教育行业信息系统网络安全风险分析与安全防护措施分析

杨 帆

重庆市教育信息技术与装备中心，重庆 400020

[摘要]随着信息化在各个领域的渗透，为教育改革发展做出重要贡献。基于信息化开展教育，形成网络系统，为学习者带来更丰富的教育资源，满足学习者的需求。与此同时，网络安全风险会攻击教育行业信息系统，对系统内容篡改，影响系统安全。随着教育信息资源上线，提高网络安全风险意识不容忽视。基于教育行业信息系统网络安全问题，分析安全防护措施，增强网络安全防御能力，落实好网络安全责任制，确保信息系统网络能够完善防护措施，明确保护对象，构建安全管理体系，防患于未然。

[关键词]教育行业；信息系统；网络安全；风险分析；安全防护

DOI：10.33142/fme.v3i5.7097 中图分类号：G434 文献标识码：A

Network Security Risk Analysis and Security Protection Measures Analysis of Information System in Education Industry

YANG Fan

Chongqing Education Information Technology and Equipment Center, Chongqing, 400020, China

Abstract: With the penetration of information technology in various fields, it has made important contributions to the reform and development of education, so as to carry out education based on informatization, form a network system, bring more abundant educational resources for learners, and meet the needs of learners. At the same time, the network security risk will attack the education industry information system, tamper with the system content, and affect the system security. With the launch of educational information resources, improving the awareness of network security risks can not be ignored. Based on the network security problems of the information system in the education industry, this paper analyzes the security protection measures, strengthens the network security defense ability, implements the network security responsibility system, ensures that the information system and network can improve the protection measures, defines the protection objects, and constructs a security management system to prevent the trouble.

Keywords: education industry; information system; network security; risk analysis; safety protection

引言

网络的发展和移动，信息安全关乎到社会稳定、公民权益等方面。网络安全与信息化发展，需要统一谋划部署。面对教育行业信息化发展，应认识到信息系统的重要性。新时代背景下，信息化与网络安全同等重要，需要有效识别信息系统网络风险，对风险进行识别的同时，建立完善的安全防护措施。防止网络攻击进一步向系统渗透，为教育行业发展提供保障。

1 教育行业网络安全现状以及常见安全误区

1.1 发展现状

随着互联网等高新技术发展，为教育行业革新提供新的契机。基于信息化不断渗透，教育行业当前进入了信息化发展模式。但是信息化建设发展至今，网络攻击等风险不断朝向系统和现实世界渗透，带给教育行业发展极大的难题。教育工作者难以应对网络安全风险，保障行业信息系统安全，成为当前亟待解决的关键点。各类教育网站、信息系统建设过程中，方便了教育行业发展，同时也带给系统较大的网络风险。根据国家网络安全法等规定要求，将网络系统安全防控手段，看成是检验网络强国建设的重要手段。通过模拟演练，对网络安全综合防控能力进行优化。积极组织各级单位开展攻防演习。以三通两平台为主要抓手，在演习中不断对问题进行总结，从而提供有效的应对措施。

通常信息系统建设运行过程中，需要面对的网络风险，通常对以下三类信息系统造成影响。第一类是统计类系统，内部存储了大量的个人信息，涉及到教师学生等信息，甚至包含师生的家庭住址等私人信息。保障信息系统安全，对于师生的数据信息有极为重要的作用；第二类为资源类系统，系统平台上存储了大量的教学资源，也是学生登录会优先观看到的内容。一旦信息系统被侵入篡改，可能将一些不良信息发布在网站中，影响用户使用观感；第三类为教育政务办理系统，负责管理学生考试、学业测试等工作。此类系统关乎到学生发展与社会稳定，一旦遭到黑客攻击，将严重影响社会秩序[1]。

1.2 常见网络安全误区

当前，关于信息系统安全网络防护管理，部分技术人员对网络安全认知不足，导致实际维护过程中，出现以下的安全误区。技术人员忽略网络安全部署，通常采取先建

系统后维护的方式，在信息系统投入使用后，网络系统开发应是由内而外。在构建系统的过程中，根据不同风险预先做好安全防控，才能对系统进行有效保护。内部环境缺少良好的安全网络防护管理，一旦外部受到攻击，内部系统缺乏应对措施，将会导致系统被攻击。此外，网络安全是技术人员的主要职责。信息系统网络安全技术，网络系统安全薄弱的环节不加以完善，对系统本身造成影响。重大网络安全事故，多数源于人员操作失误，或是抱有侥幸心理，认为网络安全离自己很遥远。面对教育行业信息系统面临的威胁日趋严重，可以看出网络安全离现实生活并不遥远，应针对系统网络安全风险进行分析，构建完善的应对措施。

2 教育行业信息系统网络安全风险分析

当前教育行业应对网络威胁，应针对系统网络安全风险进行分析。按照系统不同，教育行业信息系统分为事业单位信息系统与学校信息系统两类，系统数据多、涉及用户广，对教育行业信息系统网络安全管理提出更高要求。在进一步完善管理体系、系统功能优化等方面，现阶段的教育行业面临较大的压力与挑战。网络安全保障应落实好系统管理体系，合理制定管理制度，保障运维管理质量；其次，应搭建基础网络，完善服务器，构建技术与安全管理相结合的安全体系。

2.1 运维管理风险

教育行业网络安全管理工作，应从制度、人才、培训管理三方面入手。从实际来看，当前这三方面都存在不足，需要进一步优化调整。尽管在管理制度方面，能够依据国家网络安全法推动工作开展。但是随着网络安全管理制度不断完善，运维管理并不够完善，在实际管理过程中存在不足。硬件设施等把关不够严谨，制定的应急预案措施不合理。系统由于不同时期建立，系统存在架构差异。早期建设的系统存在管理漏洞[2]。在前期开发过程中，未能将网络系统安全性考虑在内，导致系统处于无人维护的状态，带给信息系统极大的网络安全隐患。人员操作失误，未能对域名进行科学管理，导致未注销域名存在风险。运维人员管理系统，能够保障数据安全，但是管理过程中，端口与外网设备连接，极易造成数据泄露的风险；人才方面，由于当前国内的网络安全人才匮乏，从业人员普遍存在技能短板现象。基于教育行业信息系统网络安全培养人才，成为保障系统运行安全的重中之重。教育行业将过多精力投入在教学科研中，对网络系统第三方机构过分信任，导致自身缺乏良好的运维技术。人员技能不过关，难以对安全事故进行有效处理。

2.2 技术安全风险

教育行业不断发展，信息系统数量增加，在设备、数据安全方面，更应引起管理人员的重视。缺乏基础设备，过于老旧的设备难以支持系统升级；系统运行缺乏动态认证、解密设备等；应用过程中，部分系统因人员缺乏安全防护意识，导致系统权限设置不够明确，造成系统权限漏洞；数据安全方面，数据收集存储都可能面临安全隐患。尤其是教育行业数据资源庞大。需要保证数据收集阶段，完成分类整理分析，这也是数据安全管理开展的基础。面对关键的系统，一旦遭到外界攻击，会导致系统崩溃，影响工作进展[3]。

3 基于教育行业网络安全的防护措施

教育行业网络安全固然重要，面对技术、管理等方面的风险，也并非束手无策。网络信息不只是面对教育行业，而是面向全社会大众服务的智能化网络系统。网络安全问题基础预防与处理，可以基于网络系统的基础上，针对具体问题加以完善，从而减少网络安全风险出现，保障教育信息系统网络运行安全。

3.1 制定完善的管理措施

3.1.1 建立安全管理体系、制定安全制度

（1）教育信息系统网络安全工作，需要划分好具体的安全职责。根据系统管理体系，明确具体负责人，坚持责任到人的原则。提高人员对信息安全的重视，能够在工作中严格遵守相关规定要求。对于技术人员应明确划分好各项工作负责人，按照管理员、技术人员、安全技术员的形式划分，对系统工作有全面的了解。对具体负责的工作进行监督，确保操作符合标准。三类负责人各司其职，工作分工明确，不得出现一人多职的现象。完善的管理制度，能够保证管理工作有效落实。在网络安全管理期间，需要充分发挥制度的效用。结合具体教育系统将责任细化到个人，建立紧急安全事故应急小组，对可能发生的事故进行预测，事先制定有效措施，将系统损失降到最低。

（2）制度管理应严格按照教育部指示行动，建立统一的部署策略，明确运维人员与网络设备等布设要求。关闭不必要的端口，开启日志对日常系统运行情况进行记录；完善系统登录登记制度，定期进行排查，明确管理人员责任，对老旧系统进行升级优化处理；建立日常操作规程后，完善运维管理制度，根据工作实际需求，做好开发、运维等工作，保障系统稳定性；建立系统安全隐患自查制度，针对于教育信息系统安全运行，履行监督职责，为系统稳定运行提供保障；提高防火墙防控力度，结合系统受到的攻击情况，对服务器和客户端进行防护升级，定期进行系统测试、漏洞扫描。

3.1.2 定期做好数据备份工作

由于教育行业包含的信息过于复杂，海量的信息需要较大的储备系统。设置不同层级的登录权限，对系统运行情况进行实时监控，根据监控对非法网络访问，引起网络管理人员注意。当系统遭到外界攻击时，服务器会对其擅自进入网络的次数进行记录，达到一定次数将账户锁定；系统运行过程中，还要抵御外来攻击，应定期对系统数据

进行备份。将数据按照重要性进行分类备份，采取加密措施，定期对设置的口令进行更改，避免长期使用相同的口令。口令尽可能设置较为复杂，并安装防火墙等软件，建立良好的网络环境。系统文件查找权限，应按照管理员、读写、查找等权限进行系统划分，并为不同用户指定对应权限，避免人员权限等级过高，对服务器进行访问，影响系统正常运行。备份工作完备的情况下，即便是系统遭受攻击，也能够从备份数据中及时找到相关数据，减少数据丢失带来的损失。使用云端储备技术，对数据进行管理，保障数据的完整性。丢失、被篡改的数据，能够从云端进行恢复，强化数据管理质量。

3.1.3 人员管理水平培养

人才培养方面，加强安全管理队伍建设，强化技术人员运维水平，为系统网络管理提供保障。能够通过，提升人员的管理水平，从而更好的保障系统运行稳定性，保障数据安全[4]。定期对在岗人员进行系统化培训，开展应急演练，使技术人员接受相应安全风险。能够意识到网络安全风险不能完全避免，需要基于现有的防护策略，不断提升个人运维水平。从而在实际应急演练考核中，正视网络安全风险，将系统安全风险降至最低。

3.2 技术安全措施

防护思路上应基于网络安全技术体系，构建全生命周期的安全方案，对教育信息系统提供运行保障。基础网络环境是保障系统运行的重要前提，建设过程中，结合信息系统业务功能与特点，按照重要性进行逐一划分。按照事前检测、事中测试、事后响应的模式，对系统网络运行进行有效监管。安全防护系统应针对于系统运行过程中，可能出现的风险，进行安全评估处理。建立识别风险优化机制，在事前对风险进行识别。在系统运行过程中，对网站可用性、是否存在漏洞等方面进行监控预警，从而建立风险识别日志，发送信息到指令层，采取应急响应。

3.2.1 服务器

具体的架构需要保证网络有效接入，设置信息交换区、数据存储区、管理区等区域，形成完整的网络管理结构。能够经过路由设备与防火墙联系，从而实现数据交流。在服务器安全方面，由于服务器承载着系统运行的关键业务类型，需要对其进行重点防护。定期开展检查检修工作，对服务器进行运维管理，排查威胁、病毒、漏洞等，确保服务器配置符合要求；收集服务器基本信息，结合硬件设备对信息进行检查，避免病毒传播。对服务器做好防护管理，对日常维护工作进行详细记录，为技术人员分析提供参考数据[5]。

3.2.2 系统测试

技术能够为系统运行提供保障，为了保证系统网络安全性，需要加强技术手段，对系统进行测试，面对可能出现的故障与异常现象，能够及时发出警报，确保应用安全。对系统进行测试开发等操作，确保系统全生命周期都能得到安全防护。并制定开发编码，引入开发安全框架对可能出现的安全漏洞进行预防和检测。针对系统建立完备的信息系统监控中心，并委托第三方对系统源代码进行审计，保存审计报告，实现信息系统科学监管。对于防范非法入境，应从访问、隔离等方面建立分段管理模式。并对网站、系统进行实时扫描，检测系统中是否存在非法入侵的痕迹；系统运行过程中能，使用监控系统对信息系统进行全面监督，面对非法攻击，及时启用应急应对措施，防止数据被篡改；运维阶段确保设备运行质量，对用户行为、网络环境等进行检测，一旦发现安全隐患，告警给管理人员，对发现的隐患进行记录。

3.2.3 数据安全

保障信息系统数据安全方面，需要根据具体的业务需求，对系统后台进行操作设置。针对不同用户设置登录权限，重要数据加密管理。一旦数据落入不法分子手中，等待其对数据破解时，数据会自动销毁，有效防止数据泄露出去。利用通信网络传输数据至特定服务器端口。用户鉴别信息在认证结束后，痕迹自动清除，保护用户隐私和数据安全。

4 结论

综上所述，教育信息化程度不断发展，各种技术升级优化，也使信息系统面临危险之中，网络安全防护措施显得尤为重要。网络安全保障工作，能够为教育系统运行保驾护航。加强网络安全管理，完善安全管理体系，增强安全技术防护能力。针对系统安全防护制定具体措施，最大程度降低损失，为教育行业信息化发展提供有力支撑。

[参考文献]

[1]刘毕成.中国政府信息安全管理体系问题及对策研究[D].长春:吉林大学,2021.
[2]李杨.新版高中信息技术必修模块教材比较研究[D].山东:山东师范大学,2021.
[3]孙翊嘉.甘肃省“互联网+政务服务”的商用密码安全保障研究[D].甘肃:兰州大学,2020.
[4]高凯.智慧城市信息安全风险评估指标体系构建研究[D].湖南:湘潭大学,2019.
[5]杨姗媛.信息安全风险分析方法与风险感知实证研究[D].北京:中央财经大学,2019.

作者简介：杨帆（1981-）男，汉族，重庆人，成都理工大学电子信息科学与技术专业本科毕业，现就职于重庆市教育信息技术与装备中心，担任该中心信息技术部副主任。