网络安全及信息化应用工作简报

2019 年第 3 期（总第 3 期）

郑州工程技术学院网络安全和信息化领导小组办公室

2019 年 11 月 10 日

本期导读：

- 主题教育学习情况；
- 图书馆网络安全事件处理情况；
- 信息化网络安全排查；
- 信息化应用系统维护与推广；
- 网络故障问题处理

主题教育学习情况

根据郑州工程技术学院“不忘初心、牢记使命”主题教育实施方案要求，信息与网络管理中心组织部门全体人员开展了“不忘初心、牢记使命”的主题教育， 10 月 21 日，信息与网络管理中心党员参与了机关三支部组织的支部书记上党课活动，学习了习近平总书记讲过的红色故事中的《龚全珍跟随丈夫——开国将军甘祖昌回到农村艰苦奋斗》的英雄事迹，并观看了《我们走在大路上》（二）专题片，10 月 30 日，党员们又共同观看了爱国主义影片《我和我的祖国》，影片通过七个小故事，充分的向我们展现了我国自建国以来在各行各业的快速发展。同时让大家认识到“不忘初心，牢记使命”的重要性，给大家在今后的工作中树立了一个新的指导。

10 月 28 日，信息中心全体教职工在 A601 开展了“不忘初心、立德树人”大研讨活动，根据我校《关于开展“不忘初心、立德树人”大研讨活动的通知》要求，我们对讨论的内容、范围和着力点进行要求，建议教师围绕推进学校“一二三四”工程和“三步走”发展战略，紧扣整改落实这个关键点，对如何推进“立德树人”往深里走、往心里走、往实里走进行深入思考和思路整理。

按照学校“不忘初心、牢记使命”领导小组要求，每周四上报一次主题教育开展情况汇报，信息与网络管理中心每周按时上报，分别包括学习情况、调研情况、先进经验和典型、主题活动开展情况、本周实际解决的问题和下周开展的工作计划六个方面。

图书馆网络安全事件处理情况

- **图书馆病毒事件**

10 月 15 日，图书馆服务器中病毒后，导致系统瘫痪，信息与网络管理中心接到图书馆情况说明后，立即拟定处理方案，首先确认中毒时间和服务器地址，安排专业人员对中毒服务器进行分析，通过查看系统日志，在 2019 年 10 月 14 日凌晨 4 点左右发现勒索时，查看到中勒索前半小时有大量的登录失败信息，因此可以确认病毒通过暴力破解的方式进入到服务器中。

360 企业安全监测到 2018 年 8 月 21 日起，多地发生 lobeImposter 勒索病毒事件，经过定性分析，攻击者在突破边界防御后利用黑客工具进行内网渗透并选择高价值目标服务器人工投放勒索病毒。此攻击团伙主要攻击开启远程桌面服务的服务器，利用密码抓取工具获取管理员密码后对内网服务器发起扫描并人工投放勒索病毒，导致文件被加密。病毒感染后的主要特征包括 windows 服务器文件被加密、且加密文件的文件名后缀为*.RESERVE。

处理措施：对于已中招服务器，下线隔离；对于未中招服务器，采取 1、在网络边界防火墙上全局关闭 3389 端口或 3389 端口只对特定 IP 开放；2、开启 Windows 防火墙，尽量关闭 3389、445、139、135 等不用的高危端口；3、每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种组合以上）。4、按照网络安全规范要

求将图书馆所有应用系统和数据库资源等迁移到学校网络机统一管理。

事件结束后，信息与网络管理中心对图书馆整体网络信息安全进行了排查，包括网络拓扑结构、服务器及系统基本信息、有线和无线信息点及接入设备情况均进行了进一步排查，并对本部门中心机房网络信息安全开展了全面排查，以防类似事件的发生。

- **安全信息通报**

1 对学校的虚拟服务器进行补丁加固，安装杀毒软件。

2 配合 360 软件公司对图书馆感染病毒的三台服务器进行分析，写出分析报告，见附件 1。

3 接到河南教育系统网络安全工作群《关于泛微 OA 系统 sql 注入漏洞预警》，联系泛微公司对学校的 OA 办公系统服务器进行漏洞处理，及时打上补丁。

信息化网络安全排查

十月份，本部门重点对我校信息化系统网络安全进行了全面排查，发现了目前存在的一些问题，及拟定的相关措施，具体如下：

问题 1：目前发现很多部门存在服务器和业务系统未进行安全保护现象，主要存在于图书馆、财务处、文科中心、开放学院、继续教育学院、信息学院这些部门。

措施：各部门原则上不允许有自己的服务器，所有服务器均需要

存放在信息与网络管理中心进行集中管理，信息系统也应全部迁移到学校的虚拟机上，针对信息学院的服务器和系统，由于教学实验使用，要求不能对外开放访问，如果确实需要，应采用 VPN 方式访问。

问题 2：各部门和学院对校外托管的服务器、服务器上存放有郑州工程学院明显标志的部门业务系统、公开服务的信息系统排查不到位。

措施：各部门需要根据要求，进一步对以上情况进行排查，以后若发现还存在这些问题，由各部门自行负责。

问题 3：发现航海校区和龙子湖校区 VPN 通道未进行实名认证，存在安全隐患。

措施：两个校区各增加服务器，并进行认证服务器升级，争取到 11 月底实现实名认证

信息化应用系统维护与推广

为进一步做好信息化应用推广工作，信息与网络管理中心于 10 月 26 日邀请华腾包永福等工程师现场为大家培训指导，其中包括服务大厅应用如何接入企业微信和业务流程如何建设等问题的学习培训，这次培训，信息与网络协会的部分成员也参与其中，他们作为将来信息系统的学生推广队伍，已经基本掌握服务大厅中部分流程的制作，培训结束后，信息与网络管理中心老师带领社团学生进行了实战练习。

信息与网络管理中心本着精益求精的业务精神，为了进一步方便大家实现无纸化办公，完成“最多跑一次”的服务承诺，本次对服务

大厅的功能又进行了完善，新增了固定电话申请、公共实验室申请、修改了虚拟机申请等流程，并处理翻转校园的数据问题以及教学视频统一身份认证对接问题，对服务大厅中的个人数据中心功能进行完善，通过系统集成服务，实现了企业邮箱在企业微信中的绑定，制定并发布教师和学生的企业微信注册流程，以求广大师生都能尽快使用企业微信进行办公，提高工作效率。

网络故障问题处理

10 月 16 日，信息与网络管理中心重新绘制了学校网络拓扑图，并优化康邦 IT 域内平台拓扑图，修改制定运维规范，整理网络故障报修流程；

10 月 18 日，调试 8 号楼新增教师 8510 的网络，对 A212 办公室进行布线施工安装电话，联系移动维护人员处理保卫处电话布线问题；

10 月 19 日，针对 OA 办公网络不稳定，联系公司对网络进行排查，并处理教学监控视频系统同学以身份认证问题，为教务处开通山石 VPN 临时账号；

10 月 22 日，航海校区和龙子湖校区分别接收服务器一台，留作准入认证使用，并处理龙子湖校区出口线路切换问题；

10 月 23 日，航海校区新装的多媒体设备已验收完毕，报销手续也全部完成，等待资金到位支付货款。

本月已和后勤服务中心交接了多媒体工作，并将 10 位同志的工作调整到位，后期等待国资处出方案进行资产交接；由于部门工作重

新调整，后勤服务中心和本部门交接了固定电话安装与维修工作，信息与网络管理中心已结合学院需要，处理了几个安装业务单，基本掌握流程，后期还需要进一步完善制度和流程规范。