Active Defense: A Comprehensive Guide to Network Security

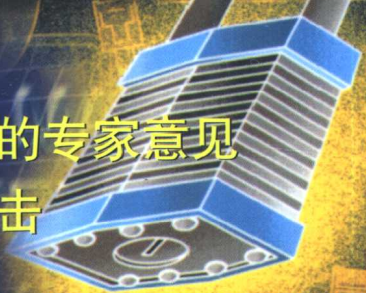
网络安全积极防御

从入门到精通

〔美〕Chris Brenton
Cameron Hunt 著
马树奇 金 燕 译

A Comprehensive Guide to Network Security

- 保卫网络安全的专家意见
- 抵御黑客的攻击



SYBEX
PHEI
電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

Active Defense: A Comprehensive Guide to Network Security

网络安全积极防御从入门到精通

〔美〕 Chris Brenton
Cameron Hunt 著

马树奇 金 燕 译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 提 要

随着网络应用的日益普及，网络安全防范的重要性和必要性也愈加凸显，人们已不再把安全问题看作是一个静态软件包所能解决的问题，而是将其看作一个涉及网络和信息技术各个层面的持续过程。

基于这一现代理念，本书全面介绍了网络系统多层安全保护方面的知识，内容涉及风险分析和安全策略、网络通信和逻辑拓扑、过滤器和防火墙、身份验证和加密技术、灾难预防和灾难恢复等，非常适合网络安全领域中的相关工作人员阅读。

图书在版编目（CIP）数据

网络安全积极防御从入门到精通/（美）布里多（Brenton，C.）著；马树奇等译. - 北京：电子工业出版社，2001.9

书名原文：Active Defense: A Comprehensive Guide to Network Security

ISBN 7-5053-7023-5

Ⅰ. 网… Ⅱ. ①布… ②马… 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（2001）第066290号

书　　名：**网络安全积极防御从入门到精通**

著　　者：〔美〕Chris Brenton　Cameron Hunt

译　　者：马树奇　金　燕

责任编辑：李　莹

印 刷 者：北京天竺颖华印刷厂

装 订 者：三河金马印装有限公司

出版发行：电子工业出版社　URL:http://www.phei.com.cn

北京市海淀区万寿路173信箱　邮编：100036　电话：68279077

北京市海淀区翠微东里甲2号　邮编：100036　电话：68252397

经　　销：各地新华书店

开　　本：787×1092　1/16　印张：28.25　字数：720 千字

版　　次：2001年9月第1版　2001年9月第1次印刷

书　　号：ISBN 7-5053-7023-5 / TP・4027

定　　价：47.00元

版权贸易合同登记号　图字：01-2001-2424

谨以本书献给我亲爱的儿子，你给我的生命带来了无限的欢乐，愿你能够拥有更多的欢乐。

——Chris Brenton

谨以本书献给全世界的安全技术人员，因为只有这些真正执著追求的人才知道真正的和平！

——Cameron Hunt

致　谢

感谢所有为本书而工作的Sybex人士。感谢Guy Hart-Davis（他又称为“Text Butcher”）帮助我的工作走入正轨，我会准备一瓶好酒来报答他。感谢Maureen Adams所做的初始开发工作和制作的CD-ROM。还要感谢技术编辑Jim Polizzi，他那前卫而富于挑战精神的风格督促着我前进。

我还要多多感谢马萨诸塞州Holliston的Alpine Computers公司的一些人员，他们为我提供了大量的信息来源、提出了不少意见，十分出色。其中有Cheryl Gordon，她曾经开玩笑地说“我曾经是个邪恶的女王，但是现在我却只是地窖里的一只扫帚”，她利用自己丰富的经验给了我不少指导。感谢Chuckles Ahern、Dana Gelinas、Gene Garceau、Phil Sointu、Ron Hallam、Gerry Fowley。感谢ARMOC的人们，他们有Bob Sowers、Steve Howard、Alice Peal以及防火墙和安全组的所有成员，他们保证了本书在技术上的领先水平。

我个人还要感谢Sean Tangney、Deb Tuttle、自称“我是你背后的BFG”的Al Goodniss、Maria Goodniss、Chris Tuttle、Toby Miller、Lynn Catterson以及所有这些友好的“巴比伦”伙伴。感谢Morgan Stern，他是我所认识的最聪明的计算机天才之一，而且他非常乐意与询问他的人分享自己的知识。还要感谢Fred Tuttle这位老式的佛蒙特人，他向人们展示了行政办公室的工作人员也能够带有幽默。

感谢我的父母Albert和Carolee，感谢我的姐姐Kym。我今天能够拥有的幸福都来自你们多年的爱、呵护和抚养。这个家在我的心目中是无可替代的。

最后，我要感谢亲爱的妻子和精神伴侣Andrea，你进入了我的生活是我生命中最快乐的事。如果没有了你，我的生活将残缺不全，如果没有你的支持，这本书也不可能出现。谢谢你使我成为一个最幸福的人。

—Chris Brenton

感谢我的朋友的耐心，感谢我的家人的宽容，当然还要感谢Nikka，她了解我的所有缺点和弱点，因此她能够使用一种令人意想不到的办法督促我按时完成本书。

许多安全技术人员与我分享了他们的先进安全技术、思想以及观点，使我能够为本书做好准备，我欠他们的情。这本书的成功也有你们的一半功劳。

Jill Schlessinger为我提供了这个工作机会，因此我尤其要感谢她。她耐心地聆听了我原先不成熟的著作计划，取消了这个计划，并且迫使我回到正轨。她总是那么正确。Maureen Adams在本书的开发中实现了一个组织管理的奇迹，而Elizabeth Campbell和Colleen Strand则采用了最富于想像的“好警察”和“坏警察”的角色，督促着我不断前进，并且如期完成开发工作！感谢这些女士们！衷心地感谢你们！

—Cameron Hunt

前　言

我们中有些人还能够回想起，许多年前保护网络环境的安全比现在要容易得多。只要每位用户都有一个口令并且设置了适当的文件许可权级别，我们就尽可以放心地睡大觉，因为网络环境已经相当安全了。这种信心可能有道理，也可能没道理，但是至少我们从感觉上认为它是安全的。

后来就出现了因特网，一切都改变了。因特网使得信息传播的速度惊人地不断加快。在20世纪90年代早期，大多数人还都没有听说过什么叫做安全性薄弱，除非见诸报端。即便如此，新闻机构中提到的一般也都是一些很老版本的软件，大多数都已经不再为人所用了。但是现在，在短短一小时之内，成百上千的人都会涉足某种特定安全性薄弱的细节。

这并不是说所有关于产品弱点的讨论都不好，实际上，这种讨论起到了相当好的作用。具有险恶用意的人通常总有一些场合能够彼此交换意见。从20世纪80年代就已经出现了专用的电子公告牌。通常，恰恰是我们这些网络系统管理员急需这些知识来维护一个安全的系统环境。因特网已经成为从负责网络环境安全的人手中获取易受伤害信息的出色手段。

人们了解得越多，负担的责任就越大。不仅对于负责修补程序弱点的软件公司如此，对于负责布署这些补钉程序、保护网络安全的专家和网络系统管理员而言也是如此。任何订阅了邮递列表的最终用户都能够与网络从业人员同时获得关于系统弱点的信息。这也使补钉程序一旦开发出来，就立即进行布署的任务变得更为紧迫（因为我们的手中已经没有足够多的保障了！）。

因此，除了肩负着其他许多责任之外，我们还需要有一个良好的安全姿态。第一个问题是该从何处开始。是不是该购买一本关于防火墙或者保护网络服务器安全的书？也许你需要学习关于网络通信的更多知识，以便于能够理解这些系统弱点为什么会存在。你是不是还要为运行备份或者冗余服务器而操心呢？

自从本书出版，第一课就是教会读者，不要再把安全问题看作是一个静态软件包所能解决的问题，而是应该将其看作一个涉及网络和信息技术各个层面的持续过程。也就是说，你不能只研究网络中的一个方面就期望自己的环境处于很安全的状态。同时，这些过程也不能与其他网络活动割裂开来。本书就是要为系统和网络管理员介绍他们在运行一个拥有多层安全保护的网络系统时所需的知识，同时考虑到系统的可用性、专用性和可管理性。

本书包含的内容

第1章从解释为什么会有人想攻击一个组织的网络资源开始。读者在此会看到各种不同类型的攻击方式，以及攻击者通过这些攻击可以获得什么。在第1章结束的时候，你会看到一张工作表，它可以帮助你衡量你自己的网络存在的潜在危险程度。

第2章介绍的是风险分析和安全策略。进行风险分析的目的是对你的网络环境所需的安全水平进行量化分析。安全策略定义的是你所在的机构用于保护安全环境的方式。这两方面

的文档确定了你在将来选择和实施安全措施时的基础。

第3章将综述系统如何通过网络进行通信。内容涉及信息如何打包，以及协议的使用。在此你将看到路由协议中的弱点，以及哪些协议有助于创建最安全的环境。最后，这一章将介绍FTP、HTTP和SMTP等服务，并且提供一些关于如何安全使用的提示。

第4章开始进入安全技术。在这一章中，你会学到不同类型的布线以及不同类型的逻辑拓扑固有的安全优势和弱点，如以太网（Ethernet）和帧中继（Frame Relay）。最后，本章会介绍不同类型的连网硬件，如交换器、路由器和第3层交换器，了解这些设备如何用于使系统环境更安全。

第5章讨论的是外围安全设备，如分组过滤器和防火墙。在这一章你会创建一个访问控制策略（根据第2章建立的安全策略）并且检查不同防火墙设置方法存在的优点和缺点。这里还包括一些很有帮助的表，可以用于制定用户自己的访问控制策略。界时，还要介绍所有的TCP标记，和ICMP类型代码。

在第6章中，我们将讨论如何在一台Cisco路由器上创建访问控制列表。这一章从保护Cisco路由器自身的安全开始，接着介绍标准的访问列表和扩展的访问列表。在此你将看到使用分组过滤器可以阻挡哪些信息，不能阻挡哪些内容，并且可以看到许多访问列表的示例。这一章最后会介绍Cisco的新型自我过滤技术，这一技术使得路由器可以作为一个动态分组过滤器使用。

在第7章读者将看到如何在自己的系统环境中布置防火墙。这里会一步一步地介绍Check Point公司的FireWall-1的安装和配置步骤：保护基础操作系统的安全、安装软件并且应用一套访问控制策略。

第8章讨论的是入侵检测系统（IDS）。在此你会了解IDS能够监视到的传输类型，还有一些技术上的限制。本章还将Internet Security Systems的RealSecure产品作为一个示例来讲述。这里包含了操作系统方面的准备、软件的安装以及如何配置RealSecure来检查特定类型的系统弱点。

第9章介绍的是身份验证和加密。这里会谈到使用强有力的验证技术为什么很重要，以及哪些攻击类型利用了验证方法上的薄弱环节。这里你还将看到不同类型的加密技术以及如何根据自己的加密需要选择正确的加密算法和密钥长度。

阅读到第10章时，读者会看到虚拟专用网络（VPN），这里会介绍何时应该实施VPN，并且有哪些实施选择。本章以使用两个FireWall-1防火墙来创建VPN为例介绍整个过程。在此你还将看到在处理之前和之后跟踪信息流的情况，了解VPN对数据流进行了哪些处理。

第11章介绍的是病毒、特洛伊木马和蠕虫程序。内容涉及这些应用程序之间的不同以及它们能够在系统中做什么，不能做什么。在这一章读者会看到不同的保护方法，还有一些实施预防性软件的设计示例。

第12章讨论的都是关于灾难预防和灾难恢复的内容，通过深入剖析网络的各个层面，了解灾难会在何处发生。讨论从网络电缆连接开始，逐步进入到网络服务器。读者甚至会在这里看到为WAN创建冗余链接的内容。这一章最后讨论的是Qualix Group公司的群集产品OctopusHA+的安装和使用。

关于Novell NetWare操作系统的内容在第13章介绍。在这一章中，你会看到如何通过

用户账户的设置、文件许可权和NDS设计来保护NetWare环境的安全。这里将讨论Novell NetWare操作系统自带的审核功能。最后，你将看到NetWare环境中存在什么弱点，以及如何避免这些情况的出现。

第14章介绍的是微软公司Windows系统的连网技术，特别是NT Server和Windows 2000 Server系统。这里你将看到该如何设计域的结构以便增强自己的安全水平，还有如何使用策略。我们将讨论用户账户登录和文件许可权，以及Windows NT/2000中一些不安全的口令。最后，读者会看到NT系统中可用的IP服务，以及实施这些服务时一些安全方面的注意事项。

第15章介绍的是关于UNIX（及类UNIX系统、Linux和FreeBSD）的一些情况。你在这里将会看到如何运行一个Linux操作系统的计算机。内容涉及用户账户、文件许可权和IP服务。这一章还将详细介绍了如何重建操作系统内核，以便进一步增强安全水平。

很多人都想知道心怀恶意的人是如何攻击他人网络资源的，这些内容将在第16章介绍。在这一章会讨论攻击者如何收集信息、如何探测系统的弱点，以及他们可以利用哪些类型的系统弱点。这里还会介绍可供网络攻击者使用的一些现成的软件工具。

第17章介绍该如何随时了解到安全系统弱点的信息，以及通过产品提供者及许多第三方资源可以获得的信息。关于系统弱点数据库、Web网站以及邮递列表的情况都将在此讨论。最后，本章将使用Kane Security分析程序对示例环境进行审核，这个工具软件可以帮助你检验是否你的所有系统都符合既定的安全策略。

本书的读者

本书的读者是在网络安全领域工作尚不足10年，但仍然希望在此领域有所发展的相关人员。如果你已经是网络安全方面的专家了，希望能够把自己知识库中剩余的5%空白填满，那么本书可能并不适合你的需要。

但是，如果你在寻找一本实用指南，以帮助自己识别系统中最突出的弱点，那么这就是你的最佳选择。本书在编写中考虑到了典型的网络和系统管理员的需要，这些系统管理员已经对网络技术和自己管理的服务器有了良好的掌握，同时仍然需要了解该如何查出系统的缺陷，以免自己成为安全漏洞的牺牲品。

如果人们都可以每小时花费350美元来聘请一位网络安全专家对自己的计算机环境进行审核，那么这将是一个很容易实现的任务。但是对于我们大多数人而言，这已经远远超出了我们的预算。拥有较高的安全水平并不一定需要花费昂贵的代价，但是确实需要投入大量的时间和精力。你在自己的网络环境中弥补的缺陷越多，其他人进行网络攻击破坏你的正常生活的难度就会越大。

如果你对于本书中的内容有任何问题或者建议，请通过下列电子邮件与我们联系：

cbrenton@sover.net或cam@cameronhunt.com。

目 录

第1章　为什么要保护网络的安全

只要翻开每天的报纸，你就会看到与计算机有关的攻击事件在不断增加。几乎每天我们都会听说一些政府机关和专门机构的系统被攻击或者遭入侵。即使像美国军方这样具有极高安全保护水平的组织以及微软这样大名鼎鼎的公司也曾经被黑客入侵过。人们可能会联想这样的机构也会被攻击，在这样一种人人自危的环境下，我们该如何保护自己的公司。

更糟糕的是，并不是所有的攻击行为都得到了报道。虽然对FBI的攻击可能会在报道的封面出现，但也有许多较小的攻击根本就没有为公众所见。如果一家公司向公众宣布自己的金融信息或者关于最新产品设计的信息被人窃取了，那将会产生非常严重的经济后果。例如，如果一家银行宣布其计算机安全系统已经被人攻击并且大量的资金失窃，你会怎么办？当然银行将对这类事件保守秘密。

最后，还会有大量的攻击活动根本没有得到记载。其中最常见的是内部攻击，在这种情况下相关机构除了开除相关职员之外并不想过份地张扬。例如，一家很著名的博物馆曾经要求我对其目前的网络系统进行评估。该博物馆的负责人怀疑其网络技术人员可能参与了一些不光彩的活动。

我发现，那位网络技术人员已经入侵了所有用户的邮箱（包括这位博物馆负责人的邮箱）、薪金数据库以及捐助者数据库。他还使用了博物馆的资源经营自己的业务，并且发布可以用于攻击其他网络的软件工具。基于这些情况，这家博物馆开除了这位职员，但并没有采取任何法律行为。这位职员被解雇之后，他使用了许多“后门”来攻击，这些“后门”都是他在作为本机构的网络技术人员期间留下的。即使是在这样的情况下，这家博物馆也没有诉诸法律，因为他们不想把这件事公诸于众。

没有人能够清楚地统计出来有多少安全事件未被人记载。笔者本人的建议是做好大多数攻击活动都没有被记载的思想准备。很清楚，对系统安全进行攻击活动在增加，每个网络系统都需要采取相关策略防止这种攻击。

提示： 你可以向计算机紧急响应组（Computer Emergency Response Team，CERT）协调中心（Coordination Center）报告系统被入侵的情况，他们的电子邮件地址是cert@cert.org。CERT负责发布系统安全方面的电子公告牌，还可以为发布所需厂商的补钉程序提供便利。

在我们介绍如何最好地保护自己系统环境的安全之前，还需要做其他一些工作。首先，我们要看一看谁可能攻击你的网络，以及为什么要攻击。

攻击者的思维方式

为了确定如何最好地守护自己的资源，先要想一下谁会来破坏它们。多数攻击行为不是偶然的，而是因为攻击者相信进入某些网络之后会得到一些东西。例如，骗子更会去欺骗

看起来富有的人，衣着华丽意味着有良好的收入。确定谁想盗窃网络中的资源或破坏网络资源，是迈向网络保护的第一步。

攻击者、黑客和破解者

人们经常不加区别地使用“攻击者”、“黑客”和“破解者”这几个词，不论是商业杂志还是好莱坞电影。人们说“我们被黑客入侵了”通常也就意味着“我们被恶意攻击了”。

但是，这三个词有显著区别，理解了它们的不同点，可以帮助你理解谁可能加强用户的安全水平，即谁在试图入侵你的系统。攻击者指想盗窃或破坏用户资源的人。攻击者可能是技术水平很高，也可能是个初学者。攻击者的活动更像间谍或破坏者。

黑客（hacker）一词最初是指一些对计算机及网络有很深入了解的人。黑客不仅仅满足于运行一些简单的程序，他们还要理解运行中的方方面面的问题，也就是一些希望深入系统内部进行研究的人。进行系统分析的办法既可能用于正当场合，也可能用于非法领域，由使用者的人品和动机决定。

黑客的行为已经形成自己的文化，有自己的语言，并且接受社会实践的检验。正是他们的人格因素才使得外界的人们既可能把他们认作黑客，也可能认为是攻击者或无政府主义者。笔者个人认为，黑客更像一些技术革命者。

历史上大量出现过一些在思想上超出当时主流文化的人们。达芬奇、伽利略、贝隆、莫扎特和泰斯拉——都被当时的社会认为是古怪而不符合社会节拍的人。在信息时代，这个革命性的角色就被黑客占据着。

黑客并不在意表面现象。例如，有人宣称“我们的产品是百分之百安全”的时候，可能会有一位黑客把这句话视作对个人的挑战。而在这种情况下，一个黑客选择对尚未揭开的秘密做何处理，决定了该黑客将会带何种颜色的帽子。

为了区分是想理解信息系统的黑客，还是想利用这些知识非法或者不道德地入侵其他系统的黑客，计算机领域里常把后者称为破解者（cracker），这是为了保持黑客一词的传统含义。但这种努力却并没有取得成功。偶尔公共出版物上仍然使用这个词。而在法律上并不刻意去区分两者，只有与非授权系统入侵类似的行为认定。

白帽子黑客、灰帽子黑客与黑帽子黑客

如果一位黑客找到一种办法发现了程序中安全方面的一个漏洞，并且把这些结果发表出来，则他被称为白帽子黑客。如果一位黑客找到一个安全漏洞，并且选择了使用这种办法对付无辜的人以达到个人的什么目的，则他被称为黑帽子黑客。灰帽子黑客是指“白天带白帽子，晚上带黑帽子”的黑客。也就是说，这些黑客通常有一个合法的安全系统顾问的身份，但是在自己的业余时间从事非法活动。

下面看一个灰帽子黑客的例子。假设Jane是一位安全技术顾问，她在一个操作系统中发现了一个不安全的后门。虽然Jane自己没有利用这个发现攻击毫不知情的受害者，但是为了保护她的客户不受攻击，她还是收取了很高的费用。也就是说，Jane并没有利用这些缺陷进行攻击，但却利用它得到个人的收入。实际上，她从一些机构得到这笔钱的目的是防止他们系统中存在薄弱环节。Jane并没有与厂家合作开发公用的程序修改这些问题，原因很清楚，

只有厂家不发布免费的修改程序才符合她的利益。

为了混淆视听，许多人还错误地理解那些在公共论坛中公布已知软件存在的内部缺陷的人。人们经常认为这些人公布软件存在的缺陷目的是培养其他网络攻击者。这是不正确的——向公众公布软件缺点的信息会引起销售商和系统管理员对该问题的注意，考虑对策。多数情况下，公布软件的缺点是因为有人受到了相应的挫折或感到有公布的必要。

例如，在一段时间以前，英特尔公司的Pentium处理器还是最新型产品的时候，用户发现其中存在缺陷，导致芯片的数学协处理器计算错误。当人们刚刚发现这个问题时，确实有许多人试图直接与英特尔公司联系了解事情的真相。我也曾经与一些人谈过这个问题，但他们都说得到的是否定的答复或根本不与理睬。

直到该缺陷在因特网上发布出来，并且在公开的论坛上进行讨论的时候，英特尔公司才开始采取步骤纠正这个错误。虽然英特尔公司最终以免费对所有有缺陷的产品进行更换保住了自己的位置，但人们仍然对英特尔公司在修改错误时对待公众的不友好态度不满。使公众认识到产品的缺陷是促使问题解决的最好办法。

注意： 出于礼貌，应该先把产品的缺陷通知它的销售商，而不是公诸于众，直到厂家做出处理办法。一般至少给厂家两星期的时间做出补救决定，然后再在公众论坛中发布。

多数制造商对这种报告非常负责。例如，微软公司一般对这些与安全相关的问题会在得知后的很少几天中拿出解决办法。一旦公众得知了某种缺陷，多数厂家都会在尽可能短的时间里做出修正。

这些问题在公开场合公布后也给一些人带来了错误的观念。当有人发现某个与安全相关的问题并且把它公布出来时，就会有一些人认为这个人是网络攻击者，是出于个人利益才研究软件的弱点。正相反，这种公开讨论与安全相关的问题可以促进软件提高完整性。

为什么有人要和我过不去

攻击者进行网络攻击的动机是什么？如前面所述，这些攻击行为很少是偶然发生的。攻击者总希望通过攻击获得些什么。到底是什么在吸引攻击者，要取决于用户所在的机构和发动攻击的具体人。

从内部攻击

案例分析表明，大量的攻击活动是从网络机构内部发起的。实际上，一些研究表明多达百分之七十的攻击行为发自这些机构内部，或者由一些了解机构内情的人（如被单位解职的人）发动。在使用防火墙阻挡外界对资源的攻击风行一时的同时，还是机构的雇员——他们了解网络运行的情况，应该对网络的巨大损失负责。这些损失可能是偶然的事故造成的，但有时也是有人故意所为。

最典型的真正破坏行为往往由一些心怀不满的雇员或被解雇的职员发起。我曾经接过一位新客户的求助电话，他的网络与因特网完全失去了连接。因为这是一家研究机构，因此访问因特网是至关重要的。

很明显，该研究所曾经决定让一位雇员“去寻找其他机会”，而那人却不想离开。表面上，他平静地请求收拾一下自己的东西然后再离开。这是一家小型机构，公司觉得没有必要硬把他赶出去。

在他走的时候，这名雇员在运行公司防火墙软件的UNIX系统中逗留了一下。这个系统完全是开放的，没有使用任何形式的控制台口令保护。他似乎是简单地收拾自己的文件，清理系统中散布的各种程序，而且还拆除了路由器的V.34电缆，把它藏在附近的一张桌子里。可以想像，这家公司花费了巨大的费用才从这场灾难中恢复出来。如果网络的关键设备都保存在一个可靠的地方，这场灾难完全可以避免。

多数系统管理员都过分重视保护网络不受外部攻击，而忽视了来自内部攻击的巨大威胁。如果有人想破坏公司的资源，他完全可以不进行网络攻击。有时网络破坏完全是出于偶然。

例如，一家公司的老板坚持要拥有该公司NetWare服务器的所有超级管理权。他对计算机并非很精通，也不需要拥有那么多的访问权限，这样做的原因仅仅是因为他对这家公司具有所有权。

可以想像这样会发生什么事情。在做一些普通整理工作的时候，他无意中删除了M:驱动器的CCDATA目录。如果读者管理过cc:Mail，就会知道这个目录保存着邮局中所有的邮件和公共文件夹。

在cc:Mail中，主邮件文件通常都是打开的，很难通过普通方法进行备份。公司丢失了除个人文件夹外的所有邮件信息，而剩余信息又是一般雇员都很少使用的。大约两年工作中积累的数据顷刻间消失了。这不是蓄意的攻击，但也使公司付出了惨痛的代价。

越来越多的危胁并不是破坏数据，而是窃取和利用。这通常是指工业（或者公司）领域里的间谍行为，虽然一般不被看作是普通的内部数据破坏，但这种行为对于任何拥有机密专利技术或者信息的机构都是非常重大的危胁，特别是当这些数据被对手利用后会承担法律责任的时候。这方面的一个例子是康复中心。根据美国健康保险可携带性和义务法案（Health Insurance Portability and Accountability Act，1996—USA）规定的权限，根据HIPAA的管理简化条款（Administrative Simplification provisions），相关机构必须采取相应的安全标准来保护病人的信息。任何在保密方法上的失误都将导致联邦政府对其在司法上的惩罚。

外部攻击

外部攻击可能来自多种不同的方面。这些攻击仍然可能来自心怀不满的雇员，但潜在的攻击者范围却已经大大增加了。惟一具有共同点的线索在于，攻击者通过攻击网络可以得到什么。

竞争者

如果用户从事的是竞争十分激烈的行业，则竞争者可能希望从攻击别人的网络中受益。他们可能采取盗窃设计或金融信息的方式，或者仅仅要阻碍别人网络的运作。

盗窃竞争者的设计所带来的好处是显而易见的。有了这方面的信息，盗窃别人信息的机构可以使用别人的设计缩短自己开发产品的时间或使自己的产品具有更好的性能。如果一

位竞争者知道了别人即将发布的产品，就可以通过发布更具有吸引力的产品来获得市场竞争的胜利。

盗窃金融信息也是十分有害的。竞争者通过这种手段可以了解其他公司整个财政年度的资金情况，从而在市场上获得不正当的竞争优势。这种不正当竞争优势可以通过了解其他公司的内部金融状况，或者收入来源等情况获得。

例如，笔者曾经听说一家计算机顾问公司渗透进他的竞争者的计算机网络，盗窃了该公司财务状况的数据表。攻击者发现对方百分之六十的收入来自销售传真机、打印机和复印机。然后这个窃贼进入一个客户站点并且询问："您肯定只依靠Computer X公司满足网络的需要吗？他们毕竟只是家办公设备供应商，多数业务来自销售传真机和复印机。"这种策略可以争取许多客户。

然而，有时攻击者不需要删除对手的信息就可以获得利益。例如，假设你开了一家通过Web网站进行销售的公司，设有在线的产品目录，客户可以通过具有保密措施的表格订购。由于你的工作出色，因此价格很低。

现在假设笔者是你的最大竞争对手，但笔者的产品价格较高。如果笔者能够采用入站连接停止你所在公司的网上销售，就会对笔者的企业带来好处。这样，潜在的客户会觉得你的Web网站已经关机了。客户无法与你的Web站点连接，可能紧接着就会来看笔者拥有的站点。由于你拥有的站点不可用，因些客户无法对比两家的价格——他们可能会进而在笔者拥有的站点购买产品。

没有贼在其中，但这种对服务的封锁会直接造成收入的损失。这种攻击不但很难被证实，也更难进行量化评估。如果你拥有的站点离线八小时，天知道会损失多少销售额！

一家公司被竞争者攻击的可能性直接与自己公司的竞争力相关。例如，一家普通中学完全不必担心会有竞争对手盗窃下个学期的课程表。当然，中学更可能遭到来自内部的攻击。

好战的观点

如果公司的业务很有争议，则它更可能受到持不同观点的人的威胁。

例如，曾经有一家出版医学研究信息的公司与笔者联系，该公司的Web站点有一些关于堕胎的文献。一些看过该站点的人通过电子邮件通知站点的负责人，提议说站点中的部分内容不符合该公司的初衷。管理员发现所有讨论堕胎问题的网页都被换成了生命至上的标语和圣经中的内容。

当然，这种攻击也属于一种模棱两可的行为。没有人盗窃信息，因此无法起诉攻击者。法律条文最多会将这种攻击定性为一种破坏行为。

但是情随境迁，一些十分出名或经常为公众所见的机构，因为知名度很高而成为新闻媒体追逐的对象，也有许多人想借之达成自己的目的。第一种类型是真正的恶意攻击者，他们在网络虚拟世界里挑起争端，这里有三个著名的事例：

- 1998年春天，在许多观察家认为不过是战争叫嚣的时候，巴基斯坦和印度进行了核试验并且开始互相指责。巴基斯坦人和印度黑客都开始在Web网站上对另一方进行攻击。
- 1999年春天，北约轰炸塞尔维亚期间，塞尔维亚和阿尔巴尼亚的黑客相互渗透入对方的网站。