良好的信息安全管理策略是构建信息安全平台的前提条件。

1.1 全球信息安全发展形势Internet是信息传输的集中地，在上面充斥着大量有用和无用的信息。

Internet是一个庞杂的系统，其设计本身不可避免会出现很多不安全的因素。

Internet是一个开放式的网络，任何使用者都可能成为它的安全威胁者。

1.1.1 互联网骨干网络面临的安全威胁Internet主要由路由器和DNS服务器两大基本架构组成，其中路由器构成Internet的主干，DNS服务器负责将域名解析为IP地址。

攻击互联网骨干网络最直接的方式就是攻击互联网主干路由器和DNS服务器。

如果一个攻击者能成功地破坏主干路由器用来共享路由信息的边界网关协议（BGP），或者更改网络中的DNS服务器，就会使Internet陷入一片混乱。

为了寻找一些能够使主干路由器和DNS服务器彻底崩溃或者能够取得其系统管理权限的缓冲溢出或其他安全漏洞，恶意的高级攻击者通常会非常仔细地检查一些主干路由器和DNS服务器的服务程序代码和它们之间的通信协议的实现代码。

路由代码非常复杂，目前已经发现并已修复了许多重要的安全问题，但是仍旧可能存在许多更严重的问题，并且很可能被黑客发现和利用。

DNS软件过去经常发生缓冲溢出这样的问题，在以后也肯定会发生类似的问题。

如果攻击者发现了路由、DNS或通信协议的安全漏洞，并对其进行大举攻击，那么大部分Internet将会迅速瘫痪。

2002年8月，互联网赖以运行的基础通信规则之一——ASN NO.1信令的安全脆弱性就严重威胁了互联网骨干网基础设施的安全。

黑客利用ASN NO.1信令的安全漏洞开发相应的攻击程序，关闭ISP的骨干路由器、交换机和众多的基础网络设备，可最终引起整个互联网瘫痪。

ASN NO.1信令的安全脆弱性使得超过100家的计算机网络设备提供商将要为此付出代价，而弥补这些缺陷的投入将超过1亿美元。

由于多个互联网通信协议都是基于ASN NO.1计算机网络语言的，因此ASN NO.1的脆弱性将广泛威胁通信行业。

最为显著的例子就是造成SNMP协议多个安全漏洞。

## <<信息安全管理基础>>

### 编辑推荐

《国家信息化计算机教育认证CEAC指定教材·信息安全管理基础》结构清晰，讲解详细，并在每章后配有丰富的思考与练习题。非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导教材，还可供读者自学使用。

<<信息安全管理基础>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>