终端安全风险管理

李小平　等编著

机械工业出版社
CHINA MACHINE PRESS

终端安全风险管理

李小平　倪静石
于海波　孙　鸿　　编著
王国强　袁　宏　李雪莹

机械工业出版社

尽管人们已经认识到终端是网络中大部分行为的源头和起点，是最终的端点，并且认识到终端安全是网络与信息安全管理的重要内容，因此采用了大量产品和技术解决所面临的终端安全问题，但终端仍旧屡屡发生“问题”。其原因在于现有产品的技术工具色彩浓厚，单一功能性强，整体性不足。本书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。本书从实际出发，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。本书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。

本书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。

图书在版编目（CIP）数据

终端安全风险管理 / 李小平等编著. —北京：机械工业出版社，2012.6

ISBN 978-7-111-37390-2

Ⅰ. ①终… Ⅱ. ①李… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 139077 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：丁 诚 宋 丹

责任编辑：丁 诚

责任印制：乔 宇

三河市宏达印刷有限公司印刷

2012 年 7 月 • 第 1 版第 1 次印刷

184mm×260mm • 18.5 印张 • 1 插页 • 456 千字

0001 - 6000 册

标准书号：ISBN 978-7-111-37390-2

定价：52.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社 服 务 中 心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者购书热线：（010）88379203

网络服务

门户网：http://www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

序

信息革命是当今世界发展的大趋势，我国信息化也正快速发展，极大地促进着国民经济和社会的发展。但与此同时，信息安全也成为全球关注的焦点。

信息安全保障是多层次的复杂系统，其中终端是网络安全行为的源头，是安全防范的重点。据 IDC 统计，对于企业来说，来自内部终端的安全威胁占整个安全威胁的 70%以上。由于企业内部终端数量多，人员素质不同、流动性大，而产生病毒泛滥、终端滥用资源、非授权访问、恶意终端破坏、信息泄密等安全事件不胜枚举；政府部门也出现了不少的终端安全事件。

终端设备的多样性和复杂性，以及安全产品和服务的频繁更新，都使终端安全问题变得十分复杂，而头痛医头、脚痛医脚的安全防范策略是无法解决终端安全问题的。

在本书中，作者根据多年安全管理实践经验，体会到终端安全管理的实质就是终端安全风险管理，终端安全管理工作应以风险管控为主线。

作者采用分级分类的方法构建了终端安全风险体系，阐述了终端安全风险内容，从全生命周期、全过程和重要对象保护三个方面出发建立终端安全风险管理体系，力争做到终端安全管理工作“可知、可控、可管”。

本书把“终端安全风险体系”和“终端安全风险管理”二者在“防管一体化”的思想指导下统一起来，构建终端安全平台，对信息安全工作者具有借鉴意义。

中国工程院院士 何德全

前　言

1946 年，在美国宾夕法尼亚大学的莫尔电气工程学院揭幕典礼上，一个占地面积达 170 多平方米、重约 30 吨的庞然大物，为来宾呈现了一场精彩的“表演”——在 1 秒钟内进行了 5000 次加法运算，这比当时最快的继电器计算机的运算速度要快 1000 多倍。这个庞然大物——ENIAC 的完美亮相，不仅使得来宾们喝彩不已，也开启了科学计算的大门，成为人类进入信息时代的重要标志。1969 年，互联网的到来，又将人类带入了以计算机网络为核心的信息时代。21 世纪的今天，计算机已经成为社会生产和生活中必不可少的工具。

随着互联网在全世界的迅猛发展和广泛应用，网络也成为了悬在人们头上的达摩克利斯之剑，危机和风险无处不在，信息安全问题越来越严重。一则来自网上的报道说：“去年夏天，在拉斯维加斯举行的 DefCon 黑客安全会议上，两名安全顾问在一屋子黑客和计算机安全专家面前，演示了如何用 6 美元和几行代码就攻击并占领了一家公司的网站两个小时”。这个案例在让我们震惊的同时，也让我们感到了潜在的危机。在数字化、网络化的今天，网络上早就难有秘密可言，网络已经将我们变得透明。不过，这并不可怕，世界上很多的事情都大抵如此，可怕的是我们对此毫无防备，却主动一头扎进了陷阱里，还茫然不知。其实，从电脑诞生的那天起，信息安全就已经和它形影不离，但是，从来没有像今天这样备受瞩目，这样被广泛重视。

“千里之行始于足下”，解决信息安全问题，就要从基础和源头入手，从每个人使用的计算机——终端开始。因为，终端不仅关系着个人和单位的信息安全，同时终端也是网络的边界，影响着单位整个网络的信息安全。因此，终端安全是信息安全的基石，关注终端安全，就是关注信息安全，从使用者开始着手，防患于未然；解决终端安全风险，也就是解决了“托管”于使用者的网络边界的潜在危机。

本书从终端安全管理及其发展、终端安全风险分析、终端安全风险管理体系及其实现和终端安全风险行业化管理及应用案例四个方面，对终端的安全管理做了详细阐述和分析，并探索性地提供了终端安全在实际应用和行业型单位中的解决方案。书中提出终端安全管理就是风险管理的新理念和以风险管控为主线的新方法，对以前终端安全管理工作中存在的问题和弊端进行了深入分析，力求全面系统地展现终端安全问题的来源和发展方向；对终端安全体系和分类的构建方法作了介绍；通过终端“全生命周期”的风险分析，围绕安全重要对象保护和风险全过程管理，建立风险管理体系，力争实现终端安全风险的“可知，可控，可管”。本书倡导以安全效益为导向，以国家相关信息安全法律法规为依据，以终端安全规范建立为基础，以终端安全管理工作自动化开展为目标，以信息化为手段，建立“防管一体化”的终端安全平台，实现终端安全从“三分技术，七分管理”转向“七分技术，三分管理”，强调了技术支撑的必要性，提出了技术支撑的着眼点和落脚点。书中还构建“终端安全风险体系”和“终端安全风险管理体系”，提出了建设“终端安全防护平台”，建立终端安

全管理基础，及时发现、评估和防护风险，通过“机人”自动交接，实现从安全防护到安全管理的过渡衔接；提出了建设“终端安全管理平台”，建立终端安全管理架构、管理策略、残余风险处理和安全日常运维监控等体系，形成终端安全管理工作规范，强调安全重点对象、重要风险的管控和分析，建立终端安全保护基线。通过“防管一体化”终端安全平台的建设，努力实现能规避的风险自动防护，不能规避的风险，在风险发生之前，降低风险级别，减少风险发生次数，在风险发生之后，降低风险损失，缩短风险影响时间，实现现有终端安全从被动式管理向主动式管理的转变，保障终端安全的有序和全面系统管理。

知己知彼，方能百战不殆。作者编写本书的目的是为了让读者从不同角度、不同层面去认识和了解终端安全，在信息安全风暴来临前，有一个充分的准备。期望本书能成为读者了解信息安全知识的一个窗口，开拓现代科技事业的一条纽带，让终端安全风险管理为人类享受科技生活保驾护航。

本书编撰过程中得到了各方面的大力支持，特别是江苏省地方税务局，江苏省盐城地方税务局和北京天融信公司等单位的倾力协助，鸣谢（不分先后）：赵连才、刘斯宇、孙艳、朱惠林、刘红霞、罗秀春、朱俊龙、徐小兵、倪习同、钱磊、黄春亮、叶杨、惠喜岷、张凌云、刘扬、张铁铮、熊毅、唐宁、杨燕森、刘勇、杨圣峰、汤泰鼎、高晶、周国华、康新强、章露、李小刚、毕向阳、李林、杨光、黄善宇、魏琪、卢喜、孙艳丽、杜蕊、秦荔刚、陈俊、江志峰、张祯、郭艳峰、杨木超、项文峰、吴青松、杨军、李颖、彭鹏、黄蒙蒙、王栋、吴之奇、朱启坤。

作　者

2012 年 7 月

目　录

附录 终端安全风险分析报告

第1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

偶然一个机会听了一堂营销管理的讲座，讲师重点讲解的是“终端营销”的方法。其中“终端”是指与消费者直接发生买卖关系的经营场所，即销售给最终客户的卖场、商家，是流通环节的最后一环，是产品的投放地，如大型物流中的沃尔玛、家乐福、国美和苏宁都属于“终端”。在营销领域谁控制了销售终端，谁就找到了创造企业价值的通路。图 1-1 为营销终端示意图。

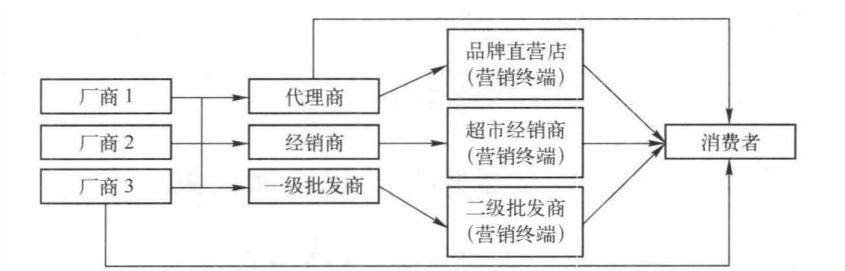

图 1-1　营销终端示意图

在通信行业，也会频繁听到“终端”这个词，在这里“终端”指的是“移动终端”，又叫做移动通信终端，如图 1-2 所示，这些终端通过通信网实现互联和信息交换。顾名思义，移动终端是指可以在移动中使用的计算机设备，广义上包括手机、笔记本、POS 机、车载电脑等。在通信行业中，大多数情况下终端指的是智能手机。就国内三大运营商争先恐后推出自己的智能终端的情况看，终端在运营商的心目中备受关注。

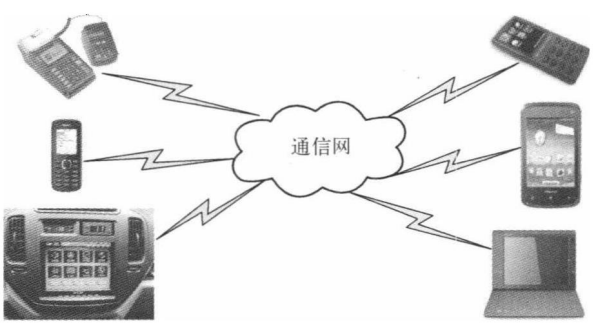

图 1-2　移动终端示意图

可见，“终端”一词在不同行业、不同领域有不同的定义，本书的内容紧紧围绕着“终

端”展开。那么“终端”概念最早出现在何时呢？本书中的“终端”具体指什么呢？

让我们回到40多年前。

1969年，为了军事研究的需要，在ARPA资助下，ARPA net于1969年投入使用，由此现代计算机网络产生，随之，计算机被分为主机（Host）和终端（Terminal）。当时的主机通常指大型机或功能较强的小型机，而终端则是指一种计算机外部设备，是一种字符型设备，包括多种类型。图1-3中展示了工作人员在早期的字符终端设备上工作的情景，其中工作人员面对的就是一台字符终端设备，主要作用是作为输入/输出信息的展示，实际操作的数据和相关的处理是在主机上进行的，就是旁边的“大设备”。

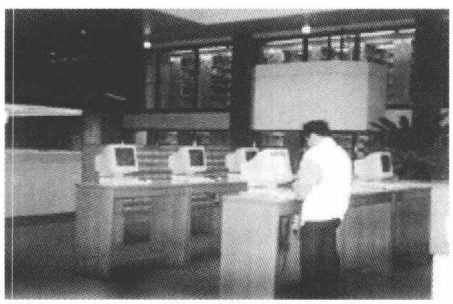

图1-3 早期的字符终端设备

这个早期的字符设备就是最早的终端。终端的概念最早出现在计算机领域，当时的终端指的就是计算机终端。随着名字的宽泛化、关联化和象形化，终端一词逐步被其他领域引用并推广，其中就包括前面提到的营销领域和通信领域。

早期计算机主要是作为计算的工具被使用。主要应用于科学计算、工业过程自动化控制和军事应用（例如，雷达数据处理、武器控制、军事情报等）。其中的核心应用就是计算（表现在软件中计算指令使用率高）。20世纪80年代中期，计算机网络和可视化技术的发展使计算机的应用迅速普及，其中心工作已经不是计算，而是逐步转为满足各种用户需要的业务任务的处理，主要是解决人类活动所产生的大量问题，计算机信息系统已经纳入人类活动的范围内，信息系统使用与人类活动与行为有直接关系，而且关系越来越密切。许多行业的业务活动已经离不开信息化系统支持。此时，计算机与计算机网络完全是人类活动的工具。[㊀]

随着业务信息化的推进，终端在业务专网中大量使用。本书重点讨论的终端，不是泛指计算机领域中的所有终端，而是指使用者在与互联网隔离的业务专网中直接使用的设备和网络安全的发生节点，包括PC、工作站、服务器、笔记本等，这些终端共有的特征是接入网络，可以接收和发送信息与数据，可以在使用者的操作下，通过操作系统产生网络访问和数据交互，可以对网络环境产生影响。

1.2 终端的配件

终端在发展过程中，一开始是大型设备或者项目的附属工具，但是随着科技的发展，终端从设备的辅助和支持角色，逐渐转换成了工作中的主体角色，而在使用过程中，为了弥补和增强终端功能，使用了其他设备与之配合，这些设备通常称为终端的外部设备（简称外设）。终端外设现在已经成为了一个规模庞大的产业，拥有大量的行业规范和标准，甚至反过来约束和影响终端的发展。

终端外设种类繁多、功能多样，而且有的设备还是具有多种功能的组合型外设，从功能

㊀ 该段文字引自屈延文先生的《网络世界白皮书》。

的角度来分类，外设分为：输入设备、显示设备、打印设备、外部存储器和网络设备。

输入设备主要是指人机交互类设备，用于其他类型（文字、图像、声音等）数据的处理和转换，输入到终端设备中，使得终端设备可以继续处理。输入设备一般包括键盘（图 1-4）、鼠标（图 1-5）、扫描仪器、手柄、摄像设备等，这些设备的使用是数据采集的需要，其设备本身并不会产生安全风险，但是使用或者数据保存不当就容易产生安全问题，因此人机交互类设备往往以数据跟踪为监管重点，设备控制以支持和兼容为主。

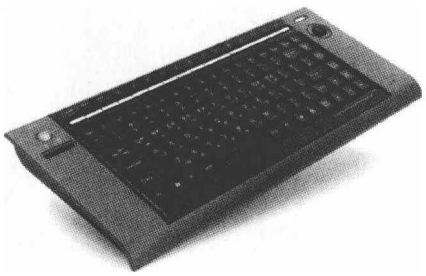

图 1-4　键盘

图 1-5　鼠标

显示设备主要是指显示器（图 1-6）、投影仪等显示信息的设备，用于了解当前终端的操作过程和运行过程。现在终端设备往往需要复杂的操作和运行来实现功能，例如键盘输入、鼠标操作等，如果在没有显示设备支持的情况，基本上是不可使用的。同样的，操作之后终端的运行过程和运行结果也需要显示设备的支持，才能全面了解，由此可见显示设备对于终端的重要性。

打印设备主要是指打印机（图 1-7），打印机是最传统的外设，也是最常用的外设，因此也是安全管理过程中的重点。打印设备可以将终端的数据转化成纸质的信息，可以脱离终端使用和流通，不受终端的控制和监管，在方便工作和生活的使用过程中，也增加了信息的扩散和泄密的风险，对于打印设备的使用情况和打印内容的监管是终端安全的重要内容。

图 1-6　显示器

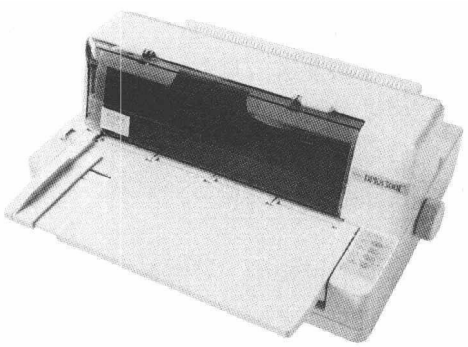

图 1-7　打印机

外部存储设备是终端使用过程中的有益补充和安全辅助，外部存储设备解决了数据长期保存、安全备份和快捷传递等问题。从经济角度来看，相对终端内部存储设备而言，使用低速、大容量和低成本的外部存储设备，可以有效提高设备的实用性。外部存储设备包括磁带

机、磁盘阵列和移动存储设备，其中移动存储设备由于使用灵活和携带便捷，已经成为现在工作和生活中不可或缺的一部分。移动存储设备的优点同样也是其发生安全问题的重大隐患，近年由于移动存储设备造成的泄密事件屡见不鲜，对于移动存储设备的监控也成为终端问题，甚至成为信息安全问题的重中之重。移动存储设备种类多样，根据设备基础类型分为U盘（图1-8）和移动硬盘（图1-9）两种类型，U盘的体积越来越小，容量越来越大，正是因为其经济实用的特性应用非常广泛。U盘的应用广泛也带来了管理上的问题，数据可以通过U盘进行传递，而U盘本身的管理存在困难，U盘的盗用和冒用现象非常多，通过U盘进行数据的非授权复制现象也很难有效控制。

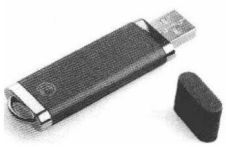

图1-8 U盘

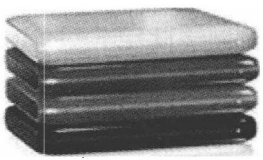

图1-9 移动硬盘

网络设备是指终端与终端之间连接在一起的硬件实体设备，包括调制解调器（Modem）、集线器（Hub）、交换机、路由器（图1-10）、防火墙等，网络设备除了可以完成网络连通的基础功能之外，还可以通过网络准入、网络过滤等方式解决网络安全问题。

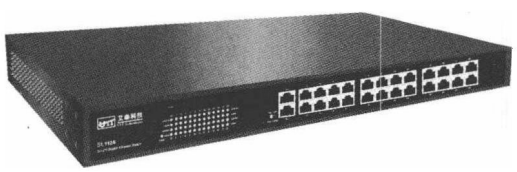

图1-10 路由器

1.3 终端所处的环境

从单一终端出发分析终端的使用环境时，可分为其自身的运行环境和终端应用的网络环境。

终端自身运行环境包括Windows类操作系统、非Windows类操作系统，通常被称为Windows类终端和非Windows类终端。

Microsoft公司推出的Windows类操作系统以其友好易用的人机交互界面，在推动终端的普及过程中起到了决定性的作用，因此其在商务和家庭用户终端操作系统中占比最大。目前，国内主要的工作终端运行操作系统以Windows系列为主，常见的版本有XP、Vista、Win7等个人版本和NT、2003、2008等服务器版本。2005年4月25日，Microsoft公司在西雅图WinHEC 2005大会上正式推出64位操作系统后，业务网终端所使用的操作系统逐渐呈现从32位到64位的转变，目前很多企事业单位在用的终端操作系统的版本有32位和64位两种。

广大的用户群也使Windows类操作系统成为黑客、恶意软件最为青睐的攻击目标。尽

管 Windows 操作系统在漏洞修复、系统安全属性完善上做了大量的工作，但遭受病毒、木马入侵等的报道仍层出不穷。

非 Windows 类终端主要指不使用 Windows 类操作系统的终端，主要为 UNIX 类和非 UNIX 类，UNIX 类包括 BSD、Solaris、AIX、HP-UX、Linux，等等，非 UNIX 类包括 APPLE 公司的 MAC OS 等。非 Windows 类操作系统的终端普及范围远远低于 Windows 类终端，其遭受的攻击也远远少于 Windows 类系统。

网络的普及和业务信息化的趋势，使终端的使用从个体独立运行逐渐转变为集群协作，无论是工作协调还是信息传递，单一终端独立工作的情况越来越少，终端之间的影响也越来越大，终端在所处环境中与其他终端之间的联系也越来越紧密。网络有很多种，包括从网卡直连的对等互访，到网络设备连接的小型局域网，再到网络链路组成的专网和互联网。在这些网络中，专网的安全性问题最为引人关注。在实现业务的专网中，计算机终端是网络中大部分行为的源头和起点，也是安全问题（如病毒传播、从内部发起的恶意攻击、内部保密数据盗用或失窃等）发生的源头。对每个单位来说，终端安全管理都是非常重要的，良好的终端安全控制技术能够保证企业的安全策略真正得到实施，从而有效控制各种非法安全事件，遏制网络中屡禁不绝的恶意攻击和破坏。

终端的使用环境，可以从广义和狭义两个角度来看，狭义的终端环境，指单一终端自身的操作系统和所处的网络情况，即终端环境包括终端自身的运行环境和终端应用的网络环境；从广义上看，所有终端所处的网络环境也同样是终端环境，差别在于广义上终端不是独立的个体，而是所有环境中的一个影响因素，并且互相作用和影响。

1.4 终端的使用者

对于企事业单位而言，接入其业务网络的终端包括其自有终端和外来终端两种。终端的使用者就其与接入网络的企事业单位之间的关系可分为内部人员、临时人员和外来人员 3 大类。就这 3 类人员在实际工作中所承担的工作不同，对于终端的使用方式和操作内容也不同，可对这 3 类人员进行细分。

内部人员通常包括管理人员、业务人员、网络/系统管理员 3 类；临时人员主要指在一些辅助岗位工作的人员；外部人员包括单位所在系统内的外来人员、厂商运维人员等。

不同的人员涉及的终端类型不同，参见表 1-1。

表 1-1 终端使用者-管理规范对应表

终端使用者		使用终端设备	操作内容
内部人员	管理人员	固定终端设备	业务系统 公文 个人信息
		移动终端设备	公文 个人信息
	业务人员	固定终端设备	业务系统 公文 外部信息 个人信息

（续）

终端使用者		使用终端设备	操作内容
内部人员	业务人员	移动终端设备	公文 外部信息 个人信息
	网络/系统管理人员	固定终端设备	公文 资产信息 网络管理系统
临时人员	辅助岗位工作人员	固定终端设备	公文 外部信息 个人信息
外部人员	厂商运维人员	固定终端设备	外部信息 网络管理系统
		自带移动终端设备	外部信息 网络管理系统 专业工具软件 个人信息
	系统内外来人员	固定PC设备	业务系统 公文 外部信息 个人信息
		自带移动PC设备	公文 外部信息 个人信息

表中涉及的设备名称定义如下：

（1）“固定终端设备”指组织配备的固定办公用业务终端或者公共终端设备，包括PC和服务器。

（2）“移动终端设备”指组织配备的可移动办公的移动终端设备，如笔记本电脑。

（3）“自带移动终端设备”指非组织配备的可移动办公终端设备，如笔记本电脑。

1.5 聊聊终端的安全问题

计算机网络技术迅速发展，网络应用快速普及，使办公信息化成为一种趋势。得益于终端和网络的支撑的“无纸办公”，一方面带来了管理的规范化，提高了整体的工作效率；另一方面因为网络与生俱来的安全性问题带来诸多安全问题的困扰。

随着人们对计算机安全意识的加强，逐渐认识到在网络攻击面前最薄弱的环节和最容易出现问题的地方是终端，终端是人类世界与网络世界的接口，是真正的网络边界。终端作为网络行为的发起者和执行者，终端安全问题是信息安全领域的重要组成部分。终端安全已经成为制约信息安全的瓶颈，尽管在安全技术和培训中已经投入了大量人力和资金，但终端安全问题仍频频发生。

终端具体面临着哪些安全问题呢？

日常终端使用中常见到以下几种现象。

现象1：终端使用中，基本配置工作，“去繁就简”。

“每次开机都要输密码，太麻烦了，设置为空，很方便的。”

“离开一会儿给电脑锁屏，回来还得重新登录，不方便，我离开从来不锁屏。屏保也不