计算机信息管理技术在维护网络安全中的运用

王翔宇
四川省机场集团有限公司成都天府国际机场分公司　四川　成都　610000

摘　要：计算机信息管理技术在维护网络安全中发挥着至关重要的作用。通过综合运用数据加密、防火墙配置、入侵检测、身份认证、访问控制、安全审计、日志管理、应急响应与恢复机制以及安全培训与意识提升等多种技术手段和管理措施，该技术能够有效地识别、防范和应对网络安全威胁，确保网络系统的稳定运行和数据的安全。本文深入探讨计算机信息管理技术在网络安全中的具体实践，为组织构建全面、高效的网络安全防护体系提供有益的参考。

关键词：计算机信息管理技术；网络安全；安全防护；数据管理

1 计算机信息管理技术概述

计算机信息管理技术，融合计算机技术和管理方法，旨在有效整合和管理信息资源，支撑组织决策与业务发展。其基本原理涵盖信息资源整合、信息化管理、数据安全及信息价值最大化。信息资源整合确保信息跨源跨部共享，信息化管理提升信息处理效率与准确性，实现动态管理。数据安全通过加密、权限控制、备份等措施，保障信息机密性、完整性和可用性。信息价值最大化则通过挖掘信息价值，促进决策和业务活动。该技术功能多样，包括信息采集、存储、检索、分析及报告生成，助力用户快速获取信息，提高决策准确性。数据分析揭示信息趋势，为决策提供依据。报告生成以可视化形式展示分析结果，支持业务活动。计算机信息管理技术广泛应用于企业管理、医疗卫生、金融服务、教育培训等领域。在企业管理中，它优化内部信息流，提升运作效率。在医疗卫生领域，它提高医院工作效率和服务质量。在金融服务中，它增强金融机构效率和风险管理能力。在教育培训中，它促进教育资源共享和优化[1]。随着计算机技术发展，该技术已成为各领域不可或缺的一部分，推动信息化建设和数字化转型。未来，面对人工智能、区块链、云原生架构等新技术挑战，计算机信息管理技术需不断创新以适应市场变化，为企业和社会发展提供更强支持。

2 网络安全与计算机信息管理技术的关联性分析

网络安全是指网络系统中的硬件、软件等受到保护，不被恶意破坏，能够持续稳定运行的一种状态，具有保密性、完整性、可用性、可控性以及可审查性。随着科技的飞速发展，网络已成为现代社会不可或缺的一部分，无论是个人生活还是企业运营，都高度依赖于网络，网络环境的开放性也为黑客攻击、病毒传播等提供了可乘之机，使得网络安全问题日益凸显。计算机信息管理技术则是针对网络信息的管理技术，包括IP地址管理、用户账号密码管理等多个方面。它的主要目的是促进信息的安全传播，保障网络系统的正常运行，并为用户提供稳定、可靠的网络服务。通过计算机信息管理技术，可以实现对网络信息的有效监控和管理，及时发现并处理潜在的安全威胁，从而确保网络的安全性和稳定性。在网络安全方面，计算机信息管理技术发挥着举足轻重的作用。一方面，它可以对网络中的数据进行加密处理，防止数据在传输过程中被窃取或篡改；另一方面，它还可以对用户的访问权限进行严格控制，防止未经授权的访问和操作，计算机信息管理技术还可以通过建立安全管理体系、加强网络安全意识教育等措施，进一步提升网络的安全性。

3 计算机信息管理技术在网络安全中的应用原理

3.1 数据加密技术

数据加密技术是计算机信息管理技术在网络安全中的核心应用之一。其基本原理是通过加密算法和密钥，将明文（原始数据）转换为密文，使得未经授权的用户无法解读数据内容，从而保护数据的机密性和完整性。数据加密技术的核心在于密码学，它分为加密和解密两个过程，加密是将明文通过加密算法和密钥转换为密文的过程，而解密则是通过解密算法和密钥将密文还原为明文的过程[2]。加密算法是公开的，但密钥必须保密。常见的加密算法包括对称加密算法（如AES）和非对称加密算法（如RSA）。对称加密算法使用相同的密钥进行加密和解密，效率较高；非对称加密算法则使用公钥和私钥，公钥用于加密，私钥用于解密，安全性更强。在实际应用中，数据加密技术通常用于数据传输和数据存储两个方面。数据传输加密技术确保数据在传输过程中不被窃取或篡改，常见的有线路加密和端-端加密两种方式。线路加密是在数据通过的线路上进行加密，而

端-端加密则是在数据发送端进行加密，在接收端进行解密。数据存储加密技术则确保数据在存储过程中不被非法访问或泄露，常见的加密方式包括密文存储和存取控制。密文存储通过加密算法将数据存储为密文形式，存取控制则通过审查用户资格和权限，防止非法用户访问数据。数据加密技术的优势在于其能够提供高强度的数据保护，即使数据被窃取，攻击者也难以解读其中的内容，数据加密技术也存在一些挑战，如密钥管理和分发、加密算法的选择和更新等。

3.2 防火墙与入侵检测系统

防火墙和入侵检测系统是计算机信息管理技术在网络安全中的另外两个重要应用。防火墙位于内部网络和外部网络之间，通过预定义的安全规则过滤进出网络的数据包，阻止潜在的威胁进入网络，同时允许合法流量通过。防火墙的工作原理基于包过滤技术，它会检查每个数据包的头部信息，包括源地址、目的地址、端口号等，并根据这些信息与预先设定的安全策略进行比较，只有符合规则的数据包才会被放行。防火墙的类型包括包过滤防火墙、应用级网关防火墙、状态检测防火墙和下一代防火墙（NGFW）。包过滤防火墙只检查数据包头部信息，应用级网关防火墙能够理解特定的应用层协议，并进行更深入的内容检查。状态检测防火墙结合了包过滤和应用级网关的优点，能够跟踪连接的状态，提供更高效且安全的服务。下一代防火墙则集成了应用识别、用户身份验证、入侵防御等高级功能。入侵检测系统（IDS）则是一种能够监控网络或系统的活动，寻找可疑行为或安全政策违规迹象的安全工具。IDS通过分析网络流量或主机系统的活动来检测异常行为，可以基于已知的攻击模式（签名）或通过行为分析来识别潜在的威胁。一旦发现潜在威胁，IDS会生成警报，并可能采取行动阻止入侵。IDS的类型包括基于网络的IDS（NIDS）和基于主机的IDS（HIDS），前者部署在网络的关键位置，监控整个网络的流量，后者安装在单个主机上，监控该主机上的文件和活动[3]。防火墙和入侵检测系统共同构成了网络安全的第一道和第二道防线。防火墙作为第一道防线，通过过滤机制阻止非法访问；入侵检测系统则通过监测网络活动，帮助组织及时发现并响应潜在的安全威胁。两者通常会协同工作，以提供更全面的保护。

3.3 身份认证与访问控制

身份认证与访问控制是计算机信息管理技术在网络安全中的关键应用之一。身份认证的方式包括用户名和密码认证、双因素身份认证、单点登录（SSO）、生物特征识别等。用户名和密码认证是最常见的身份验证方式，用户输入用户名和密码，系统验证用户提供的密码是否与存储在服务器上的密码一致。双因素身份认证则结合用户名和密码与其他身份验证因素，如指纹、智能卡等，提高身份验证的安全性。单点登录允许用户只需要进行一次身份验证，即可访问多个不同的系统。生物特征识别则通过扫描识别用户的生物特征，如指纹、虹膜等，用于验证用户的身份。访问控制的方式包括强制访问控制（MAC）、自愿访问控制（DAC）、角色访问控制（RBAC）和基于属性的访问控制（ABAC）等。强制访问控制基于安全级别和标签的访问控制模型，系统管理员通过设置标签和安全级别来限制资源的访问。自愿访问控制则允许用户拥有资源的所有权，并有权决定其他用户能否访问自己所拥有的资源。角色访问控制将用户分配到不同的角色中，每个角色拥有一组权限，用户通过分配给自己的角色来获得相应的权限。基于属性的访问控制则基于用户的属性和资源的属性进行访问控制，访问决策基于用户的属性、资源的属性和上下文信息。身份认证与访问控制共同确保系统的安全性。身份认证保证只有授权的用户能够访问系统，访问控制决定用户能够访问的资源和操作的权限。两者共同作用，防止未经授权的访问和操作，保护网络资源和系统的安全。

3.4 漏洞扫描与修复管理

漏洞扫描与修复管理是计算机信息管理技术在网络安全中的另一个重要应用。漏洞扫描技术通过远程检测目标主机TCP/IP不同端口的服务，记录目标的回答，搜集目标主机的各种信息，并与网络漏洞扫描系统提供的漏洞库进行匹配，如果满足匹配条件，则视为漏洞存在。漏洞扫描技术可以发现系统中的安全漏洞和错误配置，帮助网络管理员及时更正漏洞和错误设置，防止黑客利用漏洞进行攻击。漏洞扫描技术的原理包括基于端口扫描的漏洞扫描和基于模拟攻击的漏洞扫描。基于端口扫描的漏洞扫描通过扫描目标主机的TCP/IP端口，搜集目标主机的服务信息，并与漏洞库进行匹配。基于模拟攻击的漏洞扫描则通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等[4]。漏洞扫描技术的类型包括基于应用的检测技术、基于主机的检测技术和基于网络的检测技术，基于应用的检测技术检查应用软件包的设置，发现安全漏洞。基于主机的检测技术对系统进行检测，涉及系统的内核、文件的属性、操作系统的补丁等。基于网络的检测技术则通过一系列的脚本模拟对系统进行攻击的行为，然后对结果进行分析，发现系统的漏洞。漏洞扫描与修复管理是一个持续的过程，需要定期进行漏洞扫描，及时发现

并修复漏洞。还需要加强系统的安全配置和更新管理，防止新的漏洞产生。漏洞扫描与修复管理能够提升系统的安全性，减少被黑客攻击的风险。

4 计算机信息管理技术在网络安全中的具体实践

4.1 网络安全策略制定与实施

在计算机信息管理技术中，网络安全策略的制定与实施是确保网络安全的基础。具体实践中，网络安全策略的制定通常包括几个步骤：首先，对网络架构、应用程序、数据存储等进行详尽的审查，以确定可能存在的安全漏洞和弱点；其次，基于审查结果，结合行业标准和最佳实践，制定一套详细的安全策略，包括访问控制策略、密码策略、数据保护策略等；最后，将这些策略转化为可操作的流程和规范，通过技术手段和管理措施确保策略的有效实施。实施网络安全策略的过程中，还需要建立持续的监控和评估机制，以确保策略的有效性和适应性。这包括定期审查策略的执行情况，收集和分析安全事件数据，以及根据评估结果对策略进行必要的调整和优化。

4.2 应急响应与恢复机制

应急响应与恢复机制是计算机信息管理技术在网络安全中的关键实践之一。在应急响应与恢复机制的具体实践中，组织通常会制定详细的应急预案，包括应急响应的流程、责任分工、资源调配等。这些预案通常会涵盖不同类型的网络攻击和故障场景，以确保在发生安全事件时能够迅速做出正确的应对。组织还需要建立应急演练机制，定期对应急预案进行演练和评估，以检验预案的有效性和可操作性。通过演练，组织可以熟悉应急响应的流程和方法，提高应急响应的速度和准确性[5]。在恢复机制方面，组织需要建立数据备份和恢复策略，确保在发生数据丢失或损坏时能够迅速恢复数据。同时还需要建立系统恢复策略，包括系统重装、配置恢复等，以确保在发生系统故障时能够尽快恢复系统的正常运行。

4.3 安全培训与意识提升

在安全培训的具体实践中，组织通常会针对不同岗位的员工制定个性化的培训计划，包括安全政策培训、安全技能培训、安全操作培训等。这些培训通常以线上或线下的形式进行，包括讲座、案例分析、模拟演练等。除了培训外，组织还需要通过定期的安全意识宣传活动、安全知识竞赛等方式，提高员工对网络安全的认识和重视程度。这些活动可以帮助员工了解最新的安全威胁和攻击手段，掌握基本的安全防范技能，并在日常工作中养成良好的安全习惯。为了评估安全培训和意识提升的效果，组织还需要建立相应的评估机制，包括培训后的考核、员工安全行为的观察等。通过评估，组织可以了解员工的安全意识和技能水平，以及培训的效果和不足之处，进而对培训和宣传策略进行必要的调整和优化。

结束语

计算机信息管理技术在维护网络安全中具有不可替代的重要性。随着网络技术的不断发展和安全威胁的日益复杂，组织需要不断更新和完善其网络安全防护体系，充分利用计算机信息管理技术的优势，提升网络安全防护的智能化和自动化水平。加强员工的安全培训和意识提升，形成全员参与、共同维护网络安全的良好氛围，为组织的稳健发展提供坚实的安全保障。

参考文献

[1]齐雪.浅谈计算机信息管理技术在网络安全中的应用[J].中国新通信,2023,25(1):91-93.

[2]吴蒙.网络安全中计算机信息管理技术的应用[J].信息与电脑(理论版),2022,34(22):216-218.

[3]孙丽丽.计算机信息管理技术在网络安全中的运用研究[J].电脑爱好者(普及版),2021(2):19-20,27.

[4]唐维杰.计算机网络技术在医院信息化建设中的应用分析[J].数字技术与应用,2020,38(6):60-61.

[5]许阳春.医院信息管理中计算机数据库技术的应用研究[J].中国新通信,2020,22(3):89-90.