

基于大数据时代计算机网络安全技术应用探讨

马云贤

(山东省成武县技工学校 山东 菏泽 274200)

[摘要] 目前,现代化建设的发展迅速,我国的网络安全建设的发展也越来越迅速。人类社会已步入大数据发展时代,大数据的广泛运用带动了计算机技术的应用与普及。随着网络化的创新与发展,大数据完全融入于人们生活的方方面面,大数据信息的广泛应用,使数据、资源、信息实现共享,但也使计算机网络出现诸多的安全隐患。如果不加强对计算机网络信息安全的保护,一旦信息被不法分子窃取,将会造成非常严重的后果。因此,在大数据背景下,我们应加强对计算机网络安全保护,找出影响计算机网络安全因素,并针对这些问题采取有效措施,提高计算机网络安全性与稳定性,从而为计算机网络安全健康发展营造一个良好的环境。

[关键词] 大数据时代; 计算机网络; 安全技术; 应用探讨

引言

目前我国已全面进入信息时代,计算机及网络覆盖到人们工作、生活的方方面面,成为一项基础性工具。网络环境开放程度较高,且当前有关网络环境监管的法律法规还不完善,在计算机网络应用过程中常出现信息泄露、信息篡改等网络安全问题,给单位或个人造成重大经济损失。计算机网络安全已成为相关领域健康发展的急需解决的问题,总结网络安全漏洞及防范措施,有利于计算机网络安全水平的提升。

1 大数据技术和计算机网络安全技术整合的必要性

网络安全分析的数据量正从TB朝着PB发展,数据的内容更加细化、数据分析的维度更为多元、信息数据的发送速率也在逐步提升,0day等漏洞日益增多,多阶段组织APT攻击发生也越发频繁,对计算机网络安全提出了更高要求。传统计算机网络安全技术在数据储存方面主要采用“结构化数据库”,数据的储存成本相对较高。储存时间较长的数据容易丢失,寻本溯源较为困难,尤其是对体量较大、降噪较为困难的数据,分析效率极为低下,数据分析的准确性也难以得到保障。大数据技术支持海量非结构化数据的整合、分析、储存、计算,相较于传统的数据库分析技术,处理成本更低、安全投入更低、对于非结构化数据的分析效率更高、检测的相应速度更快。同时,大数据技术能够实现精准化挖掘,支持对多维度非结构化数据的关联性分析。大数据技术和计算机网络安全技术的整合是必然的发展趋势。

2 大数据时代计算机网络安全技术应用

2.1 加强网络安全防范,防止病毒入侵

为了提升网络安全防范能力,防止网络病毒入侵,有关企业必须要着手开发和设计更加优质的病毒检测和控制杀毒技术。用户通过安装相应的网络安全技术软件,进行定期的检测和杀毒工作,全面排除日常网络生活中存在的病毒,从而提升网络生活质量。在研发杀毒软件时,有关技术人员一定要保证后台检测和杀毒技术,在最大限度内,方便用户的网络生活。另外,在实际检测与杀毒过程中,一定要做到精准打击病毒,切不可因怀疑而执行杀毒,从而避免破坏用户的数据信息,或使用户数据信息丢失的情况出现。

2.2 定期进行漏洞扫描

定期进行漏洞扫描是计算机网络安全漏洞防范的最直接措施,对计算机运行空间进行扫描和分析,及时发现恶意入侵、攻击行为,监测信息的合法性与合理性,第一时间进行漏洞修复,避免带来更严重的计算机网络安全问题。计算机系统中的数据交换通过服务器及核心硬件响应、申请及应答完成,漏洞扫描能够有效检测安全漏洞并对其进行控制,模拟计算机安全防护缺陷,指导系统管理人员安全防护系统优化工作的开展。漏洞扫描技术包括Ping扫描技术、端口扫描技术、弱点探测技术等。例如,Ping扫描技术以计算机主机IP地址为监测目标,判断计算机端口网络状态及服务条件是否处于正常范围,以此对计算机网络安全情况进行分析。在使用Ping扫描技术时,需定期进行技术升级,提高技术性能,确保其能够有效识别新型

病毒。使用时,适当扩大漏洞扫描范围,并确保扫描后计算机环境质量,提升计算机网络安全。

2.3 提升计算机自身的抵御能力

大数据时代,计算机更容易遭受病毒的入侵,导致系统瘫痪,给用户造成不必要的麻烦。因此,要加强计算机自身对病毒的抵御能力,如果计算机被病毒入侵,首先要对病毒进行分析,有针对性地对病毒进行查杀。在防御病毒方面,防火墙的安装时非常有必要的,可以配置更高级别的防火墙,对自己最重要的信息设置更高级别的保护。当前,防火墙种类很多,有软件防火墙、硬件防火墙、芯片级防火墙。其中,芯片级防火墙基于专门的硬件平台,没有操作系统,相比于其他防火墙有速度更快、处理能力更强、性能更高等特点。

2.4 学校计算机机房的网络安全防范措施

①提高管理人员的安全意识。机房管理人员是高素质的技术人员,在对机房的管理上除了对机房的日常看得到的隐患做好清理,还要关注来自网络上的安全隐患,做到这一点就要要求机房的管理人员有很高的职业道德。要定期的做好机房的维护工作,给电脑及时的安装和更新杀毒软件或者防火墙。这些都是管理人员必须做到的事情。②网络访问权限。做好对网络的访问权限是保证计算机网络安全的重要手段,设置权限可以保证没有被授权和非法的用户不能访问,这样既做到了信息的内部交流,又做到了就计算机网络安全的信息安全。在一般的机房网络中都有内部的信息是关系到相关单位的生存的,而有些信息的存在是不可以公开的,这样的信息就是需要高度隐秘的,而针对计算机网络的开放性、信息共享以及安全性不高等的特性,加强网络访问权限是一种保证信息安全,数据内部共享的重要做法。③数据库内容的备份。数据库信息内容的备份是保证数据完整性和安全性的重要做法。这样可以防止信息在被篡改或者窃取之后及时的恢复信息的做法。特别是数据库的容量比较大的时候做好数据库内容的备份是不影响单位正常工作的重要做法。而在日常的机房网络安全管理中主要采取的方法是只备份数据库、对数据库和事务日志都进行备份以及增量备份等三种备份的方式。而在进行备份的时候要根据实际情况采用最合理的备份方法。

结语

综上所述,在大数据时代的计算机网络安全面临着全新的考验,应积极探索新方法,提高解决计算机安全问题能力,明确威胁有哪些,并对其进行分析,尽快制定出合理的解决方案。与此同时,用户也要加强防范意识,做好一切防范措施,不给不良分子可乘之机,切实保障自身利益不受损害。

参考文献

- [1]李国园.大数据时代计算机网络安全防范策略[J].科技创新与应用,2019(22):131-132.
- [2]张富成.大数据时代计算机网络信息安全及防护策略探讨[J].电脑知识与技术,2019,15(17):49-50.

浅谈多媒体教学技术在小学数学教学中的应用

计幼华

(江西省上饶市鄱阳县油墩街镇西湖小学 江西 上饶 333119)

[摘要] 现代信息技术的飞速发展和教育改革的逐步深化促使教育工作者逐渐转变教学思路、改变现有课堂教学模式,引进多媒体技术,任课教师必须充分利用多媒体技术直观性强、表现形式丰富多样、贴近学生生活的特性开展数学教学,提升小学数学教学效果,强化学生自主学习能力,在传授给学生数学知识的同时培养学生核心素养,为学生全面发展打下坚实基础。本文对小学数学课堂引进多媒体技术的现实意义进行了分析,明确指出应用多媒体技术为课堂教学带来的问题,以及部分教师使用多媒体技术的误区,并提出了合理利用多媒体技术提升教学效果的策略。

[关键词] 多媒体技术; 小学数学教学; 应用策略

前言

随着信息技术普及应用,人们的日常生活面貌发生了巨大变化,学生学习数学知识也有了新途径和新方法,小学数学课堂教学模式也发生了改变,传统黑板授课被立体投影、电子屏幕教学所取代,多媒体技术成为了课堂教学不可或缺的重要工具,逐渐融入了数学教学模式之中。现代多媒体技术能够为任课教师提供丰富多样的网络教学资源,教师可充分利用该技术搜集整理各类可用素材(网上电子课件、音频视频、教学动画等),为数学教学添加新内容,使学生保持注意力集中,唤起学生学习数学知识的热情,教师通过多媒体技术深入讲解学生所学知识的重点,将数学知识形象直观地展现在学生面前,极大地降低了学生学习数学的难度,提升了学生学习效率,使课堂教学效果得到了切实保证。

1. 引进多媒体技术改进小学数学课堂教学的现实意义

1.1 丰富课堂教学内容,调动学生学习积极性

由于多媒体技术具备各种各样的信息表达方式,任课教师利用该技术涵盖音频、视频、图像等不同传播媒介的特点,能够调动学生的学习积极性,处于心智未成熟阶段的小学生难以理解形式单一的数学理论知识^[1],但是对引进多媒体技术后教师展现的形式丰富的教学内容充满兴趣,唤起了学生的学习兴趣,课堂教学效果就得到了保障。

1.2 提升课堂教学效率,培育学生核心素养

多媒体技术的应用极大地改变了小学数学课堂教学,使传统的灌输式单向教学被新的直观生动、形式多样的互动式课堂教学模式所取代^[2],任课教师利用多媒体技术搜集与教学主题有关艺术文字、动画图片、音视频等可用教学素材,经整理后可在现实课堂上为学生集中展现以多种形式表达的数学知识,以此加深学生对数