高校网络安全现状分析及风险应对

李梦轩
（南京信息工程大学，江苏 南京 210000）

摘要：信息技术的迅猛发展助推高校信息化平台建设，高校信息化网络安全问题也逐渐受到重视。高校网络安全体系防护能力参差不齐，也有部分高校存在网络安全重视程度不足的问题，致使高校成为网络安全事件发生的重灾区。高校网络安全风险管控应当从体系建设方向着手，从多个角度加强安全建设，国家教育管理部门和社会企业等多主体共同参与，推进校园网络安全防护体系建设，维护好高校网络安全空间。

关键词：高校；网络安全；风险应对

随着时间的推移，计算机技术的迅猛发展，使得人们对于网络实践需求愈加强烈，在教育领域同样如此，进而让校园网络、信息服务体系建设等流程，使得高校管理工作和运行模式更加便捷，也能为学校网络安全建设带来勃勃生机。高校在传统网络建设过程中，并未对安全问题加以重视，高校近年来频繁出现网络安全事故，在检测网络安全风险过程中，需要及时应对现阶段出现的安全事故问题，已然成为各大高校安全建设亟待解决的问题。

一、高校网络安全现状

（一）校园网络基础建设相对陈旧

从 20 世纪九十年代始，我国高校逐渐完善校园网络建设，校园网络也是践行学校各项信息化基础的前提条件，同时也能辅助教学活动、实践探究、数据检索和设备通信。学校内部的网络通信建设起步较早，其使用周期时间较长，也会产生大量的维修费用，通过多年的建设活动，学校内部的网络数据量激增。然而高校使用的建设经费受限，不能让校园网络全面升级，很多存在网络基础建设不均衡、网络终端建设使用期限等等。网络攻击人员会使用不同漏洞获取各类权限，从而对校园网络完成入侵或是攻击，进而给学校内部的网络环境产生安全隐患。

（二）信息系统建设并不规范

学校内部的网络建设和体系建设数量较多，在实际建造过程中会重视其使用效能，并没有重视这一应用的安全性，缺少对信息建设的标准化建设和实际需求，大多存在不同部门之间并未互通交流的情况。部分学校系统网站是由小组或是个人建立的，使用的技术能力相对薄弱，并未经过系统的安全性测试，很多功能性问题以及安全漏洞；部分系统运营的服务其终端体系使用版本较低，一旦出现问题不能及时补充安全漏洞；部分终端运营服务使用环境版本较低，有的系统在运行维护阶段缺少相应的维修人员，致使安全配置并未完善，又或是存在后门的风险。高校内部的信息系统会大量存储师生信息，网络攻击人员会使用漏洞部分完成数据剽窃，进而造成校园网站瘫痪、内容被篡改等事故。

（三）系统管理者及用户安全意识薄弱

大多数情况下学校内部的信息系统管理人员由校内教师担任，部分管理人员不见得具备相应的技术管理素养，大多存在管理尚未规范、信息保密意识不强、信息化素养较低等问题；学校内部师生是校内各类信息体系的主要使用者，在应用各类实践活动时，大多重视其应用的便捷性，安全意识相对薄弱。

不论是后台管理还是前台终端应用弱口令、账号密码维护问题层出不穷，容易被网络攻击者破解入侵，导致信息泄露等严重问题。

（四）安全体系及配套人员缺乏

网络安全的本质是攻防对抗，高校配备专业的安全管理人员是提升高校网络安全防护能力的重要保障，决定着高校网络安全防护体系的建设发展。然而，大学的安全系统建设普遍不完善，对网络安全工作的投入人数不足或缺乏专门的安全人员，导致大学的网络安全管理力度不强，处理安全漏洞的速度缓慢，网络安全风险难以控制。

二、当前校园网络安全中存在的风险因素

（一）不同学校之间的信息安全防护能力不同

由于互联网的使用与管理的系统保护状况各异，学校的大多数网络安全使用及管理通常是由不同的供应商负责，而这些供应商的能力对整个系统的网络安全防御有重大影响，这使得其安全防卫能力差异较大，并且这种差距也反映在所有校园的信息平台上，同时一些大学没有建立完善的网络安全架构，从而增加潜在的风险。

（二）学校网络安全重视程度不足

许多人误以为学校的网络安全问题不如其他研究机构那样关键，因此其保护级别相对较低。此外，当出现安全问题时，学校往往采取的是事后修补的方法，而非实时评估并作出反应。他们没有足够的防范手段来防止潜在的安全威胁。最后，很多大学对与网络安全相关的基础设施和软件工具了解不够深入，即便有这些装备，却难以充分利用它们。当前，大部分高等院校尚未建立完善的网络安全系统或配备专业的网络安全管理者。这种状况使得他们的网络安全意识落后于互联网行业的进步。

（三）师生缺乏正确认知

新时期的建设发展，互联网络逐渐成为人们日常生活中不可缺少的部分，在高校教学过程中，互联网络的应用普及愈加高涨，但是仍存在部分认知不足的问题。在 2017 年，一场全球范围内的网络危机——“永恒之蓝”爆发了，其中包括中国的一些大学成为了主要受害者，他们遭受了勒索软件攻击并需要支付巨额费用以获取解密和恢复文件的能力，这给重要的数据带来了严重的破坏。这次的事件表明，只要我们在日常生活中保持良好的互联网使用行为，积极学习网络安全知识，就一定能在预防方面发挥出一些效果，即使是在事情发生之后，也可以减少或防止可能产生的损害。目前，大学生们对网络安全的理解不足已经构成了高等教育机构网络安全的潜在威胁。

三、建设高校网络安全风险防控的主要路径

（一）按照科学原则，合理划定安全防护体系

构建全方位的安全防御架构能增强学校内的总体防卫力量，同时也有利于推动高等教育机构的信息科技进步。这要求我们遵守以下几个准则：首先是级别保护的原则，即所有安全系统的设计都需严格按照教育部和公安机关对信息技术的安保等级评定标准来执行，并且要依据每个应用程序所对应的保安水平进行搭建；

其次是以集成方式设计的理念，通过整合技术框架和管理框架的方式优化安全系统的发展；再次是重视技能和管理的结合策略，采用技术手段和运营管理方法共同实施安全防范措施，把不同的安全技术融入到运作管理体制中，正确的安全观念指导，技术训练，以及安全规定制定等环节；最后是基于现有网络构架和管理模型的安全区划规则，要在确保安全的前提下，实行灵活且易于使用的区域分割，用最低成本实现安全区的划分和网络整理。

（二）加强网络安全体系建设，提升运营维护能力

加强高校网络安全防护设计，离不开下述操作：第一，对于安全技术环境的设计时，首先要考虑安全区域的边界设置，比如在外网出口处配置应用安全防护系统，以抵御和减少 Web 安全威胁和风险。其次，需要提升内网主机的防病毒能力，搭建防病毒服务器，负责规划终端主机的防病毒策略，例如在内网设立统一的升级服务器。其次，关于安全通信网络的设计，应首先实施流量管控，对网络流量进行全面监测和管控，优化带宽使用，增强网络管理的可视性，帮助组织构建可视化、可控制、可优化的高效网络。其次，要确保通信完整性，采用强加密方法保障重要敏感字段的机密性和通信安全性。最后，关于部署综合运维审计平台，收集所有服务器、网络设备和应用系统的日志，进行智能关联分析。为了构建网络安全管理体系，我们需要重点关注几个关键领域：首先是创建专门的安全管理部门来负责学校的网络信息化建设和运营维护任务；其次是要遵循并执行国家的相应法规，以制定符合校园实际需求的网络安全管理办法；再者要设定专业的网络安全技术职位，全职处理学校的网络安全事务；此外还要强化对网络安全系统的整体运营管理，例如网络运行环境控制、资源管理、媒介管控、硬件设施管理、监测与安全保障、系统安全监管等等；最后还需要建立紧急应对机制和事故处理方案，为可能发生的网络安全问题提前准备一套科学合理且高效的工作程序，以便在出现网络安全危机的时候，能迅速、有条理、有效地启动应急反应措施。

（三）加强安全平台预警机制建设

安全的警报制度涵盖了多项内容，其核心是由四大模块组成：首先是入侵检测，这是一种利用仿真进攻方式来识别软体安全隐患的方法，它能直接向负责人展示他们网络可能遇到的风险状况；其次为危险度评定，这是借助第三方的力量全面审视现有的系统，通常会使用如实地考察、手动审查或其他设备探测等方式完成此任务后，再依据评价的结果制订出有关危害性和管理的计划；再次就是安检程序。这需要运用专门的技术装备去检验信息的完整程度，找寻到任何可疑的地方并将它们记录下来形成一份详细的信息反馈文件供参考处理意见；最后则是加强防御措施。根据具体的情况设计合适的试验策略、防护办法及其恢复步骤，再用像打上修正包、调整保护设置或者增设新的保安功能这些手法提升网络抵御危机能力以此达到整体更高的安全感水平。

（四）建设文件式校园安全网络整体策略

设计涵盖了网络安全的各种规则和指南，包括场所、设施、设备、系统、数据、构建、运营及技术文件等方面，以确保详尽的安全管理准则得以实施，同时明晰系统的建设和运作过程中的工作人员职责和操作标准，以此作为校内网络安全管理的参考依据。确立并且建立了学校的网络安全政策，制订出整体的网络安全计划，给各相关部门提供了执行操作规范和展开安全工作的指引。持续地修正和优化管理条例，以便应对网络安全挑战，进一步提升管理效率。对于网络安全负责人来说，他们需要增强自身的网络安全管理能力；而拥有较高权限的使用者必须遵循严谨的操作步骤；所有网络使用者都应严格遵照相关的法规。由于互联网技术的快速进步，网络病毒和恶意软件也随之升级，因此我们需加强日常预防措施，降低网络安全事故的风险。具体而言，由学校的信息技术部门负责编写关于硬件、操作系统、数据库和应用程序维护的所有阶段的具体操作方法和行为准则，并对这些细节做出更深入的规定，定期公布潜在的安全风险提示，使全体师生都能了解到并采取相应的防护行动。

（五）加强技术防护体系建设

鉴于互联网的信息传播渠道广泛且难以追踪的特点，加上存在安全隐患、有害网站和“网络黑客”等问题，这对于大学校园网络安全带来了巨大的压力。特别是在无法有效监管匿名用户时，一些不适合公开或者不健康的资讯可能轻易地进入学校。为了保障系统建立和日常运营的管理，需要实施自动化的防护机制以增强系统的防御能力，并为应用程序和服务用户创建稳固的安全屏障，具体包含：首先是访问控制。大学的网络安全主要依赖于防病毒软件、防火墙技术和认证方式等手段。首要任务就是设立访问控制，其目的在于防止未经授权的人员接触到学校的网络资源，并且要求所有登录校园网络的用户必须输入唯一的密码。同时，利用防火墙来隔绝外网和内网之间的连接，并对数据流动进行严密监测，并在防火墙处留下详尽的日志记录以便日后追溯。其次，打造三种独立的环境，确保正常运作环境的安全。把系统研发、测试和实际操作分成三个不同的环境，避免在开发过程中和测试期间的活动干扰正常的服务运转。构建版本控制体系以保障软件源码在开发阶段的安全性；由于项目开发通常涉及多个人员的协同工作，因此有必要追踪并记录系统的建构历程，包括相关的文件资料和源代码的变化情况，以此来防范因意外遗失或覆盖造成的代码损失。此外，我们还需关注物理环境的安全性，制定备份与复原策略，从而保全我们的系统建设成果。物理安全防御是维护校园网安全的基石，应预防如自然灾害、物理损害、电磁泄漏、操作错误和人为干涉等因素导致的网络设备和线路受损，对于关键设备必须实施严密的管理措施。我们要设立本地和远程的数据备份及复原标准计划，定期保存系统建设的成果，以免因手动操作错误或机械故障造成数据丧失，真正做到数据的安全可靠。

四、结语

综上所述，为了维护高校内部的校园网络安全平稳运行，需要从多个角度持续发力，同时也要增加自身安全防护体系建设。一同解决高校安全网络问题。对此，高校需要逐步提升学生日常工作管理体系，加大对学生的监管力度。指导学生建构更加完备的校园网络使用环境，旨在提升学校安全性能，让学生可以轻松上网，并维护校园网络的安全性。

参考文献：

[1] 朱海龙，胡鹏 . 高校校园网络安全管理问题与对策研究 [J]. 湖南社会科学，2018（5）：98-109.

[2] 陈敏锋 . 高校网络安全现状分析及风险应对策略 [J]. 生活教育，2022（36）：3.

[3] 陈跃辉，王以伍 . 高校网络安全现状分析及风险应对策略 [J]. 中国医学教育技术，2019，33（1）：4.

[4] 周争蔚 . 大数据背景下的高校网络思想政治教育安全风险分析 [J]. 科学咨询，2020（1）：1.

课题来源：南京信息工程大学党建研究课题，名称：总体国家安全观视域下高校风险防范对策，编号：2023NXDDJ-ZD03

作者简介：李梦轩（1993—05），女，汉族，江苏南京人，硕士研究生，南京信息工程大学助理研究员。主要研究方向：教育学、法学。