职业院校网络安全建设探索与改进——以培黎职业学院为例

曹心洲 宋毅 *
培黎职业学院，中国·甘肃 张掖 734100

摘要：随着智慧校园的不断建设和完善，给师生教学、科研、生活带来便捷的同时，暴露出越来越多的网络安全问题，鉴于此，院校应重视网络安全问题，做好网络安全相关建设及防御保护措施。本文笔者结合个人日常工作经验与相关文献参考，就职业院校目前面临的网络安全问题展开分析，从管理方面、技术方面、网络安全运营体系展开简述及粗浅的探讨。

关键词：智慧校园建设；职业院校；网络安全

Exploration and Improvement of Network Security Construction in Vocational Colleges——Taking Pei Li Vocational College as an example

Cao Xinzhou, Song Yi*
Bailie Vocational College, China Gansu Zhangye 734100

Abstract: With the continuous construction and improvement of smart campuses, while bringing convenience to teaching, research, and life for teachers and students, more and more network security issues have been exposed. In view of this, universities should attach importance to network security issues, do a good job in network security related construction and defense protection measures. Based on personal work experience and relevant literature references, the author of this article analyzes the current network security issues faced by vocational colleges, and briefly discusses and explores them from the perspectives of management, technology, and network security operation system.

Keywords: Smart campus construction; Vocational colleges; Network security

0 引言

培黎职业学院于 2020 年开展办学，随着学校的办学水平不断提高，学校抢抓职业教育信息化标杆学校建设机遇，全面展开智慧校园建设，一是建成校园“双网络”，有线和无线双网络覆盖校园全部场所，支持 IPV4/IPV6 双栈，二是建成超融合云数据中心，支撑各项系统稳定运行，三是积极推进智慧校园平台建设，建成一站式网上办事大厅，通过全面梳理审批服务事项，精简归并不同层级、部门的同类事项，规范工作流程，截至 2025 年 7 月底，入驻在线服务 20 项，集成业务系统 7 个，学术资源平台 10 个，同时学校以建设与信息化发展水平相符的安全保障体系为目标，信息化与信息安全同步设计与建设，内容与技术并重、管理与技术并举，推进网络安全防护体系建设，确保系统安全运行和数据完整，持续提高基础设施防护能力、信息系统防御能力、整体风险防控能力、突发事件处理能力。从巩固防线纵深到迈向积极防御，形成“人 + 技术 + 流程”协同联动的防御模式，建立从顶层设计、部署实施到运行维护的一整套网络安全模式。本文以培黎职业学院网络安全建设内容和建设思路为例，提出一些职业院校普遍存在的问题和解决措施，总结网络安全建设经验。

1 目前面临的网络安全问题分析

1.1 网络安全管理制度匮乏

因学校自 2020 年展开办学，所以面临网络安全和信息化相关管理制度不健全、制度不执行的状况，前期信息化建设工作中整体上对网络安全管理不重视，没有健全的制度和详细的顶层设计，信息化是推动院校发展的重要手段之一，以往工作中只是当作一个单个系统解决业务部门工作，并未梳理学校信息化建设定位，所以没有健全的网络安全管理制度和顶层设计，应当结合学校目前自身实际情况，依据等级保护相关政策，建立健全的网络安全管理

体系，防止形成管理上的漏洞，提升学校整体防护能力。网络安全管理是一种规范，管理者依靠规章制度规定处置流程等问题，对网络安全技术人员以及校内师生也起到管理规范作用。除此之外，学校还应建立网络安全工作领导小组和应急处置预案，对突发的网络安全事件快速做出响应。

1.2 人为因素

学校已经实现无线网络的全覆盖，校内用户类别也众多，有在校师生、后勤服务人员、临时访客等，用户量大并且缺乏网络安全意识和技术理解，随着上网设备接入增多，使用过程中会出现不规范的行为，导致出现内网木马攻击、DDOS 等，不能及时监测到这些恶意流量。网络安全专业技术人才缺少，工程师技术水平薄弱，缺乏校园网络安全运维管理，导致应急处置和应急防护严重滞后。

1.3 设备问题

网络安全设备是网络安全保障的基础，部分职业院校由于经费、业务量少等原因，只是部署出口路由防火墙，导致整个内网没有防护，黑客攻破后很容易进行内网渗透、脱库、webshell 等，随着智能计算、物联网、人工智能技术的发展，网络安全攻击也具有智能性，例如利用数据投毒攻击、AI 深度伪造数据窃取攻击，这些新的攻击方式传统的网络安全设备无法识别拦截，直接导致数据泄露，甚至内网直接沦陷。

2 建设思路

从学校实际情况出发，构建学校数字化校园安全防护体系，筑牢安全防护堤坝，学校成立网络安全和信息化工作委员会，制定《网络与信息安全工作管理办法》，充分发挥网络安全和信息化工作委员会的职能，健全学校网络安全、数据安全等管理制度，通过“人 + 技术 + 流程”协同联动的防御模式，采取相应的技术手段和管理措施，防范对校园网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，保障校园网完整性、可用性、保密性。坚持问题导向、目标导向，推进网络安全技术防护系统和网络安全管理体系相融合，建立起完整的纵深防御体系，从安全运营、数据安全、应用安全等持续改进网络安全工作。

3 网络安全管理方面建设举措

3.1 强化制度建设，全面落实制度规范标准体系

围绕学校网络安全和信息化工作统一谋划、统一部署、统一推进、统一实施的要求，建立覆盖项目、数据、应用、流程、安全等方面的标准体系及管理制度，加大对学校各项工作的指导力度。根据学校发展情况，及时展开体系和管理制度修订工作，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则压实网络安全工作制[1]，与相关业务信息系统管理处室签订网络安全承诺书，网络与信息系统的主管部门承担系统的安全管理和监督责任，网络与信息系统的运行维护部门承担系统的技术安全保障责任，网络与信息系统的使用单位和个人承担系统操作与信息内容的直接安全责任。围绕数据采集、传输、存储、处理、交换、销毁等环节，建立数据分类分级管理制度，构筑数据全生命周期安全防护体系，以“告知—同意”为核心的个人信息保护制度，维护广大师生合法权益，强化管理保障措施，加强应用业务和移动端安全管理，为学校信息化有序健康发展打牢地基。

3.2 全面落实网络安全等级保护制度

以等级保护为抓手，全面梳理信息化资产，从边界出口区、数据中心区、安全运维区等各个方面进行不同策略的安全防护设计，依据等级保护标准，进一步建设完善内外网安全设施，落实等级保护测评制度，确保各类规章制度和安全技术措施有效运行和落地。

3.3 开展“三个工程”计划

3.3.1 开展网络安全素养提升工程

建立网络安全培训工作的常态化工作机制，将网络安全相关法律法规和政策文件纳入学院重要会议学习，提高领导层的网络安全意识，将网络安全知识的学习纳入到干部培训体系当中，利用网络安全宣传周、新生入学教育等活动，对全校师生开展网络安全意识培训，提高网络安全素养。鼓励从事网络安全的管理人员参加社会化网络安全资格考试，选派人员参加专业网络安全培训学习，逐步提高网络安全工作人员的网络安全工作水平。每季度召开网络安全工作专题会议，使全校各部门广泛参与，集体研究网络安全的新态势、新问题和新做法，构建学校的网络安全协同工作机制。

3.3.2 开展网络安全改进工程

从边界安全、流量安全、主机安全、安全管理、行为安全、数据安全等多个维度不断完善网络安全防护能力，通过网管平台实现内外网、教育科研网、甘肃省教育专网统一运营纳管，将割裂的不同安全厂商的设备有机整合联动，使其具备有效的防御能力和面对新的未知威胁的研判处置能力，不断改进和完善安全运营体系，提升自身安全运营能力。以大数据和人工智能技术为核心，结合威胁情报、失陷主机检测、NTA 流量分析等，建立流量分析系统，部署 SAAS 版 DNS 威胁检测分析服务，监测挖矿类的

域名请求及涉事终端设备，及时阻断挖矿域名，提升勒索病毒和挖矿行为的监测。

3.3.3 开展应急能力提升工程

建立以学校为主、网络安全厂商为辅的信息安全服务队伍，“以练促防，以防筑基”，以桌面推演或者模拟日常网络威胁和攻击的方式，不定期组织开展网络安全攻防演练，积极参加教育、网信、公安组织的各类攻防演练活动，提升团队防护能力和应急处理水平，构建“实战化，体系化，常态化”的安全保障体系，实现动态防御、主动防御、纵深防御和精准防护、整体防护、联防联控，提升关键信息基础设施保障能力[2]。

3.4 梳理信息资产

明确信息资产范围，如硬件资产、软件资产、数据资产、虚拟资产等，建立动态的管理流程，通过人工和技术手段，摸清信息资产数量，建立清晰准确的信息资产台账，及时清除僵尸网站和僵尸系统，做好业务系统上线管理，摸清业务系统薄弱点和风险点，向业务系统主管部门明确业务系统上线使用要求和管理员职责，部门填报资产清单，核对关键系统（如财务、学工系统）的权限和配置，标注责任人、部门、合规要求，每季度全面盘点，实时更新变更。

4 网络安全技术方面建设举措

在安全建设中充分考虑校园挖矿治理、数据安全风险、网站防护、漏洞防护等典型校园网络安全场景下的安全防护能力，根据网络安全等级保护要求，结合学院实际情况及最新的安全架构模型和理念，构建技术安全体系。持续推进业务专网建设，加强网络基础设施建设，按照业务专网的思路规划和调整现有校园网络，构建独立的一卡通、监控网、电子班牌等业务专网，达到进一步提升网络服务效率。安全技术体系设计旨在全面提升校园网络安全防护能力，构建安全机制和策略，将整个校园网网络安全防护划分为 5 大区域：校园网出口区、数据中心区、数据安全区、安全管理区、无线接入区，针对每一个区域的实际业务及合规需求进行相关安全建设，规范网络资产的管理，防范其他安全风险外溢效应等目的。具体内容如下：

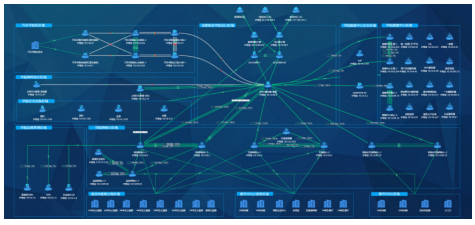

图1 学校网络拓扑图

校园网出口区：

校园网出口区部署互联网防火墙 2 台，做双链路部署，保障校园网稳定运行承载，满足校园网络边界的全方位安全防护，在防火墙上禁止所有国外流量，减少网络安全攻击；同时出口区部署 2 台上网行为管理，做好流量管控及流量分析，对违规翻墙等行为禁止，兼顾防范使用校园网发布或访问不良信息及网站的动作。

数据中心区：

部署数据中心防火墙组双机满足双链路的双机热备能力，确保不会因为单点故障导致业务中断等问题。同时为了保障后续全校所有业务的 WEB 应用层的安全防护，同步部署 WAF 设备，做全校所有业务 WEB 应用层的防护。

数据安全区：

数据安全区划分在数据中心区，数据安全区出口处部署数据库防火墙、数据防泄漏，审计对数据库的所有操作行为，发现 SQL 注入、数据泄露、窃取、篡改等违规行为及时阻断，数据区部署国产化数据库一体机。

安全管理区：

在该区域部署漏洞扫描设备、全网态势感知、堡垒机、日志审计、备份一体机设备，做到全网安全形势的整体分析、未知威胁的实时监测、对全网中的安全设备或安全组件进行集中管控。

无线接入区：

全校已全面覆盖无线网络，面对移动终端接入校园网的防护与审计，部署防火墙及上网行为管理在该区域出口，做到移动终端安全有效的接入到校园网内部，师生上网采用实名制，需登录无线网认证通过，做到可追溯。

5 网络安全运营体系方面建设举措

经过前期的建设，将配备完善的网络安全防护设备，完成了基础的网络安全体系建设。但是，这些工具能否充分发挥其安全防护的能力，取决于有没有专业的技术人才及完善的安全运营体系。如果安全建设只是停留在安全设备的堆砌，缺乏有效的使用和运营体系保障，安全人员将会在海量的日志分析、告警中疲于奔命，来自不同厂商的设备各自为战、检测割裂，难以将多个节点的痕迹自动关联成一个完整的安全事件，安全团队及时跟进告警分析与事件响应的难度大，往往不能及时发现真实紧急的网络攻击。为解决安全运营的难题，让内网各种安全设备的能力有机结合，发挥最大的作用，在建设中，部署网络安全态势感知平台，为安全管理人员提供资产、威胁、脆弱性等管理能力，并具备对威胁的事前预警、事中发现和事后回

溯的能力，对威胁进行完整的生命周期管理。通过使用态势感知平台，帮助学院实现如下四个转变：

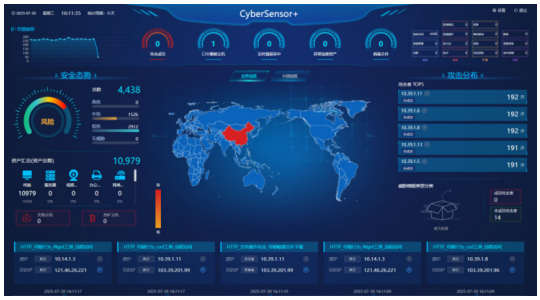

图2 网络安全态势感知大屏

5.1 由低效的分散管理，转变为高效集中的监测管理

网络安全态势感知系统通过流量探针，监测全网流量，从大量数据中屏蔽无用信息，按照等级及时告警安全事件，通过机器学习、大数据分析等技术，发现深度隐藏的安全威胁，并通过提前编排的剧本，自动拦截攻击，例如下图 3 所展示的国外 IP 永久封禁子剧本。

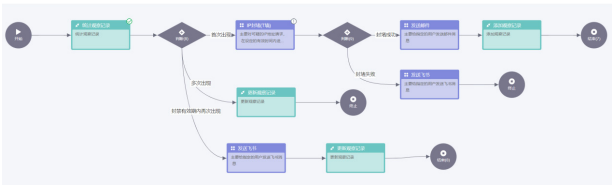

图3 国外IP永久封禁子剧本

5.2 由未知不可见的安全监控，向全面整体的态势感知转变

利用可视化技术从攻击态势、资产态势、脆弱性态势、情报态势、流态势等多个维度展现当前的安全态势，通过告警视角、攻击者视角、受害者视角、情报视角、资产视角、ATT&CK 视角等不同视角和脆弱口令、口令爆破、文件检测、违规 VPN 等不同攻击场景，明晰攻击过程及异常行为，让学院整体安全情况可见、可控。

5.3 由人为低效的事件处置，向自动化高效的协同处置转变[3]

匹配与网络安全态势感知配套的安全分析处理机制，从安全事件监控、预警、处理、修复的闭环流程，实现了整个网络安全事件处理的工作系统机制，通过登录行为分析、访问行为分析、DNS 行为分析等不同的场景分析，联动 WAF、IPS 等设备一键封堵。

5.4 由零散的不成体系的安全运维，向流程化的体系化的安全运营转变

通过网络安全态势感知平台，共享各类情报信息，有效的把平台、管理人员、技术人员、管理制度、处理流程结合起来，对整个网络安全事件流程可追溯，提升整体网络安全防护能力和效率。

6 未来工作思考及规划

建设多功能智慧校园综合指挥中心，同时承担网络安全应急响应中心功能，集中统一安全调度、舆情监控、事件分析、应急处置等功能，持续强化和提升学校网络安全管理能力，建设网络安全统一协同管理平台。根据最新发布的《职业院校智慧校园规范》，探索建设校园数据安全可信计算平台，建设学校可信教育数字身份支撑服务能力，在确保数据隐私和安全的情况下，赋能校内校外单位开展数据分析开发。兼顾人工智能安全，盘点学校各部门使用的人工智能系统，开展安全评估和审计。

参考文献：

[1] 杨巍立，陈飞. 高校校园网络与信息安全管理工作的实践与探索[J]. 亚太教育，2016,(33):193.DOI:10.16550/j.cnki.2095-9214.2016.33.158.

[2] 周文泉，单兴中，肖凤萍. 实战环境下的网络安全防护能力建设探讨[J]. 现代电视技术，2022,(01):154-156.

[3] 张健，董升来. 基于 SOAR 模式安全运营建设的探索与思考[J]. 广播电视网络，2022,29(05):57-60.DOI:10.16045/j.cnki.catvtec.2022.05.014.

作者简介：曹心洲 (1996.12-)，培黎职业学院网络信息中心副主任，研究方向：网络信息安全。

宋毅 (1997.02-)，培黎职业学院网络信息中心网络安全管理员，研究方向：信息系统管理，网络安全。