
HZ BOOKS
The Practice of Network Security
Deployment Strategies for Production Environments
信息安全技术丛书
产品环境的配置策略
网络安全实践
(美) Allan Liska 著
王嘉祯 等译
机械工业出版社
China Machine Press

信息安全技术丛书

网络安全实践

（美） Allan Liska 著

王嘉祯 等译

机械工业出版社
China Machine Press

本书从网络的整体角度讲述如何保护企业网络的安全，涉及到网络安全的方方面面：从风险分析到访问控制、从Web/电子邮件安全到日常监控。书中还指出了当前分布最广的网络安全错误和脆弱性，并提供相应的实际解决方案。本书的另一特色是把技术融入到具体的实例学习中，并教读者如何把书中的解决方案用于实践中。

本书可作为设计安全企业网络的参考书，适合网络管理员、网络安全管理员阅读。

Simplified Chinese edition copyright © 2004 by PEARSON EDUCATION ASIA LIMITED and China Machine Press.

Original English language title: *The Practice of Network Security: Deployment Strategies for Production Environments* (ISBN 0-13-046223-3), by Allan Liska, Copyright © 2003.

All rights reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Prentice Hall Professional Technical Reference.

本书封面贴有Pearson Education（培生教育出版集团）激光防伪标签，无标签者不得销售。
版权所有，侵权必究。

本书版权登记号：图字：01-2003-2000

图书在版编目（CIP）数据

网络安全实践 /（美）里斯卡（Liska, A.）著；王嘉祯等译. - 北京：机械工业出版社，2004.1

（信息安全技术丛书）

书名原文：The Practice of Network Security: Deployment Strategies for Production Environments

ISBN 7-111-13300-5

Ⅰ.网… Ⅱ.① 里… ② 王… 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（2003）第100311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：李 英

北京中加印刷有限公司印刷 · 新华书店北京发行所发行

2004年1月第1版第1次印刷

787mm × 1092mm 1/16 · 19.25 印张

印数：0 001- 4 000 册

定价：30.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线电话：（010）68326294

译 者 序

随着计算机网络的广泛普及和大量应用，网络入侵事件不断发生。入侵者利用网络基础设施的脆弱性和安全管理上的缺陷，对网络实施攻击，从而获取和篡改网络信息，或者摧毁网络设备，造成严重的经济损失和难以估量的政治和军事影响。因此，保护网络安全已经成为组织、企业、各级政府和军事部门十分关心的重要问题。

本书的目的是为处于网络安全管理第一线的工作人员提供一些保护网络的实际可行的解决方法。全书分为三个部分，第一部分为前三章，主要讲述保护网络首先要解决的问题，包含有：定量分析安全风险；定义反映公司实际的安全模型；将安全模型转换成有效的、可实施的安全策略等；第二部分为从第4章到第14章，为全书的重点内容，主要讲述保护网络的实践问题，包括路由器和交换机的配置安全；通过验证、授权和审计实施控制访问；安全VPN的配置和远程访问的安全；无线WAN和无线LAN的安全；DMZ的建立方法；保护Web/应用服务器、DNS、电子邮件服务器和文件/打印服务器。第三部分为从第15章到第18章，主要讲述如何监控和执行已经制定好的安全策略，包括执行有效的日常网络安全管理、监控和记录攻击事件以及在网络遭受到攻击后如何做出响应——检测、隔离、报告和起诉等。

本书的特点是系统性和实用性。本书的内容几乎含盖了网络安全的所有方面——从风险框架到访问控制、从Web/E-mail安全到日常的监控。作者还系统地分析了当今最普遍的安全缺陷和脆弱性并提供了实际可行的解决方案。

本书的作者Allan Liska是Symantec公司企业安全服务部的安全工程师。在此之前曾在WorldCom公司工作过六年，是该公司主机部的一名网络设计师，另外，Liska还是一名CISSP 信息系统安全认证专家，曾撰写了多本关于网络管理和Web服务器安全的书籍，在网络安全方面有丰富的知识和经验。

我们在翻译过程中力求忠于原著。由于本书涉及了计算机网络多个领域的有关内容，因此其中许多的专业术语尽量遵循本领域的标准译法，并在有可能引起歧义和冲突的地方做了适当调整。同时，我们在专业术语第一次出现的地方注上了英文原文，以方便读者对照理解。

参加本书翻译的还有胡建理、唐智勇、韩国栋、刘爱珍、徐波、彭德云、冯兵和葛秀慧等同志。由于本书涉及到网络安全的各个方面，范围广、内容新，加之译者水平有限，书中错误和不妥之处在所难免，恳请读者批评指正。

译 者

2003年10月

致　谢

写作是一个愉快的过程，但也耗费很多时间和精力。写这样的一本书意味着要花费很多时间同许多真正的智者合作并学习他们的经验。

有许多人投入到这本书的创作中来，我真的不知道该从哪里说起，因此我就按时间顺序来说。

我要感谢UUNET的Li Glover、Tony Wynes和Sean Murhpy的指导和支持，他们使我进一步加深对网络的认识，并使我认识到网络的脆弱性所在。在我写作出现偏差时，他们及时给予纠正。

Shoeb Siraj和Steve Shippa对我写作过程中所付出的艰辛表示深深的理解，并为我的写作提供了必要的物资帮助。

在我写作进度落后时，Neil Salkind和Vicki Harding与Prentice Hall进行协商解决了该问题。

Prentice Hall的Mary Franz具有惊人的耐心。她和一个初次写作，特别是还有一份全职工作，并且最终期限意识很模糊的人合作非常不易。谢谢你在写作中给我一贯的理解与支持。

Ed Skoudis对最初的设想提出了有建设性的意见，并帮助我明确本书的重点。在全书的写作过程中，Ben Liska也给予了极大帮助。

Jorj Bauer和Todd O'Boyle审阅了本书，他们的能力令人称叹。正是他们给我提供了指导、建议和批评，才使本书的质量大为提高。

Intalgent Technologies的Jeff Gunther、Packetattack的Mike Sweeney、Cisco的George Simmons和Ken Durazzo,还有Sandstorm Enterprises的James VanBokkelen及其职员，针对本书的不同部分提供了专门的意见和帮助。

Tina Bird和Norm Laudermilch对本书提出了一些非常有见地的观点，而且帮我精练了它们。

在本书的最后阶段，Elizabeth Martin和Wil Mara毫无疑问对我帮助很大。Wil将每个细节都考虑得很周到，使本书质量有了显著改善；Elizabeth审阅全文并润饰了原稿。

我也同样要感谢本书中提到的工具和网站的所有者。如果没有这些工具，网络保护就更昂贵，更费时。另外，我想感谢那些共享安全信息的人。诸如CERT/CC、CIAC、Security Focus、MITRE和Whitehats等公司和网站就网络社区提供了非常有价值的服务。

最后，我要感谢我的妻子Roseanne和我的儿子Bruce。在过去的六个月里，为写本书，我夜以继日。在此期间你们给予了坚定的支持和爱，有这样美好的家庭，我是多么幸运。我爱你们。

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

我正在写这篇前言时，听说Cisco的CatOS中新发现的脆弱性出现了警报，这个脆弱性即CatOS HTTP邮件收发后台程序中的缓冲溢出。这一脆弱性在由于管理目的而关闭HTTP邮件收发后台程序的那些设备上比较常见。

几年前，这个脆弱性还没有引起太多的关注。毕竟，当时人们还不清楚网络基础设施中的设备多久会遭受一次攻击，而且还认为攻击的目标通常是服务器和缺乏安全措施的工作站而不是路由器、交换机、防火墙或其他网络基础设施。现在情况已发生了变化。随着网络变得日益复杂，攻击者也是处心积虑并试图入侵它们。因此，现在的网络安全已不再只限于保护服务器和工作站了，而是需要从整体角度理解网络，同时还要考虑边缘和核心两方面的网络脆弱性。

攻击者变得越来越老练，他们所使用的入侵网络的工具也越来越高级。这些工具大多可以免费获得，并已被放到聊天室和一些网站上，这就使那些不具备多少网络知识的人可更容易地对单个网络或多个网络发动攻击。现在这些攻击一般来自一些不满现状的年轻人、愤怒的顾客、前公司职员或那些只想试试这些攻击是否奏效的人。

所有这些情况交织在一起使安全和网络专职人员的工作变得更加困难。一方面，需要保护的设备数量增加了，另一方面，安全预算却维持在原来的水平甚至比原来缩减了。现在网络安全管理员还必须花时间判断攻击是出自那些知道自己正在干什么，并且想获取秘密情报的人的蓄意行为，还是出自某个想试试最新的拒绝服务（Denial of Service, DoS）攻击工具是否好用的小孩的杰作。

除了上面提到的这些问题，安全、网络和服务器管理员在保护网络中还经常出现职责混乱的现象。因此，在区分不同组的职责的同时，还要确保组与组通信的畅通。

本书的目的

本书中，既有来自现实世界活生生的网络攻击个案，也有一些保护网络免遭攻击的建议。然而，重要的是要记住书本是静止的，书的内容只能作为帮助管理员制定网络安全策略的指导。

因为每种网络的实现方式各不相同，因而不可能仅在一本书中给出一种包罗万象的策略。运用本书的基础知识可以帮助管理员发现当前安全策略中的漏洞，甚至在公司内部开展网络安

全方面的讨论。

我知道，许多信手拈来本书随手翻翻的人会想：乍一看，本书所列的许多内容简直是浪费时间。许多网络管理员忙于填补网络中存在的漏洞而无暇开发安全策略，而且要他们尝试与高级管理人员合作，来解释类似和DoS攻击一样复杂的东西的想法也似乎是不可能的。这样做看上去很困难，但从长远来看，能使保护网络安全的工作更加容易。

恰如其分地放置安全处理过程有助于合理分配不同组在其中的作用，也有助于分配保护网络安全所需要做的工作。不仅如此，安全过程还有助于创建安全基本准则，该准则使管理网络的工作变得容易得多。

本书的目的是使保护网络安全的工作更加容易。依据实际经验，对如何使安全处理过程更加有效提出建议，以及提供一些要留意的常见错误，本书可用来帮助你为你的组织创建一种独特的安全策略。

本书不应单独使用，如果要制定当前完全的安全策略，那么应尽可能地使用多种工具。除了本书，我还向读者推荐如下的书籍：

- Network Security:Private Communication in a Public World，作者为Charlie Kaufman、Radia Perlman和Mike Speciner
- Applied Cryptography:Protocols,Algorithms,and Source code in C，作者为Bruce Schneier

当然，书籍不能作为安全信息的惟一来源，因为网络安全世界变化太快，不能只依赖书籍获取信息。重要的一点是与服务器和网络设备供应商合作，以跟踪到最新的网络脆弱性信息，并可得到推荐的补丁，而且供应商还提供许多关于他们产品当前最好的安全策略和建议。

最后，还要运用因特网作为工具来跟踪最新的安全信息。对于因特网上的任何信息，最好应经过自己的分析判断。因为，在因特网上既有许多真正有用的安全信息，也有许多无用的信息和错误的信息。通常访问顶级安全网站和供应商站点可以获得足够多的有用信息。下面向读者推荐一些我访问过的安全站点（排序不分先后）：

- Security Focus（http://www.securityfocus.com/）
- SANS研究所（http://www.sans.org/）
- 网络安全图书馆（Network Security Library，http://www.secinf.net/）
- CERT® 协调中心（http://www.cert.org/）
- Insecure.Org（http://ww.insecure.org/）
- 计算机事故建议能力（Computer Incident Advisory Capability, http://www.ciac.org/）

这些网站的信息通常是可靠的，并有助于保护网络。

致读者

考虑到我是从网络与安全工程师的角度来写这本书的，我知道有人会对书中的一些内容提出意见。有人会认为我本来应该提及一个本书中没涉及到的安全工具，或者认为我所提的建议是错误的。

如果你也是其中的一员，希望你告诉我。如果想提出建议、意见、批评或赞扬，你可发电子邮件给我，邮箱地址是allan@allan.org。

正如我前面所说，安全世界处在不断的变化之中。毫无疑问，本书肯定也会有第2版、第3版。读者的意见将会使以后的版本更加完善，因此欢迎广大读者批评指正。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章　本书所涉及的内容

在小的时候，你也许玩过Milton Bradley公司的游戏Stratego。这款游戏的规则相当简单：有两位选手，每个选手都有一面旗子。游戏的目标就是在尽力夺取对方旗子的同时，保护自己的旗子。

Stratego游戏与网络安全很类似。设计网络安全策略时，最终目标是保护公司的网络基础设施（旗子）免遭内部和外部攻击者的攻击。

本书旨在帮助读者建立网络安全策略。因为每个公司都采用不同的网络安全方法，因此本书并没有提供专门的策略。本书将集中研究能帮助读者达到最终网络安全目标的方法，该目标即为保护网络基础设施。

本章阐述本书所涉及的网络安全方面的内容，讨论各种类型的网络安全，并概述不严谨的网络安全策略所带来的后果。

除了阐述网络安全一些理论方面的知识，本书还讨论网络安全上的一些常见错误，并对典型的企业网络进行了描述。

1.1　什么是网络安全

进行任何关于网络安全的讨论，首先要对网络安全进行定义。如果针对网络安全的定义，对10位不同的管理员提问，可能会得到10种不同的答案。

为了讨论的需要，本书引用美国国家安全局给出的定义。即：网络安全是保护网络及其服务不受未经授权的修改、破坏或泄漏。该定义确保网络能正确地执行其重要的功能，并且不会产生有害的副作用。

无可否认，这是一个广义的定义，而这样的一般定义能为网络管理员更好地应付各种新型攻击做好准备。如果网络安全计划范围很广泛，那么就可利用适当的工具应付新型攻击。显然，一些安全事故都是网络问题。分布式拒绝服务攻击（distributed denial of service attack，*DDoS*）是明显的网络问题。当多个系统向网络，或网络设备发送大量的信息流（如Ping流），造成合法用户无法访问服务器，这就是DDoS攻击。因此，必须在DDoS攻击到达服务器之前阻止它们，

换句话说，也就是在网络层就必须阻止它们。

另一方面，e-mail蠕虫是一种更令人头疼的攻击示例。e-mail蠕虫是一个文件，它作为e-mail的一部分被发送。这种文件利用流行的e-mail程序中的安全漏洞来破坏机器的文件系统，然后通过地址簿将自身发送给其他人，并将破坏持续进行下去。乍一看，人们可能认为需要服务器管理员来对付e-mail蠕虫，然而它们除了会发送大量的信息淹没服务器之外，还会使网络拥塞。而且在极端的情况下，即使蠕虫正被清除，它也会迫使用户切断网络与因特网的连接。

1.1.1 网络安全与折衷方案

与所有的安全问题一样，网络安全也需要折衷。如前面所述，甚至在对网络安全范围进行定义时也包含了折衷。网络安全策略不是凭空制定出来的。在制定网络安全策略时，网络管理员必须与其他部门，尤其是公司的法律部门进行合作，并在有限的预算框架内来确定组织网络安全策略的范围。

但是，折衷方案常使网络管理员处于一种进退两难的境地。网络管理员发现他们面对事故时，常处于一种尴尬境地。如果所要求的预算到位，这些事故本来是可以避免的。

通常，网络安全折衷方案是教育和风险管理的结合体。安全人员必须了解最新的安全脆弱性，并将新信息传达到他们所在组的其他人。而且，还应经常地直接或通过正式操作环节向首席信息官（chief information officer，CIO）汇报，然后CIO负责将这些信息传达给组织的其他部门。

注意 本章自始至终会提到CIO。视公司的规模和结构而定，上文所描述的CIO承担的职责也可能由首席技术官（chief technology officer，CTO）或信息技术（information technology，IT）经理来承担。

当向公司的其他人传达安全信息时，通常有必要像销售人员一样不厌其烦。安全问题应该从利益，而不是从技术特性的角度做出解释——解释会发生什么情况，而不是解释攻击的技术方面的问题。如果一个新的安全漏洞可能允许DDoS对服务器发动攻击的话，就不要讨论ISO OSI参考模型或传输控制协议（Transmission Control Protocol，TCP）的细节。相反，必须关注这样的事实：如果攻击者利用了这个安全漏洞，那将使合法用户无法访问网站。

另一个策略是从费用的角度来解释问题。如果按照脉冲模型（如，只有10MB的连接带宽，但可用到45MB）对带宽收费，DDoS攻击能使组织的带宽处于满负荷，因此就会带来可观的额外开支。

实际上，对安全风险量化得越频繁，就越容易得到别人认同，或者实施起来越容易。

1.1.2 风险管理

网络问题的量化也使网络管理员能更好地处理风险管理。风险管理是指评估来自安全风险的潜在威胁的过程。

风险管理也意味着要懂得何时代价不能作为一个权衡因素。虽然本节主要关注的是确定实施安全解决方案所要付出的真实代价，但还应该意识到某些解决方案是非常重要的，因而无论付出多大的代价也要去实施。

有效的风险管理要求管理人员理解每种安全威胁的全面影响。完全理解风险之后，网络管理人员就能权衡不修复安全漏洞所付出的真实代价。例如，如果邮件服务器处于非安全状态，那么任何人都能通过它们发送消息，这就会带来潜在的安全漏洞，它存在被人利用的高风险。风险管理包括考虑修复服务器漏洞与不修复所付出的代价。修复邮件服务器的代价相对较小：只要不让局域网之外的人通过服务器来传递信息，或者如果组织有许多远程用户，实施这样一种安全系统，即要求人们在发送邮件之前对其进行验证。不修复所付出的代价是巨大的。明显的代价是有人利用服务器和网络连接给数以百万计的人发送邮件。但以下情况下中也存在管理代价：因为邮件服务器已上了黑名单，所以人们不能通过它来发送邮件，并且不得不限制对邮件服务器的访问。受到影响的人会发出愤怒的电子邮件来质问管理人员。

2002年4月，联邦调查局（FBI）和计算机安全协会公布了他们的“2002计算机犯罪和安全调理（2002 Computer Crime and Security Survey）”的结果。这份收集了一些随机挑选的公司在安全实践方面的数据的调查，提供了一般网络攻击的频率信息。表1-1中列出了那些报告遭受过成功攻击的公司的百分比。

计算机蠕虫是到目前为止最常见的、能检测到[⊖]、并有过报告的网络攻击类型。操作性词语即为检测和报告。显然，并非所有的攻击都能被检测到（甚至有些攻击还未公之于众），因此表1-1所列出的百分比也许并不能反映公司所遭受的网络攻击的真实情况。

表1-1 所报告的网络攻击统计

攻击类型	报告遭受过成功攻击的百分比
计算机病毒/蠕虫	85
系统入侵	40
DoS攻击	40
网络服务器入侵	38

尽管网络攻击是一种很普遍的现象，但一些公司认为遭受过网络攻击是一种耻辱，因此

⊖ 表中没列出的第二种最常见的攻击类型是由公司内一个或多个雇员发起的攻击。

“计算机犯罪和安全调查”一直苦于一些公司对其所遭受的网络攻击隐瞒不报，这样他们就得不到真实的数据。

为什么像这样的数据是如此重要呢？因为在制定网络安全策略时，这种数据有助于给网络管理员提供一种如何分配组织资源的思路。如果知道一个公司遭受病毒或蠕虫攻击的可能性是遭受其他类型攻击的2倍，那么服务器管理员就可据此制定合理的安全计划。

许多公司采用一种风险分析的形式来确定实施一项安全策略所付出的代价。风险分析从四个方面来评估安全风险，并使用所获得的数据给每种威胁指定优先级。

与风险管理的其他方面一样，风险分析须由安全小组来处理，并需要CIO、高级管理层和法律部门的直接参与。

这种风险分析方法是由国家标准和技术协会设计的，它包括设计一个矩阵，用于评估威胁、可见性、后果及潜在威胁的敏感性。这种风险评估与大多数网络安全模型吻合得很好，在下一章将会讨论它。

要创建风险等级，首先要设计两个表（表1-2和表1-3）。

针对风险采用所有四种测量尺度；将威胁值与可见性值的乘积与后果值与敏感性值的乘积相加，就可得到风险等级。

将这些测量尺度应用到风险之后，就可将其归为表1-4中所列的三种类型中的一类。

表1-2 风险分析：威胁与可见性

威 胁	等 级	可 见 性	等 级
当前无已识别的威胁	1	非常低的知名度，没有公开	1
未知，或多重暴露	3	偶尔公开	3
主动威胁，多重暴露	5	主动公开	5
用威胁值与可见性值相乘			

表1-3 风险分析：后果与敏感性

后 果	等 级
后果是在预算内的，无成本，或能转移风险	1
可能影响到内部功能，造成预算超支，或可能产生机会成本	3
可能影响到外部功能，并且收入会减少	5
敏 感 性	**等 级**
有部分业务运作成本，无组织影响	1
对特定的业务部门和良性成本有无法接受的影响	3
有无法接受的管理成本，并影响业务关系	5
用后果值与敏感性值相乘	

必须注意任何已完成的新网络工程中应该包括这类风险分析。分析和理解新项目中所固有的安全风险，对于把公司的未来安全风险降到最小，是很重要的。

表1-4 风险等级：最终的评估

混 合 值	风险等级
2~10	低
11~29	中
30~50	高

1.2 重要的网络安全类型

当公司首先开始制定网络安全计划时，通常要回答两个问题：我们应该从哪儿开始？网络中最重要的部分是什么？问题的答案依赖许多因素，并且针对每一种网络其答案是不同的。

一般说来，一个人，或一个部门回答不了这两个问题。并且，不能仅凭一个部门的力量来制定网络安全策略。同所有的安全策略一样，网络安全策略也必须由CIO来传达，而且要得到法律部门的批准，并且在撤消时还要得到所有其他部门负责人的同意。策略可能由网络和服务器管理员来负责起草，但须由高级管理层作最终的裁定，实施和加强网络安全策略。

在开始制定公司的网络安全策略时，管理员会提出一些问题。

1.2.1 敏感数据

任何企业都有机密数据。无论是客户数据库、私有软件、产品设计，还是一些其他敏感数据，毫无疑问，总有一些东西必须得到保护。在制定安全策略时总要优先保护这样的数据。在某些情况下，尤其那些处理医疗或金融档案的公司，如果不合理地保护这些数据，它们还要负法律责任。

当然，如果没有人能访问核心数据，那么它将毫无用处。保护核心数据的第二步就是要保护组织内的人员或客户访问这些数据的方法。必须保持数据通信线路（网络）可用。

另外，雇员的电话号码清单或人力资源档案、重要但非关键的数据也需要保护。对这类信息的保护不需要像保护核心数据所采取的措施那样严厉，但绝对必须要有。

在网络安全的所有级别上，CIO和其他组的参与是有必要的。因为一个组不能确定组织内的各种数据库的安全级别，而需要高层管理人员为所有的数据资源指定安全级别，这样就可以决定如何对有限的资源进行部署。

此为试读，需要完整PDF请访问：www.ertongbook.com