

# 新时代高校网络信息安全威胁与对策研究

葛 坤

(南京师范大学中北学院, 江苏 丹阳 212300)

摘要: 近十年以来, 网络信息安全越来越引起人们的重视, 国家先后连续出台了网络安全法、数据安全法等一系列法律法规, 表明网络信息安全从国家层面受到了高度重视。高校作为高等教育的前沿阵地, 网络信息安全事件也时有发生, 严重影响了高校教学管理和科研活动, 甚至会给社会带来恶劣影响。因此, 新时代下如何保障高校网络信息安全成为关注的重点。本文主要通过分析新时代高校面临的网络信息安全威胁, 并且提出相应对策, 从而促进高校的网络信息安全管理。

关键词: 网络信息安全; 高校; 问题分析; 对策分析

高校的信息化建设和推广已开展多年, 许多高校更花费巨大建设了智慧化校园系统。信息化平台从无到有, 是一个大的飞跃。将信息化平台建设成为一个安全稳定高效的智慧化校园系统, 则是一个更大的飞跃。目前, 高校教学管理工作已经离不开各类信息化系统和平台, 网络是基础、是根本, 一旦遭到破坏, 整个高校的教学管理秩序就会受到极大影响。本文首先描述高校网络安全现状及面临的各类安全威胁, 并研究提出相应策略, 希望为高校网络信息安全防护工作提供一些有价值的思路。

## 一、新时代高校网络安全现状及面临的问题

### (一) 网络安全制度

高校普遍存在网络安全规章制度不够完善、不太系统, 或者虽然有制度, 但是却嫌麻烦没有遵照制度执行, 如核心机房出入随意、入网流程不规范、网络设备随意接入、网络监控长期不在线、突发事件处理混乱等问题。网络安全管理制度不完善, 发生网络安全问题后没有规范的处理方法, 处理过程随意, 各项管理条例执行困难, 常常会导致网络安全事件恶化, 造成更严重后果。对于高校网络信息管理岗位的技术要求比其他行政岗位要高, 由于待遇或一些原因, 从业人员数量不足。在岗人员需要管理大量的硬件设备和网络基础设施, 工作强度大。若经费不到位, 缺乏培训, 也会造成人员的网络安全技术知识得不到及时更新。

### (二) 网络安全意识

高校师生网络用户群体人员众多, 大部分用户在网络信息安全问题上由于缺乏相关的安全意识, 防范意识不足。师生们在使用校园网络时通常由于有意无意的操作, 如浏览不安全网页、向外透露账号信息, 或下载含病毒的恶意软件造成内网传播感染大量终端, 这些行为给校园网络带来安全风险, 甚至会影响校园网的稳定运行。这暴露出高校在增强师生网络安全意识这个环节工作不到位, 相关培训没有做到深入, 或者流于形式。

### (三) 网络安全防控

高校的各类信息化平台由于基于网络的特点, 其交互性使该

网络系统在整个校园网络拓扑结构中容易存在薄弱环节, 也是病毒、木马、黑客攻击的重点部位。校园网在建设之初, 就会严格区分内网外网边界, 在边界部署防火墙、入侵检测系统等各类安全设备。校园网的连接模式本身就具有安全隐患, 在使用过程中很容易受到外部的病毒攻击。服务器系统本身存在不同程度的安全漏洞或业务系统存在软件代码 BUG, 这都会导致校园信息化系统难以抵御长期的、花样不断翻新的攻击策略。边界安全设施如防火墙没有及时升级导致规则过期, 也无法起到保护内网的作用。

### (四) 外部网络威胁

常见的外部网络威胁包括网络入侵、计算机病毒和蠕虫、后门及木马程序等。随着互联网的发展, 黑客非法入侵事件越来越多, 黑客入侵目的从起初的技术炫耀、破坏服务, 到如今以入侵系统窃取重要信息资料获取非法利益为主。计算机病毒的隐蔽性也越来越强, 越来越难被发现。蠕虫病毒会利用系统或者程序暴露出来的一切薄弱点, 一旦入侵到计算机系统中就会将带来严重损失。勒索病毒, 由于其发作时会将用户重要文件和数据进行加密, 来对用户进行勒索, 更是需要对其严重关切和防范。后门技术是黑客进入网络系统的重要方法, 木马是后门技术的一种特殊形式, 木马程序一旦成功进入计算机系统内, 黑客就可以远程控制计算机。

## 二、新时代高校网络信息安全的对策研究

### (一) 层层落实网络安全责任

高校要着力落实网络信息安全工作职责, 做到安全到人、责任到岗, 确保网络安全工作落到实处。在高校网络信息安全领导小组的领导下, 每一个部门和每一位工作人员都要承担起身上的责任、全面提高网络安全管控能力, 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的工作分工开展网络信息安全工作。

### (二) 加强网络安全意识教育

要强化高校师生的网络信息安全意识。网络信息安全意识培养工作应该从上而下, 从高校领导到师生都要树立起网络信息安

全意识。高校网络安全管理部门要根据网络安全政策和上级部门要求,规划校园网络安全框架,提出安全体系建设建议,高校一把手作为网络安全第一负责人,要提高网络信息安全维护工作的重视程度,要在人力、物力和财力上给予网络信息安全工作支持。同时,强化网络信息实时监管力度。建立起一支网络舆情管理队伍,要求各部门加大对高校网站、部门子站、专题站点的内容审核和监管力度,安排专人负责每天对网站和应用系统进行监管巡查,发现非法内容及时固定证据和技术处理。网络信息监控工作应该常态化。

网络信息安全管理位于安全工作的第一线,必须要具备扎实的网络安全技术,高校应该定期组织网络管理人员培训学习,提高网络信息安全管理人员的技能和管理水平。高校二级部门信息系统管理人员缺乏网络信息安全意识,对于网络信息安全维护工作比较敷衍,即使网络信息安全管理通过多种途径提示查缺补漏,仍然存在服务器和数据库弱口令的现象。高校需要定期组织培训,加强安全教育,提高网络管理部门的网络安全意识,并建议将安全服务商提供的系统安全漏洞作为部门业绩考核扣分项。学生是高校网络使用最大的群体,尽管学生们对于网络具有较大的依赖性,但他们网络安全意识普遍不强。高校可以考虑在新生入学时加入网络信息安全知识培训并进行考核。

### (三) 构建网络信息安全屏障

要重视构建网络信息安全屏障,建立网络安全维护机制,采取科学合理的安全保护措施。1. 加强对网络基础设施的保护。网络基础设施是网络环境的重要组成,也是网络信息安全维护工作开展的首个工作对象,要防止可以破坏网络基础设施的事件发生,采取措施最大可能避免意外事件对网络基础设施造成损伤,高校要重点加强对交换机、服务器、路由器、网络机柜和基础线路保护,为网络信息安全建立第一道保护屏障。2. 加强对高校计算机软件系统的安全保护。高校引入了种类丰富的各类计算机软件系统来开展专业教学和管理。计算机软件的增加为高校教学工作提供了便利,但同时也增加了信息安全事件发生的可能性。一些高校在计算机系统中安装了很多软件,不少在教学工作中并不常用,而软件长期闲置、得不到及时更新和维护就很容易导致其漏洞被利用。因此高校要加强对计算机软件的检测,科学引进和安装计算机软件,定期检测软件的使用频率,将无用的计算机软件及时删除卸载,对各类网站和应用系统服务器、数据库进行安全加固,采取版本升级、安装漏洞补丁、查杀病毒木马、用户密码加固、清理无关用户等技术措施,提升服务器和数据库安全。会同安全产品厂商,对校园网络安全设备进行合理的安全策略部署和调整,进一步提高服务器和应用系统的安全防护等级,减少病毒入侵的

可能性,进而提高高校网络安全,维护工作效率。

### (四) 高效防范外部威胁

随着互联网技术的发展,外部威胁的种类、复杂性不断增加和升级。与此同时,信息安全维护工作也需要不断升级。高校需要引进更新更高效的反威胁设备和技术,从上网行为管理设备、流量控制设备,至服务器群的WEB应用防火墙、漏洞扫描、下一代防火墙,以及网络杀毒软件、关键服务器区的网闸设备、堡垒机等方面着手,打造多道屏障维护校内网络信息安全。部署网络安全态势感知平台,实现事前预警、事中防控、事后审计。

比如,在优化网络信息安全过程中,高校可以加强对病毒检测技术的应用,利用病毒检测软件定期对网络系统进行病毒检测和查杀,一方面可以及时发现病毒的入侵痕迹并将其杀灭,以保障高校网络信息安全;另一方面也能做到防患于未然,避免高校网络信息外漏、损毁以及系统瘫痪,从而提升高校网络环境的安全性及可靠性。现有的专职网络信息安全管理受各方面因素影响,在技术水平上难以应对越来越多、越来越新的网络安全威胁。在这种现状下,很有必要购买第三方网络信息安全服务,利用网络信息安全公司的专业服务弥补高校在技术方面的短板,提升防御安全威胁的能力和响应速度。对于高校重要的应用系统,凡是对外提供服务的,建议一定要通过网络安全等级保护测评。

## 三、结语

网络信息安全作为国家层面这几年越来越重视的内容,高校需要把网络信息安全作为工作的头等大事来抓。高校的网络信息安全不仅仅要依靠网络信息管理工作人员,也不是部署了安全设备我们就可以高枕无忧,而是需要让每一个网络使用者参与其中,充分利用网络安全设备,提高安全意识,增强安全防护技术知识的学习,协同推进高校的网络信息安全建设,建立一个安全、稳定的网络环境。

## 参考文献:

- [1] 田由辉. 教育信息化 2.0 背景下智慧校园的网络信息安全治理研究 [J]. 信息技术与信息化, 2020 (10): 184-187.
- [2] 张伟. “互联网+”背景下高校学生网络信息安全教育与防护策略研究 [J]. 湖北开放职业学院学报, 2019, 32 (10): 49-50.
- [3] 卓家. 大数据背景下高校网络信息安全初探 [J]. 中外企业家, 2018 (33): 69.
- [4] 李学强. 高校信息化建设中网络信息安全对策思考 [J]. 黑龙江科技信息, 2016 (02): 175.