

高职院校学生素质拓展管理信息系统分析

戚振兴

(北海职业学院 广西北海 536000)

摘要: 高职院校想要优化学生素质拓展管理信息系统,提高学生的综合素养,理应重视做好高职院校信息教育管理工作,健全高职院校信息安全管理系统,避免私密数据被窃取,防止信息泄露,不断优化校园网络结构,全面建立校园安全网络。本文将简单分析高职院校学生素质拓展管理信息系统,希望能为该系统的安全管理工作提供借鉴。

关键词: 高职院校 学生 素质 拓展管理 信息系统

中图分类号: G622 **文献标识码:** A

DOI: 10.12218/j.issn.2095-4743.2022.25.177

引言

在21世纪的信息时代背景下,各高职院校非常重视提高学生的信息核心素养,加强网络环境建设,全面建立安全、文明、绿色、干净的校园网。高职院校学生素质拓展管理信息系统结构层共分为六层:第一,物理安全管理层。第二,网络安全管理。第三,主机安全管理层。第四,应用安全管理层。第五,数据安全。第六,总系统安全管理层。各层次在发挥独立功能的同时互相作用,能够做好整体安全管理工作。与此同时,高职院校引入了各种先进的技术以加强校园网安全管理,抵御网络病毒攻击,维护信息安全。

一、高职院校学生素质拓展管理信息系统特征

21世纪属于信息时代,高职院校学生教学管理工作和各项服务工作及计算机网络技术应用密不可分。当代高职院校学生素质拓展管理信息系统有五项基本特征:第一,校园网系统结构复杂。第二,学校计算机网络功能多样。第三,计算机网络安全设置涉及面广。第四,计算机网络安全维护应用人员多样。第五,计算机网络安全攻击来源具有多样性。

从校园网安全建设内容来看,高职院校学生素质拓展管理系统设有完整的安全技术体系,层次分明,信息安全管理功能良好。学校在建设和应用该系统的过程中非常重视融合信息核心素养,并将该系统应用于日常教学和学生素质测评工作中。需要注意的是,想要拓展高职院校的学生素质,提高学生的信息核心素养,教师应注重转变传统教学观念与单一化教学模式,引入先进的教学技术,丰富教学方法与内容,综合培养学生的信息核心素养。例如,对计算机课程教学来说,核心素养主要是指培养学生的信息操作能力和必备品格,让学生成为适应信息时代与社会发展的高素质人才,引导学生恪守信息网络道德,遵守相关法律法规。学生不仅要具备计算机知识应用能力,而且要树立正确的科学观、网

络观,提高个人道德涵养,在学习和应用计算机技术的过程中勇于创新 and 突破,致力于中国计算机产业发展事业。教师应紧密融合信息核心素养,引导学生树立正确网络观,学会运用有价值的信息,摒除不良信息,恪守网络道德。在开展计算机课程教育活动时,教师应协同学生深度开发数字教育资源,融合信息核心素养,秉承文化兼容理念,创建和谐的教学情境,编辑严谨的计算机语言,设计有新意的网页,让课堂教学内容贴近学生的日常生活,深度开发有特色的信息化教育资源,做好计算机语言编译工作,和学生一起编辑电子教材、信息校本、电子教辅材料等资源。

高职院校学生素质拓展管理信息系统安全技术体系设计包括物理安全设计、网络安全设计、主机安全设计、应用安全设计、数据安全设计及备份恢复。其中,物理安全设计下设有机房与办公环境安全管理、计算机和网络设备安全管理、其他安全设计。网络安全设计分为通信网络安全设计、区域边界安全设计和其他安全设计。主机安全设计分为服务器安全设计和其他安全设计。应用安全设计包括应用系统设计和其他安全设计。

二、高职院校学生素质拓展管理信息系统结构层设计

1. 物理安全管理层

对于高职院校学生素质拓展管理信息系统物理安全管理层来说,其安全防护硬件基础能够保护网络设备和计算机基础设施免于受到自然灾害的损毁,同时也可以减少人为操作失误对设备的损坏。这一结构层的安全是确保高校计算机网络信息安全的基础,该层次主要包括基础设施、线路与设备。建设规范的物理安全管理层,能够确保网络 IDC 机房的用电、消防与所处环境符合安全检测标准。设计物理安全管理层时,需要合理规划通过 IDC 机房的装饰装修材料、抗静电材料和配电项目,谨遵安全设计标准^[1]。

2. 网络安全管理层

做好高职院校学生素质拓展管理信息系统网络安全管理层设计工作方能有效解决校园通信安全，这一结构层设计工作有三大基本步骤：第一，设置部署访问控制。第二，通过认证加密。第三，设置病毒防御与入侵检测技术。在具体设计工作中，需要严格依据划分区域实施隔离，加强访问控制，满足本校用户需求。在整个校园网内，每个系统均有相应的访问用户，避免安全级别较低的系统因为遇到威胁而影响安全级别较高的系统运行效果，则需要尽量缩小影响面，针对不同安全级别的系统实施相应的划分与隔离。

其次，要做好入侵检测工作，满足校园网安全防御需求。当前各高职院校虽然在对防火墙进行不断更新和审计，可以对各类访问用户进行严格管控，却依然无法全面确保高职院校学生素质拓展管理信息系统网络的安全，其主要原因是网络安全管理具有动态性和整体性，全面确保网络安全，则需要科学部署入侵检测配置和安全防御系统，这样可以全面检测透过和绕过系统网络防火墙的攻击性病毒，并做好安全防御工作。

3. 主机安全管理层

设计完善的主机安全层能够满足整个高职院校学生素质拓展管理信息系统大量不同操作系统的安全应用需求，在设计该系统的过程中，必须准确把握以下几项要点。首先，要做好高性能操作系统的全面安装工作，优化系统安全设置，如果某些端口或者服务不会经常使用，却很容易出现安全问题，就需要将其关闭。其次，要对广大师生用户信息、授权和口令进行严格限制，定期更换口令，实现口令组合的复杂化，引导用户不可使用与自身信息相关的组合，也不能应用简单的口令组合。再次，要编辑系统自动更新程序，定期打好补丁，做好系统风险评估工作。

4. 应用安全管理层

应用安全管理层属于系统主机上安装的一种安全应用软件，主要功能是满足高职院校学生素质拓展管理信息系统所提供的安全应用服务，确保数据信息的安全性。应用安全管理层的信息系统会全面记录使用者的登录信息、退出信息和网页访问信息，同时对这些信息进行统计和分类研究，采取安全警报策略，从而及时发现非法访问，在第一时间通知本校网络系统安全管理员，也能够发生在不安全事件时全面提供查证与举证。其次，当高职院校学生素质拓展管理信息系统网页出现潜在性未经授权的访问时，该层次会立刻发出安全警示。另外，应用安全管理层能够为检查所得数据信息提供安全可靠的存储方式，维护这些信息的完整性，将信息转

变为可用资源。

5. 数据安全管理层

在高职院校学生素质拓展管理信息系统数据安全管理层中，其内部数据均属于本校学生素质拓展信息，包括学生素质拓展计划、证书管理、内容管理、上传照片、资料修改等信息。数据安全管理层能做好这些信息的保密工作，维护信息的完整性，对信息进行备份，促进信息恢复，防止信息泄露和被窃取。

6. 总系统安全管理层

总系统安全管理层能够辅助高职院校做好整个学生素质拓展管理信息系统安全管理工作，据调查了解，当代高职院校设置了配有专业技术人员的网络安全管理部门，针对本校学生素质拓展管理信息系统安全管理工作制定了一系列完善的管理制度，设置了科学的操作标准流程，明确相关岗位职责，制定了设备维护方案，对日志记录进行存档，同时制定了应急响应预案。这样可以确保系统网络安全管理工作有据可依、有志可查。其次，总系统安全管理层会做好设备维修维护管理记录，自动实施定期巡查与网络维护工作。

三、高职院校学生素质拓展管理信息系统安全管理技术

1. 防火墙技术

对于高职院校学生素质拓展管理信息系统安全管理工作来说，安全防火墙并非实体墙，而是一种有特殊功能的安全访问控制设备，能够在本校内部网络与Internet之间设置一道完整的安全屏障。在大数据时代，数据流在经过校园安全防火墙时会出现三种不同的结果：第一，允许。第二，拒绝。第三，丢弃。防火墙技术的主要功能是根据高职院校学生素质拓展系统的安全设置，对未经过授权的数据流实施全面监控、安全限制、针对性选择与屏蔽，这样有助于维护系统网络信息数据的安全。

2. 入侵检测与防御技术

入侵检测与防御系统技术的英文简称是IDP技术，该技术属于一种可以针对违规的网络行为进行自动辨识和采取主动防御措施的系统。安装该系统之后，能够自动做好重要数据的监控工作，识别数据信息内容，破坏恶意代码与记录侵入。一般情况下，在为系统安装防火墙之前或者之后均可以按照IDP系统，该系统不仅能够对入侵的数据流进行及时响应，而且能自动拦截透过防火墙攻击高职院校学生素质拓展管理信息系统的数据流。

3. 虚拟局域网技术

虚拟局域网技术简称VLAN，英文全称是Virtual Local

Area Network, 该技术属于一种虚拟的工作组, 能够对高职院校学生素质拓展管理信息系统设备实施逻辑性划分, 使其转变为多个网段。因而, 可以说VLAN技术的核心就是划分网段。在高职院校学生素质拓展管理信息系统内部, VLAN技术能根据不同的业务与相关安全等级, 按照网段实施安全隔离, 对于网段之间的互访予以严格的控制, 从而有效阻隔网络非法入侵。

4. 虚拟专用网技术

虚拟专用网简称VPN, 英文全称Virtual Private Net, 属于私有网络互联技术, 其在公共资源上组合了完整的架构体系, 运用加密技术和专用隧道能够实现数据信息的共享。VPN技术的重要功能之一是为广大用户提供专用网络, 在专用网中所传输的信息均为私有信息。目前, VPN技术主要是运用隧道、身份认证技术、加密技术和密钥来维护高职院校学生素质拓展管理信息系统的安全^[2]。

5. 病毒防治与云安全技术

基于大数据时代, 随着计算机网络基础建设的优化与完善, 网络覆盖范围也在不断扩展, 网络系统也更容易受到病毒的入侵, 因而, 需要采用先进的病毒防治技术来全面查杀和防治病毒, 避免网络系统受到捆绑软件、下载、压缩性文件、电子邮件、聊天软件和网络共享的负面影响, 在病毒侵扰网络正常运行之前, 病毒防治技术就会及时进行自动阻止。在高职院校学生素质拓展管理信息系统运行中, 查杀新病毒的检测方法主要有四种: 第一, 校验和。第二, 特征代码。第三, 行为检测。第四, 软件模拟法。目前, 云安全技术能够对网络病毒库的更新不及时产生的负面影响予以有效解决。云安全技术可以结合大量客户端对应用计算机网络服务软件的异常检测结果, 将所获取的恶意代码与木马病毒信息传输到云端, 然后, 将处理结果发送给所有用户端。该技术能够满足用户量越多越安全的需求, 可以覆盖到所有局域网, 一旦发现网络异常就会立即得到消息, 并及时将病毒库的单机查杀转换成网络查杀, 全面预防新病毒入侵问题^[3]。

6. 系统安全加固技术

系统安全加固技术能够有效提升高职院校学生素质拓展管理信息系统与各种应用服务软件质量, 做好相关优化配置工作, 进一步提高系统网络安全等级, 增强系统的防御能力。从整体上看, 高职院校学生素质拓展管理系统安全加固技术有两项应用要点: 第一, 对补丁进行升级, 实现服务最小化。第二, 加强安全认证管理工作, 严格设置每一位用户的访问权限, 同时对子目录的访问权限进行合理划分。

7. 漏洞扫描与评估技术

漏洞扫描和评估技术属于一种针对系统网络信息安全所处风险实施客观评估的技术, 该技术可以在事先识别网络受到攻击入侵性访问的可能性, 及时发出异常警告, 输出产生的后果。同时, 高职院校学生素质拓展管理信息系统网络漏洞扫描和评估技术能够对排查对象的资源进行协助辨别, 准确判断系统内部信息资源是否受到攻击, 明确当前的网络弱点, 准确评估网络信息安全风险^[4]。

8. 数据容灾备份技术

在高职院校学生素质拓展管理信息系统应用和安全维护工作中, 数据容灾备份技术属于不可或缺的重要技术, 该技术以实现网络化与虚拟化为发展方向。在系统安全维护工作中, 数据容灾备份技术能够采取科学合理的措施, 设置好备份, 做好信息安全存储工作。在发生各种事故时, 数据容灾备份技术能够将备份数据的丢失量控制到最低, 并采取应急响应的处理措施使网络系统及时恢复运行, 避免出现因为意外丢失数据而导致学生素质拓展管理工作的中断问题。

结语

综上所述, 高职院校要做好学生素质拓展管理信息系统安全维护工作, 优化系统网络防护策略。同时, 高职院校应重视提高本校计算机网络安全管理技术质量, 细化网络信息安全建设内容, 健全网络安全管理系统。

参考文献

- [1]郑喜龙. 高校学生素质综合测评系统的设计与实现[J]. 西安电子科技大学学报, 2015, 42(2): 52-57.
- [2]魏丽芬. 大学生素质拓展信息管理系统架构设计[J]. 计算机与现代化, 2017(8): 58-61.
- [3]周丽萍, 嵇天培. 大学生素质拓展学分管理系统的设计与开发[J]. 常州轻工职业技术学院学报, 2018(8): 67-70.
- [4]范汝勇. 高校学生职业素质训练管理系统的设计与实现[J]. 计算机与现代化, 2019(8): 75-80.

作者简介

戚振兴(1982.4—), 男, 广西北海人, 本科, 最高学位: 广西大学控制工程领域工程硕士, 北海职业学院, 职称: 信息系统项目管理师(高级工程师)、讲师(中级), 研究方向: 智慧校园、信息管理与信息系统, 大数据+电子商务, 管理信息化电子商务农村电商和社区商业信息系统。