

基于网络信息安全技术管理的计算机应用探析

赵洪岩

沈阳科技学院 辽宁省沈阳市 110000

摘要: 现阶段, 随着我国经济的快速发展, 计算机的应用越来越受到关注。计算机都是集合网络技术应用的, 也就是计算机网络技术, 而计算机网络应用中的一个关键点就是保障计算机网络信息的安全性, 这就需要开展落实计算机网络信息安全技术管理, 为计算机应用提供安全的环境。因此, 本文重点研究基于网络信息安全技术管理的计算机应用, 旨在为计算机及计算机网络的更好应用提供有力的支持与依据, 确保计算机及计算机网络的作用得到更好发挥。

关键词: 网络信息; 安全技术; 计算机; 应用

引言:

随着互联网的发展, 越来越多的人开始使用计算机进行各种活动, 如在线购物、网上银行和社交媒体等等。然而, 这些活动也带来了新的风险, 比如黑客攻击、病毒感染以及数据泄露等问题。因此, 需要一种有效的方法来保护计算机系统免受这些威胁的影响。

1. 基于网络信息安全技术管理特点

随着互联网的发展, 网络安全问题也日益突出。网络信息安全技术是保护数据和系统免受攻击的一种方法, 它包括了各种不同的技术, 如加密、访问控制、身份验证等等。这些技术可以帮助确保数据不会被窃取或篡改, 它们还可以防止未经授权的人员进入到系统中^[1]。在网络信息安全领域, 有一些重要的特点需要特别注意。首先, 安全性是一个复杂的概念, 涉及到多个方面。例如, 要保证系统的稳定性、可靠性以及可用性, 同时又不能让用户的数据泄露出去。其次, 网络信息安全技术必须能够适应不断变化的技术环境。因为新的威胁层出不穷, 因此需要不断地更新和改进防御措施。最后, 网络信息安全技术应该具有可扩展性和灵活性的特性。这意味着可以通过增加新功能来提高系统的性能和效率。

2. 基于网络信息安全技术管理的计算机实际应用

2.1. 防火墙技术

防火墙技术是计算机应用安全性的重要组成部分, 它通过对数据包进行分析和过滤, 防止恶意软件或攻击者从外部入侵系统内部。在实际应用中, 防火墙可以被用于保护企业网路、个人电脑以及移动设备免受病毒、木马和其他威胁。

防火墙的基本工作原理是在输入端口处检测到的数据包是否符合特定规则, 如果不符合则会被拒绝进入系统。这种方法被称为“白名单”。另一种方式则是使用黑名单, 即将不允许的数据包直接拒绝掉。这两种方法都可以有效地阻止黑客攻击, 但也存在一些局限性。例如, 当一个新漏洞被发现时, 需要及时更新防火墙以应对新的威胁。由于防火墙只能识别已知的攻击类型而无法预测未知类型的攻击, 因此也存在着一定的风险^[2]。尽管如此, 防火墙仍然是一种重要的安全措施。对于企业来说, 安装并维护好防火墙是非常必要的, 因为一旦受到攻击可能会导致严重的损失, 个人用户也可以选择购买专业的防火墙产品来保护自己的隐私和财产安全。

2.2. 入侵检测技术

入侵检测技术是用于识别和阻止未经授权访问或攻击计算机系统的一种方法, 它可以帮助保护敏感数据免受恶意软件和其他威胁, 并防止黑客从外部获取控制权。入侵检测技术通常使用多种方式来监测和分析计算机系统的活动, 以发现潜在的入侵行为。这些方法包括: 流量监控、端点扫描、协议审计以及其他各种类型的监视器。在实际中, 入侵检测技术被广泛地运用于企业级网络环境中, 因为它能够有效地提高安全性, 减少风险, 降低成本。随着越来越多的企业开始采用云计算服务, 入侵检测技术也成为了一个重要的工具, 因为云环境具有更高的可扩展性和灵活性, 因此需要更加严格的数据安全措施。

2.3. 虚拟专用网技术

虚拟专用网 (VLAN) 技术是用于在局域网中实现多用户访问和资源共享的一种技术, 它通过将物理链路划分为多个

逻辑链路,从而可以对不同的用户或应用程序进行隔离,以保护数据传输的安全性。这种技术的主要优点在于能够提高网络性能,减少网络拥塞,并提供更好的网络控制能力。此外,该技术还可以有效地降低网络攻击的风险,因为每个用户只能访问自己的区域内的资源,而不能进入其他区域。因此,VLAN技术是一种非常实用且有效的安全技术,适用于各种类型的企业网络。

2.4. 防病毒技术

在计算机应用中,防病毒技术是一种重要的安全措施,它可以防止恶意软件和病毒对系统造成损害。防病毒技术包括多种方法,如反病毒软件、杀毒软件以及其他类型的防护工具。这些工具能够检测并清除潜在的威胁,以确保系统的安全性。此外,防病毒技术还可以通过监控文件传输来保护数据免受未经授权访问的风险。因此,对于任何需要进行网络通信的企业来说,防病毒技术都是必不可少的一部分。防病毒技术的主要作用是识别和删除恶意程序或病毒。这种技术通常使用扫描器来检查电脑中的所有文件,以确定它们是否包含可疑内容。一旦发现有可疑的内容,该技术会立即采取行动,例如将其隔离或者直接删除。此外,许多防病毒技术还具有实时更新的功能,以便及时应对新的攻击方式。尽管防病毒技术已经取得了很大的进展,但仍然存在一些挑战。由于病毒不断变化,所以防病毒技术也必须不断地升级才能保持有效的,某些病毒可能会伪装成合法的程序,从而使防病毒技术无法识别它们。此外,有些病毒可能已经被设计为破坏特定的设备,而不是单纯的破坏整个系统,在这种情况下,防病毒技术很难发挥其全部功效。

2.5. 网络安全扫描技术

随着互联网的发展,越来越多的人开始使用它。然而,由于网络上的恶意软件和黑客攻击的存在,网络安全问题也日益严重。为了保护用户的数据隐私以及防止网络攻击,需要采取一些有效的措施。其中之一是网络安全扫描技术是一种用于检测并修复潜在漏洞的技术。通过对系统进行全面扫描,可以发现可能存在的威胁,例如病毒、木马、蠕虫等等。一旦被发现,就可以及时采取相应的措施来消除这些隐患。在实际中,网络安全扫描技术通常分为两种类型:静态扫描和动态扫描。静态扫描是指在没有运行程序的情况下进行扫描;而动态扫描则是指在运行过程中实时扫描。这两种方式都有其优缺点,具体取决于具体情况。总之,网络安全扫描

技术对于保障网络安全至关重要。只有不断完善和升级这种技术,才能更好地应对各种网络威胁。

3. 基于网络信息安全技术管理的计算机应用策略

3.1. 创建计算机网络安全防御系统

为了保障计算机网络的信息安全,需要采取一系列有效的措施进行防范和保护。其中之一就是建立一个完整的计算机网络安全防御体系。计算机网络安全防御体系的构建是一个复杂的过程,涉及到多个方面的技术和知识。第一,需要明确计算机网络安全防御的目标和范围,确定所需要的技术手段和资源投入。第二,需要制定详细的工作计划和时间表,确保整个建设项目按时完成。最后,还需要不断完善和升级计算机网络安全防御系统,以应对新的安全威胁和挑战。在计算机网络安全防御系统中,硬件设备是至关重要的一部分。选择合适的防火墙、入侵检测器、反病毒软件等硬件产品可以有效提高计算机网络安全性能。同时,还应该注重人员培训和意识教育,增强员工对于计算机网络安全问题的认识和责任感。只有这样才能真正地保证计算机网络的信息安全。第三,建立计算机网络安全防御系统是非常必要的,它能够有效地预防和解决计算机网络中的各种安全问题。通过合理的规划和实施,可以为计算机网络提供更加可靠和稳定的保障,从而更好地服务于社会的发展和进步。

3.2. 增强信息安全防护意识

首先,政府应该加大宣传力度,向公众传递正确的信息安全保护理念和方法,引导广大群众树立正确的信息安全观念。其次,企业也应当加强自身的信息安全管理工作,建立完善的信息安全体系,确保员工的信息安全教育培训得到落实。此外,个人用户也要意识到自己的重要性,采取有效的措施保障自身信息安全,如设置强密码、不随意下载陌生软件等等^[3]。除了以上这些方面外,还需要注重加强信息安全防护技术的应用与创新。例如,采用先进的加密算法进行数据传输和存储,使用防病毒软件及时检测并清除恶意程序等。同时,需要加强对信息安全领域的研究和发展,不断推出新的信息安全产品和服务,以满足不同层次的需求。因此,加强计算机网络信息安全防护的对策是一项长期而复杂的任务。只有通过全社会的共同努力,才能够真正实现信息安全的全面提升和稳定发展。

4. 结语

综上所述,网络信息安全技术管理在计算机应用中具

有不可或缺的作用，只有通过加强网络安全意识和建立科学的管理机制，才能更好地保护计算机应用系统，防范各种潜在威胁和风险。同时，培养更多的专业人才和加强技术创新也是至关重要的，这将为构建更安全、更可靠的网络信息环境提供有力支撑。总之，在未来的发展中，必须始终保持高度警惕，不断优化和完善网络信息安全技术管理，共同构筑一个安全可信赖的计算机应用空间。

参考文献：

[1] 唐宇. 人工智能在计算机网络技术中的应用研究 [J].

网络安全技术与应用, 2020(9):107-108.

[2] 徐海东. 基于网络信息安全技术管理视角下的计算机应用 [J]. 卫星电视与宽带多媒体, 2020(11):127-128.

[3] 邢凯. 网络信息安全技术管理与计算机应用的相关研究 [J]. 信息记录材料, 2020, 21(2):217-218.

作者简介：

赵洪岩 (1995.02-), 男, 汉, 辽宁海城人, 硕士, 沈阳科技学院助教, 主要研究方向为无人机自组织网络 (UAV Ad Hoc Network, UANET)。