网格化提升高职院校师生网络安全素养的研究

Research on Grid Improvement of Network Security Literacy of Teachers and Students in Higher Vocational Colleges

白宝来

Baolai Bai

聊城职业技术学院

中国·山东 聊城 252000

Liaocheng Vocational and Technical College,
Liaocheng, Shandong, 252000, China

【摘要】越来越多的信息化技术服务高职院校的教学和科研工作,所以,高职院校师生的信息化能力和网络安全素养显得尤为重要。高职院校不同角色需要具备不同的网络安全意识,通过对高校人员进行网格化划分,深入剖析了不同身份的人员需要具备的网络安全素养层次和存在的网络安全意识问题,最终从学校和个人两个方面提出了提高高职院校师生网络安全素养的方案。

【Abstract】More and more information technology services the teaching and scientific research work of higher vocational colleges, so the information ability and network security literacy of teachers and students in higher vocational colleges are particularly important. Different roles in higher vocational colleges need to have different network security awareness. Through the grid division of university personnel, this paper analyzes the network security literacy levels and existing network security awareness problems that different identity personnel need to have. Finally, it puts forward the plan to improve the network security literacy of teachers and students in higher vocational colleges from two aspects of school and individual.

【关键词】高职院校;信息化能力;网络安全素养;安全意识;网格化

【Keywords】higher vocational colleges; information ability; network security literacy; security awareness; grid

【DOI】10.36012/sde.v2i3.1573

1 引言

随着信息技术的发展,网络安全也越来越引起人们的重视。国家层面已经将网络安全上升到法律层次,网络安全相关的规章制度相继发布实施。高职院校作为教育行业网络空间的重点监控高地,高职院校开始重视网络安全工作,对校园网络进行安全加固,进行网络安全等级测评和风险评估,对师生进行网络安全意识培训。网络安全靠的是“三分技术,七分管理”。在网络安全管理过程中,很多高校虽然都知道提高师生网络安全意识的重要性,但是效果一般^[1]。综合评价一个学校的网络安全防护体系,需要学校每个人都要具备相应的网络安全素养。需要对全体师生进行网格化分类并进行培训,共同努力才能筑起高职院校坚固的网络安全屏障。

2 网格化分析网络安全素养

2.1 学校主要领导

学校领导是学校工作的一面旗帜。校领导对网络安全的

重视程度决定了整个学校的网络安全意识水平。通过调查发现,部分学校领导对于网络安全重视程度不足,导致整个学校的网络安全工作相对滞后。一些领导不结合学校实际和网络安全态势进行决断,一味地等上级部门明确的红头文件而忽略上级部门下发的指导性文件,出现问题以后才意识到问题严重性。

在学校领导决策层,应该熟悉当前的网络安全法律法规和全国高职院校的网络安全形势。结合自己学校的现状、国家的要求和同等学校的佼佼者,从宏观上制定自己学校的网络安全防御体系结构,成立专门的网络安全领导小组,制定网络安全管理制度体系,加大网络安全建设经费预算,重视网络安全人才培养^[2]。

2.2 信息中心技术部门

信息技术中心是高职院校网络安全防御的技术骨干,在学校领导高度重视的前提下,应该设计校园网络安全整体方案,具体包括:网络安全管理制度建立和技术手段防御。网

络安全管理制度主要包括信息技术中心内部人员和普通师生的管理制度,信息技术中心网络安全管理制度应该对部门领导、网络安全管理人员、系统管理人员提出明确的网络安全职责,做到分工明确,责任明确^[9]。在技术手段防御方面,根据学校的网络架构,设计安全防护策略,提高网络安全整体防护能力。信息技术中心有义务对全校师生进行网络安全培训,定期开展网络安全培训讲座,开展网络安全宣传活动,提高广大师生的网络安全意识。

2.3 系统管理人员

除了学校信息技术中心的运维管理人员,学校各个业务部门还有专门负责业务系统的人员。这类人员在校园网络安全中也占有很重要的地位,他们掌握着业务系统的管理员账号权限。如果学校信息技术中心制定了网络安全防御方案,那么业务系统管理员的一个疏忽可能就会造成所有的防御功亏一篑。高校业务系统管理人员目前普遍存在网络安全意识较低,业务管理方面存在安全隐患^[10]。比如,账号密码复杂度设置较低,不注重账号保护,信息共享途径不正规等。曾经有一个案例,一个学工系统管理员使用管理员账号登录学工系统,中途去厕所没有退出账号。让一个外来公司的维修人员把全校学生信息导出后牟利,最后全校学生信息泄露,造成了恶劣的影响。高校学生管理人员经常会使用 QQ 群或微信群发布工作通知,甚至因为某一个任务把整个专业的学生信息都共享到群里。系统管理人员应该提高自身的网络安全意识,主动学习网络安全知识,了解相关的法律法规,积极参加学校组织的网络安全培训活动,坚决杜绝因个人网络安全意识淡薄造成的网络安全事件。

2.4 普通的师生

广大师生是校园网的主要用户,一些黑客也常利用师生网络安全意识薄弱的弱点侵入校园网。师生应该积极参加网络安全培训讲座,了解网络安全常识,比如不随便连接陌生 WiFi、不扫描不明的二维码、不轻易打开未知邮件、不浏览不安全的网站、设置复杂的口令等。同时广大师生要规范自己的上网行为,深知网络不是法外之地。近期有教师因在网络上发表了不适言论,给自己造成了严重的影响。也有部分学生因为不注重网上个人信息的保密,最后被不法分子利用实施电信诈骗。曾经有一个黑客试图侵入某高校的校园网,从公网进行渗透攻击,久攻不下。最后他购买了十个 U 盘,并植入了木马程序,然后把 U 盘随意地丢到了校门口,被在校学生捡去插入自己的电脑后,这台电脑便成了一台可控的内网终端。黑客获取了校园内网的合法身份之后,再对学校的内部网站和系统进行攻击就容易了很多。为了营造安全、健康、文明的校园

网络环境,需要每个师生提高网络安全防护意识和网络安全防护技能。

2.5 计算机专业学生

根据调查发现,虽然计算机专业的学生有一定的专业基础,但是很多学生对网络安全的知识掌握不多。非网络安全专业的学生只是了解网络安全的一点专业术语,遇到网络安全事件的时候就束手无策。比如,软件专业学生认为网络安全是单独的一个专业方向,和自己所学的软件专业没有关系。这种认识是错误的,软件自身漏洞对软件也是一个较大的网络安全隐患。如果软件在研发过程中没有将安全性考虑进去,等软件运行上线后再去处理安全隐患,将会投入更多的人力和物力。网络安全虽然是一个专业领域,但是说有专业研发工作中必须要时刻警惕网络安全隐患。网络安全专业的学生来对一些网络攻击的手段比较了解,也具备一定的攻防能力。但是调研发现,60%以上的网络安全专业的学生只懂技术不懂政策,对网络安全法、计算机等级保护工作等法律法规概念比较陌生。作为网络安全专业的学生来说,除了要掌握网络安全专业技术,更应该重视网络安全法律法规和相关行业政策的学习。高校应该注重网络安全课程的普及,让所有计算机相关专业的学生都能有一定的网络安全意识,熟悉网络安全法律法规,分层次的掌握网络安全技术技能。

3 总结

高职院校网络安全工作是关系全校师生个人隐私安全的一项重要工作。针对高职院校不同身份的人群,应该具有不同的网络安全意识,掌握不同的网络安全技能。信息化步伐在加快,各种新技术不断出现,信息化手段助力教学科研工作,让广大师生能够提高工作效率^[8]。但是这一切都应该是建立在安全可靠的基础之上,这好比幸福和谐的小家是建立在国家强大繁荣的基础之上。高职院校应该根据学校的实际情况建立一套符合现状的网络安全管理方案。这个可以借鉴但是不能抄袭,从领导层到普通的师生,需要切实的去提高网络安全意识,这样才能构建一道高校网络安全防御屏障。

参考文献

- [1]张田力.大学生网络安全现状分析及应对策略[J].求知导刊,2017(31):71.
- [2]程君.高职院校校园网络安全技术研究[J].信息通信,2013(9):177.
- [3]刘颖.高职院校校园网络安全的现状与对策研究[J].电脑知识与技术,2019,15(35):16-17.
- [4]薛强.现今高职院校的网络安全对策[J].网友世界,2012(16):15.