# INTERNET 安全权威指南

**中国电力出版社**
2002 **年** 12 **月** 23 **日**

# 简　　介

在 9 月 11 日（是指 2001 年 9 月 11 日）以前，我们可能会在这里谈论的一件事就是：近年来没有任何东西能够像 Internet 的成长一样给我们的生活带来这么大的冲击。但按照那天（2001 年 9 月 11 日）所发生的事情，这样的一个陈述看起来又显得愚蠢和失礼。在这里我们所能够做的是：指出各种各样的网络一直是变化的媒介和前进的工具，可能是好的也可能是坏的。

网络并不是一定由路由器和电缆创建。网络能够将具有相同目标的个体焊接起来，并允许它们集中各自的努力来实现一个共同的目的。不幸的是这种目标并不一定是被允许的。每天我们都能读到或听到关于恐怖分子网络的事情。从报纸地能看到有关犯罪网络的情况和为了粉碎它们而制定的强制法律。不友好的政府运行间谍和从事破坏者网络。网络的这些图像给人的印象是一种恶意的工具，是邪恶的基础。但网络并不总是被用来制造嘈杂，同时也用网络来募集资金。在商业世界里，存在那些关心患病者福利的网络，那些增加公司发展机会的网络，当然也有帮助找男友的网络。

Internet 像其他任何网络一样，给个人提供了同样的机会来使用它为公众服务或滥用它。这本书的目的就是在真实世界为安全专家提供实施安全的一个指南，让他们能够以最小的暴露风险来建设他们的网络和系统。许多安全书籍如百科全书般介绍了安全，从讲解每个协议的细节到每个操作系统的配置参数。虽然这本书也覆盖了一些技术细节，如许多操作系统、网络组件、应用和协议，并且假定这本书的读者是没有太多经验的初学者，但你会发现本书不是常见的干巴巴的讲解和理论弱点的堆积。我们的目的是创造一本书来容纳我们这么多年来在系统开发、加密设计、保护网络和为数十家大小客户做安全顾问中所获得的经验，并带领读者走完从安全策略到安全实现的全部过程。最终你将发现我们包含了许多案例，这些案例讲述了安全概念是怎么被应用在真实公司的真实网络中的。你也会发现有几个案例讲述了当安全原则没有得到遵守时发生的事情。

许多书籍都在两者之间做出选择，或是只在策略和原则层次中进行阐述；或是忽略安全的这些方面而直接深入到一些组件的技术细节，如防火墙、操作系统和应用。我们认为讨论安全而不同时讨论安全的过程是不合适的。无论你喜欢与否，为使安全更有效，一个管理员为保护网络所采取的步骤必须是拱形安全策略的扩展。那些只是实施如防火墙和 VPN 等点解决方案而不考虑它们是怎样融入到整体策略的安全实施者其实是在虐待他们自己、他们的雇员，同时也是对他们的预算的一个浪费。一个公司如果没有保护他的重要资产，无论是信息、商业过程或服务，他就不可能长时间成功。

要保护资产，我们首先需要确定它。要充分地保护它，你需要确定是什么在威胁它。要有效地保护它，你需要依据它的价值在保护它所需要的花费和努力之间进行权衡。所有这些因素混和在一起构成了安全策略和程序的开发。最后，IT 部门还要部署它的防火墙和入侵

检测系统，经过深思熟虑之后，选择了相应的系统，并把它们放到在保护重要资产方面能起到最大作用的地方。出于这种思考方式，我们用两章内容来全面讨论风险和策略。它们不是通过干巴巴地从一本书的模板中挑选合适的陈述来开发一个安全策略。我们认为一个有意义的策略必须被开发且用于保护组织的特定方面，而且安全实施者必须能够且应该在形成策略和使其工作方面成为有价值的贡献者。

在讨论过策略以后，我们将谈论这本书的主要内容，那就是下流和肮脏的安全。在每一章，我们都尝试覆盖安全的某个方面并且使它们是相互依赖的，且最终将使这些内容引导我们开发一个“安全“基础设施。我们花费很大的努力来确定，我们谈论的不只是“象牙塔”（意为脱离实际的小天地）安全，而是把我们的讨论深入到真实世界的实现层次。例如，许多技术员会告诉你为什么数字证书能够在认证 Internet 用户方面提供普遍基础。但是他们忘了告诉你在约达 5 亿的被称为网上居民的用户中，约有 99.99%的用户仍然依靠用户名和密码来登录到他们的系统上。知道关于 PKI 的技术固然是好的，但是知道如何去以一种有效和安全的方式去利用用户名/密码则更为实际。

这一点在讨论系统脆弱性时同样成立。经典的“中间人攻击”（一个邪恶的攻击者截获两个网络节点间的通信并把自己伪装成通信的另一方）站在技术观点看是很有趣的，但从实际观点看则很难成功。这并不是说这种攻击不会发生，它只是说，按我们的经验，它很难发生。安全实施者应该更好地利用他的时间来将他的 Web 服务器打上补丁，以防止 13 岁黑客的恶作剧，而不是在所有的服务器上实施加密来防止中间人攻击。这就是现实，这也就是我们认为的本书和其他书的一个主要区别——也是你需要这本书的一个好理由。

最后，安全需要不断地学习和适应，就像生命本身一样。这本书阐述了安全哲学，并揭示了工程师使用的技术和程序，以及如何维护一个安全网络，还有其他人怎样利用这些原则在保护他们自己的同时又不关闭利用和生产的大门。我们真诚地希望这本书会有助于提高安全意识，并且有助于用特定知识来武装安全实施者，就像 Elvis 常说的，要照管好生意。

## 关于作者

Erick Schetina 是 TrustWave 公司（一个位于马里兰州的 Internet 安全公司）的 CTO（首席技术官），Schetina 先生在 1985 年开始了他在信息安全领域的职业生涯，加入到美国国防部成为一个电气工程师。在接下来的 13 年中，他主要从事国防部的智能键控信号和信息安全系统的研究，包括加密令牌、公钥加密系统和信号处理系统。Schetina 先生拥有约翰霍普金斯大学电子工程硕士学位和哥伦比亚大学的电子工程学士学位。他是信息安全联盟的成员并拥有 CISSP（思科信息系统安全）认证专家证书，同时他也是《The Compact Disc》（Prentice-Hall，1989）和《Digital Audio Tape Recorders》（Prentice-Hall，1993）这两本技术参考书籍的作者。

Ken Green 是 TrustWave 公司的高级安全工程师，在加入 TrustWave 公司之前，他是美国国防部的技术主管和资深电气工程师，它在信息安全领域、网络分析工程和操作方面都拥有丰富的经验。Green 先生在电信和数据网络分析和协议（包括 TCP/IP、IPSec、VPN、ATM、SONET/SDH、帧中继和 SS7）方面是公认的专家。他经常担当美国政府其他部门的

顾问。它的技术专长包括协议分析、面向对象软件开发和大规模数据处理系统工程。Green 先生拥有普度大学电子工程的学士和硕士学位，在普度大学他主要学习的是数字通信理论和信号处理。研究生期间他还在约翰霍普金斯大学做过网络理论、高级信号处理和无线通信方面的研究。

Jacob Carlson 是 TrustWave 公司的高级安全工程师。他在设计、开发和实现安全系统和网络领域（包括网络和主机入侵测试、事件反应和计算机策略，还有数据恢复）方面拥有丰富的经验。他使用、安装并管理过各种各样的防火墙，以及基于主机和基于网络的网络入侵检测系统。另一方面，他在加密、认证、基于加密的完整性机制和公钥基础设施方面也拥有丰富经验。他是 TrustWave 公司高级顾问和入侵测试专家。Carlson 先生在保护 Windows NT 系统方面进行过会话和缓冲区溢出测试，他还参加了名为“黑客攻击技术”开放小组讨论，在小组中一些著名的安全专家讨论了黑客团体掌握的新入侵技术，同时 Carlson 先生在数据分析方面也具有丰富经验。

## 献辞

我们想把这本在 9 月 11 日（指 2001 年 9 月 11 日）后出版的书籍献给那天的受害人，包括死难者和获得生还的人！

## 致谢

作者想感谢 Phil Smith 和 Vizo Allman 在数据分析和 Windows 安全方面的贡献。另外，我们想感谢 William Brown 在这个项目中从大纲到完成所给与我们的帮助。最后，我们想说明的是，如果没有我们周围人的支持和耐心，本书就不可能完成。特别的感谢要留给我们的家人，感谢你们在过去几个月和很多年前给予我们的鼓励。

Carlson 先生想对 Kelly O’Bannon 小姐（很快将成为 Kelly Carlson 夫人）毫无保留的帮助、理解和风趣表示特别的感谢。还有她提供的美味咖啡也为这本书的写作提供了良好的环境。同时也要感谢爸爸，为他一直的支持和引以为豪，无论我看起来多么奇怪和丢掉了多少学业他都一如既往地支持我。还有妈妈，还有所有我应该感谢的。

Green 先生想感谢他的家庭，尤其是他的父母，Kitty 和 Ralph，为他们多年来的爱和支持。

# 目　　录

CHAPTER

# 1

# 核心概念：风险、威胁和弱点

本章内容

- 第一步
- 定义你的资产
- 威胁代理
- 确定风险
- 小结

这本书的大部分内容是关于安全技术的：一个 Web 站点是怎样被黑客攻击的？入侵检测系统是干什么的？怎样编写安全代码并设计一个安全网络架构？本章和下一章有一点偏离这一轨迹。原因是太多的管理员、IT 主管、甚至一些 CIO 认为安全可以通过实施一些点解决方案而完全达到。

你也许会问，“什么是点解决方案？”点解决方案就是只着眼于安全的一个特定部分。例如：防火墙解决的是访问控制这一方面的问题。如果你认为你能够通过添加足够的点解决方案来达到一个安全的环境，你就会成为点解决方案的牺牲品。试着问你这样一个问题：“我怎么能够知道我的信息是安全的呢？”如果你的回答是：信息是安全的，因为你已经安装了防火墙或是你已经安装了入侵检测系统、你经常进行病毒的检测，那么你就偏离了目标。

# 第一步

建立一个安全环境的第一步并不是计算怎么去花费你的安全预算，同样也不是去画出你的网络结构图并决定在哪里和怎么保护你的服务器。在你采取上述步骤之前（顺便说一句，上述两者都是绝对必需的），你需要问你自己和你的组织几个基本的问题：

- 你拥有什么信息资产？
- 这些资产的每一部分有多么重要？
- 对这些资产来说威胁是什么？
- 这些资产的弱点是什么？

答案会使你得到一些简单的结论：

- 如果不知道资产是什么，你是不能保护它们的。
- 如果不知道什么在威胁你的资产，你就不能决定怎么最好地保护它们。
- 如果不能知道信息资产的重要性，你就无法决定哪些资产是值得保护的。

“点解决方案（point solution）”的一个典型例子是：一个组织运行着自己的 Web 服务器、DNS 服务器和邮件服务器。你也许发现它已经加固了系统并经常给操作系统打补丁，所以它不能轻易地被黑掉，它装有防火墙和入侵检测系统，并有专人 24 小时监视，在服务器的设置方面也没有犯错误。然而，如果 Web 站点和邮件服务对这家公司的生存来说并不是必需的那么所有的这些保护措施都不会有多大价值，对这家公司来说客户数据库是他的命根子，但是客户数据库驻留的内部服务器却已经有 6 个月没有打补丁了。这家公司关心他的 Web 站点是否被黑客攻击了吗？当然关心！那么生意会因此而中断吗？也许不会。如果一个不满的雇员将客户数据库有意泄露或者一个清洁工偷到备份的磁带并把它卖给一个竞争者，那么这个公司还能生存吗？可能不会！这儿的教训就是：如果你不知道你保护的是什么和什么人会侵害，那么你就可能在一个错误的城堡上修建了防御工事。

本书是关于安全技术的论述，你也许会问为什么我们需要覆盖如风险、威胁和弱点这样高层的概念。原因是我们认为对每个人来说，理解和应用好的安全习惯都是很重要的。我们已经无数次地遇到一些系统管理员，他们根本不关心他们的公司是否有安全政策，他们在实施入侵检测系统时对备份的磁带也没有给与重视。

虽然他们个人在技术方面都很胜任，但是他们应该更加关注整个安全进程。通常商业管理人员最了解什么信息资产对公司的继续成功是关键的，但是只有这些负责技术的人才知道这些资产被放在什么地方？它们是怎样被保护的？保护了没有？他们在帮助策略制定者开发有意义的安全策略方面可能是无价的，他们能最好地帮助管理者了解面临的威胁，他们能够帮助制定和开发，综合考虑了策略、架构和实现的有意义的安全程序。因此，让我们首先阐述几个安全方面的核心概念。

# 定义你的资产

第一步：确定你的商业财产，这一步会做一些好事情。第一，它让你的注意力集中在那些最重要的东西上（对你的组织来说）。第二，它能帮助你证明你的安全预算（关于这一点下一章会详述）。资产可以以多种形式表现出来。它可能是商业进程（例如从客户来的订单），或是数据部件（例如商业计划或是一个设计方案）。最终，你应该能在信息资产（例如关于客户信息的数据库和点解决方案）之间画一条直线。如下面的例子所示：

- ACL（访问控制列表）和数据库所驻留的服务器上操作系统的审计特性。
- 入侵检测系统用来记录尝试侵入数据库所驻留的服务器的行为。
- 高可用性的防火墙用来限制 Internet 上任何人连接到数据库驻留的服务器，但同时也保证销售人员在任何需要的时候可以访问它。
- 认证令牌和远程访问 VPN 被在家中的销售人员用来访问商业计划，并确保这些数据不会被窃听。

一些典型的信息资产在如下小节中列出。

## 私人信息和知识产权

这类资产包括客户联系信息、销售数据库、商业计划、产品设计、公司统计数据、方法学、源代码和其他的“硬”资产。保护私人信息通常会导致对访问控制、加密和入侵检测系统的需求。

## 公司声誉或形象

对那些在很大程度上依赖于名誉和品牌认可生存的公司来说，应该估价一下这种无形资产，并把它作为值得保护的资产。试想一下如果一个调查机构的 Web 站点被“黑”掉了，那么会对其客户的信任产生什么样的影响？会在公众中产生什么样的负面影响？预期的客户会不会担心他们的隐私被泄露？再想像一下，如果使用一个公司生产的服务器端软件的 Web 站点由于此软件安全方面的弱点被“黑”，那么对这个软件公司意味着什么？也许最后的那个并不是一个好的例子。

## 商业过程

任何对于组织的运作来说是重要的操作都需被列为重要的资产。例如，对电信公司来

说，给自己的客户寄账单的能力对维持现金的流动，也就是公司的生存能力来说是至关重要的。如果这一过程只能被电子化处理，那么接收来自销售人员的订单也同样是至关重要的。有趣的是：系统管理员通常都会认为雇员的新水支付功能是最重要的。但是因为大多数公司不会因为薪水被延期支付而失去生意，所以它通常放在被管理层评估的重要商业过程的最后。

## 威胁代理

现在你已经具有你的组织所拥有信息资产的一个完整记录，你可以开始调查对这些资产的威胁来自于什么地方。当考虑到威胁时一个下意识的反应就是“黑客”无所不在，因此想把其余的全部排除在外。而一个安全专家会很乐意告诉你，超过三分之二的安全事件是内部人员（不是黑客）做的坏事。对很多人来说这是一个很让人吃惊的数字，也许这是因为能上头条新闻的安全事件的 90%都与最近来自斯洛文尼亚的邮件病毒、一家著名的网上商店的 Web 站点主页被“黑”及信用卡数据被偷有关。或者公正地说，是因为公司在他们发生安全问题时不愿意公开，尤其是当安全问题来自于内部的时候。

那么什么是大多数组织面对的典型“威胁代理”呢？当然，他们包括黑客，但是在保护信息资产方面也同样存在很多其他的威胁。

### 内部威胁

到目前为止对一个组织的最大威胁来自于内部。如果你静下来想一想，你就会发现这是有道理的。内部人员了解什么是最重要的资产、它们位于什么地方、它们是怎么被防护的。而且内部人员比外部人员容易获得信任。他们能够获得对你的系统的物理访问权。他们位于防火墙后面而且可能不会被入侵检测系统监视。这些东西都是那些外部的入侵者想拥有的。通常挡在重要资产和内部人员间的只是他的犹豫。而且，他们所具有的优势也容易使他们犯下意外错误。如果一个无心的内部人员错误地点击了一封附带有可执行特洛伊木马邮件，那么就能够导致远程接入和系统破坏，而这种情况下所造成的损失是一个外部攻击者通过直接攻击很难达到的。下面是关于具体内部威胁的一个快速浏览。

### 全职雇员

这个团体具有对你的网络的物理访问权，他们知道或者可以找出什么是最重要的资产、在哪里可以找到，并且知道谁可以访问。这些人通常能够连接到你的网络上，他们位于防火墙的后面，如果他们想做的话，他们有足够的时间探测你的网络的弱点。他们可能因为个人的恩怨（不喜欢老板）或者利益关系（把客户数据卖给竞争对手），而被动地成为另一个入侵者的帮凶（“老天！我真不应该和别人共用我的安全令牌”）。管理员具有上述的所有能力，同时他们还有对系统的根访问权限，并且有能力安装新系统或者将系统设置完全更改。

## 顾问

今天为你工作的顾问明天也可能为你的竞争对手工作——甚至变成你明天的竞争对手。很多公司在了解顾问的底细方面做得很差，尤其是顾问的工作完成之后其计算机记录也随之被清除。一个顾问经常在你允许的情况下利用他自己的膝上型电脑，因此你也许就不能控制他运行的应用程序或者运行的“工具”。

## 伙伴

许多组织都对其商业伙伴开放它们的站点，可他们没有预期到这样一个事实，那就是他们很可能在交易过程中接受了他们合作伙伴的安全风险。如果你把另一个公司加入你的WAN（广域网）而又没有采取合适的安全措施，你就会承担起他的所有安全方面的弱点和风险。关于这个方面的一个有名的例子是：一个俄罗斯公司购买了 Bloomberg 金融服务，服务提供商向它的订户提供金融报价和其他东西，并为它的订户站点安装一条专线。这家订户公司的一名雇员很快就通过专线侵入了 Bloomberg 的网络并试图敲诈 Michael Bloomberg，威胁它如果他的要求不被满足就将窃取的信息公之于众。

## 新并购

许多工业只是在近些年通过与公司合并或收购其他公司才得到巩固的。要尽可能快得将这些公司组合起来，IT 人员就必须经常进行网络互联。不幸的是，完成合并通常意味着在帧中继或租用专线被放到两个网络之间之前，没有任何一方会考虑安全方面的要求。这可能会导致一个安全的网络通过与一个非常不安全的网络的连接而被开放给外部世界。

## 混杂

对你的信息资产其他方面的威胁可以表现为各种形式。一种典型的威胁来自于清洁工，他们可能在下班时间或没有保安的情况下接触你的物理系统。在许多建筑物内，公司和建筑物内各种各样的租户共享 Internet 连接，它们都被认为是一个威胁代理。你可能会发现 CEO 的 14 岁大的小孩也是一个威胁代理，因为他决定通过宽带 modem VPN 连接侵入到你的网络。简单地说，当考虑到信息安全时，任何有可能接触你的系统或网络的人就应该被认为是威胁代理。

## 外部的威胁

对一个有相当一部分暴露在 Internet 上的组织来说，来自于外部的威胁是主要的威胁，例如商业站点或交易中心。外部入侵者能够使用的方法与内部入侵者比较起来就有限多了，外部入侵者根据其特征可以分为以下几类。

## 脚本玩家

因为已经编写很多自动工具用来搜索系统的弱点，并随后运行针对它们的攻击，所以并

不需要一个计算机专家来侵入系统。“脚本玩家”被这样命名是因为他们大部分利用其他人编写的黑客工具来侵入网络或损伤 Web 站点的外观。

### 精锐黑客

只有很小的一部分黑客属于“精锐”类。他们是那些真正理解网络协议、应用和操作系统内部工作机制的人，并且他们花费无数的时间通过阅读源代码和反汇编可执行代码来发现系统的弱点。

### 犯罪分子

无论是通过敲诈还是通过倒卖和利用信息攫取利益，都激发犯罪分子去使用他们所能支配的一切手段，从抢劫和偷窃信息到网络侵入。当你将一个犯罪分子的动机和一个精锐黑客的技巧结合在一起时，你就可以将这个人描述为职业窃贼。这种类型的个体从一个在线零售商那里偷窃信用卡号，利用零售商不敢公之于众的心理进行敲诈，并最终将卡号出售给出价最高的人。考虑到能够通过电子方式访问的资产（如银行账户和信用卡号）的价值，对通过网络进行交易的商业来说电子犯罪是他们首要关注的问题也就不奇怪了。

### 对立的个人和组织

很多组织感到他们成了反对他们的商业行为、政治或道德信仰的个体的攻击目标。例如：在美国侦察机在中国海南迫降后，中国的黑客“黑”掉几百个美国的 Web 站点作为抗议。虽然这些攻击大多数危害不大，但是一些公司和个体可能会发现他们正处于极端分子或边缘群体的威胁之下。

### 恐怖分子

就在不久以前，这一类威胁还不曾被商业公司所考虑。然而自从 9.11 以后，这一观点已经改变。实际上，联邦政府早就拉响了警报，在 1998 年，还是克林顿执政时期，紧急事件委员会就认识到不但政府机构，而且将近大约 50 000 家商业公司，都是国家安全的重要组成部分。这一委员会的发现促使总统做出指示，发布 PDD-63，要求商业公司评估他们的网络基础设施。这一指示在布什政府期间又被更新为 PDD-1。与其他政府文件一起，它指出恐怖威胁很可能在针对政府机构和军事目标的同时也针对商业公司。

## 确定风险

现在你已经将你组织的资产分类完毕并且已知道对这些资产的威胁，是时候评估它们在攻击下的弱点了。从现在起，你应该能够判断每一个资产的威胁。这听起来有点罗嗦，但实际上，这是一个非常有用的方法。你也许看见过像下面的用于描述风险的方程：风险＝威胁×弱点×资产。实际上，许多专业风险管理人员已经开发出了程序，以用于从数学上精确地估算一个组织的资产所面临的风险，该程序基于指定风险和威胁的权重。

举一个例子，如果攻击者能够获得对数据库驻留的服务器的物理访问，那么攻击者就可以利用特定信息数据库的弱点进行攻击。如果这个数据库中的信息是可以被公开获取的天气数据，那么惟一的威胁代理就是那些想通过侵入你的服务器炫耀一下“本领”的脚本玩家。然而，弱点表明这个脚本玩家必须要首先物理侵入你的设备。在这种情况下，你有最小的弱点、很小的威胁和低价值的信息资产，所有这些意味着这项资产的风险很小。现在，让我们假设这个数据库装的是关于恐怖分子的行动的信息。突然之间，威胁代理就变成了恐怖分子，一个“大数值”威胁数。即使考虑到侵入你的设备是几乎不可能的，但是与威胁相比较仍会增加它的可能性。而且资产的价值也相当高，也许是无价的。现在考虑到数据面临的威胁和它的价值，你会发现花一笔大价钱来保护一个有很小弱点的资产也很有道理。

## 小结

在这一章，我们已经概述了一个关键的安全概念：减少关键的信息资产的风险。要减少你的信息系统的风险，你首先需要弄清楚你的组织拥有什么样的资产。当你了解到什么是重要的以后，你就能根据它们面临的风险和它们所呈现出的弱点对这些资产的风险进行分类。根据资产的价值、它面临的威胁和它的弱点，你就能够决定风险并做出决定应该怎样减轻风险。

这本书介绍的大部分内容是关于基本的技术弱点和解决方法的。为了更好地运用这些知识，你必须通过频繁计算风险方程来决定是否将把你的努力和预算用在最需要的地方。在 Web 场安装安全设备记录黑客行为也许在技术上很有趣并很有吸引力，但是如果那不是你公司重要资产的所在地，那么作为一个安全专家，你就不是在做你的工作。

在第 2 章中，我们将在宏观层次上更仔细查看整个安全过程。这将包括从策略到评估（通过安全设备和事件反应进行）所包括的所有事情。在随后的章节中，我们将深入到这些领域的大部分细节。

CHAPTER 2

# 发展可信赖的 Internet 基础设施

本章内容

- 安全的动力
- 什么组成了安全
- 安全过程
- 评估和策略
- 资产保护
- 监视和检测
- 反应和恢复
- 小结

前一章讨论了各种各样的威胁和代理，这些都构成了对安全的需求。最终，安全考虑的是怎样保护你的企业的最重要资产。这些资产可能是公司的形象、产品、销售机制、知识产权，或者是其从事商业行为的能力。在技术的层面上，我们倾向于保护系统而不是资产。UNIX 或 Windows 的管理员致力于使服务器上的操作系统总是打上最新的补丁，加固其应用程序以防止进攻，或者监视日志文件以及时发现异常行为。典型的管理员并不考虑它们是怎么融入整个安全功能的，以及它们的行为是如何保证整个安全策略的正确实施的。

# 安全的动力

这一章的目的是说明多个组成部分，例如管理员、系统、架构、策略和审计，是怎样用于到安全计划中的。这个计划保护了资产和商业运行，同时计划的实施最后转化为对 Web 和邮件服务器的保护。对安全实施者来说，站在一个更高的层次上来理解安全是从一个好的技术人员成长为一个真正的安全专业人员所必须具备的素质。本书大部分内容讨论的是安全技术的具体细节，例如怎样锁定 IIS 服务器、怎样加固一个 Linux 系统。本章不像其他章节，本章以更高的层次看待安全，目的是使读者的目光从点解决方案（如防火墙和 ACL）转移到全局的范围，使读者能够认识到从策略到实施的每个部件的重要性。

举一个简单的例子，让我们来看一个与安全技术毫不相干的过程：解雇一个雇员。从人力资源部的角度看，他们关心的是收回这个雇员的证件，取消他的健康福利，确定他的薪水应该支付到哪一天。而剩下来的一件非常重要的事情是通知 IT 部门这个人已被解雇，然后确定应该对这个人的账号和访问信息进行怎样的处理。那个人的 Email 账号是应立即被删除还是应该被保留一段时间。对他的台式机怎么处理，是否应该被清洗掉并给另一个雇员使用，网络文件是应该保留还是删除。最重要的，怎样处理网络访问。许多公司在解雇一个雇员后很久才发现他的远程访问账号从来没有被取消，他仍然可以通过那个账号登录上来收发邮件。类似于这类事件的处理在很多情况下都是由系统管理员指导的，但实际上是应该由策略驱动的，或者说是应该站在法律的角度上思考的。

例如，如果一个雇员因为有发送令人讨厌的邮件的习惯而被解雇，那么将他的邮件账号冻结并仅在合法程序允许的时候访问可能也是很重要的。对一个管理员来说，下面的情况并不典型：某个雇员已经离开公司并且他的账号再也不需要了。

要发展真正可信赖的 Internet 基础设施，必须要查看安全的所有方面。就像任何一个人都会告诉你，一个链条只和它最脆弱的那一环一样坚固。在这一章，我们将要检查这些环节，并且查看它们是怎样相互交互和相互独立的。要做到这一点，我们希望对安全有直接责任的每一个人都明白怎样为共同的目标而工作。

# 什么组成了安全

安全对不同的人意味着不同的事。对系统管理员来说，它可能意味着保证 Internet 系统不被攻破。对开发者来说，它可能意味着在从一个电子商业站点收集信用卡信息时使用 SSL。