浅谈构建高校网络安全治理与技术防范体系

朱明如

（武警警官学院模拟训练中心 四川 成都 610213）

[摘 要] 随着互联网+时代到来，大数据、云计算、区块链等新技术蓬勃发展，高校信息化建设与发展日趋成为高校教育现代化建设的重要组成部分，与此同时其面临的网络安全和信息安全事件面广量大、成因复杂，呈现出与网络化、信息化密切相关的特点规律，对高校网络安全工作发起了新的挑战。本文分析了高校信息系统及网站平台安全现状及其面临的常见安全隐患，初步探索总结了高校网络安全治理与技术防范体系。

[关键词] 高校；网络安全；技术防范

高校网络安全和信息安全工作是指通过制度上、技术上、管理上的手段对网络和信息系统网站平台采取安全防范措施，确保高校基础数据和师生用户信息安全。随着信息技术革命时代日渐严峻的网络安全和信息安全形势，对高校网络安全治理和技术防范体系的构建提出了新的更高的要求。

一、高校信息系统及网站平台安全现状

高校信息系统及网站平台作为服务平台，主要提供教学信息服务、机关办公、图书信息等服务。当前，高校大多数应用服务为B/S架构，其开放性造成缺乏有效的安全管理、用户IP可外部访问、开发成本低、年久失修成为“僵尸网站”、缺乏专业技术人员、缺乏必要的安全技术防范措施等原因，造成网站及系统容易感染木马病毒、被恶意攻击等情形。同时，还存在黑客、内部人员等进行恶意攻击或窃取操作的可能性，造成信息失泄密、数据丢失等严重后果。常见的安全隐患主要有以下几种：

第一类是弱口令。其一是大量默认密码、简单的密码等弱口令存在于网站系统、业务系统、服务器、数据库系统等管理设置中，以及用户初始密码多使用弱密码、弱口令，而安全产品对弱口令行为无效；其二是拖库、洗库、撞库等恶意行为，致使用户信息数据丢失或被盗。一个典型的案例就是2015年初海康威视“安全门”事件。

第二类是SQL注入。针对信息系统及网站开发程序中存在的漏洞，用户可以植入一段数据库查询代码，根据程序返回的结果，获得某些想要得知的数据，其本质是由于开发程序对输入检查不充分，导致SQL语句将植入的非法数据当作语句的一部分来执行，而高校大部分的SQL注入是高权限，存在信息数据失泄密风险。

第三类是XSS攻击。XSS攻击的本质在于插入的执行脚本，恶意攻击者利用系统漏洞往Web页面插入恶意代码，当用户浏览该页时嵌入其中的码脚本会被触发执行，从而达到恶意攻击用户的特殊目的，例如获取正在浏览的cookies信息、捕捉用户操作并定向发送、利用浏览器漏洞控制用户机器、窃取用户隐私信息等。2011年6月底爆发的新浪微博XSS攻击事件，致使在不到一小时的时间里，超过3万微博用户受到攻击，便属于典型的反射型XSS攻击。

第四类是上传漏洞。包括文件解析漏洞、常见编辑器漏洞、第三方平台漏洞等，黑客可利用上传漏洞通过特定工具进行篡改网站首页、获取管理用户名口令、数据库权限等非法行为。需要注意到的是，基于上传漏洞的Webshell攻击查杀比较麻烦，不仅需要细致排查日志，还需要利用专用安全工具扫描脚本排查端口、查找系统后门，耗时耗力且效果不明显。

第五类是操作系统漏洞。近些年多次爆发针对高校、企业等机构的大规模蠕虫病毒攻击，黑客利用Windows操作系统漏洞对缺乏杀毒软件保护的电脑终端进行攻击，通过网络进行传播感染、锁定用户主机、篡改用户文件甚至进行恶意勒索。一个典型的例子是2017年5月WannaCry勒索病毒全球大爆发事件，我国部分高校数万名Windows用户遭受该病毒攻击、感染，大量实验室数据、毕业设计和用户重要文档数据被锁定加密，造成严重损失。

二、高校网络安全治理与技术防范重点工作

高校信息网络管理机构应当针对信息系统和网站平台常见安全隐患特点，在落实网络安全等级保护制度的基础上，主要从信息资产确定与保护、建立网络准入鉴权、推进信息系统安全评测、落实安全巡查和应急响应机制等层面加强防范，有效应对各类安全风险，确保各类业务信息系统和网站平台安全稳定运行。

（一）信息资产管理。高校网络安全治理要以信息资产为中心，坚持安全建设和信息化建设融为一体，像网络管理一样来规范化梳理信息资产，建立健全信息资产管理制度。在信息资产台帐管理的基础上，通过漏洞扫描、跟踪，建立全生命周期漏洞管理；部署资产普查及技术保障，实现信息资产发现识别、自动建档，动态实时进行信息自查全生命周期过程管理，最终确保所有的网站、信息系统等信息资产“可知、可控、可管、可关”。

（二）网络准入鉴权。建立网络检测准入鉴权机制最重要目的是通过接入强制技术，进行用户身份认证和终端完整性检查，实现全周期的安全管理。这种通过强制技术手段对不符合要求的终端进行网络阻断、隔离与告警，对符合要求的终端授权接入与安全检查，实现网络层到系统层接入的全面深度控制，能够极大节省人力维护成本。

（三）推进信息系统安全评测。根据《网络安全法》要求，落实网络安全责任，建立网络安全等级保护制度，推进对各级上线的网站、系统、平台等信息系统安全评测工作，对评测合格的予以上线，对评测不合格的予以下线并限期整改，先断网后整改，整改完成通过安全评测后方可重新开放。

（四）落实安全巡查和应急响应机制。建立安全巡查制度，定期进行漏洞发现修补，定期巡检核心设备和数据中心机房，通过威胁情报共享、教育系统漏洞平台，定期通报发现危险主机、高危网站、脆弱帐号等问题，责令限期整改；同时成立网络安全应急响应小组和应急预案，应对紧急时间做到事前、事中、事后按预案有序处置。

（五）健全安全联合防护体系。积极与安全厂商、互联网企业、网络设备厂商、高校等建立合作共享机制，实现联合防护；引进云平台、Web防护等安全产品实现统一管控，对核心设备和重要目标进行必要的系统加固与升级，提高安全保护能力和异常发现能力，提高有效的溯源能力；加强网络安全培训特别是对接入用户的培训，严格身份认证、规范上网行为、屏蔽不良信息，确保网络和信息系统平台安全。

参考文献

[1]王阳.高校数字化校园信息安全策略探讨.中国教育信息化，2011，5

[2]叶周锋.高校网络安全工作的现状与对策研究.信息系统工程，2018，3

[3]袁林德.高校网络安全技术防护体系的构建.计算机产品与流通，2018，1

[4]李永娜.高校校园网络安全问题的研究和解决策略.信息系统工程，2017，12

作者简介：

朱明如（1982-5-），男，汉族，四川成都人，助教，学士，主要从事模拟仿真训练、网络安全和教育信息化工作研究。