ACCESS DENIED

拒绝恶意访问

〔美〕Cathy Cronkhite Jack McCullough 著
纪新元 谭保东 译

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

麦格劳－希尔教育出版集团
www.mheducation.com
Mc Graw Hill

拒绝恶意访问

[美] Cathy Cronkhite
Jack McCullough 著

纪新元 谭保东 译

人民邮电出版社 麦格劳希尔教育出版集团

图书在版编目（CIP）数据

拒绝恶意访问/（美）克朗凯特（Cronkhite,C.），（美）麦卡洛（McCullough,J.）著；纪新元，谭保东译. —北京：人民邮电出版社，2002.4

ISBN 7-115-10203-1

I.拒… II.①克…②麦…③纪…④谭… III.计算机网络—安全技术 IV.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 009950 号

拒绝恶意访问

◆ 著 [美]Cathy Cronkhite Jack McCullough
译 纪新元 谭保东
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67180876
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本：720×980 1/16
印张：13
字数：247 千字 2002 年 4 月第 1 版
印数：1-4 000 册 2002 年 4 月北京第 1 次印刷

著作权合同登记 图字：01－2001－5024 号

ISBN 7-115-10203-1/TP・2835

定价：28.00 元

内 容 提 要

本书深入浅出地介绍了威胁计算机网络安全的各种问题。主要内容包括：认识黑客和了解黑客的攻击方式、了解病毒和其他计算机害虫、如何保护电子邮件和电子商务安全、加密的种类及其使用、保护信息防止丢失和被盗、网络中的安全弱点及限制对计算机系统的物理访问，并且介绍了使用计算机进行远程访问时应当注意的事项以及如何防范对计算机及其网络系统的攻击、建立完善的安全保障体系等内容。

本书内容丰富、通俗易懂，适合于使用计算机网络系统的个人用户及单位用户作为有关计算机安全基础教育的参考书。本书将是各类机构的有关负责人、企业的经理、计算机安全系统的设计者在实施计算机安全工程中具有指导意义的必备参考书。

版权声明

Cathy Cronkhite, Jack McCullough

Access Denied: The Complete Guide to Protecting Your Business Online

ISBN: 0-07-213368-6

Simplified Chinese translation edition jointly published by McGraw-Hill Education (Asia) Co. and People's Posts & Telecommunications Publishing House.

前　言

为什么计算机安全如此重要

美国联邦调查局（FBI）估计每年由于计算机犯罪损失了价值 100 亿美元的财产，并且各类组织要花费 40 亿美元用于安全保护。由于这些成本继续上升，美国政府也在不断提高对计算机安全问题的响应。前大法官 Janet Reno 声明“由于计算机在我们的生活中的作用不断上升，计算机犯罪对我们的安全和隐私所造成的威胁也会增长”。她分配给司法部的计算机安全方面的资金和资源数量也在不断增加。美国前总统克林顿会见高技术产业的领导人时，与他们讨论为计算机安全而共同努力，并在 2001 财政年度预算中指明将 200 亿美元用于计算机安全的新发展。尽管（或由于）有这些考虑，大量的重大事故继续上升：从 1988 年的 6 件上升到 1999 年的 9800 件。美国 FBI 的调查（主要包括大公司和政府机构）报告在 2000 年一年中 90%的被告被检测为安全入侵。

这些攻击以多种形式出现。每一年新出现的病毒更加复杂，并且具有破坏性。它们破坏文件、使邮件服务器停机、使正常的商务活动放慢或停止。病毒不再是小的麻烦，它们对商业团体提出严重的威胁。

病毒只是一种使组织容易受到伤害的攻击。在 2000 年第一季度，包括 CNN Interactive、Amazon、Yahoo!、Excite 和 eBay 等主要在线公司都经历了拒绝服务攻击。这些攻击对网站发送大量的通信，直到它再不能处理的程度。当正常的客户试图在网站从事合法的业务时，他们就遭到 “拒绝服务”。令人啼笑皆非的是，这些攻击不是由老奸巨滑的罪犯施展的复杂的阴谋。具有一定程度的计算机技术和设备知识的令人厌烦的十几岁的孩子已经发动过许多次这样的攻击。

当公司允许雇员从家庭的计算机拨号进入公司系统，去从事公司的业务时，公司也招致了较多的风险。调查表明，有 57%的美国雇员在上班前或下班之后工作，有 17%的人经常性地用部分时间或全天在家里与公司网络连接。

不过，这些雇员中有 93%的人表示，他们没有接受过有关计算机安全方面的指导或训练。这种访问可以巧妙地绕过任何内部安全策略，并使得公司的宝贵信息极为容易地被盗窃或诈骗。

盗窃笔记本电脑也是另一种正在上升的安全问题。美国国务院报告，在 18 个月的期间内，它丢失了 15 台笔记本计算机。英国情报界也报告在 2000 年 4 月份丢失

了 2 台笔记本电脑。在这些笔记本电脑中有一些包含有未加密的高度机密的信息。研究显示每年有 15%的笔记本电脑丢失。机场、饭店和会议中心是笔记本电脑盗贼首要的目标区域。盗贼可以出卖或公开发表这些笔记本电脑内的任何未加密的信息。

由于处于如此之多的风险中，很明显，每一位总经理、经理、商店老板都需要拥有有关计算机安全的概念和解决方法的基本知识。他们必须能够了解这些事情，并且保证他们的公司合理有效地用钱。本书以一种易于理解的、实际的和面向业务的方式提供资料。

为什么不能将计算机安全问题留给信息技术专业人员

现存在商业界与技术界之间的交流隔阂对不断增长的计算机安全问题起着促进作用。每一组人讲着不同的语言。一组讲的是带宽和网络协议，另一组讲的是竞争优势与利益增长。虽然，两组人都担忧计算机安全，但他们仍然处于对立，并且用不同的语言呼喊。计算机安全太重要了，以致于在那个隔阂中不能丢掉。

在今天的商业中，许多重要的总经理和经理在他们的教育中有一种脱节之处。一个典型的 MBA 课程要求你去获得销售、市场学、会计学、经济学、伦理学和其他重要的商业纪律的背景知识。目的不是使学生准备作经济学家或会计师，而是提供概念并显示成功的组织如何管理那些纪律。不过，只是在最近，这些课程才开始将信息技术作为一个主要的研究领域。

今天，信息技术作为许多商业的核心，由于缺少知识而使组织易受伤害。常常是没有必需的背景信息或观点的人正在管理信息技术和安全。企业家和小商号的领导人特别容易受伤害。本书将提供那些背景知识并帮助去弥补那种缺陷。

谁应当阅读本书

任何处在一个单位的领导职位的人将会通过阅读本书受益。计算机安全成为先导——你能作为带头吗？或将你的病毒扫描器关掉吗？地位较高的人常常是最差的冒犯者并破坏安全策略。你对问题做什么了吗？转发欺骗吗？你支持 IT 吗？给他们需要的资金吗？你坐下来考虑过风险和应急计划吗？计算机安全已经碰到过你的雷达吗？聪明的 IT 人员、软件和硬件不会全部都做的，它采用有效的策略、有力的支持并实施那些策略。只有一个有知识并且明智的领导班子才能创立提供这种支持的文化。

IT 专业人员同他们的领导一起通过阅读本书也能受益。它可能提供共同的基础知识和工具开始一起进行工作去改进组织的计算机安全。当然，IT 专业人员会需要用更多的技术参考书扩大他们的阅读，但是这本书会帮助他们开发一个系统的计算

机安全方法。他们也可以从在附录 B 中提供的表格和样板中受益。

你应当怎样利用这本书

本书由 11 个章节组成，每一章涉及不同方面的计算机安全。你可以按顺序阅读每章，有系统地读完本书。你也可以直接跳读到任何一章，因为我们写它们以便它们也能够被分开独立阅读。首先选择对你最重要的章节先阅读它们。下面的安全检查表能帮助你找到你的最易受损害的区域。在本书的后面，附录 A 包括一个 Web 资源清单，附录 B 包含表格，词汇表提供计算机安全和相关术语的定义。

本书提供以事实为基础的最佳实施方案并给你做出有效决定的工具和信息。它会引导你开发一个系统的计算机安全的方法，而不会对最近的商业恐慌做出过强的反应。每一章都有最佳实施行动步骤供你使用，我们将它们分成两部分。组织的最佳实施行动步骤适合于大中型组织。小型或家庭式办公室的最佳实施行动步骤目标适合于较小的组织。如果某一步骤对你的组织或情况没有意义，那么就修改或删除它。

你如何使用本书，依据你的组织的结构和你在其中的作用而定。你可以选择下列建议中的一种建议或开发你自己的方法：

- 作为计算机安全的背景教育去阅读本书，较好地了解计算机安全问题和它们的影响。将它保留在书架上，以便在这些问题出现时作为参考。
- 作为中大型组织的领导阅读本书，系统地遵循中大型组织最佳行动步骤。
- 作为小商业业主、顾问、企业家或家用办公室主人阅读本书，系统地遵循小型或家庭式办公室的最佳实施行动步骤。
- 使用下面的安全检查表找出组织内的易受损害区域。阅读相关的章节并遵循可用的最佳实施行动步骤。

你选择哪种方法并不重要，重要的是你选择一种方法并开始。计算机安全常常停留在“抽出时间去做它”的状态表格上，直到危机发生和迫使组织去应付它。你可以预先主动并使用本书做准备并防止一场危机，而不是对它做出反应。用一点时间完成安全检查表。然后选择一种方法并立即采取行动改进组织的计算机安全。

安全检查表

领会安全检查表，可帮助你识别需要最注意的区域。在适当的时候，用 yes 或 no 回答问题。把没有回答的问题数目按章节加起来。数目最高的章节是最需要注意的章节。

第一章：了解黑客和黑客攻击方式

1. 你熟悉术语“黑客”吗？
2. 你熟悉各种类型非法闯入的人吗？
3. 你了解黑客的动机吗？
4. 你熟悉各种类型的攻击吗？

第二章：病毒、欺骗和其他计算机害虫

1. 你了解病毒、特洛伊、蠕虫和其他形式的恶意代码吗？
2. 你知道病毒和其他恶意代码对你的组织的威胁吗？
3. 如果病毒警告是一个欺骗，你知道如何确定吗？
4. 你知道如何防止病毒和欺骗的传播吗？
5. 你了解防病毒技术吗？

第三章：对电子邮件加以控制

1. 你了解电子邮件可能对雇员和雇主所造成的风险吗？
2. 你对雇员进行过电子邮件礼仪和法律后果的教育吗？
3. 你知道如何减少不必要的电子邮件数量吗？
4. 你明白电子邮件监控的后果吗？
5. 你劝阻过转发欺骗、连锁信、谣言和病毒吗？
6. 你了解有关新闻组和邮件清单的问题吗？

第四章：网站与电子商务安全问题

1. 你知道网站和电子商务的脆弱性吗？
2. 你了解如何防护网页毁损吗？
3. 你能识别操作系统和应用程序的脆弱性吗？
4. 你能保护你的业务防止非法闯入和诈骗吗？
5. 你知道如何保护顾客信息防止非法闯入和诈骗吗？
6. 如果选择一个 Web 主机或 ISP，你知道应考虑的标准吗？

第五章：加密的类型及其适当的用法

1. 你了解加密敏感信息的重要性吗？
2. 你熟悉各种加密类型和应用吗？
3. 你知道如何识别密码系统的脆弱性吗？

4. 你知道有关加密的政府法令吗？
5. 你了解数字签名、证书和不可抵赖吗？
6. 你熟悉虚拟专用网（VPN）吗？

第六章：保护信息免遭丢失、诈骗和盗窃

1. 你知道如何评估当前的备份系统吗？
2. 你已经执行了适当的数据备份程序表吗？
3. 你了解如何防止数据操纵吗？
4. 你知道如何限制数据访问和减少盗窃及诈骗风险吗？
5. 你能够选择最好的、用于备份的介质吗？
6. 你熟悉 SAN、NAS 和 HSM 吗？

第七章：网络安全的弱点

1. 你了解黑客是如何闯入你的网络吗？
2. 你知道主要操作系统的安全的利与弊吗？
3. 你了解口令的弱点吗？
4. 你熟悉保护口令的方法吗？
5. 你了解如何检测网络的安全吗？
6. 你能够分析软件包安全吗？

第八章：限制对计算机系统的物理访问

1. 你了解如何确定适合于公司的物理安全等级吗？
2. 你熟悉管理安全许可吗？
3. 你知道如何建立物理访问控制吗？
4. 你知道如何限制访问服务器、物理基础设施和带有敏感信息的计算机吗？
5. 你熟悉跟踪和访问登录吗？
6. 你知道如何应付未经授权的人吗？

第九章：有关远程计算的事

1. 你知道如何确立安全的虚拟办公室的惯例吗？
2. 你知道远程用户对你的网络所带来的威胁吗？
3. 你熟悉在旅行时保护笔记本电脑和其他移动设备的方法吗？
4. 你了解对无线网络和通信的威胁吗？
5. 你熟悉与海外旅行有关的信息安全威胁吗？

第十章：对攻击的响应

1. 你熟悉发现入侵的方法吗？
2. 你知道如何确定损害的根源和程度吗？
3. 你知道如何隔离证据以保证在法庭上它可被接受吗？
4. 你已开发了一个事故检测清单吗？
5. 你知道到哪里去报告计算机犯罪吗？
6. 你熟悉安全事故的事后剖析的调查吗？

第十一章：制定安全的商务惯例

1. 你已经进行过风险评估和审计吗？
2. 你知道如何起草安全策略和规程吗？
3. 你有一个应急计划吗？
4. 你知道如何建立一个计算机安全小组吗？
5. 当雇用职员或顾问时，你知道应当考虑的事情吗？

目　录