

NIST 特别出版物 800-45 第 2 版

电子邮件安全指南

——国家标准和技术研究所的建议

Miles Tracy

Wayne Jansen

Karen Scarfone

Jason Butterfield

美国商务部国家标准和技术研究所

NIST 特别出版物 800-45

第 2 版

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

电子邮件安全指南

——**国家标准和技术**

研究所的建议

Mile Tracy

Working Group

计算机安全

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

2007 年 2 月



美国商务部

部长: Carlos M. Gutierrez

技术管理局

商务部技术副部长: Robert C. Cresanti

国家标准和技术研究所

所长: William Jeffrey

目录

执行摘要

1 概述

- 1.1 权限
- 1.2 目的和范围
- 1.3 适用对象
- 1.4 篇章结构

2 背景 and 标准

- 2.1 背景
- 2.2 多用途互联网邮件扩展
- 2.3 邮件传输标准
 - 2.3.1 简单邮件传输协议
 - 2.3.2 简单邮件传输协议
 - 2.3.3 专有邮件传输
- 2.4 客户端访问标准
 - 2.4.1 邮局协议
 - 2.4.2 互联网信息访问协议
 - 2.4.3 专有邮箱访问机制
 - 2.4.4 基于 Web 的邮件访问

3 电子邮件消息的签名和加密

- 3.1 OpenPGP
- 3.2 S/MIME
- 3.3 密钥管理
- 3.4 电子邮件的加密问题

4 邮件服务器的规划和管理

- 4.1 安装和配备规划
- 4.2 安全管理人员
 - 4.2.1 高级 IT 管理官员/首席信息官 (CIO)
 - 4.2.2 信息系统安全方案经理
 - 4.2.3 信息系统安全官
 - 4.2.4 邮件服务器和网络管理员
- 4.3 管理实践规范
- 4.4 系统安全计划
- 4.5 人力资源要求
- 4.6 信息系统安全总原则
- 4.7 邮件服务器的规划和管理检查列表

5 邮件服务器操作系统的安全保护

- 5.1 更新和配置操作系统
 - 5.1.1 打补丁和升级操作系统
 - 5.1.2 移除或禁用不必要服务和应用
 - 5.1.3 配置操作系统用户认证
 - 5.1.4 适当配置资源控制

-
- 5.1.5 安装和配置附加安全控制
 - 5.2 操作系统的安全测试
 - 5.3 邮件服务器操作系统安全保护检查列表
 - 6 邮件服务器和内容的安全保护**
 - 6.1 强化邮件服务器应用
 - 6.1.1 安全安装邮件服务器
 - 6.1.2 配置操作系统和邮件服务器访问控制
 - 6.2 保护电子邮件免遭恶意软件侵扰
 - 6.2.1 恶意软件扫描
 - 6.2.2 内容过滤
 - 6.2.3 用户的安全意识
 - 6.3 拦截垃圾邮件发送服务器
 - 6.4 经过认证的邮件中继
 - 6.5 安全访问
 - 6.6 启用 Web 访问
 - 6.7 邮件服务器和内容安全保护检查列表
 - 7 执行安全的网络基础设施**
 - 7.1 网络的构成和结构
 - 7.1.1 失策的网络布局
 - 7.1.2 非军事区
 - 7.1.3 邮件网关
 - 7.1.4 管理网
 - 7.2 网络元素配置
 - 7.2.1 路由器/防火墙配置
 - 7.2.2 入侵检测和预防系统
 - 7.2.3 网络交换机
 - 7.3 执行安全网络基础设施检查列表
 - 8 邮件客户端的安全保护**
 - 8.1 客户端应用的安装和配置
 - 8.1.1 邮件客户端的打补丁和更新
 - 8.1.2 邮件客户端安全性能的配置
 - 8.1.3 认证和访问的配置
 - 8.1.4 客户端主机操作系统的安全保护
 - 8.2 消息成分的安全保护
 - 8.3 插件
 - 8.4 对邮件系统的基于 Web 访问
 - 8.5 邮件客户端安全保护检查列表
 - 9 邮件服务器的管理**
 - 9.1 日志记录
 - 9.1.1 建议的通用日志配置
 - 9.1.2 日志文件的检查和保留
 - 9.1.3 自动化日志文件分析工具
 - 9.2 邮件服务器备份

-
- 9.3 从安全破坏中恢复
 - 9.4 邮件服务器安全测试
 - 9.4.1 脆弱性扫描
 - 9.4.2 渗透测试
 - 9.5 邮件服务器的远程管理
 - 9.6 邮件服务器管理检查列表
- 附录 A 术语表**
- 附录 B 与电子邮件相关的 RFC**
- 附录 C 参考文献**
- 附录 D 电子邮件安全工具和应用**
- 附录 E 网上的电子邮件安全资源**
- 附录 F 电子邮件安全检查列表**
- 附录 G 缩略语**
