电子商务中计算机网络安全技术的应用

辛鹏程

内蒙古鸿德文理学院　内蒙古呼和浩特　010110

摘　要: 电子商务乘着“互联网 +”东风，如今已经是“遍地开花”。可以说，电子商务模式已经深入渗透到生活中的方方面面，为广大网络用户带来切实的便利。与此同时，其中的网络安全问题也值得重视，如何发挥网络安全技术的作用，推动网络安全技术与电子商务的融合，多角度保证电子商务体系的绝对安全，是促进电子商务健康发展必须要解决的一道难题。本文以电子商务为对象，首先分析了常见的网络安全问题，随后总结了网络安全技术路径以及配套的措施。

关键词： 网络安全技术；电子商务；应用；策略

电子商务体系的健康发展，与计算机网络安全有着密切的关系。结合电子商务模式的实际情况，定位常见的网络安全问题，并采取合适的技术和策略，有效强化电子商务的网络安全属性，保证各方在电子商务模式中的正当权益，为电子商务的纵深发展奠定基础。鉴于网络安全的重要意义，有必要探讨电子商务范畴内的网络安全技术和措施。

1. 电子商务中的网络安全问题分析

1.1 数据安全问题

电子商务运行过程中的数据内容加密不到位，有可能导致数据泄露的情况。例如在电子商务体系运转阶段，部分网络数据被黑客用户截获，导致数据内容丢失或者被篡改。例如在电子商务体系运转阶段，部分网络数据被黑客用户截获，导致数据内容丢失或者被篡改。在数据信息被窃取的情况下，部分黑客可能假冒用户并发起诈骗行为，侵害其他电子商务用户的合法权益并造成无法追回的经济损失。导致电子商务交易数据泄露的原因有很多，用户在电子商务网络环境内的违规操作，同样会导致数据泄露问题。从电子商务健康运营的角度考虑，网站或者 APP 的管理者应当切实保护用户提交的个人信息。如果商家缺乏信息保护意识，间接增大用户信息的泄露概率，同样损害电子商务用户的合法权益。当前诸多电子商务平台的安全体系并不是十全十美的，不法分子利用电子商务平台中的漏洞，大肆窃取用户的数据信息和财产，并通过出售用户个人信息，为自己牟取不正当的利益。不可否认的是，网络安全人员在维护电子商务安全氛围方面做出了很多努力，但是交易环境非常复杂，未必解决全部安全问题，意味着用户个人信息理论上仍然有被窃取的概率，电子商务网络安全形势依然严峻。

1.2 网站与服务器隐患

网站是电子商务模式的重要载体，电子商务网站的业务处理、数据保存等任务则由服务器承担。如果电子商务的安全体系没有考虑到网站、服务器环节，同样意味着危机四伏。当前电子商务体系中的跨站注入漏洞、传输漏洞等问题，均与安全机制不到位有关。攻击者借助电子商务中的漏洞因素，侵入电子商务体系并获取用户数据和交易数据，带来的经济损失非常可观。用户自身安全意识不到位，同样导致网站隐患。例如用户设置的密码过于简单，很容易被不法分子识破并窃取，导致用户个人信息被篡改。服务器端的常见漏洞包括 SQL 注入漏洞等等，间接增大电子商务服务器崩溃的概率，并导致电子商务体系整体陷于瘫痪。

1.3 边界隐患

电子商务体系正常运转，与网络环境和数据因素关系密切。如果防护措施不到位，则会为不法分子带来很多入侵机会，并导致安全隐患。当前针对电子商务的攻击包括欺骗类攻击、探测类攻击等等。DDos 攻击的主要目的在于过量消耗电子商务平台的资源，造成电子商务体系内部数据流通不畅并导致电子商务瘫痪。关于电子商务中的欺骗类攻击，以伪造的信息为切入点，对电子商务体系中的用户形成欺骗效应，以 IP 地址欺骗、DNS 欺骗最为常见。控制类攻击的核心在于获得电子商务计算机设备的控制权，并由此发动进攻，常见的控制类攻击行为包括木马攻击、溢出攻击等等。还有一类攻击行为，在定位目标对象的基础上，广泛收集有关目标对象的各种信息，确定电子商务计算机系统中潜在的

问题，并作为进攻计算机设备的突破口，达到入侵电子商务体系的效果。另外，电子商务系统的计算机设备自身存在一些漏洞，为攻击行为提供了很好的突破口，攻击行为不仅具有针对性，同时更趋多样化。

1.4 用户设备隐患

任何一类计算机操作系统或多或少存在漏洞，意味着电子商务用户的操作环境并不是绝对安全的，理论上提升了病毒木马入侵的概率，计算机中的信息有可能会丢失。一旦外部不法因素入侵电子商务计算机系统，很难在短时间内定位计算机设备中的漏洞，间接增大了经济损失。只有高度重视电子商务计算机设备的漏洞，落实日常修复任务，方可最大限度消除计算机设备的安全隐患。

2. 网络安全技术的应用方式

2.1 数据加密技术

数据加密技术在电子商务体系中广泛应用，根据加密原理的不同，又可以细分为对称和非对称的数据加密。在对称数据加密的工作原理中，充分发挥对称密码编码技术的作用。由于数据加密技术的加密与解密过程使用相同的密钥，因此被定义为对称加密。使用对称密钥实现数据加密的效果，将电子商务明文信息转化为密文信息，借助网络环境实现加密文件的传输效果。接受方获取加密的文件后，借助密钥解密文件并获取电子商务明文内容，保证数据内容足够安全，避免电子商务信息被盗取的现象。关于电子商务中的非对称加密，工作原理中应用到公开与私有密钥，并完成电子商务信息的加密与解密任务。由于加密与解密过程存在非对称的特征，因此被称为非对称加密。在非对称加密算法体系中，对电子商务信息的加密与解密过程使用不同的密钥，最终获得解密后的电子商务明文信息。在电子商务网络安全体系中，通常结合使用两类算法，保证验证质量和效率。

2.2 身份认证技术

传统商品交易过程在线下进行，交易双方在现场直接面对面，互相得知对方的身份。电子商务交易模式的全部交易行为都在线上进行，双方并不能直接得知对方的身份，在电子商务交易全过程中，交易双方实际上很难见面，意味着身份认证成为电子商务安全体系的关键组成部分。借助身份认证技术，为保证电子商务交易中的身份安全奠定良好基础，确保参与交易双方的身份安全准确，并为指定的用户分配对应的资源。常见的身份认证方式是口令认证和标记认证，以口令认证方式最为常见。组成电子商务用户口令的因素包括字母、数字等等，严格保证用户身份识别的效果。在电子商务交易中，充分发挥身份认证模式的独到优势，为保证交易信息的绝对安全指明具体方向，避免电子商务交易双方的正当权益被损害，并推动电子商务体系的健康发展。

2.3 网络边界防护技术

在电子商务体系中运用访问控制模式，加强对网络边界的防护能力，实现不同网络环境之间的防护效果，严格保证内部网络环境的绝对安全。在电子商务体系中，充分发挥网络控制模式的独到优势，为电子商务信息安全奠定良好的基础。换言之，在访问控制模式的支撑下，真正在内外部网络环境之间实现了边界效应，有效降低电子商务体系内的安全风险。防火墙在电子商务体系的访问控制模式中扮演关键角色，并实现安全边界隔离效果，同样起到控制风险的作用。例如在电子商务体系中应用 IPS 技术，提升防火墙的实际性能。与此同时融合防毒软件与防火墙体系，形成电子商务的入侵防御体系。在入侵防御模式的支撑下，能够在最短时间内定位电子商务体系中的风险隐患，保证各类网络安全设备处于正常状态，实现电子商务网络的监视效果。借助入侵防御模式，增强对电子商务体系中各类行为的敏感度，对于异常行为或者判定为不安全的行为，及时拟定并采取相关对策，常见的对策类型有调整、中断等等。

2.4 服务器与网站防护技术

服务器和网站之间的顺畅交互，是电子商务体系正常运转的关键。在电子商务网站防护体系中，融合 Web 应用防火墙技术，保护电子商务的 Web 界面安全，提升 Web 界面抵御外部攻击的能力，并为电子商务体系的 Web 应用提供更有效的防护。Web 应用防火墙遵循 Http 策略，为 Web 程序提供有效的防护支撑。关于电子商务体系的服务器防护，涵盖了权限分配、安全配置等多个方面的要求，并关注到端口的状态。借助服务器防护体系，安全管理人员及时掌握电子商务服务器的安全状态。例如在电子商务后台服务器中安装杀毒软件，在落实常规维护任务的同时，还能增强对病毒的检测力度，提升电子商务的安全预防效果。

2.5 数字签名技术

电子商务安全体系需要发挥数字签名技术的作用，接收用户根据电子签名的内容判断对方的身份。与此同时，签名用户不能否认自己的签名行为，接收用户同样不能改变签名

后的文件。关于电子商务中的数字签名，具有密码变换的特征。以原始数据单元为基础，向其中增加新的数据，为接收用户确定数据来源提供重要依据，并实现数据的保护效果，从根本上避免了数据被偷窃或者破坏的现象。

2.6 防火墙技术

智能防火墙在网络安全体系中扮演关键的角色，在电子商务体系中起到虚拟屏障的作用。关于智能防火墙，本质上是软件和硬件的集合体。借助智能防火墙，将电子商务体系划分为多个区域，精准识别电子商务体系中的隐患因素。在智能防火墙的支撑下，及时侦察电子商务体系中的数据资料，在此基础上进行数据的过滤和筛选，进一步保障电子商务体系的安全。将防火墙技术覆盖电子商务交易的全过程，显著提升交易过程的安全系数。

2.7 密码协议

密码协议的应用效果，直接决定了电子商务用户的信息安全。在设计电子商务的密码协议时，要注意密码协议是否可靠，从而保证密码协议的实际性能。在电子商务抵御外来攻击因素的过程中，密码协议扮演非常重要的角色。电子商务的密码协议应当尽量简明，确保密码协议的应用价值。密码协议的设计应当吻合安全、公平的原则，例如将异步协议应用在电子商务的密码协议中，切实保障电子商务用户数据和资金的绝对安全。

3. 电子商务网络安全防范措施

3.1 建立病毒管理中心

针对电子商务体系中的病毒因素赋予定义码，并注意病毒定义码的更新。在电子商务体系内的计算机设备中安装防病毒软件，提升各类设备的防病毒能力，提升计算机网络的安全性能。管理人员根据电子商务体系的运转状况，创建并更改网络配置文件，增强电子商务计算机的病毒防御能力。与此同时做好病毒库的更新工作，有效应对网络环境中的新型病毒因素，避免计算机被病毒入侵。与此同时加大电子商务体系内的邮件监控力度，及时提醒用户不要操作危险页面。针对网络环境中的杀毒软件也要加强监控力度，快速拟定应对病毒的有效措施，避免电子商务计算机被破坏。

3.2 加大网络管理力度

电子商务网络环境的绝对安全，与网络管理力度有着密切的关系。在电子商务网络维护阶段，要有“主动出击”的意识，主动应对电子商务网络环境中的各种隐患因素，将病毒处理环节前置，及时遏制病毒扩散的局面，保证电子商务网络绝对安全。在电子商务网络安全工作中，要有“安全措施与安全技术”并举的意识，有效融合措施和技术，从容应对电子商务网络安全问题。电子商务网络管理人员也要结合安全工作的新形势，及时更新自己的技术储备，为应对更多、更复杂的安全问题提供有效支撑，有助于构建更加完善可靠的电子商务网络安全体系。在网络安全工作中，必须把“预防”摆在非常重要的位置，赢得处理网络安全问题的最佳时机。

4. 结束语

综上所述，电子商务已经成为社会经济循环乃至公众社交模式的重要组成部分，意味着网络安全防护任务还会更加繁重。由于电子商务形势瞬息万变，今后还要进一步总结网络安全技术的种类和应用方式，为电子商务的健康运转保驾护航。

参考文献

[1] 米志东 . 影响计算机网络安全技术的因素与实践措施 [J]. 科技与创新 ,2021,(16):123–124+128.

[2] 吴瑞 . 基于电子商务环境下的计算机网络安全技术应用探析 [J]. 电脑知识与技术 ,2022,18(10):31–33.

[3] 郝晓康 . 云计算技术在计算机网络安全存储中的应用 [J]. 中国新通信 ,2023,25(22):104–106.

作者简介：

辛鹏程 (1989–11–22) , 男 , 汉族 , 内蒙古土默特左旗 , 硕士研究生 , 助教、经济管理系党总支副书记 , 研究方向 : 计算机、电子商务安全技术方面。