高校网络安全风险治理方法研究

张人杰[1],李　伊[1],田　刚[1],黎天人[2]
(1.湖南邮电职业技术学院,湖南长沙 410015;2.湖南工学院,湖南衡阳 421002)

【摘要】高校网络安全风险治理是一项多部门协调合作、联防联动的全方位网络安全技术与综合管理的融合工作。文章首先介绍了高校网络安全风险基础治理和脆弱性治理,然后分析了网络安全风险社工防范,最后提出了高校网络安全风险治理通用性方案,通过网络安全风险监测与阻断等各类手段实现了高校网络安全风险治理。

【关键词】高校;网络安全;风险治理
【doi:10.3969/j.issn.2095-7661.2021.02.008】
【中图分类号】TP393.08　　【文献标识码】A　　【文章编号】2095-7661(2021)02-0029-03

Research on the Management Methods of Network Security Risk in Colleges and Universities

ZHANG Ren-jie[1], LI Yi[1], TIAN Gang[1], LI Tian-ren[2]
(1.Hunan Post and Telecommunication College, Changsha, Hunan, China 410015; 2.Hunan Institute of Technology College, Hengyang, Hunan, China 421002)

Abstract: University network security risk management is a comprehensive network security technology and comprehensive management integration work of multi department coordination and cooperation, joint defense linkage. This paper first introduces the basic management and vulnerability management of network security risk in colleges and universities, then analyzes the social work prevention of network security risk, and finally puts forward the general scheme of network security risk management in colleges and universities, which realizes the network security risk management of universities through various means of network security monitoring and blocking.

Keywords: colleges and universities; network security; risk management

现在正处于信息化向数字化发展的时代,人们的生活方式和社会存在状态逐渐形成数字化生存,更加依赖网络[1]。网络系统的复杂形态、云计算、大数据、移动互联网的发展使得网络安全风险也变得更难评估和控制[2]。网络安全不仅关系到公民个人信息安全,还关系到国家安全。高校作为人才培养、科研创新和文化传承的前沿阵地,肩负着网络信息安全教育和建设的重要责任[3-4]。如何推进高校网络信息安全风险治理,已成为高校信息化建设的重中之重[5]。

为充分落实网络安全工作要求,大力加强网络安全风险隐患排查和治理,有力提升安全防护能力、增强网络健壮性,筑牢高校“安全底座”,本文对高校网络安全风险隐患排查治理进行了研究,总结并提出了基础治理、脆弱性治理、社会工程学防范三个方面的网络安全风险治理方法,最后通过网络安全风险威胁监测与阻断实现高校网络安全风险治理目标。

1 高校网络安全风险治理方法

1.1 网络安全风险基础治理

网络安全风险基础治理主要是通过开展资产信息清查实现全量资产的全生命周期动态安全管理,提升定级备案规范性、准确性。资产清查包括网络和系统资产清查、IP 地址清查、系统互联关系拓扑图梳

[收稿日期]2021-04-25
[作者简介]张人杰(1982-),男,湖南长沙人,湖南邮电职业技术学院副教授,高级工程师,硕士,研究方向:计算机网络技术、教育信息化。
[基金项目]2019 年湖南省教育厅科学研究项目“大数据背景下数据挖掘在教学诊改中的研究与应用”(项目编号:19C1369);2021 年湖南省教育科学研究工作者协会高等教育重点课题“高职在线教学资源库建设研究”(课题编号:XJKX21A056)。

理、定级备案信息清查、安全基线核查等五方面。

1.1.1 网络和系统资产清查

网络和系统资产清查应通过云网安全管理平台，对IT类和非IT类资产进行全面覆盖。IT类资产主要包括主机、应用系统、虚拟机，这类资产安全基础信息的采集应提供适应各种主流平台的轻量级代理，广泛支持对操作系统、数据库、中间件等其他关键信息的自动采集，代理运行可控。全量非IT类资产主要包括各专业的网络设备、安全设备和存储设备，该类资产安全基础信息的采集建议通过与各专业网管系统对接的方式来实现。另外可利用自动化手段定期探测网段，保证纳管资产覆盖的完整性和准确性。

1.1.2 IP地址清查

IP地址清查应梳理全量IPv4和IPv6地址段信息，准确掌握地址分配和使用情况。针对全量地址进行核查确保100%准确，建立IP地址管理台账并纳入IP地址备案管理系统，提升IP地址准确率。充分运用或推动优化IP地址“一键查询”技术手段，建立快速溯源机制。

1.1.3 系统互联关系拓扑图梳理

梳理互联网暴露面系统，并对系统进行唯一性名称标识。以互联网暴露面的每一个系统为维度，形成该系统内部拓扑图和系统信息表。对内部承载网络上的系统，进行唯一性名称标识，以内部承载网络上的每一个系统为维度，绘制该系统内部拓扑图并形成系统信息表。

1.1.4 定级备案信息清查

结合资产清查，对已知资产100%进行定级备案。聚焦核心系统及包含网络拓扑、资产的重要系统，重点开展排查梳理，形成核心系统清单，开展风险评估、符合性评测和风险整改。新增定级网络单元或存量网络单元信息发生变化时，应及时更新定级备案管理。

1.2 网络安全风险脆弱性治理

1.2.1 互联网风险防范治理

全面梳理互联网暴露面场景，多维度拉网式清查互联网暴露面。开展互联网暴露面新增、归并、退出、安全防护、稽核检查和动态管理，强化基于区域和时间的访问控制。通过检查账号台账、设备日志、审批记录等方式，对账号密码加强管理。

查看系统版本信息、补丁安装等情况，并利用自动化扫描工具、人工渗透测试、代码审计等手段对全部资产进行检测。安全设备病毒库、漏洞库、插件库等应及时更新，在发生重大漏洞预警后应立即更新。

对运营数据、敏感信息、软件源代码及其系统配置信息的安全运营情况进行筛查和基线提升，防止不当使用而引发的数据泄露风险，全面提高对各类敏感信息的安全管控能力。

1.2.2 僵尸木马蠕虫治理

针对僵尸木马蠕虫等病毒的治理包括总体治理、主机终端、网络和安全设备、物联网设备等方面。

总体治理可结合全流量、IPS/IDS，主机安装的防病毒和主机防护类软件，检查主机等对象是否存在异常进程、异常外联等行为，审计账号、日志等是否存在入侵痕迹。具体措施包括：主机和终端应安装防病毒软件或主机防护软件；定期对各类网络和安全设备日志进行审计排查，清除僵木蠕风险隐患。

各类服务器、PC机、虚拟机等主机或终端通过终端防护软件扫描排查。首先加强僵木蠕查杀能力，重要主机应具备僵木蠕等恶意程序查杀和隔离能力，除能够定期更新特征库外，同时应具备向重要主机推送紧急更新的能力；另外可在主机中部署主机防护类系统，对应用系统的流量、行为等进行持续监控，识别并防御梳理；定期对主机开展漏洞扫描和基线核查，及时整改漏洞和基线不合规项，减少恶意程序利用脆弱性传播的风险；减少端口暴露；做好权限管控，限制最高权限帐号直接远程登录。

网络和安全设备，例如路由器、交换机、防火墙等应检查设备配置，梳理网络策略台账，检查设备日志和告警。严控高风险端口、做好隔离控制、确认防护功能启用、消除网络自身隐患。

自有机顶盒、网络摄像头、LED屏等物联网终端及应用平台可通过网管或远程登录等手段，按照设备类型、型号和版本，对物联网设备配置进行核查，评估物联网组网拓扑和边界防护策略。

1.3 网络安全风险社工防范

1.3.1 社会工程学意识教育

开展覆盖全体师生的社会工程学攻击手段及防范教育，内容应包括电子邮件钓鱼、短信钓鱼、电话钓鱼、人员接触方面的社会工程学攻击防范意识教育，宣贯电子邮件及短信钓鱼的攻击原理、流程，指出恶意附件、恶意仿冒链接、伪造身份、套取敏感信息、不明身份人员非法操作设备等需要提高警惕的具体场景情形及识别恶意信息、保护敏感信息等相应的应对处置方法。

1.3.2 防范措施自查

检查办公场所等向公众开放场所的防范措施，检查高校办公楼宇、教学实训楼宇的工作、教学专用区域等非开放的门禁管理措施。高校应检查信息防泄漏措施是否完备，敏感信息处置和存储是否合规。通过摸排、联动，及时对钓鱼邮件源头IP进行封锁处理，采用技术手段封锁钓鱼邮件的转发。用户使用过程定期监督检查，比如是否定期修改密码，是否定期进行

木马、病毒查杀。

1.3.3 远程办公社工防范

确认工作沟通人员身份,不与身份不明的人员进行工作沟通、发送工作文件等。不打开来路不明的邮件链接及短信链接。全体教职员工应做好社工隐患自查、整改工作,发现异常情况及时上报网络安全管理部门。如已造成社工危害(包括打开钓鱼邮件、透露敏感信息等),立即终止行为并联系网络安全管理部门进行风险排查,采取处理措施。

1.3.4 四方安全管理

要梳理各类系统供应方、合作方、系统集成方、外部支撑方(简称“四方”)的现状,理清责任界面,严格操作权限、信息掌握、操作审计,消除责任不清、以包代管等现象。

2 高校网络安全风险治理实现

通过建设技术手段、购买能力或服务等方式,实现公网资产威胁监测和处置能力的 100%全覆盖,内网资产威胁检测和处置能力的有效覆盖,全面构建纵深防御体系。通过网络安全风险威胁监测与阻断各类手段实现高校网络安全风险治理目标。

2.1 梳理威胁监测和处置防护现状

梳理已有威胁监测和阻断防护设备、能力清单,核实其当前防护范围,尤其是对公网安全资产防护的覆盖范围,建立公网、内网安全资产、舆情系统防护设备和防护能力台账。

威胁监测和阻断防护设备清单包括但不限于:防火墙、IPS、IDS、网站拟态防护系统或 WAF、网站安全监测、流量攻击监测、网页防篡改等。内网防护设备清单包括但不限于:内网蜜罐、网络数据防泄露系统、终端数据防泄露、日志审计系统、邮箱沙箱系统、APT 攻击防护系统、账号管理系统、4A 系统。防护能力包括但不限于:自动化工具扫描和渗透防护、SQL 注入防护、文件上传防护、任意命令执行防护、文件包含防护、缓存溢出与堆栈溢出防护、逻辑漏洞防护、代码执行防护、跨站脚本防护、远程拒绝服务防护、敏感内容防护、路径穿越防护等。

2.2 加强建设威胁监测和处置防护能力

实现公网边界威胁监测和处置全覆盖。明确网络的内外部边界,在网络系统或公网流量出口处部署威胁监测和阻断防护设备。对于公网网络边界不清晰的,要进行网络梳理整合,形成统一明确的网络边界。对于已部署的防护设备,要全面核查和更新防护策略,确保防护能力的完整性和有效性。对于未部署防护设备的,则应新建防护设备进行防护,确保公网网络边界防护全覆盖,做到监测无盲点。

强化内网的监测和防护。通过在内网的重要网络边界部署流量探针,在核心系统所在网段部署 IPS、WAF、蜜罐、端口镜像、安全日志等方式,对内网进行集约防护,实现内网重点节点实时监测、集中分析和统一处置。内网边界处应对常见的病毒传播端口和高危漏洞端口进行拦截,提升终端的安全性、避免常见木马蠕虫传播,同时避免该类事件被误判为内网渗透事件。

系统和网络安全日志审计能力部署。建设具备对公网系统、网络安全设备、存在敏感信息重要系统的登录日志、操作日志、告警日志、安全日志和应用日志等进行审计的技术手段,审计是否存在账号登录异常、服务进程异常、重要进程状态异常、非授权访问目录或文件、数据库非法登录或数据非授权导出、网站页面被篡改等情况,对网络安全设备日志应进行汇总和集中研判。

2.3 开展威胁监测和阻断防护设备有效性检测

对防护设备进行持续或定期拨测,在防护期间应利用最新公布的 POC 编写测试脚本对业务进行穿测。在穿测期间检查 IPS、WAF、全流量探针、防毒墙、态势感知平台是否有对应日志以及告警产生,POC 动作是否成功执行。

对终端安全设备进行持续拨测,在防护期间利用最新的系统漏洞或可通过网络侧传播到主机侧的漏洞(RCE 或者 webshell)进行业务穿测。在穿测期间检查主机安全、防病毒软件、终端沙箱是否有对应日志以及告警产生,系统漏洞是否成功执行。应对整个链路上安全软件响应时间进行评估,对接入云 WAF 系统持续或定期拨测接入系统域名解析是否为云 WAF 地址,确认接入云 WAF 是否正常,同时云 WAF 应用策略需定时检查。

监测策略统一管理,确保监测处置高效闭环,建立一键封堵手段。开展攻击态势分析,细化 IP 地址实名制管理,建立 IP 白名单管理机制。

2.4 积极探索新技术应用

积极探索威胁监测与防护的新方法,如运用拟态防护、动态防护等主动防护手段,提升对已知和未知威胁的防护能力。使用态势感知、威胁情报、智能攻击检测、攻击回溯分析等大数据和人工智能技术手段,提升对威胁的发现识别、理解分析和响应处置能力。结合新技术手段探索主动防御、零信任安全、自适应安全等新思路,系统化加强威胁监测与处置能力。

3 结语

没有网络安全就没有国家安全,没有信息化就没有现代化。高校网络安全风险治理是筑牢高校“安全底座”的重要环节,在这个过程中,需要协同多方科学完善整个治理体系。(下转第 56 页)

激发创新创业热情，锻炼团队协作能力，培养敢想敢做的精神。

其次，积极联动企业共建创新创业实践基地。学校应以项目为载体，或以短期实习为形式，给学生提供至少一次真正实操或模拟实操的机会，为学生配备企业导师，对优秀学生项目或学生团队给予经费支持，帮助学生开阔视野，获取实战经验。同时，还需积极整合校内外资源，设立学生创新创业基金和线上服务中心，解决学生创新创业资金难题，解答学生创新创业各种疑问，为其提供及时服务。

再次，精心创设融入本土文化的系列情境任务，情境任务也是一种软性实践平台。抓住本土建设的契机，顺势拥抱技术创新和文化产业变革，把本土文化和新媒体技术相结合，融入创新创业教育教学，创设系列情境任务。比如广州餐饮老字号专业研学行动，引导学生通过制作抖音短视频、Vlog 等看得见、可传播，甚至在市场上可能创造效益的文化作品，实现创新创业教育寓教于用。

2.3 构建常态化创新创业教育保障机制

为实现常态化创新创业教育，需构建包括政府、企业、高校、学生等层面的协同育人的长效机制[5]，即校校、校企、校地、校所以及国际合作的协同育人新机制[6]。其中，高校是大学生创新创业教育的责任主体，应从经费保障、资源支持和政策扶持方面着力解决大学生的燃眉难题。

2.3.1 划拨专项经费

学校要结合创新创业教育工作的基本需要，拨付专项经费，确保各项活动的有效开展。如前所提，条件允许时应设立创新创业基金，用于扶持在校级以上创新创业竞赛中突围的创新创业项目和团队。

2.3.2 建立创新创业项目资源库

紧密结合院校专业群特色和地方经济发展需要来开发系列创新创业项目，建立创新创业项目资源库，在课程教学中期及实践阶段，由学生根据自身兴趣和条件从资源库中选取项目进行实操锻炼。

2.3.3 制定创新创业专项支持政策

政策支持是必要的，如制定灵活的学籍管理制度，实行弹性学制，延长修业年限，保证大学生学业、创业两不误。同时制定跟踪服务措施，为学生创新创业提供持续的咨询和服务。

3 结论

大学生创新创业是一种教育实践，也是一种文化体现。[7]强化创新创业教育和校园文化的共建关系，是提高创新创业教育作用力的重要途径。从微观角度看，创新创业教育与校园文化建设共生系统，包括课程教学、实践载体、宣传积淀等子系统，子系统之间相互依赖、相互影响。从中观角度看，创新创业教育与校园文化建设共生系统是文化育人、实践育人的载体，教育理念、体制的变迁都会对共生系统产生影响。从宏观角度看，创新创业教育与校园文化建设共生系统更是处于社会大生态系统中，社会政治、经济、文化的发展同样会对共生系统产生影响。由此分析，创新创业教育与校园文化共生系统涵盖了政府政策与社会政治、经济、文化等因素，也包含高等院校师生，以及创业教育与校园文化建设目的、方法、内容等，共生系统各因子之间相互作用，促进生态平衡。

【参考文献】

[1]陈燕，崔顾芳.新时代高职院校大学生创新创业教育实践探索[J].教育与职业，2019(11)：52-57.

[2]路静，高会贤.创新创业背景下的高职院校文化建设初探[J].教育现代化，2020(5)：50-52.

[3]胡晓玲.浅谈创业教育教师的基本素质[J].教育探索，2011(6)：114-115.

[4]杨华，谢仁恩.人文素质教育融入高校创新创业教育刍议[J].学校党建与思想教育，2021(4)：87-88.

[5]郭芳，张立仁，郭郁."四位一体"构建大学生创新创业教育协同育人机制[J].教育与职业，2019(9)：61-65.

[6]国务院办公厅.关于深化高等学校创新创业教育改革的实施意见[EB/OL].http://www.gov.cn/zhengce/content/2015-05/13/content_9740.htm，2015-05-13.

[7]刘静，戴钢书.嵌入型理论视域下高校创新创业文化建设路径探索[J].学校党建与思想教育，2020(9)：17-19.

（上接第 31 页）

本文结合高校网络安全风险治理相关经验，提出通用性方案，为高校网络安全风险治理提供参考。

【参考文献】

[1]邬贺铨.走中国特色的网络强国之路[J].红旗文稿，2021(7)：13-16.

[2]徐婧.网络安全领域未来面临的十大网络安全挑战[J].世界科技研究与发展，2020(6)：697.

[3]林志兴，张武威，余建，刘孙发，许力.基于模糊集的高校网络安全等级保护体系研究[J].计算机应用与软件，2021(4)：305-310.

[4]王贵，郭朕.高职院校内网网络安全问题的研究[J].湖南邮电职业技术学院学报，2020(4)：24-26.

[5]周立志，朱尚明.高校网络信息安全体系建设实践和思考[J].深圳大学学报(理工版)，2020(S1)：73-77.