

结语

“互联网+”背景下以有效性教育实施,优化创新创业教育的体系,对高校的创新创业教育的革新十分必要,能够拓宽创新创业教育的途径,助力于大学生群体创新创业能力、思维、素养全面性、科学性的培养,进而提升大学生群体的创新创业教育的质量。因此,“互联网+”背景下,开展人机交互的“双创”教育,推进“互联网+教育”在大学生群体中的创新创业教育中落实,进而实现创新创业教育的革新化。

参考文献

[1]郭光根.“两山”理念下涉林高职院校创新创业教育模式构建研究[J].黑龙江

江工程学院学报,2020,34(05):76-80.

[2]徐新洲.以“两融合”驱动“双一流”高校创新创业教育研究[J].学校党建与思想教育,2020(20):70-72.

[3]曾嘉懿.民办高校第二课堂背景下创新创业型人才培养模式研究[J].农家参谋,2020(24):184+187.

作者简介:

余晓钊(1982.7),男,汉族,广州增城人,学历:本科,职称:讲师,从事高校学生思想政治教育和高校党建工作,大学生创新创业教育教学,高校学生管理、班级管理、校园文化。

浅谈校园网络安全防控

张正厅

(四川司法警官职业学院 四川 德阳 618000)

[摘要]近些年,随着计算机网络技术的成熟,计算机网络应用迅速普及,各大院校及中小学相继建成或正在建设校园网。校园网的建成,使学校实现了管理网络化和教学手段现代化,这对于提高学校的管理水平和教学质量具有十分重要的意义。但随着计算机网络资源共享的进一步加强,信息安全问题也日益突出。在校园网络及其信息如何设置自己的安全措施,使它安全、稳定高效的运转,发挥其应有的作用,成为各学校越来越重视的问题。因此,为了保护数据和资源的安全,校园网应该考虑安全问题及防护策略。

[关键词]校园网络;安全;问题;防范策略

[DOI] 10.12252/j.issn.2096-6288.2020.07.480

前言

校园网普遍应用于高校信息数据管理,在接入Internet同时,各种各样的安全隐患也日益突出,给高校的教学、科研、管理和对外交流带来不可估量的影响。该文针对高校校园网现状,提出了加强校园网网络安全的主要措施。

随着《中华人民共和国网络安全法》在2017年6月的全面实施,网络安全成为我们各个行业都非常重视和重要的关注点,尤其是教育行业的校园网络安全。校园网络安全问题是一个较为复杂的系统工程,我们必须综合考虑各种安全因素,制定合理的技术方案和措施,确保网络和系统的正常运转;建立严格的局域网管理制度和机房管理制度,杜绝人为因素造成的网络安全问题。

一、校园网络安全现状

(一)网络安全设备短缺

学校在建立自己内网时,出于意识薄弱,或经费投入不足等多方面的原因,在网络安全方面的投入严重不足,从而导致校园网络处在一个开放状态,缺少安全预警手段和防范措施。

(二)网络信息安全意识淡薄、管理制度不完善

主要表现在:U盘、移动硬盘、手机等存储介质随意使用;学校机房的登记管理制度不健全;学校师生上网身份无法唯一识别,不能有效地规范和约束非法访问行为;缺乏统一的网络出口、网络管理软件和网络监控、日志系统;因此造成对上网行为没有有效的监控和记录;大量教学和档案管理的重要数据,随时存在被损坏、丢失和被窃取。

(三)各种应用软件不可避免的存在“漏洞”或“后门”

大部分的黑客入侵网络事件就是由系统的“漏洞”及“后门”所造成的。网络中所使用的网管设备和软件绝大多数是免费“拿来”品,加上系统管理员以及终端用户在系统设置时可能存在各种不合理操作,在网络上运行时,这些网络系统和接口都相应增加网络的不安全因素。

二、校园网络安全对策

(一)采用软硬结合的方式

1、根据学校实际的网络现状添配硬件防火墙。通过添加满足现状需求的防火墙对网络中的数据访问进行限制,提供对系统的访问控制和安全策略,防止不安全的数据访问和服务。

2、为设备安装软件防火墙:软件防火墙成本较低,安装方便,使用简单,能够满足个人用单机防护的基本需求。包括防黑客攻击、保证信息安全、监测计算机运行状况等功能。

(二)安全设备要求和所需主要技术

1、设备硬件用于网络的入口处,要内嵌内容过滤、病毒过滤技术。安装杀毒软件,及时杀毒升级,确保校园网络运行安全。

2、设备要提供行为审计与行为监控功能,对经过该设备的多种数据进行扫描,有效防止外网流入的病毒、蠕虫病毒攻击。

3、高效使用入侵检测(IDS)和入侵防护系统(IPS)技术通过执行应用层的策略进行数据阻断。引进VLAN划分技术,实现非法访问的有效限制,不断提升网络

通信效率

(三)加强校园网安全管理措施

1、制定合理的管理制度。校园网管理员通过对校园师生用户设置用户名和口令加密验证,加强对网络的监控以及对用户的管理。网管理员要对校园网内部网络设备路由器、交换机、防火墙、服务器的配置均设有口令加密保护,赋予用户一定的访问存取权限、口令字等安全保密措施,用户只能在其权限内进行操作,合理设置网络共享文件,对各工作站的网络软件文件属性可采取隐含、只读等加密措施,建立严格的网络安全日志和审查系统,建立详细的用户信息数据库、网络主机登录日志、交换机及路由器日志、网络服务器日志、内部用户非法活动日志等,定时对其进行审查分析,及时发现和解决网络中发生的安全事故,有效地保护网络安全。

2、对于管理人员要定期进行培训。加强对使用人员的管理,包括对用户和管理人员进行网络安全教育培训,尤其是新生,提高遵守相关安全制度的自觉性,增强整体安全防范能力。

三、开展网络安全知识竞赛,提高师生的网络安全技能

为增强学生的网络安全意识,学校可以组织各种形式、各种规模的网络安全知识竞赛。通过竞赛,提升广大师生的网络安全技能。在现在的网络安全知识竞赛的赛程设计上,决赛的考查方式众多,常见的包括选择题、技能分析题和冲击金银铜牌的特殊题。选择题涉及的主要范围包括网络安全原理的大部分领域,包括网络安全道德、网络嗅探、防火墙等,其主要考查的是基础理论知识;技能分析题则主要考查学生的实际操作能力,涉及的内容主要包括密码破解、日志分析等;金银铜牌的特殊题则是指学生可针对各种漏洞的靶机构成,发现其漏洞,并能成功攻入该系统,冲击大赛的奖牌。通过安全知识竞赛,既提高了学生的学习兴趣,又增加了参赛选手的核心竞争力,为其日后工作和创业奠定了扎实的基础。

校园网络安全问题是一个较为复杂的系统工程,我们必须综合考虑各种安全因素,制定合理的技术方案和措施,确保网络和系统的正常运转;建立严格的局域网管理制度和机房管理制度,杜绝人为因素造成的网络安全问题。

随着网络技术的不断发展,新的安全问题又将不断出现,如何长期保障校园网高效可靠的运行将对网络管理者提出更高的要求,这就需要我们不懈地努力,随时掌握最新的网络安全技术,不断地更新和完善校园网的安全体系,才能使校园网的运行更加稳定可靠。总而言之,校园网络安全是一个系统工程,具有较强的变动性和复杂性,因此,想要加强其安全管理,需要相应的工作人员不断改变传统的管理方式和理念,提升自己的信息技术水平,在采用传统的追堵和拦截的方式时,不断开发新技术,采用新手段,以应对不断涌现的计算机网络安全问题和安全威胁。

参考文献

[1]李卫.计算机网络安全与管理[M].清华大学出版社,2004.

[2]孟晓明.网络信息的安全问题与安全防护策略研究[J].情报杂志,2004(3).

[3]马骏,周君仪.浅谈校园网网络安全及防范技术[J].计算机科学与信息技术,2007(9).

人工智能在计算机网络技术中的应用研究

黄锐活

(海南师范大学 海南 海口 571158)

[摘要]计算机网络技术在各个行业领域中都有应用,对人们的生活和工作具有重要的意义,人工智能技术是其中非常关键性的技术,能够实现计算机网络环境的合理化调整,还能解决一些计算机网络问题,促进计算机网络技术的现代化发展。人工智能技术在计算机网络技术中的应用是现代人们发展的需求,具有很多的应用优势,本文将人工智能在计算机网络技术中的应用优势进行详细分析,并对人工智能在计算机网络技术中的具体应用进行深入探析,逐渐实现信息共享,为相关的行业领域的智能化发展提供有力的基础。

[关键词]人工智能;计算机网络技术;应用

[DOI] 10.12252/j.issn.2096-6288.2020.07.481

引言

人工智能在计算机网络技术中具有非常重要的应用意义,实现了计算机网络技术的完善,在功能方面也在不断创新,促进计算机网络技术朝着智能化、专业化的方向不断前进,计算机网络技术作用于人们的生活和生产中,具有较高的应用价值。下面将对人工智能在计算机网络技术中的应用相关内容进行深入探析,发挥人工智能在计算机网络技术中的应用价值,为人们提供更多的便利。

1、人工智能在计算机网络技术中的应用优势分析

模糊逻辑是一种方法和工具。不确定、不精确信息的表示和分析是通过模仿人的思维方式来实现的,现实世界中的模糊不清并且亟待解决的问题都可以尝试运用模糊逻辑理论来解决。将人工智能中的模糊逻辑理论切实有效地应用到计算机网络技术中,可以加强计算机网络在不确定性、不可预测信息方面的控制和管理。随着人们对各方面需求的增加,计算机网络技术的应用范围在不断地扩大,计算机网络管理也逐渐得到了更加深层次的发展,计算机网络技术逐渐形成了分层式的管理模式,并由人工智能技术进行上层与下层管理模式的连接,实现计算机网络技术的推