综合辅导：谈电子商务中的网络安全管理电子商务考试 PDF 转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/517/2021_2022__E7_BB_BC_E5_90_88_E8_BE_85_E5_c40_517457.htm [摘要] 随着互联网的全面普及，基于互联网的电子商务应运而生，近年来获得了巨大的发展。作为一种全新的商务模式，本文从电子商务网络的安全问题作一个基本的探讨，重点阐述了电子商务系统中的安全控制的方面及网络安全技术的对策，只有安全、可靠的交易网络，才能保证交易信息安全、迅速地传递，才能保证数据库服务器的正常运行。 [关键词] 互联网 电子商务 安全控制 安全对策 电子商务网络安全从其本质上来讲就是网络上的信息安全，是指电子商务网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠运行，网络服务不中断。网络安全不仅仅是技术问题，也是一个管理问题，因此要解决网络安全问题，必须有综合的解决方案，才能全方位地对付各种不同的威胁和攻击，这样才能确保网络信息的保密性、完整性、可用性。因此，加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠地运行，将起到十分有效的作用。 一、电子商务中的安全控制 电子商务的基础平台是互联网，电子商务发展的核心和关键问题就是交易的安全，由于Internet本身的开放性，使网上交易面临着种种危险，也由此提出了相应的安全控制要求。 下面从技术手段的角度，从系统安全与数据安全的不同层面来探讨电子商务中出现的网络安全问题。 1.系统安全 在电子商务中，网络安全一般包括以下两个方面：对于一个企业来说，首先是信息的安全

与交易者身份的安全，但是信息安全的前提条件是系统的安全。 系统安全采用的技术和手段有冗余技术、网络隔离技术、访问控制技术、身份鉴别技术、加密技术、监控审计技术、安全评估技术等。 （1）网络系统 网络系统安全是网络的开放性、无边界性、自由性造成，安全解决的关键是把被保护的网络从开放、无边界、自由的环境中独立出来，使网络成为可控制、管理的内部系统，由于 网络系统是应用系统的基础，网络安全便成为首问题。解决网络安全主要方式有：网络冗余它是解决网络系统单点故障的重要措施。对关键性的网络线路、设备，通常采用双备份或多备份的方式。网络运行时双方对运营状态相互实时监控井自动调整，当网络的一段或一点发生故障或网络信息流量突变时能在有效时间内进行切换分配，保证网络正常的运行。 系统隔离分为物理隔离和逻辑隔离，主要从网络安全等级考虑划分合理的网络安全边界，使不同安全级别的网络或信息媒介不能相互访问，从而达到安全目的。对业务网络或办公网络采用VLAN技术和通信协议实行逻辑隔离划分不同的应用子网。 访问控制对于网络不同信任域实现双向控制或有限访问原则，使受控的子网或主机访问权限和信息流向能得到有效控制。具体相对网络对象而言需要解决网络的边界的控制和网络内部的控制，对于网络资源来说保持有限访问的原则，信息流则可根据安全需求实现的单向或双向控制。访问控制最重要的设备就是防火墙，它一般安置在不同点域的出入口处，对进出网络的IP信息包进行过滤并按企业安全政策进行信息流控制，同时实现网络地址转换、实时信息审计警告等功能，高级防火墙还可实现基于用户的细粒度的访问控制。 身份鉴别是对网

络访问者权限的识别，一般通过三种方式验证主体身份，一是主体了解的秘密，如用户名口令、密钥；二是主体携带的物品，如磁卡、IC卡、动态口令卡和令牌卡等；三是主体特征或能力，如指纹、声音、视网膜、签名等。加密是为了防止网络上的窃听、泄漏、篡改和破坏，保证信息传输安全，对网上数据使用加密手段是最为有效的方式。 目前加密可以在三个层次来实现，即链路层加密、网络层加密和应用层加密。链路加密侧重通信链路而不考虑信源和信宿，它对网络高层主体是透明的。网络层加密采用IPSEC核心协议，具有加密、认证双重功能，是在IP层实现的安全标准。通过网络加密可以构造企业内部的虚拟专网，使企业在较少投资下得到安全较大的回报，并保证用户的应用安全。 安全监测采取信息侦听的方式寻找未授权的网络访问尝试和违规行为，包括网络系统的扫描、预警、阻断、记录、跟踪等，从而发现系统遭受的攻击伤害。网络扫描监测系统作为对付电脑黑客最有效的技术手段，具有实时、自适应、主动识别和响应等特征，广泛用于各行各业。网络扫描是针对网络设备的安全漏洞进行检测和分析，包括网络通信服务、路由器、防火墙、邮件、WEB服务器等，从而识别能被入侵者利用非法进入的网络漏洞。网络扫描系统对检测到的漏洞信息形成详细报告，包括位置、详细描述和建议的改进方案，使网答能检测和答理安全风险信息。 （2）操作系统 操作系统是管理计算机资源的核心系统，负责信息发送、管理、设备存储空间和各种系统资源的调度，它作为应用系统的软件平台具有通用性和易用性，操作系统安全性自接关系到应用系统安全，操作系统安全分为应用安全和安全漏洞扫描。 应用安全面向应用

选择可靠的操作系统，可以杜绝使用来历不明的软件。用户可安装操作系统保护与恢复软件，并作相应的备份。 系统扫描基于主机的安全评估系统是对系统的安全风险级别进行划分，并供完整的安全漏洞检查列表，通过不同版木的操作系统进行扫描分析，对扫描漏洞自动修补形成报告，保护应用程序、数抓免受盗用、破坏。百考试题编辑整理 （3）应用系统 办公系统文件(邮件)的安全存储：利用加密手段，配合相应的身份鉴别和密钥保护机制IC卡、PCMCIA安全PC卡等，使得存储于本机和网络服务器上的个人和单位重要文件处于安全存储的状态，使得他人即使通过各种手段非法获取相关文件或存储介质磁盘等，也无法获得相关文件的内容。 文件邮件的安全传送：对通过网络传送给他人的文件进行安全处理（加密、签名、完整性鉴别等），使得被传送的文件只有指定的收件者通过相应的安全鉴别机制IC卡、PCMCIA PC卡才能解密井阅读，杜绝了文件在传送或到达对方的存储过程中被截获、篡改等，主要用于信息网中的报表传送、公文卜发等。 F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com