Windows NT

网络的安全性

NT Network Security

Matthew Strebe
〔美〕 Charles Perkins 著
Michael G. Moncur

严 程 张芳兰 田立生 译
杨为理 审校

NETWORK PRESS
SYBEX

PHEI

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

NT Network Security

Windows NT网络的安全性

Matthew Strebe
〔美〕 Charles Perkins 著
Michael G. Moncur

严程 张芳兰 田立生 译

杨为理 审校

電子工業出版社
Publishing House of Electronics Industry

内 容 提 要

本书全面而系统地介绍了计算机网络，特别是Windows NT网络安全领域的知识，包括对人为安全性、用户安全性、客户机安全性、服务器安全性及物理安全性、数据安全性与组网和远程访问安全性等诸多方面都作了简明扼要的论述，并提供了丰富的实用安全工具及实例分析与应用经验。

本书适合于从事计算机与综合信息网络工程和应用方面的技术人员作为学习参考书。

书　　名：**Windows NT网络的安全性**

著　　者：〔美〕Matthew Strebe　Charles Perkins　Michael G. Moncur

译　　者：严程　张芳兰　田立生

审　　校：杨为理

责任编辑：章为华

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：电子工业出版社出版、发行

北京市海淀区万寿路173信箱　邮编：100036　发行部电话：68279077

北京市海淀区万寿路甲15号南小楼一层　邮编：100036　发行部电话：68215345

URL:http://www.phei.com.cn

经　　销：各地新华书店经销

开　　本：787×1092 1/16　印张：26.75　字数：700千字

版　　次：1999年1月第1版　1999年1月第1次印刷

书　　号：ISBN 7-5053-4374-2/TP・2010

定　　价：45.00元

著作权合同登记号　图字：01-98-0477

致　谢

我的妻子很贤惠，她耐心地等待了几年，使我完满地写成此书，继续正常的生活，她的支持给我极大的力量。衷心感谢我的两位最亲密的老朋友Mike Moncur和Charles Perkins，没有他们的帮助，这本书不可能这么快就得以出版。Sybex出版公司的工作人员为此书付出的努力甚至比作者还大。此外，还应感谢Neil、Maureen、Guy、Shelby、Vivian和Jim等人（及Rodnay Zaks，他的著作是我拥有的第一本计算机书，而且至今仍在使用），也自应当由他们来写这方面的书籍。我的家人给予我很大的支持，特别是Roy和Carol、Lee和Donna、Terry和Sharee。还应感谢我的兄弟姐妹们：Daan与Fukiko、Rachel与Kerry、Ruth与James、Chris与Phyllis、Jacqui与Bob、Duane、Gretchen与Paul、Susan与Jimm、Victor、Doug与Colleen、Margaret与Richard、David与Debbie、Don与Christine、Sharon与Ken、Linda、Scott与LeAnn、Dennis、William与Kori、Rachelle、Brent及LoraLee等。

感谢Mike，并感谢我的家人和朋友，他们为我提供了安静的环境，使我保持旺盛的精力投入写作。感谢Sybex出版公司的人们，他们一如既往，热情鼓励我写这本书，特别是Henry J. Tillman。

感谢Matthew和Charles对我写此书的帮助并为我提供参与此项工作的机会。也应感谢Sybex出版公司的工作人员，帮助我出版此书，特别是Neil Edde、Maureen Adams和Shelby Zimmerman。还要感谢Kate Kaminski、Eryn Osterhaus、Andrew Benzie、Molly Sharp和Dale Wright，他们为此书的出版作了大量的工作，包括设计和制作插页、封面、装饰图及CD-ROM等。由于编辑Vivian Perry的帮助，使本书的叙述更加清晰与确切。技术评论者Jim Polizzi提出了许多宝贵的意见和建议。我要再一次感谢我的妻子Laura及我的家人：爸爸、妈妈与Kristen、Matt、Mel、Ian。尤其要感谢我的祖母和外祖母Alice Moncur、Edna Tippets对我的爱和支持。也要向我的所有朋友致谢：Matt和Christy、Chuck、Cory和Kathleen、Dylan与Joan、Robert、Curt、James及Henry。

引　言

在各种规模的网络中，Windows NT业已成为一种最流行的网络操作系统。网络管理员最关心的问题之一是网络安全。

本书全面介绍了Windows NT网络的安全性问题，从基本的注册或登录安全到因特网（Internet）安全与防火墙（firewall），也包括了一般的安全论题（如加密技术）和人为安全性问题。

本书的读者和对象

此书是为网络管理人员而编写的，他们或许正工作于Windows NT网络，或许计划在某个时期使用Windows NT系统。本书的目的不是要写一本Windows NT的安全性指南，而是想对Windows NT网络的各个安全方面作概括性介绍。

在本书中，我们将认真分析Windows NT安全的长处和弱点，提供一些安全方面的建议，其范围包括从小公司所需的简单安全措施到大公司与政府机构所要求的复杂而完美的安全机制。

这本书对任何管理Windows NT网络的人，不管其经验和水平如何，都是有用的。然而在此我们仍作几点假设：

- 读者熟悉计算机的基础知识，对Windows NT或至少对Windows 95有一定程度的了解。本书不介绍Windows NT的安装、网络连接及完成其它基本任务方面的内容。
- 如果读者希望进行安全方面的实践或实现我们的建议，应能以管理者身份访问Windows NT网络。我们也介绍其它网络系统的某些问题，但Windows NT是本书的重点。

如何使用此书

本书的内容分别组织到二十一章和四个附录中，以安全性简介开始，逐章讲述其它更深入的问题。

第1章　为安全基础简介及在网络中应考虑的安全类型。

第2章　说明人为的安全性，即由用户的行为所引起的安全问题。

第3章　介绍各种加密方法及如何将其应用于网络安全规划中。

第4章　描述成功的安全管理所需要的技术与资源。

第5章　深入了解Windows NT的安全性模型及其组成部分。

第6章　说明如何建立、保存用户帐号和分配权限。

第7章　介绍系统的策略，用于控制对操作系统内各功能的访问。

第8章　说明如何利用文件系统的安全性来控制对文件和目录的访问。

第9章　介绍工作组和共享件，这是内建于Windows NT的两种简单、但不太安全的系统。

第10章 讨论域安全性和信任关系及较大型网络的Windows NT安全措施。

第11章 说明如何利用容错方法（如磁盘镜像与备份）防止意外的数据丢失。

第12章 讨论与远程访问服务（拨号访问Windows NT网络）有关的网络安全问题。

第13章 概述多厂家网络的安全问题，包括UNIX、NetWare和Macintosh的安全性。

第14章 介绍因特网（Internet）、内联网（intranet）和外联网（extranet）及它们的安全性。

第15章 介绍TCP/IP协议簇及与其有关的安全风险。

第16章 研究某些可用于客户计算机与应用程序的安全方法。

第17章 介绍防火墙，它是用于控制局部网络与因特网间安全性的设备。

第18章 介绍Microsoft BackOffice的几个部分，如Internet Information Server等，并说明它们与安全性的关系。

第19章 探讨某些可被黑客利用的高层缺陷和安全漏洞及防止攻击的措施。

第20章 说明网络层和数据链路层存在的安全危险及如何防止它们。

第21章 介绍保证Windows NT服务器安全的各种方法。

第22章 说明与OSI模型物理层有关的安全问题。

附录A 提供某些典型的安全政策与原则。

附录B 给出一些安全工具或实用程序。

附录C 给出一些影响网络安全及有价值的联机资源。

附录D 列出常用词汇表。

虽然我们希望读者能够通读此书，但也可把它作为一般的参考书使用。例如，当你要建立用户帐号时，可阅读第6章；当你欲将网络连到因特网时，可阅读第14章、第17章。

在大多数章节中，包含三种有特色的插入段：

专用名词（terminology） 列出某些与本章有关的术语，其定义可参见本书后所附词汇表。

策略（policies） 为保证网络某些方面的安全，我们所提出的建议。

实际考察（reality check） 我们曾经遇到的一些现实的安全方面的趣事，这些故事告诉你在实际网络中会遇到的情况及应有的概念。

保持联系

有关网络安全领域的技术与应用处于迅速发展之中。为使读者能够获得最新的、确切的安全方面信息及更广泛的知识，本书的附录C列出一些联机资源，并提供Web页面，利用地址

```
http://www.starlingtech. com/ntsecurity/
```

可访问NT安全性页面。你也可通过电子邮件与我们联系，我们很乐意听到你对本书的评论意见及有关安全方面的趣事与故事。并将尽力回答你有关NT安全方面的问题。我们的电子邮件地址是

```
ntsecurity@starlingtech.com
```

目　录

第1章 安全性概念和术语

安全性是联网技术中最关键、最容易被忽视的问题之一。许多公司建立了庞大的网络，并且使用了多年，但是从未关心过它的安全性，直到某一天网络发生灾难性的瘫痪或是安全方面出现了漏洞、事故，才不得不关心并采取安全措施。本书将讨论安全性诸多方面的问题，以预防事故的发生。

本章将讨论安全性的基础知识和解决安全问题常用的方法。还将介绍公司应当建立的处理安全性的基本原则。最后简略谈谈Windows NT和其它常用操作系统的安全性，并作一比较。

安全性的定义

当你听到安全性（security）这一术语时，脑海里可能想到两个概念：保护和平安。网络安全性是为保护网络不受任何损害而采取的所有措施的总和，并且当正确实现这些措施时，就能使网络得到保护，使之免受侵害并保证网络的平静与安宁。为保护网络的安全，需要协同使用多种安全措施，从创建用户帐号到雇用忠诚的雇员值守锁在房间中的服务器，都要考虑到。

安全防范是一种每时每刻都不能松懈的工作。不能指望在安装Web服务器时采取一下安全措施，然后把服务器锁在安全室就万事无忧，也不能凭空以为操作系统或服务器运行软件都完美无缺，任何人都不能找出它的毛病和漏洞。必须始终留心操作系统和应用软件出现的新的安全性问题，不断完善和增加新的安全措施。以下几节将介绍网络安全性的基本类型。

注意： 本章介绍的安全类型不一定是网络安全性仅有的组成部分。事实上，有一些极为特殊的类型，内容极为复杂，足以写一本书。如下几节介绍的安全性基本类型，适用于大多数网络。

登录安全性

在安全的网络中，用户遇到的第一件事就是要回答用户名和口令。这是网络第一道关口上的保安措施，就好象大厦门口的电子锁或保安门卫。虽然这些措施不能完全防止出现问题，但是它确实能保证让你知道都是谁、何时在大厦（或网络）中，而且使那些未经授权的用户不能进入大厦（网络）。

不幸的是，没有任何登录安全系统是完美无缺的。有的用户常常选择容易被猜测出来的口令、或是把口令写在明显易见的位置，或是几个人共享一个口令。这样做都可能引起安全问题。可以使用Windows NT提供的一些方法，防止这类问题的发生。在第2章我们会讨论这些问题。

专用名词

- **帐号（account）**：为赋予用户访问网络（或某一计算机）的权利而建立的用户名和口令。除此之外，帐号还包括有关用户的其它信息，如所属用户组、用户可访问的目录和文件等。
- **黑客（hacker）**：闯入其无权访问的网络、窥探和扰乱网络正常工作的人。从在网上寻求刺激的未成年人到窃取情报的外国特务都是黑客。“黑客”一词原本是指计算机高手，但现在它广泛使用已失去原义，而具有贬义。
- **入侵者（intruder）**：这是一个通用词，指未经授权而企图登录进入系统的人。入侵者可能是黑客、合伙间谍、有不满情绪的前职员，或是忘了自己口令的普通职员。

文件系统安全性

用户登录网络的一个主要目的是访问服务器上的文件和目录。文件系统的安全性涉及到管理每个用户可以访问哪些文件。对于用户来说，每人都有一个具体的权限表，可以有权访问某些文件和目录。例如某一用户可能在某一目录内有完全访问权（读取、创建和删除文件等），而在另一目录中仅有只读的访问权。

在对网络上的文件采取安全措施时，要确保服务器上的文件和局部工作站上的文件两者都要考虑施以安全措施。这一点说起来容易，做起来很难。许多用户的操作系统，如DOS或Windows 95几乎没有安全功能。最好的办法是鼓励（或要求）用户把他们的文件保存在服务器中。

DOS、Windows 3.x、Windows 95和Windows NT都能使用FAT文件系统。从早期版本的DOS系统到如今，这个文件系统无多少变化，你可以料到它不很安全。虽然有一些办法可以提高FAT文件的安全性，但是最好的办法依然是采用更安全的文件系统。Windows NT支持NTFS（NT文件系统），它完全支持安全性。

提示：在第8章中将详细讨论文件系统安全性。

数据通信安全性

安全性的另一方面涉及到数据通信。通过网络传输的数据包含许多敏感的信息，例如绝密文件。除非工作站与服务器之间的通信业务是安全的，否则只保证文件系统安全是不顶用的。

监控网上的通信业务，就可以提高对未授权信息的访问机会，除非已对数据采取安全措施。除了要保护构成网络的设备和通信线路，使之免于非法访问外，还要对数据采取安全措施，例如加密（发端加密，收端解密，使非法截获信息者无法理解它们）。图1.1示出了安全通信系统的工作原理。

虽然在局域网内通信安全性是次要问题，但是在较大型的网络中它应是一个需要关心的问题。而当一个网络接入因特网（Internet）时，通信安全就成了关键问题。

提示：从第3章开始，本书中有几章都将较深入地讨论通信安全性问题。

图1.1　利用加密技术实现安全的数据通信

管理

网络管理也是安全性考虑的一方面。如果你的网络是一个小型网络（例如在一个建筑物内，用户数不超过50个），可能有一个管理员。这个管理员掌管了各方面的安全工作。而较大的网络，具有数百个用户，分布在几个街区上，就需要均摊管理工作负担。你可以给用户访问文件和享受网络服务的权利，同时也赋予他们管理功能，起网络管理员的作用。

有许多办法可以用来分配网络的管理工作。例如，每个公司可指定一个管理员。也可以作更为复杂的安排，例如指定专项管理员，象文件系统管理员或Internet网关管理员等。

大型复杂的网络可能具有整套的多层次管理员体系，可以设有分支部门管理员，容许他们批准其他用户具有从事更低层次管理工作的权限。

提示：Windows NT含有一个称作Administrator（管理员）的帐号，此帐号被授予全部管理优先权。你可以利用这个帐号再创建其它的管理员。

审计

譬如大厦的保安，你可能注意到现在许多公司使用摄像机录象作为保安手段之一。尽管它不能预知何时出现问题，但对事后分析很有价值，它记录了何时发生了什么事情，是谁干的。就网络安全而言，审计（auditing）起着类似的监测作用。

Windows NT的审计功能是当某些事件发生时可以自动登录它们。例如你可能希望知道哪个用户访问了某一文件，利用审计功能你可以在事后查看登录文件，以便确定是否有非法访问。

在User Manager中有Domains 的审计策略（Audit Policy）的选项，可以选择启用各种审计功能。图1.2示出了该对话框。

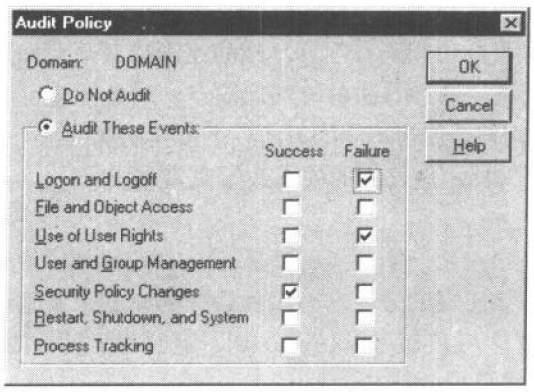

图1.2　利用User Manager中Domains的对话框，可以控制审计功能

你可以根据网络的安全层次或风险程度，要求审计时刻保持作用，或是要求它只针对某些文件起作用。也可以在保密问题发生后启用审计功能，以期该问题再次发生时获得更多的信息。

物理安全性

当然，服务器的安全程度与其所在房间的安全程度是一样的。物理安全性是指机器本身的安全。当工作站已有人登录或是无人看管时，网络安全很容易被破坏，甚至机器本身被人偷走。

提示：对于物理安全性，通常的规则是：若有人能物理地访问你的服务器，他们就有可能引起麻烦。

实际考察

当我作网络顾问时，去一公司对其管理和保护NetWare服务器的IS部门进行培训。我到了该公司发现服务器不恰当地放在复印机和咖啡器旁。虽然服务器需口令才能访问，但它在这种环境中却阻止不了一种潜在的安全威胁（即溅出或倒洒咖啡的影响）。

人为安全性

安全性涉及的另一个重要方面是网络中最混乱的因素：用户。人的安全性包含许多方面，从非法闯入者到训练用户防止别人破坏网络安全等。

由于用户是网络的核心，人为安全又与其它许多类型的安全问题都有关系，互相交织在一起，所以与人为安全有关的网络，在其它方面也不可能是安全的。第2章将详细讨论与人有关的安全性问题。

规划安全手段

当你筹划网络安全时，可采用如下基本手段之一：

- 乐观法：开始时给用户访问一切的权利，然后再禁止访问关键信息。
- 悲观法：开始时限制访问所有内容，然后逐渐放松，允许用户访问所需信息。

以后诸节你就会看到，两种方法各有其优缺点。当然你也可以采用介于两者之间的方法，或是对于网络的不同部分使用不同的方法。下面我们就讨论一下乐观法和悲观法，然后介绍为把安全手段写成文档，应建立的安全政策或策略。

乐观法

乐观法是最容易付诸实现的方法，至少从管理的角度来看是如此。在极端情况下可以使用极端乐观法：所有的用户都可以访问一切，这样做几乎不需要管理工作，事实上，Windows NT的缺省方式采用的就是这种方法。

显然这种方法的缺点就是过于乐观。除了很小的网络外，当你创建一个用户时，很难想象到所有会出现的问题。因此，这种方法是一种校正性安全，每发生一次安全事故或漏洞，

制订一次规则、增加一些安全措施，逐步改善安全性。

采用乐观法的网络管理员，往往处在一种隐患之中，他们把安全建立在不牢靠的基础上。他们常常认为只要在文件系统中，把目录埋藏的层次深一些，或是访问该信息需要知道较复杂的DOS或UNIX命令，数据自然就会安全。不言而喻，通常不是这样。当网络管理如此随意和混乱时，会造成一些机会，使某些用户对网络比管理员还熟悉。

提示： 乐观法的另一隐患是，他们假定用户不会损坏数据，除非具有某种动机。不幸的是，善意的用户有时也会引起麻烦，起到黑客和合伙间谍的作用。

当然，适当地使用乐观法，而不走极端也是可行的。如果你的网络几乎没有什么保密内容，采用乐观法是最好的选择。例如，对于小公司中的用户，一个人可能有好几个头衔，兼管多项工作，一个秘书可以查付出账、收入账和总分类账等数据。这种情况下，采用乐观法合适。多数用户需要访问许多区域，但是关键的区域（如工资单）需要采取安全措施。

悲观法

与乐观法相反，悲观法需要网络管理员付出巨大的努力和做大量的工作。起初，每个用户几乎处处都不能访问，然后，针对每项特定的需要，仔细审查，逐步增加访问权限。用户每次升职或调整工作，都要去更改帐号。

显然这种方法需要投入大量的管理工作，由于许多部门人员过少，所以此法不受欢迎。然而对于那些安全是关键的部门，如政府部门、管理严密、丝毫不能出差错的行业（如银行和卫生部门），此方法得以广泛使用。

悲观法的突出优点是：它可以避免很多安全问题发生，包括没想到的问题。对每个关注安全的人来说，这是一种非常诱人的选择。尽管严格的悲观法在你的机关不切实际，但是它的部分内容你可以考虑使用，或是在你的网络中需要高度安全的区域采用悲观法。

注意： 有一种情况肯定要采用悲观法，那就是在任何可以通过Internet访问的系统中，你公司的用户可能不会破坏你的安全，但是Internet上的某个人可能会。

安全政策

维持一个安全的网络需要组织得有条不紊，粗心大意将不可避免地造成安全漏洞。为保证网络的安全，应当建立必要的文档，规定严格的安全规则和安全措施。比较理想的是在规划和安装网络时，首先要制订安全政策与策略。

安全政策必须清晰、明确地写入文档，应当由管理部门和业务部门一致认可。可以把它张贴出来或是发给每个职员（或是通过公司内部网发布），使人人都知道他们对公司及其资料安全所起的作用。

安全政策应清晰明确地表述出如下内容：

- 部门采取的基本安全方法（乐观法或悲观法），以及网络中不受规则限制的例外部分。
- 安全规定和措施的各方面细节，包括物理的和人为的安全性。
- 对于每个职员或是小组都有何种访问权限。

网络安全应是整体安全的一部分，整体安全还包括大厦本身的安全、电话系统的安全

以及公司其它方方面面的安全。

除了你建立的管理公司安全的政策外，还有另外一类政策。Windows NT包含了几种所谓策略选项，容许你制订网络安全的基本规则。例如，帐号策略（account policy）对话框（见图1.3）包含一些选项：如口令要求、口令最小长度及其它有关用户帐号的项目。你的策略文档中应当包含Windows NT策略选项中的每一项填写的内容。

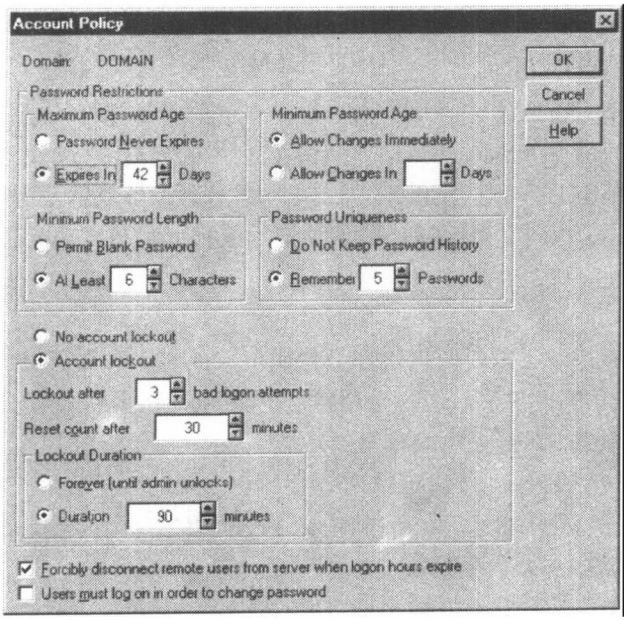

图1.3 Windows NT的帐号策略对话框，包含有关用户的帐号和口令选项

注意： *在以后各章中我们都推荐一些项目，供你建立相应方面的安全政策时考虑。遵循本书的指导，你应能建立一个涉及所有重要议题的安全政策。附录A中归纳了这些政策。*

安全问题及其后果

一般而言，任何安全政策的目的都是为避免发生损失。大厦的安全漏洞会造成商品的丢失，而网络的安全漏洞会造成资料丢失、失密、服务或公务上的损失，或是浪费了网络管理员和其他职员的时间。

以下诸节我们简略介绍一下各种安全漏洞，它们可能影响网络、造成某种损害。这些漏洞和损害都是安全政策不完善造成的后果。但是，从某种意义上说，所有的安全政策都是不完善的。所以希望你能了解各种漏洞可能产生的潜在损害，判断哪种漏洞对你的公司破坏性可能最大，以便制订合适的安全政策，重点防范，使风险最小。

偷窃

除了网络服务器设备可能被窃之外，从网络安全角度看还有两种较大的偷窃可能性：

- **偷窃资料**：未经授权的用户可能拷贝你的网络中存储的资料。
- **盗用服务**：如果你的网络提供某种服务，未经授权的用户可能设法访问它，非法享

受服务而不付费。

与窃贼不同的是，他们不是剥夺你的资料和服务，而是由于资料被盗用或盗版、服务被盗享，会使资料和服务迅速丧失其价值。如果保密的业务资料落入竞争对手的手中，可能意味着灾难。而不付费就能享受网络提供的服务，会使你丢掉付费的客户。

非法泄露信息

另一种潜在损失是非法泄露信息。除了可能是间谍外，也可能是以算不上犯罪的方式泄露，但后果极为严重。例如某些职员能够访问一定的信息，他们可能无意地泄露这些信息。为此，最好是限制每个职员的访问权，需要知道多少就访问多少。又例如一个潜在的客户向职员索要资料，职员可能传真给他一份客户单，而并没有意识到这个客户是一个潜在的竞争对手。

还有一些情况，问题并不严重，职员们可以得到原本不是提供给他们的信息。例如，如果职员能访问工资信息，并且同他人的收入比较，那么多数公司会为一些是非问题所困扰。各管理部门成员之间通信，甚至同一部门内职员之间通信，也会产生类似的问题。

信息战

怀有恶意的黑客可以造成破坏性特别严重的损害。如果黑客闯入网络，他们就能删除或修改信息。如果你有良好的备份系统，这种性质的数据损失则不是永久性的。但是它浪费你的时间，破坏用户的工作效率。此类妨害安全的方式称作信息战。

在与Internet连接的系统上，最耗费时间、破坏性最大的信息战有两类：

- **拒绝服务攻击**：黑客可以采用多种手段使你的网络停滞，使合法用户无法入网。典型的例子就是快速打开和关断TCP连接，使目标服务器消耗过度的时间，处理连接操作；或是利用软件中的已知缺陷，摧毁服务器或服务程序。
- **邮件炸弹**：发送极大量的电子邮件给服务器，使之应接不暇而丧失活力。此类攻击极易实现，任何人都可以做到。只需重复不断发送同一个大文件，或是写一个简单程序，不断重复发送含有少量信息的电子邮件。要能做到这点，大概需要上千或是几十万件报文，视服务器的规模和用途而定。

警惕：应采取特殊措施，防止这种现象发生。对于黑客来说，这两种类型的攻击实现起来比他们闯入网络要容易得多。在其它方面无害的网络应用程序之中的缺陷，也可以利用，造成网络服务瘫痪。任何具有电子邮件程序并稍具耐心的用户，都能够发送邮件炸弹。值得庆幸的是，许多黑客认为拒绝服务攻击和邮件炸弹的水平太低、不够刺激，很少使用。

数据意外丢失

虽然数据灾难往往是由怀有恶意的黑客造成的，但实际上你公司的数据还有很多可能的敌人，他们就是你自己的职员。不满的前职员可能变成怀有恶意的攻击者，但善意的职员也可能作出危险的事情。

如果你在安全方面采用乐观法，就给用户造成很好的机会来删除不是他创建的文件。当然，有法定资格和能力的用户，不会出现这种错误。但事实上许多公司培训职员时，采用了草率的办法："抛入水中让他们自己游"的方式，所以不能指望是否合格。