计算机网络安全分层评价防护体系的探究思路

孙 萍

(天津工业职业学院, 天津 300400)

摘要: 随着计算机技术的不断发展, 计算机网络安全问题成为网络计算机发展过程中非常棘手的问题。计算机网络安全防护体系的建立与完善能够提高网络信息的安全性能, 提高网络维护和管理质量。本文笔者从计算机网络安全分层评价防护体系面临的网络安全威胁和特点出发, 研究了计算机网络安全分层体系的主要应用技术, 提出了计算机网络安全分层评价防护体系的具体思路, 旨在更好地推动计算机网络安全完善与发展。

关键词: 计算机网络安全; 分层评价防护体系; 探究思路

在计算机技术不断发展的今天, 计算机网络安全系统被应用于各行各业。关于计算机网络安全问题的探究已经成为各个领域研究的重要问题, 第二代防护技术也更加广泛地应用于计算机网

络安全防护系统中。通过研究计算机网络安全及分层评价防护体系, 能够增强计算机网络安全人员的安全意识, 加强防护与管理, 从而提高计算机网络系统的安全性和可靠性。高职计算机网络安全教师通过带领学生学习计算机网络安全分层评价防护体系, 能够使他们深刻地认识到计算机网络系统正常运行的重要性, 强化他们对计算机网络安全的认知。

一、计算机网络安全分层防护体系的特点

(一) 计算机网络安全面临的主要威胁

计算机网络安全问题主要包括硬件和软件两方面, 其中防护的对象是网络数据以及网络信息。通过研究相关网络安全防护技术, 将其运用于网络安全防护中, 有助于构建良好的网络系统运行环境。由目前网络攻击的现象我们可以总结出, 网络安全面临着来自多方面的威胁, 且样式各异, 传统的防护技术已经落伍,

现状出发进行教学。这样教师就会发现, 通过信息技术能够搜集到大量促进教学开展的信息, 能够使教师在开展教学时可以从更加灵活地进行教学。

例如, 教师在对一些较为基础的程序进行教学时, 单纯地变成教会会导致教学氛围过于枯燥, 教师就可以结合当前行业发展现状, 从游戏中程序的应用, 电子商务中程序的应用等方面开展教学。这样学生会更感兴趣, 甚至学生还能够从教师的教学中找到自己的努力方向。比如, 有些高职学生在学习计算机时没有想到电子商务与计算机之间的联系, 但经过教师的引导发现了兴趣所在, 这对学生的生活都会产生一定的影响。

(二) 打造网络学习平台, 实现学习自由

大部分情况下, 学生在学习过程中都会受到时间以及空间的束缚, 初中、高中阶段学生会认为这是理所当然的事情。但是, 高职学校与普通高校不同, 它属于职业类学校, 学生的学习也相对自由, 但是过于死板的教学时间会影响学生的学习心情。为此教师可以对此作出一些改变, 大数据时代信息的传递与接收都是依靠网络开展的, 根据这一特点学校可以构建相应的网络学习平台。通过平台的建立, 学校可以对课程的结构进行调整。

例如, 学校可以结合计算机基础课程开展的状况进行调整, 最初阶段的基础教学学生需要根据课程安排到教室学习, 而之后的复习与巩固阶段学生可以通过网络学习平台开展, 但是要定时向学生做学习汇总, 遇到较难的不懂的问题时要与教师进行沟通。在此种学习模式下学生拥有更多的自主权, 同时学生也会更加积

极地投入其中。

(三) 建立多元评价模式, 提高评价有效性

在过去的教学中, 教师会主要以理论结合实践的方式对学生进行评价, 评价依据是学生在期末时的理论成绩以及实际操作成绩, 这使得教师的评价具有很大的片面性。同时, 也为学生提供了松懈的理由, 这种评价方式让很多学生认为只要在最后的考试中取得好成绩就可以, 所以很多学生在平时的学习中并不上心, 只有到了考试之前才会临时抱佛脚。所以, 教师要对评价方式进行创新, 不仅要注重期末的成绩, 还要注重平时的成绩。教师可以在网络学习平台中设置一个学习评价, 积累学生每一次的学习状况, 以更为公平的方式多学生的学习进行评价。

四、结语

综上所述, 想要在大数据背景下实现高职计算机基础类课程的教学改革, 教师需要了解大数据在教学中的作用, 之后发现当前计算机基础教学中存在的一些问题, 根据此类问题寻找对应的策略, 实现教育的改革。

参考文献:

- [1] 刘盈. 大数据视野下的“大学计算机基础”课程教学改革[J]. 计算机产品与流通, 2019(08): 245.
- [2] 罗伟俊. 大数据下的中职计算机基础课程教学改革研究[J]. 计算机产品与流通, 2019(08): 261, 288.
- [3] 钱秋荣. 大数据下的中职计算机基础课程教学改革分析[J]. 教育教学论坛, 2019(12): 267-268.

难以满足现代网络安全运行的需要。实体安全是网络安全中的硬件设备保障,如火灾、地震、水灾等的破坏。网络安全中的运行安全是实现网络系统功能的有效途径,应保证系统的安全性。信息安全主要包括数据库、访问控制这两方面,面临的威胁主要有信息泄露、破坏、篡改等问题,严重破坏了网络数据与信息完整性、安全性与可用性。计算机网络安全受到的威胁是多方面的,如黑客入侵,黑客看到了网络系统脆弱性的弊端,恶意攻击计算机系统以影响其运行,还窃取秘密信息,影响了整个网络数据的完整性。黑客通过搭线窃听来窃取机密文件,造成内部泄密,内部泄密是一种通过恶意攻击网络系统达到窃取信息的一种行为。另外,网络协议是网络系统中提供网络服务的基础,一些黑客对假冒IP进行攻击,为网络认证带来了一定的阻碍,使得网络系统更加脆弱。

(二) 计算机网络安全分层防护体系的特点

计算机网络安全分层防护体系的构建能够保证相关信息的安全,确保计算机网络安全策略正常、高效实施。计算机网络安全策略为网络系统的安全性而服务,通过定义相关的保护规制,从技术层面运用安全防护技术和措施,实现计算机网络安全体系的完善。计算机网络安全分层评价防护体系是动态的,是在系统运行过程中不断完善的,计算机网络安全分层评价防护体系目的在于构建全方位、多层面的体系结构。计算机网络安全分层防护体系是一种综合化的安全体系,主要涵盖安全评估、安全防护、安全服务三个方面。安全评估针对的是网络管理的评估;安全防护是指网络访问控制以及病毒防护体系等;安全服务解决的是应急服务体系以及数据恢复等问题。计算机网络安全分层评价防护体系的构建,能够更好地维护网络安全,有效防范网络系统运行过程中的各种威胁和不安全行为,以保证计算机网络系统的安全运行。随着信息技术的不断发展,高职计算机网络安全专业教师在教学的过程中,应强调运用网络技术在计算机网络安全问题中的运用,更好地推动计算机网络技术的长效发展,增强计算机网络系统的安全指数,这也是计算机网络安全领域中需要解决的重要课题。

二、计算机网络安全分层防护体系的主要应用技术

要想实现计算机网络安全分层防护体系的正常运行,专业的数据加密技术是不可或缺的,需要对网络系统中的数据和信息进行加密,以提高数据信息的加密效率。主要有以下几种防护技术:第一,防火墙的主要功能是增强网络系统的防御能力,操作简单,也是网络安全运用中运用较为广泛的一种技术。防火墙技术的运用能够实现对网络系统数据的实时监控,记录网络用户的网络使用情况,并以日志的形式呈现。防火墙技术具有较强的敏感性,能够及时发现网络系统中存在的安全问题,隔离处理病毒木马和相关可疑行为;第二,访问控制技术对计算机网络安全防护也发挥这巨大的作用,通过运用网络访问控制技术,能够严格验证

用户的身份信息,并在发现问题后立即停止用户的访问行为;第三,还有一种运用于计算机网络安全防护的技术被称为服务器的安全控制技术,此技术能够控制软件的下载等相关问题;第四,网络权限控制技术主要是对相关非法访问行为进行有效的控制,明确访问的信息,并进行相关操作;第五,属性安全设置技术运用的前提是属性安全,并在此基础上为用户提供可供访问的文件资料等等。

关于软件技术的分析建立在 Windows 系统操作界面技术的基础上,研究计算机网络安全分层防护体系,主要包括以下几种技术:第一, JAVA 技术采用的是主要服务器界面设计技术,以 Eclipse4.5.1 平台技术进行呈现;第二, JSP 技术主要运用与动态网页页面的开发研究和设计中,通过运用 JSP 技术能够加快 WEB 页面的开发力度,缩短 WEB 页面研发的时间和周期,有效提升服务器的包容性和兼容性。JSP 技术在服务器端中的使用,通过生成 HTML 超文本标记语言,从而保证 HTML 页面代码源文件的正常、安全运行;第三,将 Javascript 新型语言融入 HTML 超文本标记语言中,根据使用者的实际需求实现快速传输,从而提高信息传输的安全性与可靠性,使得网络系统在运行的过程中可以摆脱服务器的依托,在客户端直接完成应用程序等相关功能。Javascript 语言技术有着自身的优势和特点,被广泛应用于各个行业和领域中;第四,将结构化查询语言 SQL 运用于 JAVA 数据库中,能够在构建高级接口的同时,有助于设计开发者研发工作的顺利、高效开展。

三、计算机网络安全分层评价防护体系的具体思路

(一) 明确网络系统设计要素

由于网络系统的构建和要素比较复杂,且对相关技术含量的要求比较高,再加上网络系统是一种动态的运行系统,受人为的干扰性比较大,因此,网络系统在运用的过程中面临来自多方的威胁。基于此,我们在探究计算机网络安全分层评价防护体系设计的过程中,应充分考虑网络系统完整性、可用性、机密性以及不可否认性。完整性是确保网络系统面临诸多复杂安全问题中的完整性;可用性将用户自身操作作为出发点,实现用户对系统界面的灵活操作;机密性是建立在服务器或浏览器架构模式的基础上,运用 SSL 安全套接层协议,快速实现用户对 WEB 浏览器的访问,并在短时间内精准地完成服务器认证,实现对用户的访问控制。此外,通过在服务器与客户端之间开通安全的 SSL 通道,能够让用户利用 SSL 这一安全通道实现 WEB128 位的密钥会话;不可否认性是指通讯双方对接受信息的协议达成一致,不可否认真实信息,且在明确双方身份的前提下,实现数据的安全传输。另外,系统体系设计方面还应将物理安全、软件访问、加密保护等需求考虑进去,有效设计管理信息,做好数据备份。计算机网络安全防护体系的设计应结合具体网络应用的实际情况,最大化地满足实际需求。

（二）计算机网络安全分层评价防护体系的功能

计算机网络安全分层防护体系的每一环节都应形成一道安全防线，实现多角度、全方位防护计算机网络安全的目的。计算机网络安全分层评价防护体系层次主要分为审计响应机制层、安全技术措施层、安全人文环境层。每一层都互相支撑，各层次功能之间相互配合、互相支持，从而构成一个完整的计算机网络安全防护体系，并共同实现网络安全系统体系的防护功能。

安全人文环境层是计算机网络安全防护体系中的基础，以法律宣传手段为网络安全提供良好的人文环境，在法律层面上实现对技术的支持。安全人文环境层中的法律子层涵盖法律和制度两方面，是在计算机网络安全范围内由国家机构和相关部门制定的。规章制度层主要体现在相关单位的规章制度中，是依据国家网络安全法律法规进行制定并实施的。意识子层只要由网络管理机构的技术人员负责，主要工作室宣传并普及网络安全常识，增强用户的网络安全意识，在确保网络系统运行安全性的同时，提高技术人员的网络安全技能。

安全技术措施层作为网络安全防护体系的支柱，主要目的是建设符合安全标准要求的机房，以增强网络设备和通信媒介介质的安全性与可靠性，避免丢失损坏等情况的发生。运行安全子层主要是确保网络系统的稳定运行，及时发现安全隐患并建立完善的响应机制，以保证网络系统运行的安全性与可靠性。运用审计跟踪和备份等技术对信息数据进行安全保护。信息安全子层主要运用防攻击和防泄密等技术，保证数据库系统和信息资源的完整性与保密性，本层采用的技术措施主要有防火墙、应有网关、安全协议等技术。

审计响应机制层是网络安全防护体系中最上面的层次，也是计算机网络安全分层防护体系中的最后一道防线，包括分析—响应—调整、监控—日志—审计、备份—灾难恢复等。

（三）应用网络系统加密技术

目前，在计算机网络系统中，运用最为广泛的加密技术有公钥加密技术和私钥加密技术。在实际运用中，应结合具体情况选择适宜的加密技术，既可以选择一种加密技术，也可以将两者相结合使用。加密技术是一种利用相应技术参数，实现对网络系统的全方位控制，从而提高保护层的有效性。与此同时，通过提高网络系统加密技术，能够针对各个故障问题，更新并完善管控效果以及措施，制定与之相应的解决方案。我们在使用公钥加密技术与私钥加密技术的过程中，还应制定明确的保护措施，突出网络系统的过滤功能，不仅要提高各项信息的处理能力，还应全方位、全过程保护计算机网络系统。同时，通过科学、合理地运用加密技术，能够使得计算机系统中的信息数据得到更为权威的保护，如果条件允许，也可以建立不良数据和信息的切割机制，从而最大限度地提升计算机系统运行的安全性与稳定性。另外，加密技

术的有效应用，能够保证计算机系统中存储的文件只限用户自己打开并使用，他人无法破译，这在很大程度上提高了用户个人信息的安全性。

（四）不断强化网络系统的抵抗能力

21世纪以来，随着我国社会经济的快速发展，计算机网络技术以迅猛之势运用在各个领域中，为社会生产力的提升带来了巨大的作用。但是，与此同时，与之相应地还出现了网络病毒、垃圾文件、黑客攻击等问题，而且长期以来也没有得到很好的解决，这严重影响着我国计算机网络技术的长期、稳定发展。基于此，首先，相关部门应具体分析计算机网络病毒，制定并完善相关管控机制，从而降低恶意攻击计算机安全运行带来的影响。同时，还应运用完整的反病毒技术，为计算机网络系统保驾护航，这样不仅能够提升网络系统的安全性及稳定性，而且还能提高计算机网络系统的自我防御能力和预防功效，从而将病毒扼杀在摇篮中，避免造成严重的损失。在处理与优化计算机系统网络病毒的过程中，应将网络系统安全性延长机制的建立作为首要任务，奠定病毒优化处理的基础。因此，网络运行抵御病毒能力的提升，能够从真正意义上实现计算机网络系统的安全运行，从根本上为大数据云计算背景下网络安全技术的运行创设良好的环境。

四、结语

本文在相关理论分析的基础上，探究了大数据云计算环境下计算机网络安全技术的运用途径。高职计算机网络安全教师在教的过程中，应着重强调计算机网络安全分层评价防护体系的意义。高职计算机网络安全教师应引导学生主动发现计算机网络运行中的问题，并找出对应解决措施，为大数据环境下计算机网络系统的正常运用提供良好的环境和运算背景，从而促进我国计算机网络安全技术的长期、稳定发展。

本文系：“国家级十三五规划重点课题课题题目：‘计算机网络安全分层评价防护体系研究’课题编号：ZGJY2975的阶段研究成果。”

参考文献：

- [1] 陶睿天. 计算机网络安全分层评价防护体系研究 [J]. 科技视界, 2019 (19): 47-48.
- [2] 刘秀彬, 王庆福. 计算机网络安全分层评价防护体系研究 [J]. 电脑知识与技术, 2018, 14 (19): 26-27, 29.
- [3] 林榕梯. 计算机网络安全分层评价防护体系的思考 [J]. 信息与电脑 (理论版), 2017 (20): 185-186.
- [4] 付伟. 试论计算机网络安全分层评价防护体系研究 [J]. 计算机产品与流通, 2017 (08): 44.
- [5] 胡宇航, 陈圣健, 孙铭阳. 计算机网络安全分层评价防护体系研究 [J]. 通讯世界, 2017 (11): 123.