企业信息系统安全
——威胁与对策

林东岱　曹天杰　等编著

信息安全国家重点实验室专家
全面解析企业信息系统安全对策

◎ 如何应对复杂多变的不安全因素

◎ 如何构建可靠完整的安全体系

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

企业信息系统安全

——威胁与对策

林东岱　曹天杰　等编著

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

内 容 提 要

本书主要介绍企业信息系统面临的安全威胁和相应的对策。全书从企业信息系统安全所面临的主要威胁及不安全因素入手，介绍了企业网络的安全体系及系统的安全原则。书中详细讲述了企业信息系统的风险管理及安全控制；防火墙的体系结构及应用；恶意代码的种类、传播与防治；病毒的特征及防治；企业电子邮件的安全；企业 Web 的安全；应急响应与灾难恢复的具体措施以及企业网络的安全解决方案。

本书内容全面，简明实用，可作为企、事业单位信息系统的管理人员、信息安全技术人员和信息安全专业本科生和研究生的参考用书。也可以作为计算机科学技术及应用、软件工程及应用、信息工程、信息管理与信息系统、银行信息管理、会计信息管理和计算机安全等专业的工具书和教材。

图书在版编目(CIP)数据

企业信息系统安全——威胁与对策 / 林东岱等编著. —北京：电子工业出版社，2004.1
ISBN 7-5053-9487-8
Ⅰ.企... Ⅱ.林... Ⅲ.企业管理－信息系统－安全技术 Ⅳ.F270.7
中国版本图书馆 CIP 数据核字（2003）第 117293 号

责任编辑：张瑞喜
印　　刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：20　字数：438 千字
版　　次：2004 年 1 月第 1 次印刷
印　　数：5000 册　　定价：30.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：(010)68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

信息技术和信息产业的发展，推动了计算机及其网络在社会生活各个领域的广泛应用。以 Internet 为代表的全球性信息化浪潮，使得信息网络技术的应用日益普及，应用层次逐渐深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，如党政部门信息系统、金融业务系统、企业商务系统等。当前，各种各样完备的网络信息系统，使得秘密信息和财富高度集中于计算机中，并依靠计算机网络接收和处理，实现其相互间的联系和对目标的管理、控制。信息技术正在逐步改变企业的运营方式，成为当今企业发展的一个主题。当前我国正在加速企业信息化建设，以信息化带动工业化，以信息化促进现代化，用信息技术改造传统产业。

事物总是辩证统一的。在信息化过程中，尽管开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位的信息系统带来了革命性的变革和开放，使得他们能够利用 Internet 提高办事效率和市场反应能力，提升竞争力。但同时又要面对 Internet 开放带来的数据和系统安全的新挑战和新危险。我们知道，随着计算机技术的飞速发展，计算机系统和网络已经成为信息化社会发展的重要通信保证。在网络中存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、科研数据等重要信息。有的是敏感性信息，有的甚至是国家机密。所以不可避免会受到各种主动或被动的人为攻击，如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等。近年来，垃圾邮件日益蔓延，企业网页不时遭到黑客篡改攻击，计算机病毒泛滥成灾，网络信息系统中的各种犯罪活动已经严重危害着社会的发展和企业的安全，给全球的企业造成了巨大的损失。计算机网络犯罪案件急剧上升，已经成为普遍的国际性问题。形形色色的安全问题不仅给企业带来了巨额的经济损失，也严重阻碍了我国的信息化进程。因此，在企业信息化过程中，加强企业信息安全建设，及时采取相应的防范措施，已成为目前国内企业迫在眉睫的大事。

在攻击与反攻击、破坏与反破坏的斗争中，只要加强安全观念，提高防范意识，在信息安全技术的帮助下，通过适当的安全控制可以大大增加攻击者的难度，从而有效地遏制攻击企图，减少企业的损失。针对目前企业信息系统中存在的主要安全问题，我们编写了这本《企业信息系统安全——威胁与对策》。通过分析信息系统的安全威胁，以期为企业信息系统的构建和安全管理提供一些应遵循的安全原则和应实施的安全措施。

本书内容全面、系统，涉及到了企业信息安全的各个主要方面。既包括了边界防卫、入侵检测，也包括了应急响应与灾难恢复；既介绍了远程攻击、企业内部威胁，分析了企业电子邮件安全、企业 Web 安全，也给出了企业信息系统整体解决方案。本书在编写过程中既强调安全技术、安全产品的重要性，也强调安全保障体系建设的紧迫性。

我们必须明确，当一个系统正在使用时，要消除所有风险往往是不切实际的，甚至也是不可能的。而且所要求的安全性能越高，在安全管理上花费的成本也会越高，系统运行

的性能也会越低，所以高级管理人员和业务职能主管只能运用最小成本方法来实现最合适的安全控制，将风险降低到一个可接受的级别。另外，本书虽然系统地给出了提升企业信息系统安全的一些指导方法，但由于安全理论与技术的不断发展，企业信息安全环境的不断变迁，新的攻击手法不断涌现，但系统安全漏洞在所难免，信息系统永远不会有“完美”的安全性。本书的目的只是在一定的安全成本下，指导企业采取一定的原则与步骤，有效地应对已知的和未知的安全威胁，最大程度地保护企业的信息资产，完成企业使命。

本书参考了大量的 Internet 资源，包括 RFC 文档(http://www.ietf.org/rfc.html)、美国国家标准技术研究所出版物(http://csrc.nist.gov/publications/)、各类安全白皮书、安全漏洞公报及解决方案等，也希望读者在学习的过程中查阅参考。

本书适合于以下几类读者：第一类是企业管理人员，通过此书管理人员可以了解企业信息安全的整体概念，掌握与技术人员沟通的共同语言，为企业信息系统建设提供安全决策；第二类是企业信息安全技术人员，本书提供了企业信息安全方面的详尽务实指导，可作为保障企业信息系统安全的管理指南及操作手册；第三类是信息安全专业的本、专科学生，本书可作为他们在计算机系统安全、网络安全方面的参考书，为将来从事信息安全方面的工作打下坚实的基础。

本书得到以下项目的资助：

国家高技术研究发展计划(863)资助(项目编号：2003AA144030)

国家自然科学基金资助(项目编号：90204016)

编者衷心感谢中国科学院信息安全国家重点实验室的各位同事在本书的写作过程中给予的大力协助。保障企业信息安全是一项复杂的系统工程，本书力求系统、全面、重点突出、注重实践，但由于水平有限，缺点错误不可避免，编者衷心希望读者对本书批评指正。

电子邮件地址：zhangruixi@phei.com.cn

编　者

2003 年 11 月

作者简介

林东岱

中国科学院软件研究所研究员，博士生导师，信息安全国家重点实验室副主任

1964年出生，1984年毕业于山东大学数学系，1984年-1990年中国科学院系统科学研究所研究生，1990年获数学专业编码学与密码学方向理学博士学位。1994年-1996年日本大学理工学部博士后，1996年-1997年日本大学理工学部数学科访问学者，1999年-2000年美国肯特州立大学数学与计算机科学系访问教授。主要从事密码理论、安全协议、符号计算与软件设计方面的研究工作。目前参加承担的在研项目有国家重大基础研究规划(973)项目“数学机械化与自动推理平台”，国家自然科学基金“安全电子支付系统研究”，中国科学院知识创新工程基金课题“密码算法实验平台开发”，国家高科技发展计划(863)项目“分布式密码算法及并行化技术”等课题。

作者简介

曹天杰

副教授，中国科学院软件研究所信息安全国家重点实验室博士

1967年出生，1986年-1993年在天津南开大学数学系计算数学及其应用软件专业学习，获理学学士、硕士学位。1993年-2002年在中国矿业大学计算机科学与技术学院信息安全系任教。2002年9月开始在中国科学院软件研究所信息安全国家重点实验室攻读博士学位，方向为密码学与信息安全。发表网络与信息安全方面的论文10余篇，参加科研项目多项，获校级与省级教学奖多项。

目　录

第1章

企业信息系统安全问题概述

企业信息系统安全——威胁与对策

1.1 企业信息系统安全面临的主要威胁

1.1.1 企业信息系统的安全需求

信息技术已经成为信息时代的核心技术，它影响和决定着现代技术的发展方向。

信息技术和信息产业的大发展，极大地推动了计算机在社会生活各个领域的广泛应用，从而引发了以计算机为主体的信息革命，而信息革命的发展又促使人类社会进入一种全新的社会形态——信息化社会。信息化社会是以信息技术的广泛应用为特征的，它对人类社会的进步和企业的发展都具有重要影响。

加速企业信息化建设，以信息化带动工业化，以信息化促进现代化，用信息技术改造、提升传统产业已经成为我国企业的当务之急。

信息以多种形式存在。它可以打印或写在纸上(如书面的财务报表等)，也能以电子形式存储(如一个企业备份磁带)，通过邮件或用电子手段传输，显示在胶片上，或表达在会话中。但是，不论信息采用什么方式或采取什么手段共享和存储，今天各行各业对信息的依赖愈来愈大，信息已成为企业的一种重要的资产，必须加以保护。

信息系统包含了信息产生、信息获取、信息处理、信息传输、信息利用的全过程。信息网络的全球性、开放性、共享性和发展的动态性使得信息系统的应用范围快速拓展，从传统的文件传输、电子邮件、远程登录等应用发展到 WWW。信息服务、电子商务、计算机协同工作、虚拟企业、移动计算等信息系统已经深入应用到政治、经济、军事、科学文化等领域中并继续影响着政府机构、企业的运转和人们的生活。企业处于信息化社会的大环境中，要生存，要发展，就必须借助于信息技术。企业不仅要通过网络宣传自己及其产品，通过网络进行贸易，还要通过信息技术加快信息的传输和管理，提高工作效率，提高产品质量。企业信息系统将是企业数字化生存之本，不进行企业信息系统的建设，企业在信息社会中将无处立身。

企业信息化是指企业以业务流程重组为基础，在一定的深度和广度上利用计算机技术、网络技术和数据库技术，控制、集成和管理企业生产经营活动中的所有信息，实现企业内外部信息的共享和有效利用，以提高企业的经济效益和市场竞争能力。企业信息化意味着计算机在企业的生产、经营、设计、制造、资源管理等方面较全面的利用，且有一定程度的信息共享。

随着国家信息化基础设施的不断建设和完善，企业对外联系的两项主要业务，即物资和配套件的采购以及产品的销售将更多地通过网络来进行。电子商务、电子数据交换、电子邮件将是供销过程中最常用的方式和手段。如果银行、海关和上级部门均普遍采用信息化办公技术，而某个企业没有实现网络化，那么它将无法与自己的供应商和客户进行交流。

全球信息化使得网络系统成为社会发展的重要保证，但由于计算机网络的开放性、互连性等特征，致使信息系统易受各种人为攻击(例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等)，信息系统在安全方面的脆弱性使得攻击信息系统事件不断发生并屡获成功，如果信息系统的安全受到威胁，就会严重阻碍信息技术的应用和发展。在国外无论是政府还是企业都纷纷投巨资研究和提高信息系统的安全技术。

计算机系统(computer system)也称计算机信息系统(computer Information system)，是由计算机及其相关的和配套的设备、设施(含网络)构成的，并按一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。国际标准化组织(ISO)将“计算机安全”定义为：为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。此定义偏重于静态信息保护。也有人将“计算机安全”定义为：计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。该定义着重于动态意义描述。

当前信息系统安全已不只是人们传统意义上的安全，即添加防火墙或路由器等网络安全设备就可保证安全，而是成为一种系统和全局的观念。信息系统安全体现在使系统避免一系列威胁，保障商务的连续性，最大限度地减少业务所遭受的损失，从而最大限度地获取投资和商务的回报。

一般认为，当前对计算机信息系统的攻击，通常体现为以下四种类型的攻击。

(1) 中断。使该系统的资产变得不可用或不能使用，这是对可用性的攻击。例如硬盘的毁坏、通信线路的切断或某个文件系统的损坏。

(2) 截获。未授权方获得了对某个资源的访问，这是对机密性的攻击。例如在网络上搭线窃听以获取数据，违法复制文件或数据等。

(3) 篡改。未授权方不但获取了访问并对资源进行了篡改，这是对完整性的攻击。例如改变数据文件的值，改变网络中消息的内容，改变程序使其执行结果不同等。

(4) 伪造。未授权方将伪造的项目放入系统，这是对真实性的攻击。例如加入伪造的消息或为文件增加记录等。

四种类型的攻击如图 1-1 所示。

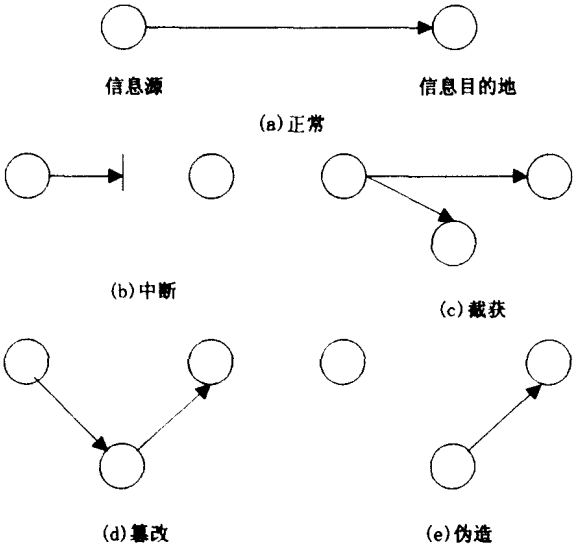

图 1-1　四种类型的攻击

企业信息系统的安全主要有以下几个需求。

(1) 物理安全(physical security)。为防范蓄意的和意外的威胁，而对资源提供物理保护

措施。

(2) 数据机密性(data confidentiality)。机密性要严格限制，只有授权可以查看数据的人才能接触到敏感数据。确保信息不暴露给未授权的实体或进程，不会被未授权的第三方所知。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人私密(如浏览习惯、购物习惯)。防止信息失窃和泄露的保障技术称为保密技术。

(3) 数据完整性(data integrity)。完整性是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改。即信息的内容不能为未授权的第三方修改。信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等。奇偶位校验和循环冗余校验(CRC)能够检测出数据的意外修改，但不能保护数据被攻击。

(4) 数据可控性(data control)。可控性是指得到授权的实体可以控制其授权范围内的信息流向及行为方式，即对信息及信息系统实施安全监控。管理机构对使用加密手段危害国家信息的传输从事非法的通信活动等行为进行监视审计，对信息的传播及内容具有控制能力。

(5) 数据可审查性(data censor)。可审查性指使用审计、监控、防抵赖等安全机制，使得使用者(包括合法用户、攻击者、破坏者、抵赖者)的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体、时间和成败情况等。

(6) 数据可用性(data availability)。得到授权的实体在有效的时间内能够访问和使用其所要求的数据，得到授权的实体在需要时可访问资源和服务。可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的，多方面的(话音、数据、文字和图像等)，有时还要求时效性，网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害(战争及地震等)造成的系统失效。

(7) 身份认证(peer-entity authentication)。确保一个实体此时没有试图冒充其他实体，或没有试图将先前的连接作非授权重演。保证信息使用者和信息服务者都是真实声称者，防止冒充和重演的攻击。

(8) 数据认证(data origin authentication)。确保接受到的数据出自所要求的来源。

(9) 防抵赖(no repudiation)。也称为不可否认性。避免在一次通信中涉及到的那些实体之一不承认参加了该通信的全部或一部分。不可抵赖性是面向通信双方(人、实体或进程)信息真实的安全要求，它包括收、发双方均不可抵赖。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认其内容的企图不能得逞；二是交付证明，它提供给信息发送者以证明这将使接收者谎称未接收过这些信息或者否认其内容的企图不能得逞。