

《终端安全风险》

图书基本信息

书名：《终端安全风险》

13位ISBN编号：9787111373902

10位ISBN编号：7111373901

出版时间：2012-7

出版社：机械工业出版社

作者：李小平

页数：285

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《终端安全风险管理》

内容概要

《终端安全风险管理》作者在多年实践经验的基础上，提出终端安全管理的实质就是终端安全风险管，并系统地阐述了管理的关键是“管理自动化”的观点。《终端安全风险管理》从实际出发，基于信息安全风险评估理论，介绍可识别和分析的终端安全风险，构建结构性的终端安全风险体系，基于管理自动化的原则，构建终端安全管理体系的方法。《终端安全风险管理》有助于读者摆脱终端安全管理工作中面向威胁被动防护的局面，构建更为有效的面向能力的终端安全主动防御体系。

书籍目录

序

前言

第一部分 终端安全管理及其发展

第1章 认识终端与终端安全

1.1 什么是终端

1.2 终端的配件

1.3 终端所处的环境

1.4 终端的使用者

1.5 聊聊终端的安全问题

第2章 怎样保障终端安全

2.1 终端安全管理到底是什么

2.2 时刻准备，及时防护

2.3 协调一致，全面管理

2.4 管理与技术并举

2.5 其他防护措施

2.6 总结

第3章 “终端安全管理”的现在和未来

3.1 国外终端安全管理是什么样的

3.2 国内终端安全管理在怎么做

3.3 终端安全管理产品有哪些

3.4 终端还有安全问题么

3.5 终端安全管理的未来

第4章 终端安全管理的标准规范及要求

4.1 信息安全相关标准

4.2 行业化相关标准

第二部分 终端安全风险分析

第5章 如何构建终端安全风险体系

5.1 终端安全风险评估

5.2 识别终端资产

5.3 识别终端威胁

5.4 识别终端脆弱性

5.5 终端安全威胁与脆弱性

5.6 终端安全风险分析模型

第6章 对终端安全风险进行分类

6.1 几种常见分类方式

6.2 构建终端安全风险立体分类模型

6.3 终端安全风险图谱

第三部分 终端安全风险管理体系及其实现

第7章 终端安全风险管理体系

7.1 构建方法

7.2 构建过程

7.3 构建体系

7.4 构建组织

7.4.1 组织结构

7.4.2 人员角色

第8章 终端安全风险管控策略

8.1 基于资产全生命周期的管理

- 8.2 基于风险管控全过程的管理
- 8.3 基于等保的合规性遵从管理
- 8.4 终端安全风险管控点
- 第9章 终端安全风险技术防护
 - 9.1 终端安全风险处置
 - 9.2 主要技术管控措施
 - 9.3 终端安全风险管控列表
- 第10章 终端安全风险日常运维管理
 - 10.1 重要风险监控
 - 10.2 运维全过程管理
 - 10.3 日常统计分析
 - 10.4 日常工作的实现
- 第11章 终端安全风险深度分析
 - 11.1 分析数据准备
 - 11.2 深度分析建模
 - 11.3 深度分析方法与实现
- 第 部分终端安全风险行业化管理及应用案例
- 第12章 终端安全风险行业化管理模式
 - 12.1 行业化的需求
 - 12.2 行业化管理的技术支撑
 - 12.3 行业化管理模式
 - 12.3.1 垂直管理
 - 12.3.2 垂直管理实例
 - 12.3.3 分布式管理
 - 12.3.4 分布式管理实例
 - 12.3.5 混合型管理
 - 12.3.6 混合管理实例
- 第13章 经典案例
 - 13.1 项目背景
 - 13.2 项目需求
 - 13.3 项目目标
 - 13.4 建设方法
 - 13.4.1 部署模型
 - 13.4.2 部署方案
 - 13.4.3 行业管理策略
 - 13.5 建设效果
- 附录 终端安全风险分析报告
- 附录A 终端安全基础风险
 - A.1 终端自身安全风险(BRI.1)
 - A.1.1 密码口令风险(18个风险点)
 - A.1.2 B10s弱密码风险(11个风险点)
 - A.1.3 杀毒软件检查风险(10个风险点)
 - A.1.4 终端应用软件检查风险(8个风险点)
 - A.1.5 终端系统补丁风险(6个风险点)
 - A.1.6 终端软件自动分发风险(8个风险点)
 - A.2 终端环境安全风险(BRI.2)
 - A.2.1 终端网络运行环境风险(7个风险点)
 - A.2.2 终端防火墙风险(14个风险点)
 - A.3 终端外设安全风险(BRI.3)

- A.3.1 外设端口管理(15个风险点)
- A.3.2 外设设备管理
- A.3.3 终端注册表风险(9个风险点)
- A.3.4 终端系统驱动风险(16个风险点)
- A.3.5 基本配置风险(6个风险点)

附录B 终端安全运行风险

- B.1 网络运行安全(RR1.1)
 - B.1.1 网络设备运行风险(12个风险点)
 - B.1.2 终端流量异常风险(12个风险点)
 - B.1.3 终端违规网络访问风险(11个风险点)
 - B.1.4 IP / MAc地址篡改风险(9个风险点)
- B.2 终端运行安全(RRI.2)
 - B.2.1 进程 / 服务运行的风险(20个风险点)
 - B.2.2 违规软件安装的风险(20个风险点)
 - B.2.3 异常资源占用的风险(19个风险点)
 - B.2.4 操作系统用户管理的风险(20个风险点)
- B.3 网络边界安全(RR1.3)
 - B.3.1 违规内联(30个风险点)
 - B.3.2 违规外联(12个风险点)
 - B.3.3 漫游管理(9个风险点)

附录C 终端安全信息风险

- C.1 信息扩散风险
 - C.1.1 信息传输(8个风险点)
 - C.1.2 移动存储介质违规使用(15个风险点)
 - C.1.3 信息文档保护(5个风险点)
 - C.1.4 信息共享(3个风险点)
 - C.1.5 信息的非技术性泄漏(7个风险点)
 - C.1.6 人为灾害(3个风险点)

章节摘录

版权页：插图：（4）终端外设使用监控 对终端外设接口、外联设备使用的监视和控制能有效地控制计算机的资源利用率，规范计算机资源使用，防止因滥用计算机外接存储设备造成的木马、病毒的泛滥传播等。（5）操作系统密码口令检查 定期改变具有一定复杂度的密码及密码策略可以有效地防止非授权人员进入计算机终端，防止非法人员窃取计算机终端信息，所以，对操作系统口令的检查能有效地督促计算机终端设置合规的用户口令，保证终端安全。（6）网络配置信息监控 网络配置信息包含计算机网卡的MAC、IP地址和计算机路由器的接口信息等。对网络配置的有效监控可以及时发现非法接入信息系统的非法终端，防止非法终端接入可信网络窃取信息、传播病毒等。

2.运行类风险防护

（1）操作系统网络流量监控 对操作系统各用户、各时段的流量监控可以有效地判断计算机内是否存在程序、服务在上传或下载信息，及时判断计算机是否感染木马程序致使信息外发，或成为共享服务站造成信息泄漏。（2）操作系统网络访问监控 对计算机终端进行的系统网络访问控制能有效地防止计算机进行违规互联，防止信息因共享等方式进行违规流转，防止木马、病毒在信息系统内大规模爆发。（3）操作系统运行状态监控 对操作系统运行状态的监控可有效地了解到计算机终端长时间未登录、企图进入安全模式等绕过行为，监控主机调用的端口、服务等系统信息，保证计算机终端时刻处于被监控状态。

3.信息类风险防护

（1）安全准入控制 非法主机接入可信信息系统可能导致内网信息外泄、病毒、木马传播扩散和对内外服务器攻击等严重后果，因此对计算机终端的安全防护中，准入控制是极为重要的一项防护手段。（2）终端使用者变更监控 计算机终端可能归属不同人员使用，不同用户及使用者对计算机终端有着不同的操作权限，对于变更使用者的计算机终端应及时改变资产所属人员以保证计算机使用权限正常，资产归属正常：防止计算机终端使用者非授权登录、使用计算机，保证计算机终端信息安全性。

《终端安全风险管控》

编辑推荐

《终端安全风险管控》特别适合作为信息安全、计算机、通信、电子工程等领域的科技人员的技术参考书，或作为相关专业的教材。

《终端安全风险管理》

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:www.tushu000.com