第一图书网, tushu007.com

<<信息安全原理>>

图书基本信息

书名：<<信息安全原理>>

13位ISBN编号：9787302124931

10位ISBN编号：7302124930

出版时间：2006-3

出版时间：清华大学

作者：[美]MichaelE.Whi

页数：423

译者：齐力薄

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

第一图书网, tushu007.com

<<信息安全原理>>

内容概要

本书详细介绍了信息安全领域的各方面内容，为每一位有志于成为商务决策人员的读者提供了全面的指导。
作者借此次再版的机会，在真实的企业环境下讨论信息安全，包括目前专业人员面临的许多问题，还在每一章的“相关资料”中介绍了有趣的故事。
本书从管理和技术两方面介绍了这一学科，并注重讲述了CISSP(认证信息系统安全专家)认证所需掌握的知识。
其他主题包括信息安全中的法律和道德问题、网络和系统安全、密码学、信息安全维护等。
本书特色：为未来的信息系统安全决策者介绍了信息安全的技术内容；信息安全问题、工具的使用范例，以及信息安全在当今企业中的实现；包含相关资料和技术细节部分。
相关资料中介绍了许多文章，可供读者进一步学习；技术细节部分讨论了所在章中高度技术化的信息，便于读者阅读；扩展了每一章末的习题，包括练习和案例，以加强概念和技术的学习。

第一图书网, tushu007.com

作者简介

Michael E.Whitman博士是一位经过认证的信息系统安全专家，现为美国乔治亚州Kennesaw州立大学的信息系统教授、硕士生导师，并担任KSU中心主管，致力于信息安全教育和意识的培养，在信息安全政策领域的研究成果颇丰。

第一图书网, tushu007.com

<<信息安全原理>>

书籍目录

第1章 信息安全简介1.1 引言 1.2 信息安全发展史1.2.1 20世纪60年代1.2.2 20世纪70年代和80年代1.2.3 20世纪90年代 1.2.4 现在 1.3 安全的概念 1.4 信息的重要特性 1.4.1 可用性 1.4.2 精确性 1.4.3 真实性 1.4.4 机密性 1.4.5 完整性 1.4.6 效用性 1.4.7 所有性 1.5 NSTISSC安全模型 系统的组件 1.6.1 软件 1.6.2 硬件 1.6.3 数据 1.6.4 人员 1.6.5 过程 1.6.6 网络 1.7 保护IS组全 1.8 平衡信息的安全和访问权 1.9 实现信息安全的方法 1.10 系统开发生命周期 1.10.1 方法学 1.10.2 阶段 1.10.3 调研 1.10.4 分析 1.10.5 逻辑设计 1.10.6 物理设计 1.10.7 实现 1.10.8 改 1.11 安全系统开发生命周期1.11.1 调研 1.11.2 分析 1.11.3 逻辑设计 1.11.4 物理设计 1.11.5 现 1.11.6 维护和修改1.12 安全专业人士和机构 1.12.1 高级管理者 1.12.2 信息安全项目小组1.12.3 数据所有人 1.13 利益团体 1.13.1 信息安全管理和专业人士1.13.2 信息技术管理和专业人士1.13.3 机构管理和专业人士 1.14 信息安全：是一门艺术还是一门科学 1.14.1 作为艺术的安全 1.14.2 作为科学的安全 1.14.3 作为社会科学的安全 1.15 信息安全的术语 1.16 本章小结 1.17 复习题 1.18 练习 1.19 案例练习 第2章 安全需求 2.1 引言 2.2 业务需求在前，技术在后 2.2.1 保护机构运转的力 2.2.2 实现应用程序的安全操作 2.2.3 保护机构收集和使用的数据 2.2.4 保护机构的技术资产 2.3 威胁 2.3.1 人为过失或失败的行为 2.3.2 知识产权的损害 2.3.3 间谍或者蓄意入侵行为 2.3.4 信息敲诈蓄意行为 2.3.5 蓄意破坏行为 2.3.6 蓄意窃取行为 2.3.7 蓄意软件攻击 2.3.8 自然灾害 2.3.9 服量差 2.3.10 技术硬件故障或者错误 2.3.11 技术软件故障或者错误 2.3.12 技术淘汰 2.4 攻击 2.4.1 意代码 2.4.2 恶作剧 2.4.3 后门 2.4.4 密码破解 2.4.5 暴力 2.4.6 词典方式 2.4.7 拒绝服务(DoS 布式拒绝服务(DDoS) 2.4.8 欺骗 2.4.9 中间人 2.4.10 垃圾邮件 2.4.11 邮件炸弹 2.4.12 嗅探器 社会工程 2.4.14 缓冲区溢出 2.4.15 定时攻击 2.5 本章小结 2.6 复习题 2.7 练习 2.8 案例练习 信息安全中的法律、道德以及专业人员问题 3.1 引言 3.2 信息安全的法律及道德 3.3 法律的类型 3.4 美国相关法律 3.4.1 一般计算机犯罪法 3.4.2 隐私 3.4.3 出口及间谍法 3.4.4 美国版权法 财务报表 3.4.6 1966年的信息自由法(FOIA) 3.4.7 州和本地法规 3.5 国际法及法律主体 3.5.1 欧洲计算机犯罪委员会条例 3.5.2 数字时代版权法 3.5.3 联合国宪章 3.6 政策与法律 3.7 道德和信息安全 3.7.1 不同文化中的道德差异 3.7.2 软件许可侵犯 3.7.3 违法使用 3.7.4 公司资源的滥用 3.7.5 和教育 3.7.6 不道德及违法行为的防范措施 3.8 道德规范和专业机构 3.8.1 IT的主要专业机构 3.8.2 其他安全机构 3.8.3 美国主要联邦机构 3.9 机构的责任和忠告 3.10 本章小结 3.11 复习题 3.12 习 3.13 案例练习 第4章 风险管理 4.1 引言 4.2 风险管理概述 4.2.1 知己 4.2.2 知彼 4.2.3 的作用 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 信息资产分类 4.3.4 息资产评估 4.3.5 按照重要性列出资产 4.3.6 数据的分类及管理 4.3.7 安全调查 4.3.8 分类数据的管理 4.3.9 威胁识别 4.3.10 识别威胁及威胁代理，并区分其优先次序 4.3.11 漏洞识别 4.4 风险评估 4.4.1 风险评估概述 4.4.2 可能性 4.4.3 信息资产评估 4.4.4 风险的确定 4.4.5 识别可能的控制 访问控制 4.4.7 记录风险评估的结果 4.5 风险控制策略 4.5.1 避免 4.5.2 实现避免 4.5.3 转移 缓解 4.5.5 灾难恢复计划 4.5.6 接受 4.6 选择风险控制策略 4.6.1 风险控制的估计、评估及维护 4.6.2 控制的种类 4.6.3 可行性研究 4.6.4 其他可行性研究 4.7 风险管理的讨论要点 4.7.1 风险可接受程度 4.7.2 残留风险 4.8 验证结果 4.9 推荐的控制风险实践 4.9.1 定量评估 4.9.2 Delphi技术 4.10 本章小结 4.11 复习题 4.12 练习 4.13 案例练习 第5章 安全规划 5.1 引言 5.2 信息、标准及实践 5.2.1 定义 5.2.2 企业信息安全政策 5.2.3 特定问题安全政策 5.2.4 特定系统政策(SysSP) 5.2.5 政策管理 5.2.6 信息的分类 5.3 信息安全蓝本 5.3.1 ISO 17799/BS 7799 5.3.2 NIST模式 5.3.3 IETF安全结构 5.3.4 VISA国际安全模式 5.3.5 基线和最佳业务实践 5.3.6 信息安全系统蓝本的混合结构 5.3.7 安全体系的设计 5.4 安全教育、培训和认识计划 5.4.1 安全教育 5.4.2 安全培训 5.4.3 安全意识 5.5 持续性策略 5.5.1 业务影响分析 5.5.2 事故响应计划 5.5.3 灾难恢复计划 业务持续性计划 5.5.5 统一的应急计划模型 5.5.6 相关法律的实施 5.6 本章小结 5.7 复习题 5.8 习 5.9 案例练习 第6章 安全技术：防火墙和VPN 6.1 引言 6.2 物理设计 6.3 防火墙 6.3.1 防分类方法 6.3.2 防火墙体系结构 6.3.3 选择正确的防火墙 6.3.4 配置和管理防火墙 6.3.5 内容过滤器 6.4 保护远程连接 6.4.1 拨号 6.4.2 虚拟专用网络 6.5 本章小结 6.6 复习题 6.7 练习 6.8

第一图书网, tushu007.com

<<信息安全原理>>

习 第7章 安全技术：入侵检测、访问控制和其他安全工具 7.1 引言 7.2 入侵检测系统(IDS) 7.2.1 IDS术语 7.2.2 使用IDS的原因 7.2.3 IDS的类型和检测方法 7.2.4 IDS响应行为 7.2.5 选择IDS方法 产品 7.2.6 IDS的优缺点 7.2.7 IDS的部署和实现 7.2.8 评估IDS的效果 7.3 蜜罐、蜜网和填充单元系 统 7.3.1 诱捕和跟踪系统 7.3.2 积极阻止入侵 7.4 浏览和分析工具 7.4.1 端口扫瞄仪 7.4.2 防火墙 析工具 7.4.3 操作系统检测工具 7.4.4 漏洞扫瞄仪 7.4.5 包嗅探器 7.4.6 无线安全工具 7.5 访问控 设备 7.5.1 身份验证 7.5.2 生物测定学的有效性 7.5.3 生物测定学的可接受性 7.6 本章小结 7.7 题 7.8 练习 7.9 案例练习 第8章 密码学 8.1 引言 8.2 密码简史 8.3 密码系统的原则 8.3.1 密定义 8.3.2 加密方法 8.3.3 加密系统的元素 8.3.4 加密密钥的长度 8.3.5 密码原则的总结 8.4 加 工具 8.4.1 公钥基础结构 8.4.2 数字签名 8.4.3 数字证书 8.4.4 混合加密系统 8.4.5 密码术 8.5 通信协议 8.5.1 用S-HTTP和SSL保护Internet通信 8.5.2 使用S/MIME、PEM和PGP保护电子邮件 8.5.3 使用SET、SSL和S-HTTP保护Web事务 8.5.4 用IPSec和PGP保护TCP/IP 8.6 密码系统的攻击 8.6.1 中间 人攻击 8.6.2 相关性攻击 8.6.3 字典式攻击 8.6.4 定时攻击 8.6.5 防御攻击 8.7 本章小结 8.8 题 8.9 练习 8.10 案例分析 第9章 物理安全 9.1 引言 9.2 物理访问控制 9.3 防火安全 9.4 发生故障和建筑物倒塌 9.4.1 取暖、通风和空调 9.4.2 电力管理和调整 9.4.3 水问题 9.4.4 建筑物的 倒塌 9.4.5 设施系统的维护 9.5 数据的侦听 9.6 可移动和便携系统 9.7 物理安全威胁的特殊考虑 本章小结 9.9 复习题 9.10 练习 9.11 案例练习 第10章 实现信息安全 10.1 引言 10.2 信息安 项目管理 10.2.1 制定项目计划 10.2.2 项目计划的考虑 10.2.3 范围考虑 10.2.4 项目管理需求 10.3 现的技术主题 10.3.1 转换策略 10.3.2 信息安全项目计划的靶心模型 10.3.3 外购还是自行开发 10.3.4 技术监督和改进控制 10.4 实现的非技术方面 10.4.1 改进管理的文化氛围 10.4.2 机构改进的考虑 10 本章小结 10.6 复习题 10.7 练习 10.8 案例练习 第11章 安全和人员 11.1 引言 11.2 确定安 的人员配备 11.3 信息安全专业人员的认证 11.3.1 认证信息系统安全专业人员(CISSP)和系统安全认证 从业者(SSCP) 11.3.2 认证信息系统审计员(CISA)和认证信息系统经理(CISM) 11.3.3 全球信息保险认 证(GIAC) 11.3.4 安全认证专业人员(SCP) 11.3.5 TruSecure ICSA认证安全联合(TICSA) 11.3.6 Security+ 11.3.7 认证信息系统辩论调查员 11.3.8 相关认证 11.3.9 获得认证的费用 11.3.10 给信息 安全专业人员的建议 11.4 招聘政策和实践 11.4.1 工作描述 11.4.2 面试 11.4.3 背景检查 11.4.4 合同 11.4.5 新员工的定位 11.4.6 工作期间的安全培训 11.4.7 业绩评估 11.4.8 解聘 11.5 非员工 全考虑11.5.1 临时工 11.5.2 合同工 11.5.3 顾问 11.5.4 业务伙伴 11.6 责任的分离和共谋 11.7 人 数据的秘密性和安全 11.8 本章小结 11.9 复习题 11.10 练习 11.11 案例练习 第12章 信息安全维 护 12.1 引言 12.2 安全管理模式 12.3 维护模式 12.3.1 监控外部环境 12.3.2 监控内部环境 12.3 划与风险评估 12.3.4 漏洞评估和补救 12.3.5 备用状态与审查 12.4 本章小节 12.5 复习题 12.6 练 习 12.7 案例练习 术语表

第一图书网, tushu007.com

<<信息安全原理>>

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