NIST 特别出版物 800-61
第 2 修订版

国家标准和技术研究所
美国商务部

计算机安全事故处理指南

国家标准和技术研究所的建议

Paul Cichonski
国家标准和技术研究所信息技术实验室计算机安全部
Tom Millar
国土安全部国家网络安全局美国计算机紧急反应小组
Tim Grace
国家标准和技术研究所信息技术实验室计算机安全部
Karen Scarfone
Sacrfone 网络安全公司

2013 年 **8** 月

美国商务部
Rebecca Blank，代理部长
国家标准和技术研究所
Patrick D. Gallagher，商务部副部长兼 **NIST** 所长

目录

执行摘要

1. 介绍

1.1 权限

1.2 目的和范围

1.3 适用对象

1.4 篇章结构

2. 建立计算机事故响应能力

2.1 事件和事故

2.2 事故响应需求

2.3 制定事故响应策略、计划和规程

2.3.1 策略元素

2.3.2 计划元素

2.3.3 规程元素

2.3.4 与外部相关方共享信息

2.4 事故响应小组的组织结构

2.4.1 小组模式

2.4.2 小组模式选择

2.4.3 事故响应人员

2.4.4 机构内的依存关系

2.5 事故响应小组的服务

2.6 建议

3. 处理事故

3.1 准备

3.1.1 事故处理准备

3.1.2 事故预防

3.2 检测和分析

3.2.1 攻击向量

3.2.2 事故的迹象

3.2.3 先兆和指标的来源

3.2.4 事故分析

3.2.5 事故记录归档

3.2.6 排列事故处理的优先顺序

3.2.7 事故通知

3.3 遏制、根除和恢复

3.3.1 选择抑制战略

3.3.2 证据的收集和处理

3.3.3 识别攻击主体

3.3.4 根除和恢复

3.4 事故后活动

3.4.1 总结教训

3.4.2 利用收集来的事故数据

3.4.3 证据保留
3.5 事故处理检查列表
3.6 建议
4. 协调和信息共享
4.1 协调
4.1.1 协调关系
4.1.2 共享协议和报告要求
4.2 信息共享技术
4.2.1 特殊方法
4.2.2 半自动化
4.2.3 安全考虑
4.3 细粒度信息共享
4.3.1 业务影响信息
4.3.2 技术信息
4.4 建议
附录 A 事故处理情景
A.1 情景问题
A.2 情景
附录 B 与事故相关的数据元素
B.1 基本数据元素
B.2 事故处理人员数据元素
附录 C 术语表
附录 D 缩略语
附录 E 参考文献
附录 F 常见问题解答
附录 G 危机处理步骤