

电子商务面临的安全问题



电子商务安全简介

一、电子商务安全的含义

电子商务安全从整体上可以分为计算机网络安全和商务交易安全两大部分。

计算机网络安全



商务交易安全



电子商务安全简介

计算机网络安全主要包括计算机网络设备安全、计算机网络系统安全、数据库安全等，主要解决的是计算机网络本身存在的安全问题，要采用一系列网络安全增强方案来保证计算机网络自身的安全。



电子商务安全简介

商务交易安全则主要是针对传统商务在网络应用时产生的各种安全问题。

计算机网络安全和商务交易安全相辅相成、缺一不可，它们是电子商务活动得以实现的重要支撑。



电子商务安全简介

（一）计算机病毒

根据1994年2月18日我国正式颁布实施的《中华人民共和国计算机信息系统安全保护条例》可知：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。



电子商务安全简介

近几年来，计算机病毒主要呈现的特征可以归纳为以下几个。

智能手机成为病毒的下一个攻击目标

经济利益驱使计算机
病毒技术不断突破



病毒变种快、更新快、
存活能力强

网银病毒迅猛增长

病毒更加“智能化”

病毒更加“人性化”，
更具有欺骗性



电子商务安全简介

（二）黑客攻击

黑客攻击指的是黑客非授权入侵其他程序、系统或网络，破坏该系统、程序或网络的行为。



电子商务安全简介

常见的黑客攻击方法主要有



电子商务安全简介

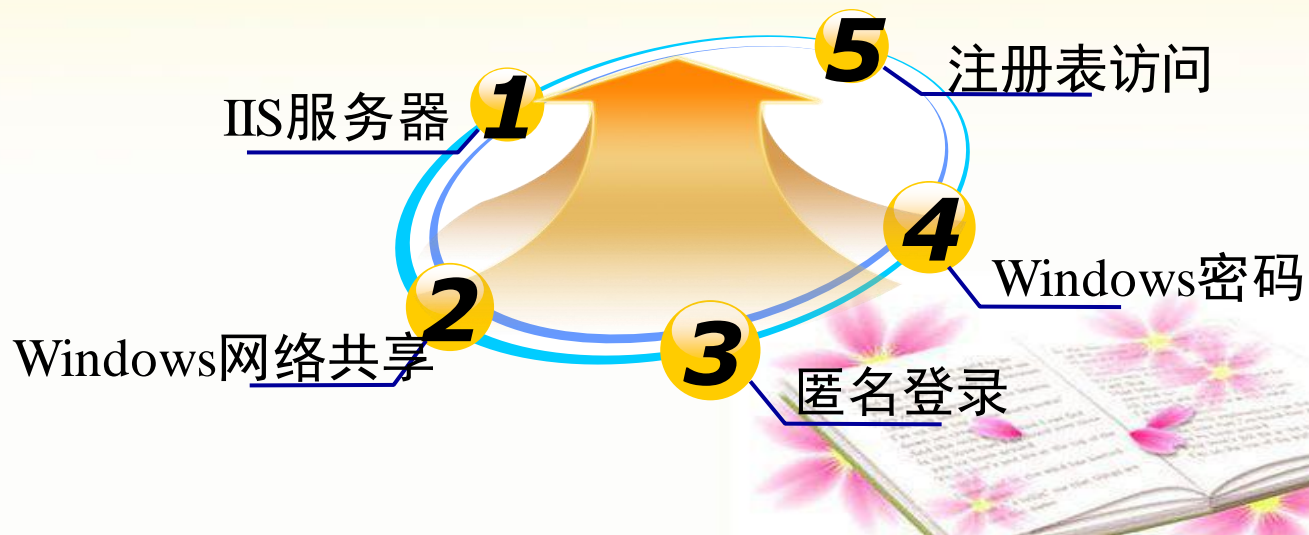
（三）系统安全漏洞

系统安全漏洞也叫系统脆弱性，简称漏洞，是计算机系统
在硬件、软件、协议的设计与实现过程中或系统安全策略上
存在的缺陷和不足。



电子商务安全简介

用户使用最多的Windows系统有以下几种常见漏洞



电子商务安全简介

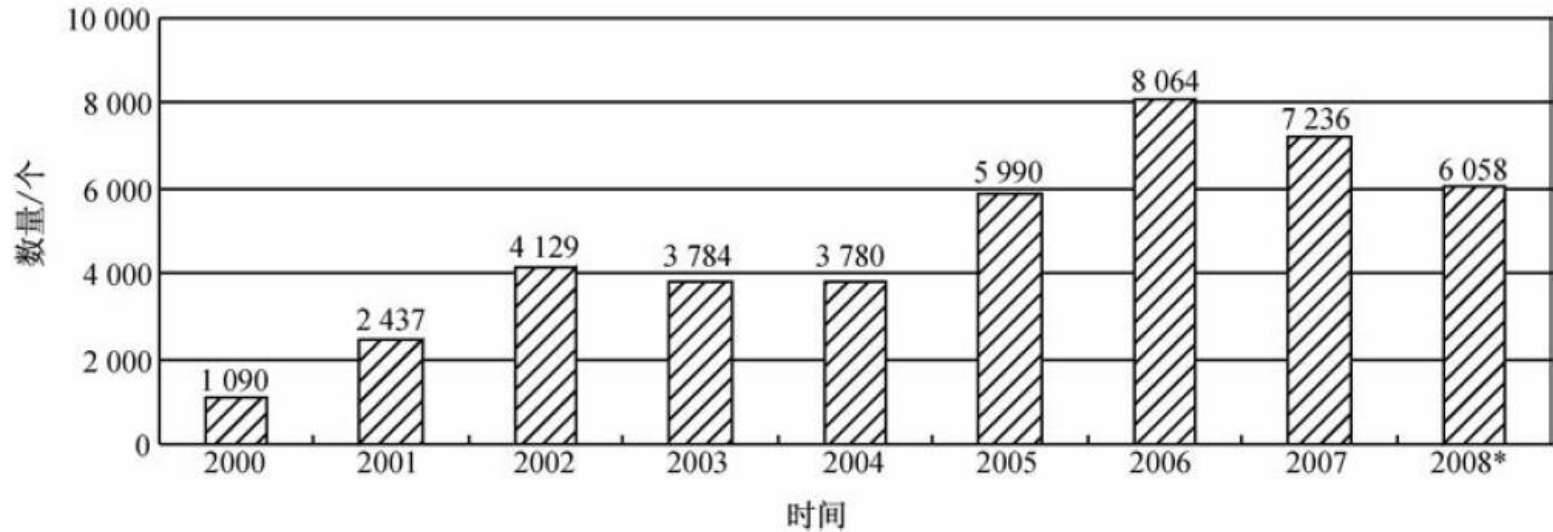


图 2-2 2000—2008 年 CERT/CC 统计并公布的漏洞数量



电子商务安全简介

二、电子商务安全的要求

电子商务安全的具体要求如下



电子商务安全简介

三、电子商务安全的体系结构

电子商务安全的保证主要体现在3个方面：技术保障、安全管理保障和法律环境保障

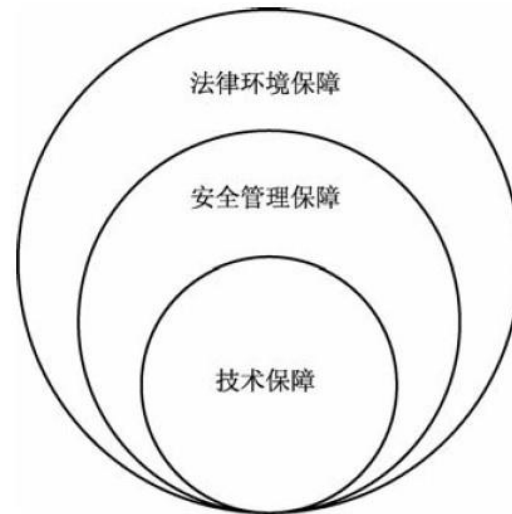


图 2-3 电子商务安全的体系结构

电子商务安全简介

（一）技术保障

技术保障是指实现电子商务所需要的设备、技术等能够稳定、安全地提供所需的功能。

其中主要包括实体的安全和网络技术的安全。



电子商务安全简介

1. 实体的安全

环境安全



设备安全



电子商务安全简介

2. 网络技术的安全



电子商务安全简介

（二）安全管理保障

安全管理保障是在安全技术的基础之上，对系统的实时维护和设备的日常管理。从某种意义上来说，安全管理比安全技术更为重要。

安全管理保障包括人员和制度的保障。



电子商务安全简介

1. 人员的保障

电子商务不是电子设备之间独立进行的交易行为，其交易的主体仍然是人。既然人作为一种实体在电子商务交易过程中存在，则其必然对电子商务的安全产生重要的影响。由于人所产生的安全问题多为主观性的，如员工无意中泄露系统的密码，对企业心怀不满的员工对系统的恶意攻击等。因此，加强人员管理，对于保障电子商务安全十分重要。



电子商务安全简介

2. 保密制度

信息的安全级别一般可分为以下三级：



电子商务安全简介

3. 跟踪、审计、稽核制度

跟踪制度是以系统自动生成日志文件的形式来记录系统运行的全过程。

审计制度规定网络审计员应经常对系统的日志文件检查、审核，以及时发现异常状况，监控和捕捉各种安全事件，并对系统日志进行保存、维护和管理。



电子商务安全简介

3. 跟踪、审计、稽核制度

稽核制度是指工商管理、银行、税务人员利用计算机及网络系统，借助稽核业务，应用软件调阅、查询、审核、判断辖区内电子商务参与单位业务经营活动的合理性、安全性，堵塞漏洞，保证电子商务交易安全，发出相应的警示或作出处理处罚的有关决定的一系列步骤及措施。



电子商务安全简介

4. 数据容灾制度

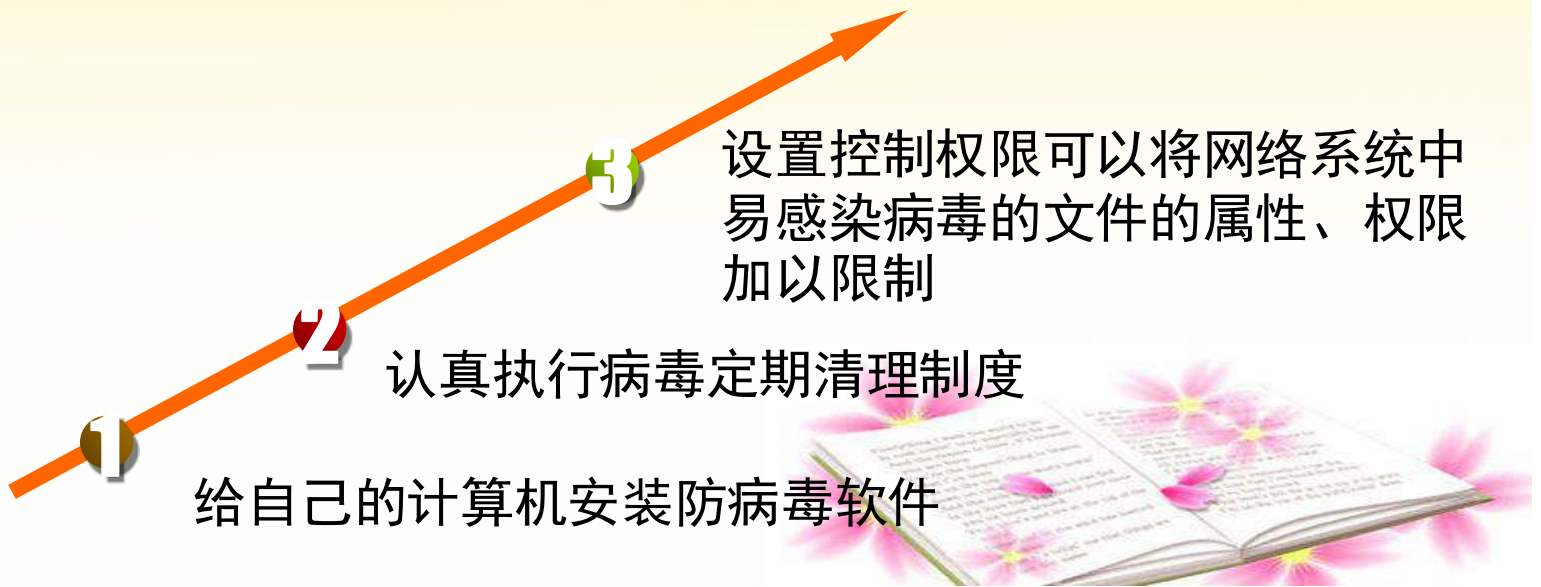
按容灾能力的高低，容灾系统可以分为多个层次。

企业应该根据自身情况，对不同安全级别的数据制定不同的数据容灾制度。



电子商务安全简介

5. 病毒防范制度



电子商务安全简介

6. 应急措施

应急措施是指在计算机灾难事件发生时，利用应急计划、辅助软件和应急设施，排除灾难和故障，保障计算机信息系统继续运行或紧急恢复正常运行。



电子商务安全简介

（三）法律环境保障

目前世界上的电子商务相关法律主要涉及计算机犯罪立法、计算机安全法规、隐私保护、网络知识产权保护、电子合同相关法规等方面，初步满足了电子商务保密性、完整性、可认证性、可控性和抗抵赖性的安全需求。但是，电子商务安全不可能一劳永逸，必须以发展的眼光来看待它，所以进一步的法制建设还应继续进行。



电子商务安全面临的问题

一、电子商务网络系统的安全问题

(一) 网络系统软件自身的安全问题

(1) 操作系统的体系结构会造成其本身的不安全性，这也是计算机系统不安全的根本原因之一。

(2) 操作系统的一些功能，如支持在网络上传输文件的功能，包括可以执行文件映像，即在网络上加载程序等，必然会带来一些不安全因素。



电子商务安全面临的问题

(3) 操作系统不安全的另一个原因在于它可以创建进程，甚至支持在网络的结点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。

(4) 操作系统在运行时，一些系统进程总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去，这也是黑客可以利用的。



电子商务安全面临的问题

(5) 操作系统要安排无口令入口，这原本是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽信道。

(6) internet和intranet使用的TCP/IP及FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程进程调用）、NFS（网络文件系统）等都包含许多不安全的因素，存在着许多漏洞。



电子商务安全面临的问题

（二）网络系统中数据库的安全设计问题

因为在数据库系统中存放着大量重要的信息资源，在用户共享资源时可能会出现以下现象：授权用户超出了他们的访问权限进行更改活动；非法用户绕过安全内核，窃取信息资源等。因此提出了数据库安全问题，也就是要保证数据的安全可靠和正确有效。对数据库数据的保护主要针对数据的安全性、完整性和并发控制3个方面。



数据库安全面临的问题

数据的安全性就是保证数据库数据不被故意破坏和非法存取。**数据的完整性**是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入或输出而造成无效操作和错误结果。**并发控制**是指数据库是一个共享资源，在多个用户程序并行地存取数据时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。



电子商务安全面临的问题

（三）网络系统的运行安全

运行安全是指为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。

电子商务网络系统的运行安全具体由四个部分组成：风险分析、审计跟踪、备份与恢复和应急措施。



电子商务安全面临的问题

1. 风险分析

风险分析主要涉及四个方面的安全功能：

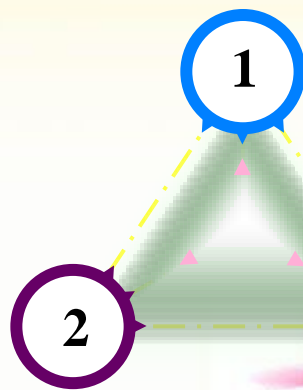


电子商务安全面临的问题

2. 审计跟踪

记录和跟踪各种系统
状态的变化

实现对各种安
全事故的定位



保存、维护和
管理审计日志



业务安全面临的问题

3. 备份与恢复

- (1) 提供场点内高速度、大容量、自动的数据存储、备份和恢复。
- (2) 提供场点外的数据存储、备份和恢复，如通过专用安全记录存储设施对系统内的主要数据进行备份。
- (3) 提供对系统设备的备份。



应急准备安全面临的问题

4. 应急措施

应急计划辅助软件



应急设施



电子商务安全面临的问题

二、电子商务信息传输的安全问题

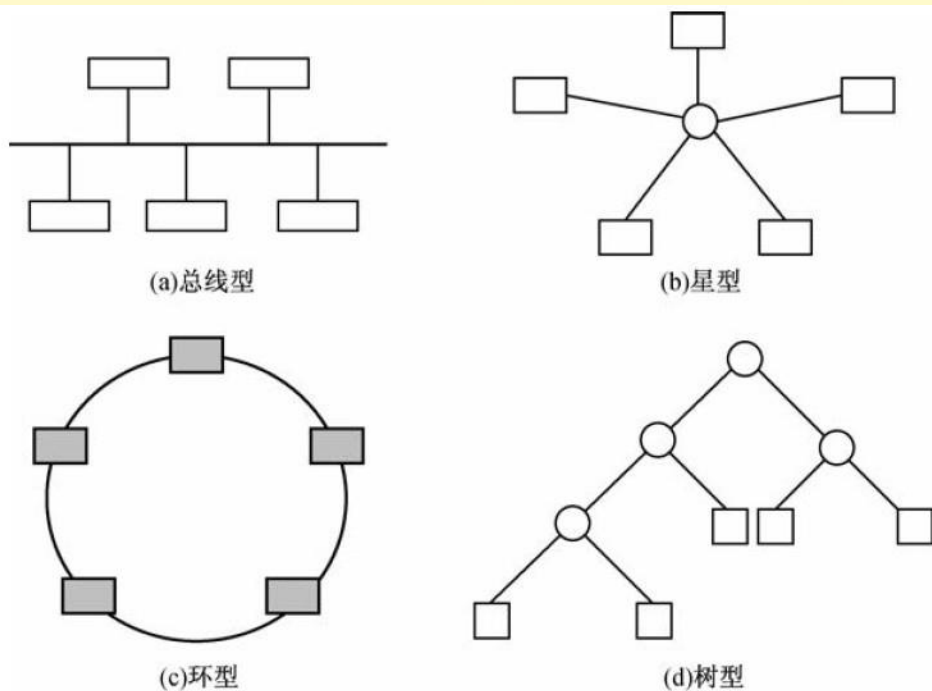


图 2-5 典型的计算机网络结构

电子商务安全面临的问题

三、电子商务安全管理问题

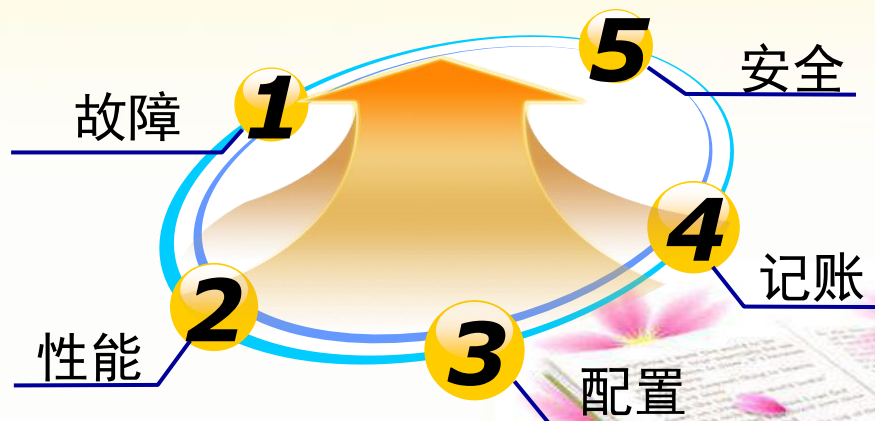
通常安全管理领域涉及两类要求：一类是安全管理，防止未授权者访问网络；另一类是管理安全，防止未授权者访问网络管理系统。

安全管理必须解决下列基本问题：需要保护的对象、需要保护的原因、保护的方法、采取保护措施的方法、实施保护的地点。



网络运营安全面临的问题

国际标准化组织把网络管理划分为五个领域，分别是故障、性能、配置、记账和安全。

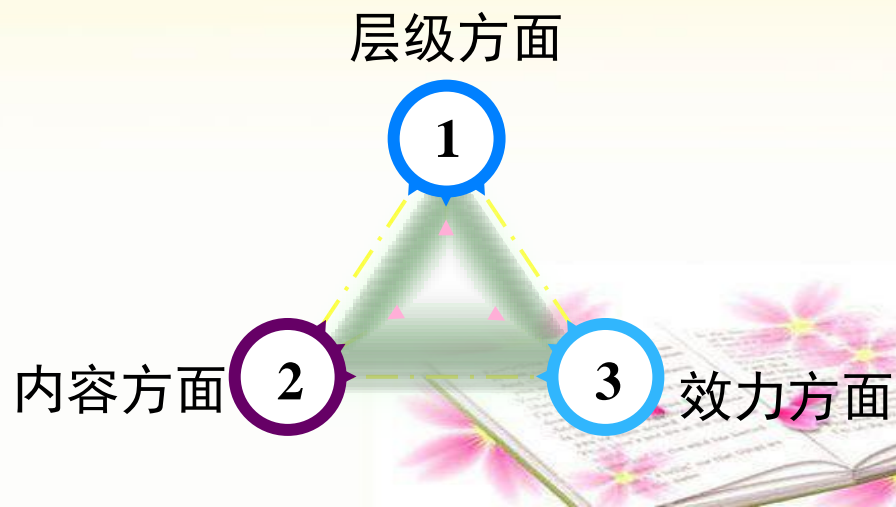


电子商务安全面临的问题

四、电子商务法律保障问题

1. 我国互联网安全的法律保障

从目前的互联网法律保障现状来看，主要存在以下几个问题：



电子商务安全面临的问题

2. 我国电子商务安全的法律保障

有代表委员指出，我国电子商务的相关法律法规内容应包括立法宗旨、电子商务概念、基本原则、交易主体、电子合同、电子签名及认证、电子支付、信用保障、交易安全、个人信息保护、消费者权益保护、知识产权保护、电子商务税收、行业自律、争端解决机制、法律责任等内容。

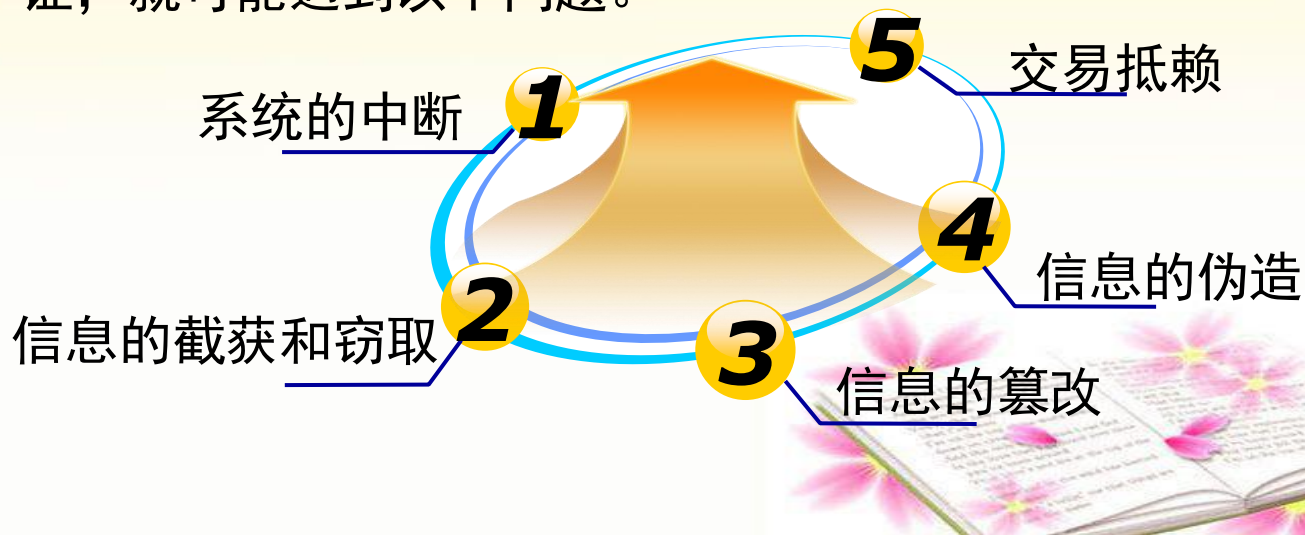


电子商务安全面临的问题

五、电子商务客户、商家和银行可能面临的安全问题

(一) 总体安全问题

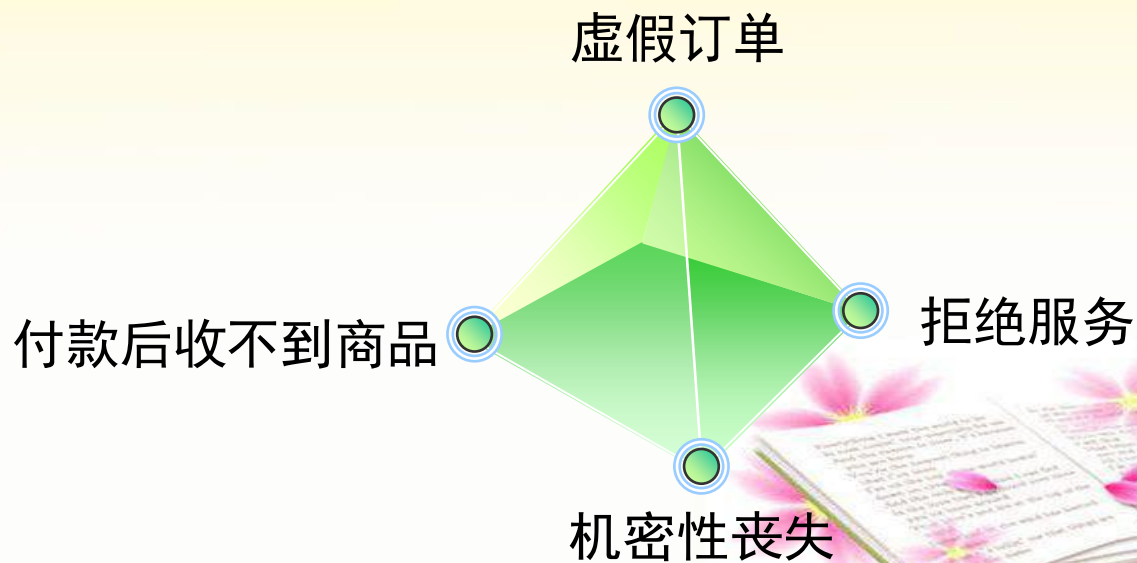
对于客户、商家和银行来说，一旦电子商务安全得不到保证，就可能遇到以下问题。



电子商务安全面临的问题

(二) 具体安全问题

1. 客户可能面临的安全问题



电子商务安全面临的问题

2. 商家可能面临的安全问题

中央系统安全性被破坏

竞争者检索商品的
销售情况

客户资料被
竞争者获悉

被他人冒名而损害企业的名誉

商家的个人或集体信息
遭到泄露，或者商业机密
遭到泄露

消费者提交订单后不付款



电子商务安全面临的问题

3. 银行可能面临的安全问题

中断（攻击系统的可用性）

窃听（攻击系统的机密性）



伪造（攻击系统的真实性）

篡改（攻击系统的完整性）



本章小结

本章主要是对电子商务安全进行简单的叙述，介绍了电子商务安全的概念，其主要内容有电子商务安全的含义、要求、体系结构等；同时还介绍了电子商务安全所面临的各种问题，包括网络系统的安全问题、信息传输的安全问题、安全管理问题、法律保障问题。最后分别分析了电子商务客户、商家和银行可能面临的安全问题。

综合训练

1. 简述电子商务安全的含义。
2. 简述电子商务安全的要求及其体系结构。
3. 电子商务安全都面临着哪些问题？
4. 电子商务网络系统存在哪些安全问题？
5. 简述电子商务客户、商家和银行可能面临的安全问题。



综合训练



实训目标

了解电子商务安全的基本常识及其相关知识，正确理解电子商务安全的重要性以及电子商务安全所面临的问题。





实训环境

一个连接互联网的机房，机器设备数量保证上课班级的学生每人一台。





实训内容

- (1) 查找5个以上的专业电子商务网站，并搜索有关电子商务安全的基本概念。
- (2) 查找当前国际和国内电子商务安全技术的发展状况的文章，阅读并总结。
- (3) 结合你的电子商务经验，找到电子商务发展中存在的安全问题。
- (4) 描述你进行电子商务过程中遇到安全问题时的解决方法。

实训设计



实训内容

- (5) 查找电子商务安全对策。
- (6) 查找《中华人民共和国电子签名法》的内容，并分析该法所涉及的技术问题，体会它被称为我国第一部“真正意义上的信息化法律”的含义。
- (7) 查找现有的电子商务安全方法及其效果说明。
- (8) 课堂讨论，发表自己的意见，就电子商务安全提出自己的创新观点。

