

<<安全计划与灾难恢复>>

图书基本信息

书名：<<安全计划与灾难恢复>>

13位ISBN编号：9787115116840

10位ISBN编号：7115116849

出版时间：2003-11

出版单位：人民邮电出版社

作者：梅沃德

页数：224

字数：359000

译者：孙东红

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>

<<安全计划与灾难恢复>>

内容概要

要解决信息安全问题不是简单地依靠安全技术人员就可以的，对于所有从事IT业务或者倚仗IT基础设施来辅助业务运作的公司或组织而言，制定适合本单位的安全计划是非常重要的。

本书层次清晰地介绍了安全计划的建立、实施和管理，紧急事件处理等方面的具体细节。

针对安全计划所涉及的政策、过程、审计、监控、培训、时间和资金投入以及意外事件的应急处理等进行了专题讲解。

本书内容环环相扣，具有很强的指导性和可实践性。

本书适合政府、企业等行业中订相关部门的管理人员，以及网络和信息安全服务行业的从业人员使用。

<<安全计划与灾难恢复>>

作者简介

Eric Maiwald是Fortrex公司的首席技术官，负责管理公司全部的安全研究和培训活动以及Fortrex网络安全中心的运行工作。

此外，Maiwald先生还参与过很多其他类型的工作，比如对大型的金融机构、服务公司和生产厂商进行风险评估，制定企业的开发策略和部署安全解决方案等等。

<<安全计划与灾难恢复>>

书籍目录

第一部分 制定安全计划的指导原则 第1章 信息安全计划的任务 1.1 正确的开端 1.2 确定安全部门的任务 1.2.1 报告的机构 1.2.2 任务声明 1.2.3 长期目标 1.2.4 短期目标 1.3 关系 1.3.1 技术关系 1.3.2 业务关系 1.4 检查清单：计划的关键任务 第2章 美国的相关法律和法规 2.1 与执法部门合作 2.2 法律背景 2.2.1 计算机欺骗和滥用法（1986年版） 2.2.2 电子通信隐私法（1986年版） 2.2.3 计算机安全法（1987） 2.2.4 国家信息基础设施保护法（1996） 2.2.5 Gramm - Leach - Bliley金融服务现代化法案（GLBA） 2.2.6 医疗保险信息携带及责任法案（HIPAA） 2.3 网络资源 2.4 检查清单：信息安全法律问题的要点 第3章 评估 3.1 内部审计 3.2 外部审计 3.3 评估 3.3.1 自我评估 3.3.2 漏洞评估 3.3.3 穿透测试 3.3.4 风险评估 3.4 检查清单：评估的要点 第二部分 计划的实施 第4章 制定政策与程序 4.1 政策的目的 4.2 制定政策 4.2.1 可接受使用政策（AUP） 4.2.2 信息安全政策 4.3 现有文档的处理 4.4 使他们认可 4.5 政策审查 4.6 检查清单：制定政策与程序的要点 第5章 安全计划的实施 5.1 从何处开始 5.1.1 建立计划书 5.1.2 风险评估 5.1.3 降低风险的计划 5.1.4 制定政策 5.1.5 解决方案的部署 5.1.6 培训 5.1.7 审计和报告 5.1.8 重新再做一遍 5.2 和系统管理员们一起工作 5.3 和管理者一起工作 5.4 教育用户 5.5 检查清单：安全计划实施的要点 第6章 部署新项目和新技术 第7章 安全培训和安全意识 第8章 安全监控 第三部分 安全计划的管理 第9章 安全预算 第10章 安全人员 第11章 报告 第四部分 如何响应意外事件 第12章 事件响应 第13章 制定意外事件的应急计划 第14章 灾难响应 第五部分 附录 附录A 处理审计 附录B 安全外包 附录C 管理新的安全项目 附录D 安全计划与灾难恢复蓝图

<<安全计划与灾难恢复>>

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>