设计研究与应用

等保 2.0 技术在数字化校园信息管理系统安全测评中的应用研究

胡智方 侯文平
（湖北国土资源职业学院，湖北武汉 430090）

摘 要：本文根据 2019 年 5 月国家标准化管理委员会发布的《信息安全技术网络安全等级保护基本要求》文件精神，以湖北国土资源职业学院数字化校园信息系统为例，在现有系统架构的基础上，结合等保 2.0 新标准及技术要求，对校园信息系统进行安全评测，针对测评结果，分析该系统中存在的安全隐患，提出整改建议，学校可据此进行系统优化，最终确保该信息系统正常安全地运行。

关键词：信息安全；等保 2.0；数字化校园
中图分类号：TP393.08 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2021.12.025
本文著录格式：胡智方,侯文平.等保2.0技术在数字化校园信息管理系统安全测评中的应用研究[J].软件,2021,42(12):077-079

Application Research of Equiguarantee 2.0 Technology in Security Evaluation of Digital Campus Information Management System

HU Zhifang, HOU Wenping
(Hubei Land Resources Vocational College, Wuhan Hubei 430090)

【Abstract】：This article is based on the spirit of the document “Basic Requirements for Information Security Technology Network Security Graded Protection” issued by the National Standardization Administration in May 2019, to vocational college digital campus information system of land and resources of Hubei province as an example, on the basis of the existing system architecture, combined with 2.0 new standards and technical requirements, such as the campus information system security evaluation, according to the evaluation results, the hidden dangers in the system are analyzed and rectification suggestions are put forward. Based on this, the school can optimize the system and finally ensure the normal and safe operation of the information system.

【Key words】：information security;Equiguarantee 2.0;digital campus

0 引言

随着网络技术及计算机技术的不断发展，网络与信息安全问题日益严重，而数字化校园信息系统是我校智慧校园建设中的重要组成部分，本文通过对信息系统基本安全保护状态的分析 [1]，对面临的主要安全威胁使用等保 2.0 技术对该系统进行测评 [2]，针对评测结果采取相应的安全机制，以期能达到保护信息系统安全运行的目的。

1 什么是等保 2.0

等保 2.0 是指网络安全等级保护制度 2.0 国家标准，该标准已于 2019 年 5 月 13 日正式发布，并于 2019 年 12 月 1 日正式实施。等保 2.0 以“一个中心，三重防护”为网络安全技术设计总体思路，其中一个中心即安全管理中心，三重防护即安全计算环境、安全区域边界和安全通信网络 [3]。安全管理中心要求在系统管理、安全管理、审计管理三个方面实现集中管控，从被动防护转变到主动防护，从静态防护转变到动态防护，从单点防护转变到整体防护，从粗放防护转变到精准防护。三重防护要求企业通过安全设备和技术手段实现身份鉴别、访问控制、入侵防范、数据完整性、保密性、个人信息保护等安全防护措施，实现平台的全方位安全防护。

2 数字化校园信息管理系统介绍

数字化校园信息管理系统是湖北国土资源职业学院为校内教务人员、学生及相关管理人员提供高效便捷的一站式信息服务平台。师生可通过电脑或手机终端进行

作者简介：胡智方（1985—），女，湖北武汉人，硕士，讲师，研究方向：计算机科学与技术、职业教育。

登录。实现了校园网内数据资源的高度共享及各种应用软件的高效集成。该系统主要包括接入区、管理区、交换区、服务器区及终端区。其中接入区为互联网边界，进出口防火墙和上网行为管理接入交换区。交换区部署有核心交换机、服务器交换机和楼层接入交换机。核心交换机下连管理区、服务器交换机和楼层接入交换机。服务器交换机下连服务器去。楼层接入交换机连接终端区。

管理区为系统设置提供安全监测服务，部署了日志审计和旁路部署。服务器区部署有系统各业务服务器，终端区部署有运维终端和管理终端。

3 测评过程

等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。

测评准备活动：是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。主要任务是掌握被测系统的详细情况，准备测试工作，为编制测评方案做准备。

方案编制活动：是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。主要任务是确定与被测信息系统相适应的测评对象、测评指标及内容。

现场测评活动：是开展等级测评工作的核心活动。主要任务是按照测评方案的总体要求，严格执行测评任务，以了解系统的真实保护情况，发现系统存在的安全问题。

分析与报告编制活动：是给出等级测评的结果，总结被测系统整体安全保护能力的综合评价活动。

4 评测对象选择

根据信息安全等级保护要求及安全风险评估标准与模型，从信息系统的核心资产出发，以威胁和弱点为导向，对比信息安全等级保护的具体要求，对信息系统进行全面评估，主要从整体网络拓扑结构图、机房环境、配套设施、网络设备、安全设备、应用系统、管理终端、管理员及安全管理制度和记录等方面考虑测评对象。

5 评测案例结果分析及整改建议

5.1 安全物理环境

5.1.1 已有安全措施分析

（1）物理位置选择：经核查，机房部署在学校行政楼 5 楼，大楼具备防风防雨能力，机房周围无用水设备。（2）物理访问控制：经核查，机房门口配备有指纹电子门禁系统，设备工作正常，可对出入机房人员进行控制、鉴别和记录。（3）防盗窃和防破坏：经核查，机房内各服务器、网络设备、安全设备均用螺丝固定在机柜内；机房通信线缆铺设在机柜上方桥架内。（4）防雷击：经核查，机房内各机柜均接地，各设备均连接交流电源地线。（5）防水和防潮：经核查，机房窗户密闭，窗户周围、天花板无雨水渗漏痕迹；机房内配备有精密空调，设备工作正常，可对机房环境进行除湿。（6）防静电：经核查，机房地面铺设有防静电地板，各设备均接地。

5.1.2 安全物理环境存在的安全问题及危害分析

（1）机房消防系统灭火气瓶压力不足，可能导致火情未及时发现，或火情发生后，无法及时灭火。（2）机房所在建筑未通过抗震设计验收，无法在建筑物遭受地震时对机房内设施进行保护。（3）系统主要设备均未设置标签标记，不利于系统运维和故障排查。（4）机房建筑材料耐火等级未知。增加了在发生火情时助燃火灾的风险。

5.1.3 整改建议

（1）建议提供机房所在建筑抗震设计验收文档。（2）建议为系统内所有重要设备及通信线缆设置明显的不易去除的标签。（3）建议维护机房消防系统灭火器，确保压力正常，工作正常。

5.2 安全通信网络

5.2.1 已有安全控制措施分析

（1）网络架构：实际网络运行环境与网络拓扑图情况一致，互联网边界已部署出口防火墙，且已配置访问控制策略。（2）通信传输：网络中网络安全设备的远程管理协议均采用安全的 SSH 或 HTTPS 协议。

5.2.2 安全通信网络存在的安全问题及危害分析

系统未采用可信计算技术，无法对设备的引导程序、系统程序、重要配置参数和通信应用程序等进行动态可信验证。可能导致设备的引导程序、系统程序、重要配置参数在执行过程中遭到篡改。

5.2.3 整改建议

建议所有服务器、终端、网络通信设备、安全设备均采用符合国家要求的可信技术。

5.3 安全区域边界

5.3.1 已有安全控制措施分析

（1）边界防护：互联网边界已部署出口防火墙，并已配置访问控制策略。（2）访问控制：出口防火墙上最后一条控制策略为拒绝所有通信。出口防火墙设备未发现多余、无效的访问控制策略，访问控制策略逻辑关系及前后排列顺序合理。出口防火墙的访问控制策略项包含序号、源地址、目的地址、源端口、目的端口、服务、动作、生效、命中数等。出口防火墙为状态检测类型防火墙，可根据会话状态信息进行访问控制，并生成会话状态列表。访问控制策略有效。（3）安全审计：出口防火墙已开启系统日志和安全日志。均可记录设备各管理员登录和操作情况，系统安全事件等信息。日志审计系统的

日志记录包括事件级别、事件名称、源地址、目的地址、接收时间等内容。系统日志记录已转发至日志审计系统。日志审计系统已启用自动备份，定期备份日志记录。

5.3.2 安全区域边界存在的安全问题及危害分析

（1）系统未采用可信计算技术，无法对边界防护应用程序等进行动态可信验证。可能导致设备的运行数据在执行过程中遭到篡改。（2）网络中边界处出口防火墙入侵防御模块特征库已过期，无法对可能潜在的网络攻击行为进行检测和报警。存在不能及时发现网络攻击行为而造成系统信息泄露或损坏的风险。（3）网络中边界处出口防火墙防病毒模块特征库已过期，不能在网络层面对恶意代码进行检测并清除。可能会造成恶意代码流入系统造成破坏的风险。

5.3.3 整改建议

（1）建议更新出口防火墙入侵防御特征库，对可能潜在的外部发起的攻击行为进行检测并报警。（2）建议更新网络中边界处出口防火墙防病毒模块特征库，以便及时发现、阻断、清除网络中的恶意代码。（3）建议所有服务器、终端、网络通信设备、安全设备等均采用符合国家要求的可信技术。

5.4 安全计算环境

5.4.1 已有安全控制措施分析

（1）身份鉴别：核心交换机采用账户 + 口令的方式进行身份鉴别，用户标识具有唯一性。口令大于 8 位，数字字母字符组成，登录失败 3 次断开连接，空闲超时 10 分钟，远程管理采用 SSH 协议，可防止鉴别信息在网络传输过程中被窃听。（2）访问控制：核心交换机已为登录用户分配管理员账户，未见多余和过期账户。未发现多人共用一个账户情况。（3）安全审计：核心交换机已开启系统日志，级别为“debugging”。可记录每个账户的登录行为、设备重要状态信息和操作行为，系统日志项包含日期、时间、登录 IP、接口、账户名、事件类型，日志已传输至日志审计服务器上，日志留存大于 6 个月。（4）入侵防范：核心交换机已关闭 Telnet、HTTP、FTP 等服务，未发现其他多余开放的服务和端口，已对终端管理地址进行限制，未发现系统存在高风险漏洞。（5）数据完整性：远程管理核心交换机采用 SSH 协议，可对传输过程中的数据进行完整性校验。（6）数据备份恢复：核心交换机配置每次发生变更后备份一次，配置文件保存在运维终端。

5.4.2 存在的安全问题及危害分析

（1）核心交换机及接入交换机管理系统存在超级管理员用户，未进行权限分离，未根据不同账户执行的任务进行最小权限分配。存在越权或权限滥用的风险。（2）核心交换机及接入交换机口令未进行定期更换。存在使用穷举法进行口令的暴力破解或口令被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问的可能性。（3）核心交换机及接入交换机系统已经修改了账户的默认口令，但未重命名系统默认账户。可能导致外部能猜测用户名口令，造成信息泄露。

5.4.3 整改建议

（1）建议不使用默认超级管理员账户，增加系统管理员、安全管理员、安全审计员等账户。（2）建议将设备口令更换周期修改为 90 天。（3）建议重命名系统默认账户。

5.5 安全管理中心

5.5.1 已有安全控制措施分析

审计管理：网络中已部署日志审计系统，并使用账户和口令对审计管理员进行身份鉴别。系统日志审计范围已经覆盖到各审计管理员的操作行为。已通过日志审计管理员账户对日志记录进行查询和分析。

5.5.2 存在的安全问题及危害分析

（1）网络中未部署运维审计系统，未通过运维审计对设备进行配置管理和审计。无法对保护对象进行统一监视和控制，当安全事件发生时无法及时对威胁源进行阻断和干预。（2）未启用运维设计设备对系统各设备管理员操作进行审计。可能导致不能及时发现系统中的安全风险。

5.5.3 整改建议

（1）建议部署运维审计系统，通过安全管理中心的运维审计等设备对系统管理员的操作记录进行审计。（2）建议启用运维设计设备，并配置专门系统管理员用户对设备进行管理，并对其操作进行审计。

6 结语

《中华人民共和国网络安全法》规定我国实行网络安全等级保护制度，对于不执行网络安全等级保护的单位将追究其法律责任。本文结合湖北国土资源职业学院数字化校园信息管理系统的安全等级测评实例，提出了该系统可能存在的安全风险，并给出了整改建议，为系统整改提供了切实可行的优化路径。

参考文献

[1] 刘俊杉,段莉.等级保护2.0下通信系统网络安全体系研究[J].互联网天地,2020(5):33-40.

[2] 莫新建.网络安全等级保护建设探索[J].网络安全技术与应用,2020(5):10-11.

[3] 马力,祝国邦,陆磊.《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J].信息网络安全,2019(2):77-84.