网络管理员丛书

网络管理安全资源指南（第一卷）

Tech Republic 著　　尹建国 译

你的计算机系统遭到未知的入侵吗?

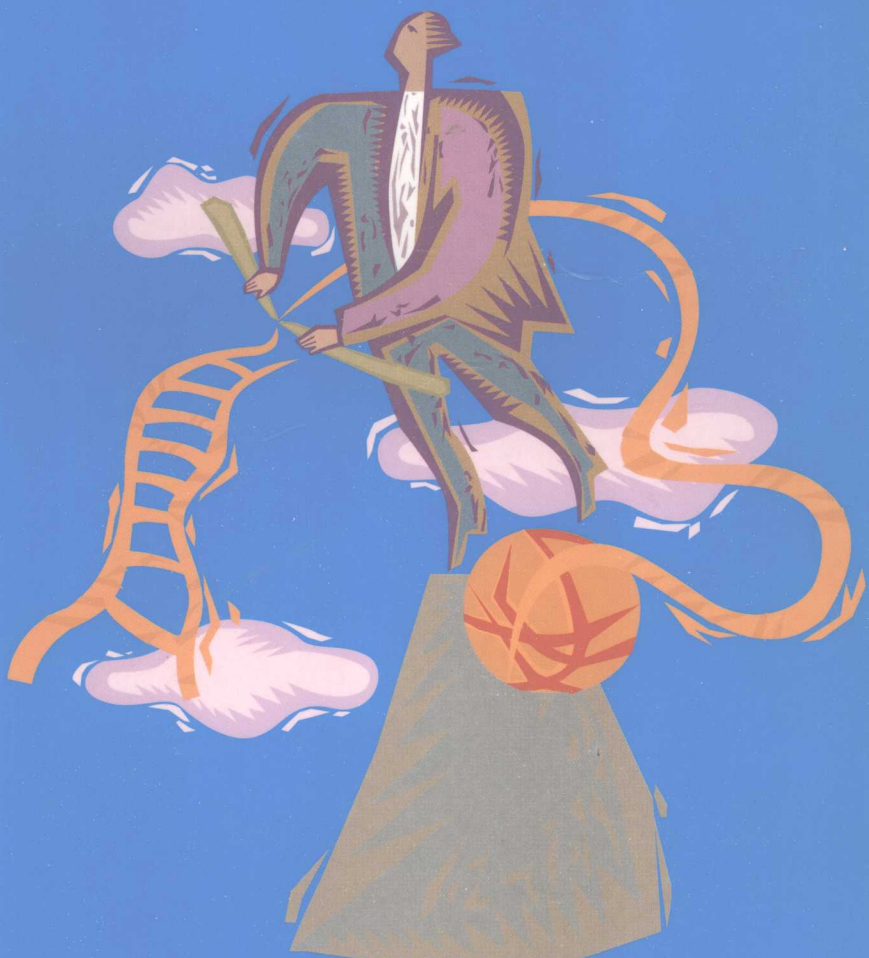
在这个资源手册中你将学会

如何确定系统中的弱点，

消除潜在的危险，

当安全出现问题的时候

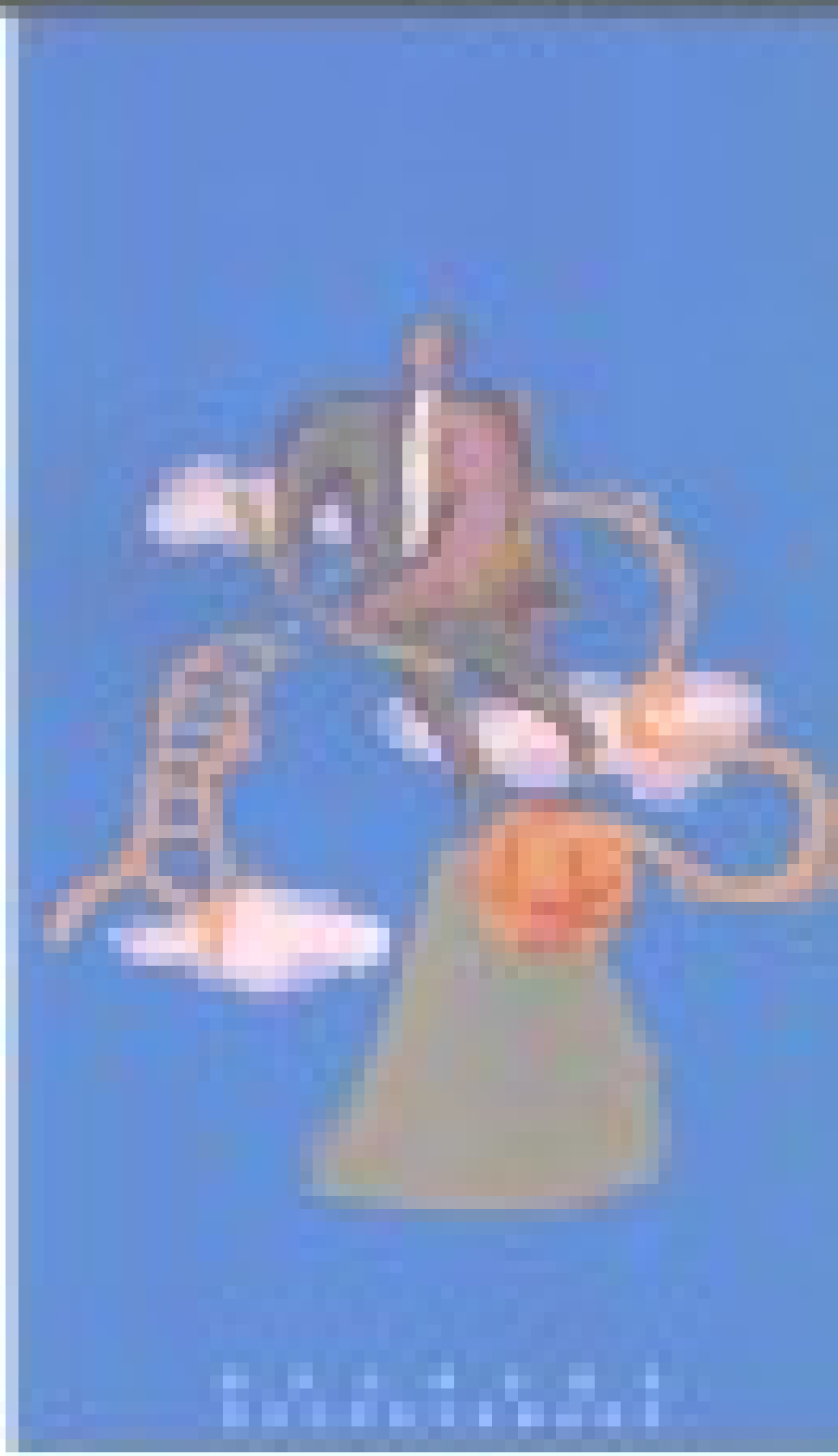
如何修补漏洞。



TechRepublic

南开大学出版社
南开大学电子音像出版社

网络管理安全资源指南



网络管理员丛书

网络管理安全资源指南（第一卷）

Tech Republic 著

尹建国 译

南开大学出版社
南开大学电子音像出版社

内 容 简 介

屋漏偏逢连夜雨……最新的电脑病毒又把整个公司的邮件系统和服务器给弄瘫痪了。公司的其他人都来找你寻求帮助，希望你给他们一些建议。那么你该怎么做呢？来看一看《网络管理安全资源指南》吧。

在本手册里，你会学习如何防止新的安全漏洞，如何将已有的安全漏洞逐一修补。此外你还会从本手册和光盘了解到：

- ◆ 建立完美的防火墙
- ◆ 将“错误”的电子邮件过滤掉
- ◆ 使用最新备份的磁带将系统重启
- ◆ 了解网络安全的基本准则
- ◆ 更深刻地理解密码的含义

丛书名称：Tech Republic IT中文版网络管理员光盘手册
光盘名称：网络管理安全资源指南
标准书号：ISBN 7-900628-51-7/TP·51
程序制作：Tech Republic
手册原著：Tech Republic
翻　　译：尹建国
出 版 人：肖占鹏
责任编辑：尹建国　李江卫
出版发行：南开大学出版社
南开大学电子音像出版社
地　　址：天津市南开区卫津路94号
邮政编码：300071
服务热线：(010) 82656677　(022) 23504636
营销电话：(022) 23500755　23508542（传真）
技术支持：pcmag@pcmag.com.cn
光盘复制：北京中新联数码科技股份有限公司
手册印刷：北京科技印刷厂
开本规格：787mm×1092mm　1/16开本
印张字数：16.75/223千字
定　　价：37.00 元（ 1张光盘 + 手册）

前　言

欢迎使用 TechRepublic 的这本安全资源指南。通过本书可以得到安全方面的建议、提示、技巧和对你有帮助的文件，使每个 IT 专业人士和网络管理员的的工作更加轻松。

这本资源汇编把许多具体的内容放在一起指导你走向网络安全之路。所有这些章节的主题就是安全。在每一章里面都能找到 TechProGuild 的练习和 TechRepublic 的内容。你可能会问自己“我能通过在线得到什么好处吗？”好了，朋友，这种日子已经过去。当你遇到问题的时候，你将享受并从你的网络中获得好处。这时，TechRepublic 会对你有很大的帮助，这就是我们将本书奉献给你的原因！

本书第 1 章简单地包括了一些基础。内容包括：安全的方法、原则和技术等基本知识。本章覆盖了你在应用安全技术前应该知识的一些知识。

第 2 章专注于操作系统。在本章中可以找到关于 Windows、Linux、Netware 的内容。尽管许多内容是需要多人运行于跨平台的系统上，但你还是可以找到一些与自己解决方案相关的内容。

第 3 章很短，是关于防火墙的。尽管由于页数的限制，但是你还是在这里找到与安全相关的有价值的建议。

第 4 章是关于攻击的。攻击可能来自黑客或者是病毒。本章将告诉你如何防御。本章中很多重要的忠告来自多个安全盟友。

第 5 章主要是讲述加密工具的。第 6 章是关于建立安全计算的重要技巧。使用这些技巧是很好的，因为他们经常单击并运行嗅探器而迅速将你锁定。在最后，第 7 章，包含了最近更新的 Gartner 安全研究成果。。

希望这些资源汇编能最大程度地给你的计算机系统带来安全。尽管本书不能穷尽所有安全资源，但它确实是你学习的重要资源。

目　录

第 1 章　基础知识

第 1 章的基础知识包括如下三个部分：

- 开始之前。
- 原理。
- 技术。

本章之所以分成这三个部分，原因是显而易见的。第一部分是为了让我们静下心来仔细考虑一些问题，这些问题是每个网络管理员在建立安全网络时都应仔细思考的。

除了一些硬件安装的内容外，第一部分还涉及其他问题，如：

- 关心什么？
- 什么时候外购？
- 安全市场。
- 网络安全的重要性。
- 电子商务的安全。
- 更好的工具。
- 合法性。

我们试图让您仔细想想正在做的事情，我们会讨论和您的情况相关的问题。

第二部分包括网络安全的一些基本原理。这一部分的最精彩内容是 TechProGild 的作者 Chris Dinsmore 所写的一系列文章。

在第三部分中，将发现很多和第一部分相似的话题，但这部分会讨论更多技术性的问题，如：

- Kerberos。
- 虚拟个人网络（VPN）。
- 建立在线零售付款系统。
- IP 伪装。

1.1 向 ASP 提出尖锐的安全问题

ASP 通过运行并且管理一些笨重的应用程序使您的生活变得轻松，但有个和您息息相关的问题：您无法放弃和第三方的链接，从而出现数据安全问题。

很多经理错误地认为他们所担心的所有安全性的问题只不过是和 ASP 签定的备忘录中的历史。实际上，Winn Schwartau（Security Expert 公司的首席执行官）说："应该采取相反的态度来看待这个问题"。

Schwartau 说："如果使用 ASP，则应该更加关注安全性问题，因为您在扩大企业、拓展企业规模、把 Internet 变成网络的一部分，并在现有的体系结构中加入全新的结构"。

外购应用程序时，数据的安全程度究竟有多高？应该保留多少控制？能够保留多少控制？

Sreeram Krishnamoorthy（纽约州 Montvale 市 KPMG 的专业咨询服务公司的高级顾问）说："这很难回答，这是一个非常微妙的平衡。"。Krishnamoorthy 认为，如果您习惯于完全控制企业的应用程序的话，试图和 ASP 建立一种关系将是比较困难的。

1.1.1 需要提出的问题

下面是 Ron Hale 的一些宝贵建议。Ron Hale 是为 Telenisus 公司 Illinois 州分部的副经理，这家公司是 Internet 解决方案提供商，它提供信息保护服务和计算机安全咨询服务。Hale 建议在签协议之前提出如下问题：

- 环境的安全性怎样？
- 是否要对共享体系结构的用户需要隔离？
- 采用什么样的安全控制来保护信息？
- 有没有能够证明保护安全的记录或者安全评估？
- 如果发生了意外，能否阻止攻击并恢复体系结构？
- 您们公司的技术水平如何？
- 您们是不是只靠几个核心技术人员？是否有足够的技术水平保证各种情况下的服务质量？
- 使用什么样的安全评估和完整性工具？使用的频率如何？
- 有没有外部组织定期检查和证明？或者说是不是只进行内部质量检测？

1.1.2 需要独立研究

Hale(Deloitte & Touche LLP's Information Protection Consulting 公司的前任董事长)也建议进行独立研究，如：

- 要求查看审计和安全报告，或者一个来自会计公司的 SAS70 报告。应该和安全性相关的人进行交流。
- 审计或类似的表格应该包括安全管理者详述安全措施的信息。

Hale 说："管理者应该可以查看被收集起来证明服务等级的文档。如果 ASP 正在提供服务，客户应该能够在不通知 ASP 的情况下，通过运行独立的测试程序来确定服务等级。"。

1.1.3 ASP 市场对安全性需求的反应

ASP 行业对提供一种安全的环境持严肃的态度。Meredith Whalen(波士顿 IDC 研究中心的 ASP 研究的项目经理）认为：

“顾客对安全性的关注对 ASP 市场产生了一定的影响”。

Whalen 说：“我们已经进行了需求调查，询问顾客什么因素会促使他们调查一个 ASP。在调查结果中，安全性因素名列前茅。当我们向 ASP 询问他们的顾客一般采用什么方式使用他们的服务的时候，我们发现回答不是 Internet。客户们是使用安全专线和虚拟个人网（VPN）。客户们已经注意到，并开始关心安全隐患了”。

她警告说：“还没有注意到这个问题的 ASP 要么需要在安全性体系结构上下功夫，要么就会被竞争所淘汰”。她还补充说：“尽管很多 ASP 有安全性服务，但是还没有强调或者公开宣传它。如果不针对安全性措施提出一些问题，就有可能对 ASP 作出错误的判断”。

提出问题的最主要原因是保护商业利益。Hale 说：“用户依靠提供商来确保业务的安全性和完整性。所以一定要确保您的 ASP 和您一样认真严肃地考虑了安全性问题。”，

1.2 需要外购 Internet 安全吗？

很多公司很晚才发现提高 Internet 的安全性不仅仅是在 T1 线上加一个防火墙。保护企业的信息是非常重要的，这不仅需要专家，还需要时间（这往往是您所没有的）。您的 IT 员工能否做出有效的安全程序来避免对公司数据的非法访问？您是否应该考虑向 ISP 外购 Internet 安全性服务？ISP 可以提供企业自身无法做到的监视服务。下面来解答这些问题。

1.2.1 什么时候应该考虑外购？

Tony Valletta（SRA 国际安全专家，控制、通讯和智能的副主席和主任）说：“如果您的企业有时间达到很好的安全性，并且拥有技术专家，显然内部解决安全问题比较高效。”Tony Valletta 还说：“或者就像现在大多数正在实现相关重要技术的公司一样，最好开始考虑保护您自己的财产，否则会出现一大堆让人讨厌的事情。”

Mike Marrucci（中小型企业提供安全外购的 WatchGuard 公司的市场部副经理）说：“很多小型公司和在家办公的人仅仅使用简单的安全协议，但是随着复杂性的提高，对外购安全性的需求也在逐渐增加”。Mike Marrucci 说：“如果安全策略不复杂的话，您可以自己做。但随着复杂性的提高，就需要雇一个或者更多的人来作这件事情，这样开销就增加了。渐渐地，向 ISP 每月支付 800 美元，要求 ISP 帮助公司控制网络安全、制定新策略、升级并监控网络安全、作出安全报告对企业越来越有吸引力。

1.2.2 如何选择 Internet 安全？

Valletta 建议首先通过外购的方式启动，然后逐渐增大能力并把它转化到内部。他强调说：“无论采用内部的方式还是外部的方式，至少要作一些事情。”有三种方式可以供 IT 管理者选择：

1. 自己做。

您的员工能够把网络安全系统的所有组件都装配起来，并把它们安装到位吗？这个前提是需要公司内部有专家和必要数量员工保证不间断地监视，Valletta 认为这对一些公司而言是很难作到的。Martucci 认为：“如果您认为您有聪慧的员工，请仔细观察。我们打赌（他或者她）

是一个网络管理员，而不是安全方面的专家。网络管理员花大量的时间来配置以太网电缆及类似的事情，但是如果问及他们是否知道如何安装安全协议？HTTP 的代理应该为开或者关？需要何种 VPN？他们就不会回答。您可能想对他们进行教育投资，但网络管理员不一定有时间做安全方面的事情”。

2. 订阅服务。

如果选择这种方法，需要购买一个包括实施网络安全策略的网络安全应用程序，以及一套集成的网络安全软件，从而用完善的网络安全产品管理自己网络的安全。然后，通过厂商的基于 Internet 的订阅服务，就可以及时地得到建议和最新的信息，并更新网络安全软件。Martucci 说：“我们发送软件更新版本和应对威胁的方法。比如当 Melissa 病毒出现的时候，我们有一个专家小组，他们的唯一任务就是针对新的安全威胁，及时地给您发送软件更新版本以免网络受到侵害。我们把升级信息发送给客户，客户需要阅读这些信息，并自己进行更新。这是最起码的服务。”

3. 完全外购的网络安全。

如果员工中没有专门的网络安全专家，就需要从 ISP 那里购买完整的、完全外购的 Internet 网络安全服务。您的 ISP 应该拥有数据中心、网络、back-office 系统和专门为网络安全需要提供技术支持的专家。您的 ISP 应该提供多种服务，包括：

- 安装具有安全和管理特征的软件。
- 可以为您的网站提供定制的网络安全应用程序。
- 网络更新和应对威胁的方法。
- 每月报告。

1.2.3 IT 员工的专业技能及其可用性

Martucci 说：“必须知道您的员工中是否有网络安全专家，也必须决定是否需要一个这样的专家，这是个经济问题。PSInet 服务大概一个月需要花费 795 美元，而这些钱是无法雇佣到一个网络安全专家的。另一方面，网络安全性问题无处不在，因此您需要的不是一个网络安全专家，而是两个或者更多，因为他们需要不停地换班才能保证完成任务。”

WatchGuard 公司的控制安全服务部的产品经理 David Bovee 说，“一些系统或者网络管理员觉得当其他人和他们一起管理体系结构一部分网络的时候，就像他们的领地受到了侵犯。我遇到过一些系统管理员，他们管理电话系统和所有的客户端、服务器。他们规定公司可以接受的使用政策，他们管理杀毒、企业数据库、以及其他的各种事情。不过，一个人管理这么多事情必然会出现麻烦，也就是说很可能会遗忘某些事情。比如当讨论网络安全的时候，其他的一些事情就被忽略了。”

Bovee 说：“每当我为一个网络安全管理员安装一个防火墙，并且这个网络安全管理员是个不愿放弃对网络任何部分控制的人，他就会尽力保留自己的控制，在这样做的过程中，他就会忽略他的体系结构中的某一部分。最终他的某个外围网站就会因为网络安全不够强壮而受到攻击，这是他未曾遇到过的。然后，整个公司的网站都会受到攻击。他将不得不重新构筑 40 个客户系统和自己的服务器系统。”

1.2.4 技术的集成

另外一个需要考虑的问题就是如何

把新技术集成到现有的平台中。eAdvantage.net 的经理 Tim Landgrave 说："您需要向现在的网络安全商询问'这种外购是否会影响我们采用我们自己开发或购买的新系统的能力？我们添加了应用程序以后，您们会采取一些什么措施？是自己开发的还是外包？我可以增加或改变应用程序吗？我是不是要因此而付出巨资？'"。

集成当然是一种方案，但是您应该能够和外购商一起找到某种解决途径。Martucci 说："一个 ISP 会和客户一起设计符合客户具体需要的系统。因此把合适的安全包组合到一起可以节省大量的时间。我们保证您添加到软件包中的每一样东西都可以和其他部分很好的配合，现在这些都不要您操心了。"

1.2.5 安全方案的设计

"设计一个网络安全方案，管理维护它是一个让人头疼的问题。这是个非常非常大的工作，需要很多专家来做。"据 Martucci 所说："通过外购网络安全得到解决方案的一个优点是 ISP 会为您量身定做网络安全方案。他们会了解关于公司营业的情况，然后他们会据此为公司定制方案和技术，并实现这些方案。"

"网络安全方案就是规定了公司员工在网络上的行为的所有规则。允许哪些人进入（通过姓名、部门、分公司或者 IP 地址），允许他们到哪里去？他们可以得到那些服务？他们可以访问哪些文件？一天中哪些时间他们可以进入？谁可以在 VPN 上，谁不可以？所有这些规则都需要设计好，并且记录下来。他们应该能够反映企业的运行情况。"Martucci 说。

1.2.6 改变策略：多长时间更新一次？

Martucci 说："大多数网络安全专家建议至少一年更新两次网络安全策略，事实上大型电子商务公司更新次数远远多于两次。" Bovee 说："当需要改变策略的时候，外购服务提供商可以为企业提供相应的服务，这样可以最大限度的减小错误发生的可能性。 当使用防火墙访问 Internet 的时候，一个错误会影响到企业中的其他服务器，从而中断对客户的服务。对大多数公司来说，如果他们错误地改变了防火墙，可能不会马上意识到他们已经影响了顾客的访问。比如，一个没有经验的 IT 员工在星期五下午 5 点回家的时候改变了公司的防火墙策略，然后和公司失去联系，客户一直无法访问公司的站点。"

1.2.7 通过定期报告保护网络安全系统

Bovee 说："唯一可以知道网络安全系统是否正常工作的方法，就是创建报告，并评估它的不一致性、错误和异常"，。大多数服务提供商只是在月底提供为用户定制的报告。然而，Landgrave 提醒到："请确保他们确实检查了所有的信息，并为客户提供了有价值的报告，而不是仅仅包含 IP 地址和数字的报告"。

在 Landgrave 看来，提前通知很关键，他说："我不想要告诉我上周某人偷了我的数据的报告，我想知道是否以及何时一个非法的企图能够被检测到。我想被告知有人正在通过使用这套证书登录，以及他们使用了这 15 个密码。我想知道网站是否被关闭了。" Landgrave 举了一个例子，几年前，两个俄国黑客在两天内试图侵入印第安纳州南部的一个计算机系统。"由于没有提前通知机制，黑客最终

关闭了整个企业的系统，该公司花了很多　　天才恢复运行。”

1.3　信息安全市场空间侵入已经开始

信息安全管理工具提供商从单个产品逐渐发展到成套工具和供应商联盟。

在网络安全的大舞台上，最初出现的是填补操作系统（比如 Unix，Windows NT）或者网络平台（比如虚拟个人网、VPN 和防火墙）漏洞的实用工具，最后出现了台式机上的强大认证和反病毒机制。大部分技术领先的安全套装软件提供商为了巩固服务管理，开始着重用户管理功能，而把其他功能，如病毒保护、虚拟个人网、公共关键体系结构（PKI）、防火墙管理，分离出去。如今技术领先的安全套装软件提供商（如 Axent Technologies，IBM，Entrust，BullSoft，RSA Security Dynamics）有三到五个安全管理工具。

安全套装软件供应商期望能够进行联盟或者合并以扩展其业务范围。由于信息安全被认为是技术上的马后炮，所以信息安全的市场增长比较慢。纯粹的信息安全提供商正在奋力拼搏，因为：

- 他们在信息安全组织中处于较低的层次，他们的产品也较集中（比如：杀毒、防火墙、虚拟个人网、验证机制）。他们的客户主要是资金有限的信息安全官员或者安全专家。总之，他们还没有引起商业预算和企业经理的注意。
- 在融合了复杂的技术合并、部署并定制解决方案的新领域里，他们面临新的安全要求。任何一个信息安全提供商都没有足够的资源来满足这些需要。
- 安全市场的增长还不足以促使安全提供商开发关键安全体系结构技术，比如知识库、动态事件管理控制台等。他们不得不处理日益增长的分布式、实时的电子商务安全系统。大多数单个产品的安全提供商（比如：Axent、ISS、Comdisco、Unisys 和 Inacom）计划把他们的产品集成到事件控制台和标准目录服务中。

信息安全销售商没有解决全部安全问题的技术理解水平。对交易意外管理（TIM）而言，大型 NSM 销售商，如 CA、IBM/Tivoli 和 BMC 比信息安全销售商处于更加有利的地位。因为他们能够利用核心技术和销售渠道，并且可以改变安全市场的规则。到 2003 年，信息安全销售商和 NSM 领导者的战略合并的一部分将占领 TIM 市场（70％的可能性）。企业不应该对这些 NSM 套装软件销售商期望太高，除非他们在 12 个多月内发布下一代工具软件。我们推荐企业应该：

1) 不要相信未来功能会增强的承诺。

2) 如果工具软件解决了他们自身的安全问题，就不要担心工具会过时。

3) 为工具计划一个两到三年的生命期。

1.4 帮助用户理解网络安全的重要性

用户不必知道所有的事情。实际上，大多数用户可能从来都不理解网络的复杂结构以及网络安全是如何组织的。然而，向用户传授一些安全处理方面的知识能够大量、有效地减少求助电话的数量。

为了达到这个目的，我为用户准备了一个文档，用来解释系统是如何处理安全问题的（在开始向用户传达这些信息的时候，我的老板还没有相应的安全措施）。给用户上课有些难度，我尽可能把问题讲得浅显易懂。您可以照搬我的这种方式。

1.4.1 网络安全简介

对所有的最终用户而言，我们需要做更好的工作，保证网络的安全。下面是达到网络成功的步骤。请记住，当我们提及“网络”的时候，指的是 Windows NT。如果在打开计算机时看到的第一个信息框是“请按下 CTRL＋ALT＋DEL 登录”，说明使用的是 Windows NT（如下方法不适合大型机的用户）。

网络安全包括以下三个领域：

- 入侵者检测。
- 网络登录限制。
- 密码限制。

入侵者检测是为了防止未经授权的用户猜测密码而设置的。网络登录限制和密码限制用来保证用户定期改变他们的密码，使用唯一的密码并且每次只能连接一个计算机。

而且，密码限制使用户可以使用“grace logons”，这是指用户可以用过期的密码最多登录的次数。例如，假定用户要试图登录一个网络，计算机认为密码已经过期，但是还有四次 grace logon 可用，则系统允许用户再进行四次网络登录，然后就不再允许用户访问网络。一旦剩余的 grace logons 为零，就必须求助网络管理员才能使用户重新访问网络。

表 1.1.A 说明了网络安全设置。请仔细看这个表格，熟悉密码和网络登录的规则。

表 1.1.A 控制网络访问的规则

安全功能	设置	描 述
入侵检测		
不正确的网络登录企图	5	在 30 分钟内输入了 5 次错误的密码，服务器将会在 15 分钟内不允许您访问网络，除非网络管理员消除这个限制
登录限制		
限制登录个数	1	每次只能在一台计算机上登录
密码限制		
最小密码长度	5 个字符	密码必须具有 5 个字符
强制期间改变	是的，60 天	用户的密码 60 天过期，此时需要改变密码
需要唯一的密码	是的	不能重复使用相同的密码
限制 GraceLogons	是的，6 次	密码过期后，有 5 次网络登录的机会来改变密码，第 6 次网络登录时计算机会禁止用该用户名登录

可以期望什么？

计算机第一次作一些不正常的事情可能是混乱造成的。下面是当网络登录时，出现密码过期的情况应该如何处理：

1. 网络登录后，系统会提示密码过期，有 5 次 grace logons 的机会来改变密码。“是否愿意现在改变密码？是或否。”
2. 单击“是”。