

高职院校网络信息安全及其防护对策

周军

(广西职业技术学院 广西南宁 530226)

摘要: 高职院校在实际开展网络信息安全建设的过程中,必须要提升对其重视程度,同时要团结所有个体的力量,才能够真正去营造一个更加良好的网络环境。本文主要对当前高职院校网络信息安全建设的迫切程度进行了强调,分析了在实际进行相关安全防护体系建设的过程中所需要解决的问题,包含了不断去进行技术的更新,提升高职院校教职工作者的网络安全意识,完善相关管理体制,帮助培养更专业的人才,提升相关的建设资金投入等等。

关键词: 高职教育; 高职网络信息安全; 信息安全与防护; 防护对策

引言

随着网络信息科技的不断提升,当前我国多数高职院校在日常教育开展的过程中,都会注重对网络技术的应用,且部分高职院校在信息化建设方面已经取得了一定的成果。但高职院校在借助信息化技术提升日常管理工作效率的过程中,对相关的网络信息安全问题没有足够的警惕,可能会造成高职院校中的个人数据、科研、教务相关信息面临被泄露的风险,整个网络体系也随时可能遭受计算机病毒或者一些黑客的非法攻击。

一、高职院校网络信息安全建设中存在的问题

(一) 技术方面的问题

高职院校在实际开展网络安全建设的过程中,对于要部署怎样的安全防护设备其实时比较了解的,譬如说,安全入口的防火墙,进行VPN设备的假设,对上网设备进行购置,进行流量控制设备的安装等等,且高职院校对于这些设施的建设也是比较重视的。但网络信息本身是处在一个不断变化的动态环境下的,其中存在的不确定因素比较多,包含了网络终端存在系统漏洞,出现网络病毒,存在黑客的恶意入侵等等^[1]。尤其是高职院校中网络用户比较多,所产生的网络数据是极为庞大的,终端种类以及用户都比较复杂。这意味着普通的安全产品已经无法满足高职院校网络信息安全的实际需求,还需要有更先进的设备以及技术去进一步保障高职网络信息安全。

(二) 高职院校网络安全意识比较淡薄

高职院校相较于一般的本科院校,其建设资源是比较少的,无论是在占地面积还是在师资力量储备方面都是比较落后的,从某种程度上这也意味着高职院校在校园网络安全建设方面的等级是比较低的。其中很大一部分的原因是高职院校的网络设计者在初始设计的过程中并未充分考量到对相关信息安全的建设,而在后期进行校园网络维护的过程中也比较缺乏安全意识,没有及时地去处理相应的安全漏洞以及其中存在的一些潜在不安全因素。甚至于一些网络管理中心的教师本身就缺乏足够的网络安全知识,在实际管理中也更注重技术,对于管理比较清湖,在进行了安全设备的部署之后,不再对其进行积极维护。这对于整体高职院校网络信息安全性是有着极大阻碍的。除此之外,高职院校中的学生因为社会经验比较缺乏,对于网络安全的意识比较薄弱,在收到一些陌生邮件或者接收到一些比较新奇的通知时会忍不住打开去进行查看。而不法分子正是利用这些学生的这种好奇心理,借助于一些链接来进行网络病毒的传播,最终去窃取学生的个人信息甚至是学生的财产相关信息。而还有一些人则利用学生无意间泄露的信息去进行违法诈骗活动,对学生以及他人的日常生活都造成了极为严重的伤害。

(三) 网络信息安全管理体制不够完善

当前,无论是高职院校还是其他院校,都在不断提高信息安全

建设,各种与之相关的保护管理制度也逐渐被建立起来。但在网络信息安全方面,我国还处在一个比较初期的探索阶段,相关的管理体制其实是不够完善的。譬如说,与网络信息安全相关的比较重要的《中华人民共和国网络安全法》2016年才被正式推出,从2017年才开始真正去执行。这种大的环境对于高职院校网络信息安全建设也是有着极为不利的影响的^[2]。尤其是,高职院校校内本身也并没有专门的对网络信息安全负责的部门,没有专业的网络管理者,当前执行该工作的基本是院校内的懂点儿计算机技术的管理层。但其对于网络信息安全相关的法律法规本身就是一知半解的,而仅仅根据相关文件以及自身的理解去制定高职院校网络信息安全管理度,注定了其中必然存在各种漏洞。学生法律意识淡薄,学校内部相关规定又不够完善,造成部分学生在实际进行网络应用的过程中可能并没有意识到自己的行为是不适合的,自然也就无法真正保障整体校园网络信息的安全性。

(四) 缺乏专业的人才

我国网络安全相关的教育起步是比较晚的,多数院校是在2015年之后才成立的与网络安全相关的教育专业,这意味着,真正懂得相关技术的人才并不多。而这些为数不多的学生在校期间所学的也大多为理论知识,其本身的实践经验是极为缺乏的。再加上,高职院校因为建设资源有限,能够给予相关教职工作人员的待遇相较于企业或者普通本科院校来讲又会更低一些,很多优秀的网络安全从业者因为待遇问题会更倾向于其他用人单位。这就导致了高职院校对于网络安全方面的人才极度缺乏的,在实际工作中一个人可能需要同时负责多个岗位的工作,任务繁重,个人精力有限,效率自然也就比较低。

二、增强高职网络信息安全防护的对策

(一) 要有更加成熟高效的技术

1. 要及时进行网络信息安全硬件设施的更新

在实际开展网络信息安全建设工作的过程中,必须要有相应的安全设备。我国当前在这方面做得比较好的企业有启明星辰、华为、深信服、绿盟科技、安恒信息、天融信、新华三等等,尤其是这些企业有自己的研发部门,可以持续不断地进行安全设备的更新。高职院校中负责网络信息安全建设的教师需要时刻对这些企业的研究成果进行关注,及时采购新的更加高效的安全防护设备去替代旧的设备,从而避免因设备问题造成的校园网络安全隐患。

2. 要有更具防护效力的管理体系

高职院校在开展网络信息安全防护建设的过程中,除了要及时更新相应硬件设备之外,还需要不断地去引入更高效的软件防护技术,包括信息验证技术,对入侵进行检测的技术,对网络安全进行运营管理的技术的等等。高职院校的网络安全问题涉及到的人员是比较多的,但实际上负责相关管理工作的管理层却比较少,因此必

须要借助于更加先进的技术来帮助提升整个管理工作的效率^[3]。更先进的网络管理软件可以对整个网络进行实时的远程监控,从而减轻管理者在巡查方面的负担,以便于其更迅速地发现网络中存在的问题。当然,高职网络安全管理体系还必须有着比较强的统一性,以便于相关的管理员能够对其进行统一控制,更好地进行网络信息安全防护工作地开展。

3.要做好重要数据的备份

高职院校中各种网络信息数据关乎教职工以及学生的隐私及安全,除此之外还有一些公共信息,校园内部信息等是有着极为重要作用的,一旦损坏,对整个高职院校造成的损失将是极为巨大的。因此高职院校在增强网络信息安全建设的过程中还需要注重对重要数据信息的备份,且这种备份应该选择异地备份模式,以便于校园内部设备出现故障后,可以借助于这些备份数据来帮助相关信息得到恢复。

(二) 高职教师及学生要有更强的网络安全意识

1.提升网络信息安全管理的安全意识

在对高职院校中的整个网络体系进行管理的过程中,相关管理员必须要有意识地去建立账户管理以及用户身份验证相关机制,不同用户所拥有的信息获取权限是各不相同的。再者,网络信息管理人员还必须要对整个的网络系统以及一些重要的设备设置管理账号及密码,且密码需要进行定期更换,在难度上也必须要打到一定的标准^[4]。而为了进一步增强这些安全设施的防护效果,还需要对整个的外部环境进行维护,这一方面可以借助于防火墙技术来辅助进行操作。尤其是管理人员必须要积极参与各种与网络信息安全相关的培训工作,通过学习不断提升自己,从而更好地服务于高职院校。

2.要不断增强学生的网络信息安全意识

计算机网络信息安全问题关系着的不仅仅是高职院校所有数据信息的安全,更关乎着国家的整体安全。譬如说,前段时间美国黑客就对我国高等院校——西北工业大学的网络体系进行了攻击,其目的自然是为了窥探我国最为先进的科研技术。因此网络信息安全的重要性是不言而喻的。高职院校在实际应用网络信息技术的同时一定也要保障好校园网络的安全性。但当前我国很多高职院校因为自身资源以及技术层面的一些问题对于网络信息安全方面的保障还不是很好,因此还需要持续推进网络信息安全防护工作。

高职院校的网络信息管理中心在制定了各种与校园网络信息安全相关的制度之后,还需要将学生需要遵守的与之相关的各种制度,法律规范等印制在相应的学生手册中,在学生入学之初就不断地向学生强调网络信息安全的重要性,提醒学生能够加强自我警惕心理,并约束自身在网络中的行为,不盲目地泄露个人信息与咨询,也不随风逐流,成为网络键盘侠中的一员。不断地去强化学生关于网络信息安全的正确认知,从而引导高职学生可以有更健康的网络应用习惯。

3.对相关法律法规进行完善

在增强高职院校网络信息安全的过程中,国家方面也需要不断地推出相关政策发挥,要不断地完善网络安全相关的法律规范,尽可能地补充网络犯罪相关的法律漏洞,而高职院校在进行与之相关的信息安全管理制定制度的过程中也需要紧跟国家法律的脚步,再结合自身真实需求来制定更科学合理的制度。这些制度包含了对于信息系统的备案,有关于文明上网的标准,一些信息的发布与审核,数据安全相关的管理制度等等。高职院校除了自己去执行相关工作之外还可以与电信运营商合作,从而构建更加健全完善的网络信息安全管理体系。

(三) 要有更高素质的网络安全管理队伍

1.成立网络安全职能部门

高职院校要做好网络信息安全的防护工作,仅仅依靠网络管理中心来对其进行推广是远远不够的,还应该聚集全体师生的力量来共同为这件事奋斗。网络信息安全管理应该将相关的安全建设责任明确到高职院校中的每一个部门及院系。要制定更加完善的网络信息安全管理保障体系,将具体的责任落实到每一个个体上。当前,有很多高职院校的网络信息管理中心其实只是作为教育辅助部门存在的,除了给院校提供正常的技术支持之外,对于其他部门日常事务并不干涉。但在网络信息管理这方面,相关院校部门必须要能够担负起其在网络安全方面的管理职能,主动积极参与到其他部门与网络信息安全有关的管理工作中去,不断提升自身在网络安全建设方面的话语权,才能真正聚合高职院校的力量为高职院校更安全的网络信息体系提供支撑。

2.要不断完善相关用人制度

高职院校还应该进一步重视网络信息安全管理中心相关人才配置,要注重对高层次管理人员以及专业技术人才的不断引进。同时要确保这些人才在实际进行相关管理工作落实的过程中要有最为明确的分工,分别负责网络信息安全相关的一个分支,如网络建设,信息安全治理,资源管理等等。当前网络信息安全方面的优秀人才是比较缺乏的,因此部分高职院校会直接与专业的安防企业合作,将相关网络安全技术工作交给第三方机构。但在实际落实相关工作的过程中还是需要有一定的专业人才负责整个工作的对接,如此高职院校网络信息安全的建设与防护才能够更有保障^[5]。故而,高职院校还需要有更科学合理的人才聘用机制,要在薪资标准方面有适当地改良,从而吸引具有丰富经验以及理论基础的专业技术人才。除此之外,高职院校还可以进一步去发展校内的学生以及教师,借助于各种网络安全技术相关的竞赛来刺激对网络信息安全有兴趣的教师以及学生不断地在这方面进行钻研,也通过这种竞赛进行人才的选拔,进而去组建更加专业的网络信息安全维护队伍。

结束语

随着大数据时代的到来,以及各种计算机、信息技术的不断发展,网络信息呈现出一种大爆炸的局面,在这种背景下,高职院校学生及教师在借助于网络技术来完成日常学习与工作的过程中很可能会遭受到一些恶意的网络攻击,从而造成自身信息数据的泄露或者损坏,给学生及教师乃至学校都带去极大的损失。因此高职院校在使用网络信息技术的同时还需要构建更加完善的网络信息安全体系,要做好相关的防护工作,要有更强的网络信息安全防护意识,更高效的安全设备与防护技术,还需要不断地引进专业人才来加入到整个网络信息安全体系的建设队伍中来,不断增强对高职网络体系的防护,为教师及学生提供更有保障的网络环境。

参考文献:

- [1] 庞静娟. 高校网络信息安全与防护策略研究[J]. 计算机应用文摘, 2022(038-011).
- [2] 刘阳. 分析计算机网络信息安全及其防护对策[J]. 大东方, 2022(18).
- [3] 张波, 王韬, 代兵. 基于计算机网络信息安全及其防护对策研究[J]. 网络安全技术与应用, 2022(3):3.
- [4] 肖立志, 汤紫霖, 阳亦斌. LMD 系统网络信息安全风险分析与防护策略研究[J]. 大功率变流技术, 2022(000-001).
- [5] 杨浩然. 计算机网络信息安全在电力系统的防护[J]. 科学与财富, 2022(2):97-98.

基金项目: 2022 年度广西高校中青年教师科研基础能力提升项目教育信息化专项项目《等保 2.0 框架下校园网络安全风险识别及防护措施研究》(序号:2022XXH0010)