Oracle 技术系列丛书

ORACLE®

HZ BOOKS

AUTHORIZED ORACLE PRESS™—EXCLUSIVELY FROM OSBORNE

Oracle 安全手册

Oracle Security Handbook

(美) Marlene Theriault
Aaron Newman 著 潘德宏 等译

OFFICIAL • AUTHORIZED
Oracle Press
ONLY FROM OSBORNE

机械工业出版社
China Machine Press

McGraw Hill OSBORNE

Oracle 技术系列丛书

Oracle 安全手册

(美) Marlene Theriault
Aaron Newman
著
潘德宏 等译

机械工业出版社
China Machine Press

本书提供了经过验证的可以保护 Oracle 环境的技术和策略——涵盖范围从操作系统到网络。通过阅读本书，你可以一步步地掌握怎样使用 Oracle 的内置工具开发周全的安全计划。本书还讲解了如何避免黑客的攻击，以及如何审计和调试整个系统。由于得到了Oracle公司的官方认可，本书甚至还讨论了 Oracle 安全实现的部分细节。

本书内容丰富，讲解生动，是 Oracle 数据库管理人员及 Oracle 数据库开发人员宝贵的参考资源。

本书版权登记号：图字：01-2001-4778

图书在版编目（CIP）数据

Oracle 安全手册/（美）特瑞亚奥特（Theriault，M.）等著；潘德宏等译．-北京：机械工业出版社，2002.4
（Oracle 技术系列丛书）
书名原文：Oracle Security Handbook
ISBN 7-111-09985-0

Ⅰ.O… Ⅱ.①特… ②潘… Ⅲ.关系数据库-数据库管理系统，Oracle-安全技术
Ⅳ.TP311.138

中国版本图书馆 CIP 数据核字（2002）第 014180 号

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：周 睿
北京牛山世兴印刷厂印刷·新华书店北京发行所发行
2002 年 4 月第 1 版第 1 次印刷
787mm×1092mm 1/16·25 印张
印数：0 001-4000 册
定价：48.00 元

译 者 序

随着计算机网络的进一步发展，尤其是因特网的极度扩张，安全问题越来越严重，攻击与反攻击、防御与反防御不仅仅是信息世界中的事情，而且影响着我们生活的方方面面，甚至影响着国家的安全。现在常说的“信息战”就是指这种看不见的战争形式，而且越来越成为现代化战争的主要模式。

本书阐述了与 Oracle 有关的信息系统安全，是迄今为止有关 Oracle 安全最完整、最权威的书。本书提供了经过验证的可以保护 Oracle 环境的技术和策略，涵盖范围从操作系统到网络。本书从安全体系结构、基本安全原理以及 Oracle 安全机制等方面进行了讨论；并讨论了如何使数据库系统与操作系统等其他系统组件相互配合以建立整体安全防御体系。通过阅读本书，你可以一步步地掌握怎样使用 Oracle 的内建工具开发周全的安全计划。本书还讲解了如何避免黑客的攻击，以及如何审计和调试整个系统。从根本上来说，本书是非常实用的，而且是非常宝贵的参考资源！

现在，我们很荣幸能够有机会承担本书的翻译工作。在翻译过程中，我们经常为一句话、一个术语进行反复的讨论，到处查找资料，力图使本书的翻译能正确、贴切地反映原文的意思，同时注意使句子、段落符合中国人的语言习惯。我们真挚地希望你能够从本书中有所收获，这是作者的初衷，也是我们的愿望！

本书由潘德宏组织翻译，万方工作室的全体同仁都参加了本书的翻译、校正和输入等工作。具体参加本书翻译、录排、校对工作的人员为：田哲、丁小天、牛志、刘万堃、刘之砚、黄建春、丁胜利、蒋雯丽、葛丽、罗盟锋、罗天浩、王洞宾、赵文凯、夏宣哲、李树玲、孙小楠、葛宛析、龚露娜、马其军、李秀芬、田军、牛献忠、金百万、薛鹏飞、叶欣哲、邓南燕、邢倩丽、王煜、李文军、刘思、钱凯、赵策、江南、李昌浩、王凌霄、李锡林、张芝莉、范蕾、袁垒、邓笛、李林鸽、聂宛敏、王笑天、李飞、天昊鹏等。

由于时间仓促，且译者经验和水平有限，译文难免有不妥之处，恳请读者批评指正！

万方工作室

2001 年 12 月

前　言

最近，Marlene Theriault 去了一家廉价商店。在购买一些商品之后，她来到了出口处，并等待刷卡付款。这时，她注意到该出口处的营业员心情非常郁闷。她问出什么问题了。该营业员说他刚刚得知身份证被偷窃了，并且小偷使用他的名字、社会安全号、甚至临时警务人员的职业进行赊购账。幸运的是，其中一家信用卡公司通知他去验证某些信息，并告诉他所出现的问题。听说他的个人信息是从以前曾经交易过的 Internet 公司泄漏出去的，他非常惊骇。这是偶然事件么？实际上不是。现在，越来越多的人面临着如何防止最重要的个人信息被盗窃，并且许多公司正在积极地处理安全漏洞和信息盗窃问题。

黑客攻击和因特网信息受威胁现在是不争的事实。我们感觉目前是编写有关 Oracle 安全图书的时机了，应该从 Oracle 安装和配置、网络传输以及因特网服务等角度讲解在操作系统之上保护 Oracle 数据库的细节。因而，我们从安全和 Oracle 的历史开始讲解，以便于你更好地理解那些可以驱动安全技术解决方案革新的问题和相关事宜。

由于我们认为解决任何问题的最好方案是制定活动规划，因而我们接下来讨论当创建自己的安全规划时必须考虑的问题。我们假设你已经对 UNIX 和 Windows 安全方法有很好的理解，然后直接围绕 Oracle 数据库讨论有关安全问题。在本书中，你将学会如何逐步实施系统和数据库安全的方案，有助于你尽快地完善本公司敏感性数据的安全保护措施。

我们编写本书的目的是为了帮助读者增加安全方面的知识，以便你在规划本公司 Oracle 数据库信息安全保护的手段、工具和措施时轻松如意。

目　录

第三部分 保护 Oracle 数据库

第四部分 保护网络通信

第五部分 黑客和问题解决

附 录

第一部分 基础知识

第1章 安全构架

世界已经变成一个很小的地方，在新的每一天，信息变得越来越容易获取。计算机已经明显地改变并且提高了我们日常生活的质量，使我们能够做许多令人称奇的事情，例如相距几千英里的人们能通过计算机交流彼此的意见。

与此同时，随着数据变得很容易分享，也使保护私有数据的需求不断增长。想想你的医疗和财务记录，如果这些记录落入了恶人之手将会造成什么影响？无论对你个人还是负责保管这些记录的公司，都是毁灭性的灾难。数据安全可以定义为：一个公司用来保护信息不落入邪恶之手的综合方法和行为。

我们相信要知晓未来，就必须反省过去。为了证明这个理论，我们将对数据安全的历史进行一个简要的回顾。在我们回顾数据安全的历史之后，我们将解释一些被广泛应用的安全术语和讨论这个行业所依赖的一些安全特性。在第2章里，我们将向你展示Oracle公司是如何构建其产品以适应行业的安全需要。

1.1 安全的发展

最早关于数据安全的记录大约发生在两千年前。朱丽斯·恺撒使用一种简单的加密格式给各地的将领们传送消息。这个算法是通过把消息中的每一个字母向右移三位来实现的，这就是现在所说的恺撒密码。用我们的字母表来举个例子：短语“I love security”就变成了“L oryh vhfxulwb”。对于恺撒来说，这种安全措施保证了那些作战计划不会落入敌人之手。其代价是万一某人破解了这些密码，将意味着成千上万罗马士兵的死亡。

为了看清楚前面的那个短语是怎样被编码的，让我们将字母表的每一个字母向右移三位，请校验我们正确转变的短语。

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
d e f g h i j k l m n o p q r s t u v w x y z a b c
```

为何恺撒使用如此简单的算法呢？恺撒运用密码的成功归因于以下三点：

1）他的敌人不知道这个加密的主意；

2）这个算法是高度机密的；

3）破解加密的数学方法还没有被发现。

然而，这个算法存在很多问题，不能经受时间的考验。当然，最糟糕的问题就是一旦这个秘密被人知道，任何消息都会很容易地被破解。

今天的计算机安全基于类似恺撒密码一样的原理。我们使用复杂的方法来改变数据的表示，因此，人们就不容易读懂我们的信息。加密是指为了隐藏信息的确切涵义而改变信息的行为。加密允许我给你发送只有我们之间才能理解的消息，并且可以防止那些即使可以看到该消息的人理解这个消息的含义。通过互联网传送加密的消息是我们如何利用这种技术来隐藏信息的一个典型例子。当你得到一个被加密的词、短语或者消息，并且运用某算法将它转换为最初的形式，就可以说你已经将其解码。

安全实现类似于链子——它的强度等于其最脆弱的部分。保持安全的惟一方式就是领先你所要防备的人一步。保护数据安全就像保护你的家。选择一个有适当安全能力的系统只是管理你家庭安全的第一步。首先，你得决定在你的前门安装一个多大的锁。也许你还会购买一个安全报警系统。有人会破窗而入，所以你要在窗户上安装护栏。有人会发现你有个宠物入口，所以你得将它锁定。当丢失了一把钥匙，你会换一把新锁。当锁生了锈，你也会换了它。正如你所知的，安全是一个持续过程，促使你在其他人认识到这些问题的存在之前发现并及时解决它。

进入计算机

在过去的 50 年中，安全和技术是一起发展起来的。计算机的出现产生了决定哪些人可以访问这个新机器而哪些人不能的需求。从 20 世纪 50 ~ 70 年代，大多数的计算机存放在空调房间里，并由穿着白大褂的人维护着的庞然大物。让计算机听从你命令行事的惟一途径就是在控制台上拨动开关或者是将打孔的卡片插入其中。对于那些早期的计算机来说，安全是非常简单的。计算机安全规划就是在房间的门口安排警卫，为每个计算机用户查验证件。对于这些孤立的巨人来说，这样的安全措施已经是相当够用了。

在 20 世纪 70 年代，随着大学和政府计算机网络的蓬勃发展，网络工程未来前景的征兆就已初现端倪。仿佛突然之间，你不需要直接接触计算机就能够获得信息。由于可以节省费用，大学很乐意接受这种联网的概念。在网络的帮助下，几个人可以更有效地共享一台打印机或者计算机。然而，网络的出现标志着系统安全需求有了一个重大转折，虽然在那时只有非常少的人知道如何利用这些机器通信。任何能够连接网络的人可能会试图控制别的机器。那些通晓计算机和网络通信的人一般都有良好的企图，并且能够连接进网络不是一件简单的事，因此这时缺乏安全设置并不会引起严重的风险。

到了 20 世纪 80 年代，在各种办公场所的办公桌上开始出现了供个人使用的计算机。软盘被用来在个人计算机之间传递数据，保证它们的安全就是防止恶人偷走计算机内的重要信息。把敏感的文件加密以确保获得它的人无法读懂其中的内容。作为个人计算机的用户，你经常要面对的就是给一大堆软盘排序，并记住它们的来龙去脉。虽然保护硬拷贝的带锁的文件柜是被普遍使用的一种办公设备，但是越来越多的办公室现在还使用可锁的保险柜来存放软盘以及九磁道的磁带。

在 20 世纪 90 年代，一种难以置信的现象发生了。个人计算机到处都是，而且通过调制解调器和网卡，它们之间可以相互随意“交谈”。只要你想说什么，你就可以与其他人说什么；

也就是说，你的计算机与另一台计算机使用兼容的语言和网络协议。在这种形势下，安全需求很快地被提到议事日程上来。

虚拟世界的安全

数字革命使我们具有可以随时与世界任何一个地方通信和获得信息的能力。根据虚拟世界的法则，人们可以使用虚拟身份。以匿名的身份出入虚拟世界比在现实生活里冒充他人身份要容易得多，也快得多。

随着计算机的日益普及，越来越多的人通过学习，逐渐通晓了计算机是如何工作的，从而成为计算机学者。人们开始明白只要有足够的聪明，就可以让计算机做任何想做的事，甚至那些不允许的行为。获得为计算机解锁的技能开始成为一个小的秘密行业。这个秘密的世界开始共享计算机信息和仔细研究计算机安全、揭示它的漏洞。一个密法成为和计算机比智慧的挑战。在早期计算机安全观念的形成中，媒体扮演了一个很重要的角色。如《战争游戏》、《鬼鬼祟祟的人》等这些电影给了人们一个有关什么可以做而什么不可以做的误导。媒体所实现的就是使人们意识到缺少计算机安全将会对世界造成毁灭性的影响。军事机密被泄露，金融系统被摧毁，潜在地导致了一片混乱。

第一个表明计算机是如此地易受攻击的例子出现在 1998 年，当时康奈尔大学的一名毕业生无意间释放了一个互联网“蠕虫”。这个美国国家计算机安全中心首席科学家的儿子 Robert Morris，Jr. 编写了一个可以自我复制和在计算机之间自我传播的程序。这个程序利用了电子邮件程序的 sendmail 和 finger 后台程序 fingerd 中的缺陷。sendmail 程序用于发送和接受电子邮件信息，fingerd 程序负责 finger 命令。Finger 命令用于罗列出登录到系统的用户名单，为管理员提供查看谁当前正在与系统进行连接的一种方法。

通过一种特定的方法格式化发送这些程序的消息，可以在这些将被服务器程序运行的消息里嵌入命令。这样，那些在服务器上没有账号或权限的人就可以利用这些漏洞让服务器为他们运行命令。“蠕虫”在服务器之间“跳来跳去”，通过互联网在成千上万的计算机中蔓延。在占领一台服务器之后，“蠕虫”将复制自身，利用这个服务器试图去占领其他服务器。结果是什么？大量连接到互联网的服务器因为“蠕虫”引起资源的耗尽而最终崩溃。

为机器清除“蠕虫”和增加预防措施需要各地的组织投入人力、物力来消除“蠕虫”所引起的灾难。这些费用可以从以下几方面来估量：

- 为计算机“消毒”所必需的人员开销。
- 创建和安装补丁程序的时间。
- 计算机有效性的损失。
- 计算机脱机时所耗费的人力资源。
- 这次入侵给互联网带来的恐惧。

Morris 的“蠕虫”引起的经济损失估计高达一亿美元。幸运的是，“蠕虫”不是破坏性的，没有删除或者修改计算机中的文件。Robert Morris 因为制造了“蠕虫”而被判处三年的缓刑，罚款一万美元，还被判处参加 400 个小时的社区服务。

Morris 的“蠕虫”还产生了一个建设性的结果，那就是唤醒了那些在计算机上工作的人们

对虚拟世界的真正危险的注意。这是危险程序第一次攻击互联网，威胁计算机。人们开始对计算机安全投以更多的关注。“蠕虫”的技术被分析，制定了更多新的开发软件的预防标准。作为对这次事故的反应，美国国防部组建并投资了 CERT（Computer Emergency Response Team，计算机危机处理小组）。CERT 的职责就是敦促管理员意识到这些攻击的潜在性，以防止这类灾难的再次发生。

1.2　了解面临的威胁

正如我们将在这本书中使用的术语，威胁是指为保护你的系统而应加以防范的对象，包括人、政府、公司或者其他组织。威胁会引起有意或无意的破坏。威胁所引起的破坏范围包括：

- 删除数据。
- 以无法侦测的方式改变数据。
- 将数据泄露给与你组织对立的一边。
- 摧毁系统。

确定要防范哪种威胁取决于被保护的数据的类型。如果你要保护的是公共信息，你就不在乎谁读取了它。一些系统需要允许用户改变他们自己的数据。你要做的就是确定你需要担心哪种威胁及如何来减轻这些威胁。

军事组织有着不同级别的数据和多种需要担心的威胁。在军事组织和政府组织里，数据可以被分为从顶级机密到可公开的许多级别。对于顶级机密，最大的威胁就是那些有着雄厚资源，致力于研究和寻找系统漏洞和入口的外国政府。这就是为什么你无法在互联网上发现顶级机密的原因。不能用因特网来保管国家安全机密，因为因特网的安全性有太多的薄弱环节。

当你试图保护相对不那么重要的数据时，好奇的人们也许是更大的威胁。你经常听说一个十几岁的小孩成功地使用黑客的手段进入一些存放着有关体能测验结果和士兵职责记录的军事计算机。军方只是利用他们现有的资源，采取必要的步骤来对付安全威胁。没有足够的资源用于保护所有军事数据的整体安全。同样的，公司也不能够总有足够的资源来保护他们的每一条信息。总有一块灰色的区域，表示没有把数据保护到它们应该受到保护的程度。当然，什么数据是至关重要的取决于你的看法。

我们都相信银行会正确地存放我们的钱，正确地处理我们的交易。对银行而言最大的担心和最大的威胁就是那些企图非法取走钱的人。你是否意识到贼的威胁不仅来自于外部也来自于内部？正如银行抢劫案内部作案和外部作案几乎差不多多。抢劫数字银行经常是内外勾结的。因此，银行必须保证没有一个人可以对任何特定的计算机系统有着无限制的访问权限。银行的计算机必须被设置成执行独立的交易核准制度。

非赢利组织要面对的是另外一种类型的威胁。很少有人想从这些组织中偷取钱财，因为它们一般只有非常有限的资金。这些组织也很少有需要保护的机密数据，对它们来说破坏者（vandals）是主要的威胁。在这里，破坏者是指那些和这些组织有着不同政治观点的人。他们也许想给这些组织带来麻烦或者是不想让人们获得这些组织的信息。非赢利组织经常有着最差的安全，因为它们没有足够的钱用来支付给管理员以彻底地保护它们的系统；而且它们不认为

有存在这种攻击的可能性，因为它们觉得只有很少的破坏者能够从攻击它们中获益。然而，有许多破坏者将进入这些地点当作一个挑战，而且因为相当松懈的安全防范，使得非赢利组织成为一个容易被破坏的目标。

在理想世界，威胁是不存在的，你可以完全地像相信你的邻居一样相信世界上的任何一个人。然而，这不是理想世界；这里有各种各样的人，你要防止你公司私有信息落入他们手中。如果你有保护公司资产的责任，你就应该知道要防止谁和防止什么。现在让我们看看你和你的系统要面对的各种不同类型的威胁。

1.2.1 来自内部的威胁

那些经过授权进入你内部网络的人可以被归为内部威胁。这些人通常是在防火墙后直接访问网络的，而且你对他们有着一定级别的信任。他们可能是雇员、顾问、临时工或者是被当作雇员的工业间谍。

当处理这些雇员时，你经常发现一些灰色的区域。清白的雇员也许会不怀恶意的逾越界限。可以将一个授予自己超级用户权力的雇员看作是违反了安全条例，即使他在获得这些权限时没有执行过任何非授权的操作。你可以将这种情况等同于复制银行金库的钥匙且自己保存了一套。这是一种犯罪行为吗？也许是，也许不是，但这是不恰当的行为，可以给雇主一个明确的理由来解雇这个雇员。

还一些清白的雇员，无论是出于方便、必要还是懒惰的原因，违反了已制定的安全制度或者是执行了无法保证安全的行为。尽管这些雇员没有恶意但是这仍然构成了危险的安全威胁。雇员可能因为方便的原因共享密码，这样做就将你的系统置于危险之中。如果你使创建新用户的过程变得更容易，雇员就不觉得有共享密码的必要了。换句话说，如果你发现最终用户不支持你的安全制度的理由，你可能就要寻找一个解决方案来减少用户违反规定的想法。

通常，仅仅靠提高雇员对安全规定处罚条例的意识来帮助公司避免安全隐患还有很长的路要走。在正确的态度和得体的用户教育下，许多潜在的威胁可以被消除。记住大部分雇员都想做好工作，获得荣誉和承认。表扬一个雇员在维护安全方面的有效成就可能足以鼓励其他雇员跟着做。

1. 来自管理员的威胁

要对待的最大威胁来自于管理员。为什么管理员会成为威胁？正因为你完全信任他们。产生这个问题是因为人们会更换工作，你最聪明的管理员也许明天就会为你最大的竞争对手服务。有时正直的人也会变成有争议的人。随着人们走来走去和情况的改变。在一个经理手下快乐的、有成就的雇员可能会在不同的公司管理下成为悲伤的人。随着人事变动和职位变迁，他们也许不再有权力接触他们在做早期工作时所接触的信息了。

处理来自管理员的威胁可以用行政手段和怀疑主义。要记住的一点就是不要将你所有的信任放在一个雇员身上。防止需要管理权力的人不滥用他的权力是没有好办法的，但是你可以建立一套程序，使得一个人很难在不被发觉的情况下进行恶意的行为。你可以采取的方法包括：

- 对管理任务需要审核。

- 建立在执行代码或者任务之前由另一个部门进行复查的程序。
- 建立需要两个人才能完成的过程。
- 将不同的任务由不同的管理员负责。
- 分配完成任务所必需的最小权限。

2. 最终用户的威胁

最终用户引起几种常见的无恶意的威胁。然而，不能因为它们是无恶意的就认为它们比起有恶意的威胁来就不重要了。在这个范畴内的大部分威胁属于我们在本章前面提到的“清白的雇员”这一类威胁。修补最终用户安全问题的最好方法就是使用一个技术与教育相结合的解决方案。

通常最终用户被授权来查看、更改、增加还有可能删除一些数据。他们可以存取他们自己销售区域的信息或者是雇员的信息，但是你不希望他们有对其他雇员的数据进行操作的权限，除非他们的工作确实需要这一级别的权力。

尽管最终用户一般都是无恶意的，但是如果访问信息过于容易，一些好奇的雇员就会试图逾越他们的可访问级别。对于大多数人来说，对别人的薪水好奇是人的天性。如果知道可以得到这些信息，大多数人都会做出某种努力来了解其他人的薪水。当然，依赖于销售业绩谋生的销售人员也许更试图去看看别的销售员的情况。

当你处理管理员的事情时，你经常会遇上一些比较出众的雇员。而对于一个系统的最终用户，情况是很不一样的。计算机可以处理大量的并发用户，并且随着用户数量的增加，你对每一个连接到系统的用户个性的控制会越来越少。如果你的计算机系统只有十个用户，跟踪每一个用户的所作所为是很容易的事。当最终用户的数量达到一千时，了解某个特定用户的行为或者确定哪些用户需要仔细监控是相当困难的。

如果安全是在客户端应用程序设置而不是在服务器上设置，就存在另一种类型的来自内部用户的威胁。许多应用程序依靠客户前端程序的逻辑在数据被送往服务器之前进行适当的验证或者预处理。聪明的雇员常常寻找为他们的组织提高生产力的捷径。不幸的是，捷径不一定都是好主意，特别是如果一个最终用户绕过应用程序，直接从系统里删除记录且没有正确地结束操作。许多管理员已经意识到这种危险，有些应用程序，如 Microsoft Access 或者 SQL * PLUS，只要在略知一二的用户手里就可能引起这样的麻烦。

要防止这类问题发生，在设计时就要从根本上考虑安全问题。决不要依靠客户端的代码来验证或是校验权限。确保这类的校验在无法被绕过的服务器上完成。

3. 组织规模的影响

当遇到计算机安全问题时，小组织更愿意对它们的雇员抱以完全的信任。它们常常没有足够的资源用于采取合适的安全措施，因为它们没有足够的雇员来进行权利和义务的分工。觉得因为公司很小，并且雇员都是精选的，他们都是可以被完全信任的。本书的作者之一曾经在一家小公司工作过，在他第一天上班时就被告知：“我们就是这样工作的。我们将给你全部的系统权限因为我们认为你是一个受过训练的专业人员，需要用这些权限来完成你的工作。如果你滥用这个权力，你将被解雇。”对于这家公司，这种方法看起来好像挺好，虽然你可以用另外

一种看法来看它。你可能会说："迄今为止，他们还没有发现任何问题"。

在更大的公司，在发现雇员不值得信任之前一直信任他们的制度是不可行的。一个公司滥用信任所要付出的代价是很大的。确切地说，大公司有更多的钱用于投资，这就更可能有计算机间谍会为愿意冒险的人慷慨地支付报酬。因此，公司越大，越有破坏安全的考验，公司也就要更小心地确保安全措施的实施和加强。

要确保你的系统安全，需要一点点的偏执。当你公司发展时你可以认为今天所信任的人将来将不可信任。没有检测每种威胁的风险的固定公式，但是要考虑如下所示的因素：

- 内部网络的用户数量。
- 可以访问系统的人数。
- 组织内的职责分工。
- 要保护的数据的种类。

1.2.2 外部威胁

在前几节里，我们概览了来自你组织内部或者来自经过授权可以访问系统的人们的威胁。在当今的计算环境里，你的公司可能正在与外部代理或者团体做生意或者在未来的一两年里会和在你的内部网之外的团体做生意。你可能已经不止一次地被告知，如果你的公司在不久的将来还不通过因特网做业务的话，你的生意将无法生存。这是否是一个引起惊慌的想法？

在本节里，我们将讨论你公司与外界联系所引起的威胁。首先，让我们解释一下我们所说的外部威胁是什么。外部威胁就是指那些没有授权访问你系统或网络的人。这些人通常位于你的组织的防火墙之外。现在，要记住防火墙一般只能阻止大部分但不是全部的威胁。不幸的是，有很多聪明的方法可以绕过或者是穿透你的防守。

1. 进入你的组织

当你试图阻止不受欢迎的人进入你的系统所遇到的第一个问题就是你的防火墙可能没有正确地设置。你可能因为一些业务上的需要而使一些特定的端口保持打开状态。我们遇到过很多因业务上的理由而使用安全性很差的防火墙的例子。防火墙软件本身的漏洞可能会使一些攻击得以通过。当发现防火墙软件的漏洞时，软件商很快就会提供补丁程序。最大的担心是那些怀着恶意的想对你的系统进行某种形式的破坏的黑客可能在别人还不知道这些漏洞之前就已经发现了这些漏洞。当这些攻击危及到你的防卫时，你将只有很少甚至没有机会防止你的系统受到破坏。

使用一种很普通的称为 war dialing 的手段可以找到你的系统的备用路由。在 war dialing 里，可以用一台计算机随机拨叫一个公司电话的末尾几位来寻找在电话另一端的计算机。例如，如果你知道总机号码是 234 - 1000，你可以试着拨叫 234 - 1001 到 234 - 9999 之间的所有号码。这样的目的是想发现是否有人将计算机设置为可以接受呼入的电话连接以便他可以在家工作。你可以防止你的用户的这种行为，但是很不幸，在一个拥有成千上万的计算机的公司里，完全解决这个问题是非常难的，尤其是当用户明明知道他们这样做是错误的但他们还是隐瞒所做的事实。一点点错误就会威胁整个网络。

最近，最普遍的入侵方式是在 email 里嵌入“特洛伊木马”病毒。我们曾经听说过“美丽沙”病毒和“我爱你”病毒。这两种病毒都是利用公司 email 目录将它们自身发送给其他用户。许多公司在受到攻击后，为清除病毒终止了几个小时的 email 服务。和我们所见到的危害一样，这些病毒实际上没有我们曾经见过的其他更为复杂的病毒那么有害。如“美丽沙”这样的病毒像一群受惊的大象一样在你的网络里到处乱窜，虽然你可能不知道是什么病毒引起这些麻烦，你很快就会看到破坏，知道你的地址簿有问题了。

其他病毒，像“QAZ 特洛伊”，比所觉察到的危害要严重得多。“QAZ 特洛伊”悄悄地在你的服务器上安装它的有效载荷，并启动与攻击者的通信，将你的系统的信息发送给攻击者，这样就使得攻击者得寸进尺，获得更大的权限以便入侵。侦测这样的攻击是很困难的，因为这意味着要死死盯住安全工具和管理器的显示窗口。

这种形式的攻击曾经在 2000 年 10 月被用于攻击微软公司。一个粗心的雇员接收到一封包含一个附件的 email。当这个雇员毫无警惕地打开这个附件，“QAZ 特洛伊”就被安装在微软的系统上，并和位于亚洲某个地方的攻击者联系。一个用户的疏忽打开了一道可穿越微软防卫的虚拟的门。幸运的是，只造成了很小的破坏，但你可以看到即使是最注重安全的组织，只要存在一点薄弱环节就容易被黑客所渗透。

2. 黑客是如何攻击的

开始时，外部威胁可能没有你的系统的任何信息。一个耐心的黑客首先采取的步骤就是开始收集信息。他可能开始观察其他人在网络中做了些什么，或者可能开始收集一些诸如软件版本和补丁的信息。利用这些信息，入侵者开始制定一个攻击计划。

对你的系统最著名也是最常见的外部威胁就是黑客，这是一个充满争议和混乱的名称。许多人，主要是那些自称为黑客的人觉得这个称号被误用了。

最初，黑客是指那些有着丰富的计算机编程技能以致于可以完成以下几种任务的人：

- 能读懂其他程序员的代码。
- 能理解最初的程序员的意图。
- 能为更好地执行旧功能或者为执行新功能而更改代码。

因此，黑客是指能够理解和改进他人的代码的人。

现在黑客团体有着几个不同的派别。其中一派是指那些更愿意被称为“黑客”或者“白帽子”的团体，意味着一种荣誉。这些人将他们的动机归结为好奇心和帮助使计算机更安全。“白帽子”们为安全公司工作或者把安全作为他们的业余爱好。要符合这一范畴，黑客不能触犯法律或者是访问他们没有被授权使用的机器。这个组的人不会对你的计算机安全造成威胁。实际上，你的公司可以雇佣一个“白帽子”来验证你的系统的安全性。

另一个派被称为“骇客”（cracker）或者“黑帽子”。这一组人常常靠吹牛来决定在组里的强弱地位。黑了谁或丑化了哪个网站将给他在这一群体里带来荣誉。不幸的是，在这一组里有许多非常聪明的人，且他们的动机通常是恶作剧。“骇客”和“黑帽子”团体是一个成分复杂，范围从有太多时间的十几岁小孩到在计算机科学专业领域有着高学历的职业罪犯。职业罪犯不是那些已经被捉住的人，而是那些你很少听说过的人。

在“骇客”或者是“黑帽子”中有一个独立的组织叫做“脚本羔羊”(script kiddy)。这些人使用脚本或者黑客工具来闯进网络。其他的黑客看不起这些“脚本羔羊”，因为他们利用了其他人的工作，而不是使用逻辑和技巧来破坏系统。虽然使用自己的知识闯进系统可能是更高贵的，但是底线要合法且不要没有经过许可就进入其他系统。

虽然本意是无害的，但作为“白帽子”还是有一些不好解决的道德上的问题。“白帽子”常常开发出用于证明其想法的工具。这个工具或者利用了系统的弱点或者用于测试“白帽子”自己的网络。如果这些工具没有落入“黑帽子”之手，开发这样的工具是没有消极影响的。如果“白帽子”公布他的工具以便其他的管理员可以使用它来检测自己的网络，这个工具将肯定会落入一个或者更多的“黑帽子”手里。如果“白帽子”自己保留这个工具而不将它公布，那么许多网络的漏洞可能得不到修补，且这个“白帽子”就对这个团体做了一件不友好的事。

第三个派别，也就是称为“灰帽子”的派别，最近常常被提起。这个“灰帽子”派起因于在“黑帽子”和“白帽子”之间存在一个中间团体。许多黑客曾经是“黑帽子”，但是再也不做那些将他们定为此类的事；许多“白帽子”与“黑帽子”之间有着很强的联系。计算机安全和威胁总是互消互长的。不同于“黑帽子”和“白帽子”，“灰帽子”承认黑白之间存在的差别。

1.2.3 安全漏洞来自何方

到现在，你肯定会问自己，“为什么会存在安全漏洞？难道我们不能修复它？”这两个问题都是极好的问题。我们需要看看什么引起了麻烦，要做什么来修补它们。

1. 系统错误配置

安全缺口产生的最普遍的原因就是系统的安全特性没有正确地启用。相当容易地安装了服务器却忘记更改默认的密码。你也许会认为这是个微不足道的问题，但是这种情况比我们想象的要多得多。你的系统也许有从加密到验证等全部最新的安全特性，但是如果这些特性没有被启用或者是没有被正确配置，那么它们对你和你的系统没有任何好处。

这究竟是谁的责任？这些问题经常是从缺少良好训练的雇员到没有正确的默认设置等多种因素综合产生的。让我们面对它——让计算机投入并一直工作不总是一件简单的任务。安全是管理员任务单上一个主要的令人头疼的事。

如果你是一个系统管理员，应该已经知道你经常加班，还是根本没有时间从复杂的系统中查找出一个不正确的设置项。查找一项不正确的安全设置就等同于大海捞针。你经常会被安排去管理一些你不熟悉的系统，即使你熟悉这个系统，系统中的软件包有着如此多的新特征以至于跟上这个新版本是件非常困难的事。

如果你是一个软件开发人员或者是软件供应商，你也有一项同等困难的工作。作为开发人员，你的目标是在尽可能地实现一些新的特征以保证你的产品可以为公司获得长期利润的同时，使你的软件安装和设置尽可能地容易。不幸的是，软件安装的简便程度通常是和正确的安全标准背道而驰的。因为软件供应商希望使他们产品强大的新特征能尽可能被简单地使用，他们常常鼓励甚至是强迫你使用系统的最高权限来安装他们的产品。实际上，如果你想维持目前