

高校网站安全防护措施与管理制度的探讨

郭 锋

(黑龙江林业职业技术学院信息工程学院,黑龙江 牡丹江 157011)

摘 要:随着高校信息化的发展,高校网站安全问题日益突出。本文分析了高校网站的现状,针对如何提高高校网站安全防护能力提出了几种参考意见,并对高校网站管理制度进行了初步的探索。

关键词:网络安全;网站;管理制度

[DOI]10.12231/j.issn.1000-8772.2021.02.320

1 引言

二十一世纪伴随着互联网信息化的高速发展,高校网站在高校教育教学、科学研究、管理服务中扮演着越来越重要的角色,是高校信息交换和信息发布的重要平台。高校网站也是对外服务的窗口,是高校重要的宣传互动平台之一,是高校与社会沟通、传递分享信息的重要桥梁,也是了解高校和获取高校重要信息的主渠道。与此同时,高校网站也会直接面对各种网络安全威胁,被黑客恶意攻击现象屡见不鲜,重要数据被窃取、篡改或破坏,甚至全站崩溃,对高校造成非常严重的影响。因此,高校网站如何做好安全防护工作,已经成为各高校急需解决的问题。

2 高校网站管理现状

现阶段,我国高校的网站管理主要存在网站建设和管理不统一、网站维护技术力量不足、对于网站安全意识淡薄、网站信息保护措施薄弱等安全隐患,为黑客入侵提供了机会。

(1)高校网站建设和管理不统一。我国大部分高校由于网站建设人员和经费等问题,一般高校门户网站和二级部门网站分属于不同的部门建设与维护,其中很多网站由高校教师、学生等进行建设、管理和维护。由于网站建设、管理、维护的技术和水平参差不齐,从而导致高校网站安全整体上管理十分困难。

(2)网站维护技术力量不足。高校网站中的大部分二级部门网站的维护人员基本上都是进行网站内容的维护,维护人员的技术能力水平有限,甚至有很多网站维护人员只会简单的计算机操作,缺乏必要的网络安全知识和网络安全维护技术,网络安全意识淡薄,对网站经常遇到的安全威胁知之甚少。对网站的服务器安全和系统漏洞等问题根本没有能力进行维护,即使被检测出有安全威胁也无法处理。常见漏洞如 SQL 注入漏洞、弱口令漏洞、远程命令执行漏洞、权限绕过漏洞等对高校网站的攻击重复出现。

(3)对网站安全不重视,网站信息保护意识差。虽然 2017 年《中华人民共和国网络安全法》已经正式实施生效,明确的网络运营者的责任和义务,但是各级领导依然抱有不会出现安全事故的侥幸心理。制定了很多规章制度,但是没有得到充分落实,形同虚设。

3 如何提高网站防护能力

针对目前高校网站普遍存在的安全性问题,笔者建议可以采取以下五个方面的应对策略来提高网站防护能力。

(1)网站安全性设计。如果采用自主开发或定制开发,在开发设计之初就要有总体要求和统一的标准,尽可能避免网站程序漏洞。网站程序运行前要聘请专业安全测试单位进行网站安全测试。如果经费条件允许的情况下可以购买成熟的、专业的、安全性高的高校网站群管理系统,这样可获得及时的维护和升级服务,提高网站安全性。

(2)构筑网站安全防护对策。可以采用防火墙技术强化网络安全策略,对网络存取和访问进行监控审计,防止内部信息的外泄;可以采用入侵检测系统主动保护自己免受攻击,可以作为防火墙后的第二道安全防线,能够做到准确防御,可以有效保护网站系统安全;可

以采用防毒墙,部署在防火墙与服务器之间,专业过滤病毒、蠕虫,可以针对重点网段进行深度的保护;可以采用 WEB 应用防火墙(WAF)实时对 Web 层访问进行入侵检测,并对发现的入侵行为进行及时拦截;可以采用网闸通过硬件隔离网络,拦截未知的木马程序;可以采用上网行为管理来规范高校教职员工和学生的上网行为。

(3)网站服务器的安全加固配置。可以采取操作系统定期更新;配置 IIS 服务器的安全;在服务器上安装 EDR(终端安全响应系统)、防篡改软件等安全软件;不定期更改管理员用户名和密码,密码一定要使用强壮性高的安全密码;卸载不需要的网络服务,关闭系统默认端口,禁止远程桌面等服务。

(4)加强网站文件的安全备份与恢复。为了进一步保障高校网站的安全,应该定期对网站文件进行本地备份和异地备份,以确保网站数据安全,当网站一旦出现安全事件,可以很快恢复网站的运行。

(5)进行网络安全等级保护测评。可以通过网络安全等级保护测评,找出自身网络安全不足,积极进行整改,快速提高网络安全水平。

4 高校网站管理制度建设

4.1 提高高校各级网站管理人员的网络安全意识

定期对网站管理人员进行网络安全培训,从意识和技术两个层面提高网站管理人员的水平。对网站上传内容进行严格审核,实现分级分类审核、先审后发。

4.2 建立严格的网站管理规章制度

实行安全责任人制度,明确安全责任主体,强化网站管理人员的责任心。定期对网站进行安全检查,定期备份,发现问题及时处理。

4.3 建立网站安全应急预案

要针对网站可能的网络安全事件,建立应急处置预案和专项应急预案,并定期做应急处置演练。如针对木马病毒要实现一键断网、迅速恢复网站。针对系统故障,立即启动备用服务器。针对操作系统漏洞要及时安装漏洞补丁程序等。

5 结束语

高校网站安全防护与管理是一项长期而艰巨的工作,任何一个细小的漏洞与疏忽都可能导致整个网站受到网络恶意攻击威胁。因此,我们要不断的探索网络安全防护策略和管理制度,提高网络安全意识,确保高校网站安全、稳定、可靠的运行。

参考文献

- [1]中华人民共和国网络安全法,2017.
- [2]中央网信办,国家网络安全事件应急预案,2017.
- [3]信息安全技术 信息系统安全等级保护定级指南,GB-T22240-2012.

课题:本论文为黑龙江省教育厅 2019 年度高等职业教育教学改革研究项目《网络安全等级保护 2.0 制度下智慧校园网络安全防护措施与制度建设研究》(课题编号: SJGZZ2019030)阶段性成果