

综合辅导之电子商务中的安全控制与管理策略电子商务考试
PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/559/2021_2022__E7_BB_BC_E5_90_88_E8_BE_85_E5_c40_559753.htm

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路从开放、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并自动调整，考试/大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，考|试/大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，使网管能检测和管理安全风险信息。

(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，操作系统安全性直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，通过不同版本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、数据免受盗用、破坏。

(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)，考|试/大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卡才能解密并阅读，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。

二、电子商务网络安全技术对策

1.使用网络监测和锁定监控

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形或文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该帐户将被自动锁定。通过分析记录数据，可以发现可疑的网络活动，并采取措施预先阻止今后可能发生的入侵行为。

2.对通信端口和通信线路进行保护

远程终端和通信线路是安全的薄弱环节，对目前已有各种各样的端口保护专用设备，要选择符合实际需要的技术先进的产品。对于通信线路，应尽可能埋在地下，并且尽可能采用光缆，因为光缆不存在因各种电磁辐射引起的电磁泄漏，而且抗干扰性能极好。若采用电缆，要抑制和防止电磁泄漏，目前主要措施有两类：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，可采用电磁屏蔽措施和干扰

方式的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

3.采用信息流安全控制 防止不法分子通过流量和流向分析手段来确定攻击的目标。这类安全控制包括：掩盖通信的频度、掩盖报文的长度、掩盖报文的形式、掩盖报文的地址。考|试/大具体方法是填充报文和改变传输路径。为掩盖报文地址，一般采用物理层的链路加密方式，为掩盖报文的形式，常采用带反馈的加密方式。

4.安装高性能的防火墙 防火墙是一个用以阻止网络中的黑客访问某个机构网络的屏障。如果内部网络要进入Internet，必须在内部网络与外部网络的接口处设置防火墙，在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入，确保内部网络中的数据的安全。在具体应用防火墙技术时，还要考虑两个方面：首先，防火墙是不能防病毒的，工作站是病毒进入网络的主要途径，所以应该在工作站上安装防病毒软件。其次，防火墙技术的另外一个弱点在于数据在防火墙之间的更新，如果延迟太大将无法支持实时服务请求。

5.采用访问控制 从计算机系统的处理能力方面对信息提供保护，它按照事先确定的规则决定主体对客体的访问是否合法。当主体试图非法使用一个未经授权的资源时，访问控制机制将拒绝这一企图，并将这一事件报告给审计跟踪系统。审计跟踪系统将给出报警，并记入日志档案。对于文件和数据库设置安全属性，对其共享的程度予以划分，通过访问矩阵来限制用户的使用方式。

6.采用数据加密技术 分为对称密钥加密技术和非对称密钥加密技术，对称密钥加密技术在发送方和接收方使用相同的密钥

，对数据使用相同的密钥进行加密和解密，如DES加密算法。在非对称密钥技术中，数据加解密的双方使用不同的密钥，但两个密钥之间拥有一个特定的关系:可以使用其中一个密钥进行加密，使用另外一个密钥进行解密，如RSA加密算法。电子商务是以互联网为活动平台的电子交易，它是继电子贸易(SDI)之后的新一代电子数据交换形式。计算机网络的发展与普及，直接带动电子商务的发展。因此计算机网络安全的要求更高，涉及而更广，不但要求防治病毒，还要提高系统抵抗外来非法黑客入侵的能力，还要提高对远程数据传输的保密性，避免在传输途中遭受非法窃取，以保证系统本身安全性，如服务器自身稳定性，增强自身抵抗能力，杜绝一切可能让黑客入侵的渠道等等。对重要商业应用，还必须加上防火墙和数抓加密技术加以保护。在数据加密方面，更重要的是不断提高和改进数抓加密技术，使不法分子难有可乘之机。编辑推荐：电子商务师考试复习方案电子商务师考试 - 电子商务员辅导电子商务师考试模拟试题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