《终端安全风险管理》

图书基本信息

书名：《终端安全风险管理》

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

《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理，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。

《终端安全风险管理》

书籍目录

《终端安全风险管理》

《终端安全风险管理》

《终端安全风险管理》

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。

《终端安全风险管理》

编辑推荐

《终端安全风险管理》特别适合用作信息安全、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