DOI：10.16661/j.cnki.1672-3791.2201-5042-5034

高职院校网络安全事件应急响应机制研究

肖宇　陈秉洁
(江海职业技术学院　江苏扬州　225101)

摘　要：随着互联网信息技术的不断进步，高职院校校园网络也随之优化与发展，在为校园的数字化教学、管理、服务提供助力的同时，其安全性、稳定性对学校的进一步发展有着重要影响。该文以高职院校网络安全事件及应急响应机制为研究对象，通过研究建立适合高职院校的动态网络安全模型，并就高职院校校园网网络在新时代下存在的问题以及相应的对策展开探讨。

关键词：高职院校　动态网络安全模型　网络安全事件　应急响应机制

中图分类号：TN915.08　　**文献标识码：**A　　**文章编号：**1672-3791(2022)08(a)-0015-03

纵观当前时期，网络信息化技术在高职院校中得以全方位应用，使得学校教育教学工作及常规管理工作的实施更具便捷性，其为师生的工作、学习、校园生活提供了优质服务。但是，面对日益变化、层出不穷的网络安全威胁，传统、被动的防火墙和防毒软件两层安全防御策略，已然无法有效防止内部攻击，也不能主动跟踪监测入侵者，新时代下的校园网络系统优化及革新工作势在必行[1-2]。

因此，我们需要利用新技术、新方法、新手段，通过建立符合高职院校网络安全事件特征的应急响应机制，来保障校园网络和信息系统安全，确保学校各项业务信息系统安全运行。该次课题研究中，我们基于动态网络安全模型，就高职院校网络安全事件应急响应机制加以研究，期望可以促使高职院校信息化稳步推行，以更为完善且科学的应急响应机制，确保我国高职院校网络系统的安全与稳定[3-4]。

1　高职院校的网络安全情况分析

1.1　我国网络安全概况

近年来，我国互联网蓬勃发展，截至2020年12月，我国注册的网站数量为443万个，网页数量为3 155亿个，较2019年底增长5.9%，我国网民规模为9.89亿，互联网普及率70.4%。构成了全球最大的数字社会，也充分享受着信息化服务的便利。与此同时，网民遭遇网络安全问题的比例得到进一步提升。2020年，全网漏洞数量和网络攻击数量都有所增长。其中，以远程代码执行漏洞利用攻击为主的Web攻击事件危害加大，以诱骗欺诈为目的移动恶意程序的事件占比最高，威胁网络安全的高危安全漏洞数量不断增多[5-7]。

1.2　高职院校网络安全现状

2018年，我国教育部公布了一项关于高职院校网络安全的信息统计。文件表明，高职院校网络容易成为攻击的对象，高职院校的服务器和网络一旦被攻破，遭受数据泄露、设备损坏、网络瘫痪等情况，将严重影响师生的校园生活，威胁师生的信息安全，危害学校的社会声誉。

1.3　高职院校网络安全情况分析

虽然现代网络技术迅猛发展，各类网络、设备和软件仍然存在漏洞，不法分子会利用漏洞窃取个人信息进行谋利。同时，高职院校网络安全性不高，容易成为黑客的攻击对象，变成其检验自身技术、展示自身能力的试炼石。此外，新概念、新技术的出现既加快了教育信息化的发展，也吸引了黑客的目光，DDos攻击、网络病毒、信息窃取等纷至沓来。综合分析，以下3个因素是造成高职院校网络安全事件发生的主要原因。

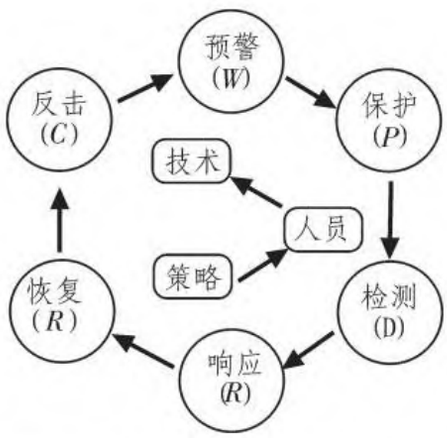
1.3.1　网络安全管理缺位

高职院校在学校的网络安全建设和管理方面重视程度不够，没有按照国家网络安全要求及相关制度的要求，从顶层进行合理规划与设计，网络安全管理制度不完善，网络安全管理方法不健全，使学校自身的网络安全管理存在较多漏洞，一旦被攻击容易产生不利影响。

1.3.2　网络安全技术缺乏

高职院校对于校园网络安全技术的资金投入捉襟见肘，在建设和维护校园网络上花费了大部分经费，在配置所需的网络安全平台及运维设备时就只能量力而行了。同时，高职院校一般不会专门设置网络安全技术岗位，主要是由其他技术岗位人员兼职完成网络安

作者简介：肖宇(1985—)，男，本科，馆员，研究方向为信息化管理。



	预警	保护	检测	响应	恢复	反击	人员	策略	管理
PDR	无	有	有	有	无	无	无	无	无
PPDR	无	有	有	有	无	无	无	无	无
PDRR	无	有	有	有	有	无	无	无	无
MPDRR	无	有	有	有	有	无	无	无	有
WPDRRC	有	有	有	有	有	有	有	有	有

图1　动态网络安全模型防护功能对比

全管理工作。因此，工作人员在缺少丰富的网络安全管理经验和相关技术的情况下，很难做好对学校的网络安全防护工作。此外，随着5G等新技术的加快应用，各类网络终端层出不穷，网络接入方式的改变将导致新型攻击方式的迭代。

1.3.3 师生安全意识缺失

高职院校师生的网络安全意识偏弱，对于潜在的网络安全风险没有足够的认知和辨识能力，既是自身的网络安全知识不足的体现，也是学校网络安全意识教育宣传不足的表现。比如：没有良好的安全防毒意识，共用U盘时没有主动扫描杀毒的习惯；没有较强的信息保护意识，常用的登录密码不够复杂或者通用；没有足够的安全辨别能力，会打开陌生的文件、转发或者点击来路不明的图片和链接等。这些都给了不法分子可乘之机，危害个人信息和校园网络的安全。

2 适合高职院校的动态网络安全模型

传统的、被动的、静态的信息网络安全技术，侧重于网络和系统本身的加固与防护，能够起到一定的网络防御作用，但是面对动态发展的网络技术，传统的网络安全技术就显得力不从心了。随着新技术、新协议、新软件和新应用的更新迭代，需要采用动态网络安全模型建立主动式、全方位的网络安全防御体系，在不同的层级实施防护，能够自主评估防御漏洞和主动修补，能够主动检测入侵行为和及时预警，能够有效进行应急响应和灾难恢复。

自从美国国际互联网安全系统公司ISS提出第一个动态网络安全模型PDR以来，网络安全理论经过不断完善，已发展出PPDR、PDRR、MPDRR和WPDRRC等动态网络安全模型，用以指导网络信息安全防护实践。其中，WPDRRC是我国“八六三”信息安全专家组提出的适合中国国情的动态网络安全模型，包含预警、保护、检测、响应、恢复和反击6个环节，以及人员、策略（法律、法规、制度、管理等）和技术3大要素，能够针对不同的安全威胁，采用不同的安全措施，对网络、设备、业务、数据等受保护对象进行多层次保护。同时，通过图1综合分析，我们发现其他模型都没有综合考虑人员、策略、管理要素，不利于实施网络安全的整体防护。因此，高职院校 根据实际情况，应该选用WPDRRC动态网络安全模型建设学校的网络安全防御体系。

高职院校匹配WPDRRC动态网络安全模型，应在其6个环节做足功夫：在预警环节，通过动态感知预测威胁信息可能的行动；在保护环节，设立好信息安全防护措施，定义好网络访问控制；在检测环节，及时更新入侵检测特征库，以便有效应对网络攻击；在响应环节，积极完善响应方案，及时处理好网络安全事件；在恢复环节，利用备份信息恢复网络与数据资源；在反击环节，监控与记录入侵行为特征，作为追责的有效证据。同时，要通过管理加强师生的网络安全意识，保证网络安全策略的有效执行，发挥网络安全技术的应用功能。

3 高职院校建立健全应急响应体系

在高职院校匹配的WPDRRC动态网络安全模型中，应急响应是其中一个重要环节，往往也是容易被管理者忽略的环节。相比较而言，应急响应起到承上启下的重要作用，既能弥补保护和检测环节的不足，又能促使管理者发挥好主观能动性，成为实施恢复和反击的有力抓手。因此，高职院校应通过建立健全应急响

应体系，提高应对网络安全事件的能力，预防网络安全事件的危害，降低网络安全事件的损失。

3.1 明确应急响应体系的目标和原则

按照《国家网络与信息安全突发事件应急预案》，应急响应体系建设的目标是提高应对网络信息安全事件的能力，减少网络信息安全事件造成的损失和危害，保障网络与系统运行平稳、安全、有序、高效。

应急响应体系建设主要有以下6个原则：(1)规范性原则。为保证应急响应体系的有效实施，应该建立清晰、完全的描述文档，并健全规章条例，明确工作职责，以保证其有效运行。(2)动态性原则。网络安全时刻都在发生变化，要发挥应急响应体系的实效就必须依据网络安全的发展动态实时做出必要调整。(3)信息共享原则。在应急响应过程中，需要秉承信息共享的原则，对重要信息、数据内容进行筛选和分析。(4)整体性原则。应急响应体系要从技术和管理两个层面进行统筹安排，兼顾考虑全局和局部、整体和细节的关系。(5)现实可行性原则。应急响应实时要确实可行，能够在实际操作中不断改进以符合预期效果。(6)指导性原则。应急响应系统体系对于处理同类网络安全事件具有指导意义，为整个网络安全工作提供全局性指导。

3.2 建立健全应急响应体系的主要任务

3.2.1 做好网络安全事件分类分级

参照《信息安全事件分级分类指南》，按照高职院校网络安全事件的影响范围和程度进行分类分级，可分为有害程序事件、网络攻击事件、信息破坏事件、信息泄露事件、信息内容安全事件、信息系统故障、灾害性事件和其他信息事件8个类别，以及一、二、三、四级4个级别。

3.2.2 落实应急响应组织和保障

高职学校应建立好应急响应的组织体系，在处理网络安全事件需要多部门协作时，可以确保统一指挥、联动联调、快速反应、高效处理。通过明确各层级、各岗位的相关责任考核，加强对应急响应工作执行的监督，保障高职院校内部形成有机整体，能有效应对网络安全事件。

3.2.3 做好应急响应的启动和处置

高职学校要做好日常网络安全的监控与预警，对于事件隐患可以早发现早处置。在日常的监控与巡检中一旦发现可疑事件，通过检测和评估确定网络安全问题后，要及时启动应急响应，采取合理有效的应急处置措施，联合多方力量全力以赴，直到彻底解决问题，并将网络安全事件处理结果和报告及时反馈。

3.2.4 落实应急响应的定期演练

高职院校要认真落实应急响应的定期演练，检验自身网络安全防护是否到位、应急响应措施是否合适、网络安全人员是否能正确处置相关事件，通过暴露自身的缺陷和弱点，及时改进网络安全防护体系。

3.3 建立健全应急响应体系的建议

3.3.1 加强管理、落实责任

随着信息科学技术的发展，网络安全防护的压力会越来越大，高职院校要积极建立符合本校实际的、行之有效的网络安全管理制度。一方面，明确师生用户在校园网络范围内的权利和义务，依规依法进行管理。另一方面，按照管理制度实施工作考核，强化责任意识，并成立专门网络安全管理部门，做到权责清晰。

3.3.2 加强宣传、防微杜渐

高职院校要加强对师生网络安全意识的宣传、教育和引导，通过国家网络安全宣传周的各类宣传活动，警示忽视网络安全的风险和隐患，促使其养成良好的上网习惯。既要“会用网”，有定期杀毒、不定期更换密码和保护个人敏感信息的安全意识，又要“用好网”，避免点击未知链接，扫描不明二维码，访问高风险的网络和使用非正版的软件。

3.3.3 加强合作、联动共享

高职院校需要加强和互联网企业、服务提供商、政府网络安全部门的交流和合作，通过合作共赢获得其技术和信息上的支持，完善网络安全防护手段、提高网络安全防护能力、提升应急响应处置水平。同时，可以加强兄弟院校之间的合作，共同建立应急响应中心，共享网络安全情报，联动实施应急管理，协调各类应急资源，协同处置网络安全事件。

基于动态网络安全模型，通过对高职院校网络安全事件应急响应机制的研究，我们可以提高网络安全风险应对能力，解决各种网络安全威胁，降低网络攻击造成的损害，保护学校的网络资源和设备资产，保障师生个人信息的利益，从而打造一个符合现代化要求的教育、管理和服务的网络环境。

参考文献

[1] 顾子康.高校网络安全应急响应处理机制研究[J].数码世界,2020(2):241.
[2] 王克栋.高职院校数字化校园网络安全防控体系探讨[J].信息与电脑:理论版,2020,32(16):186-187.
[3] 刘海龙.高校网络安全应急响应处理机制探讨[J].产业与科技论坛,2020,19(15):277-278.
[4] 周向东.高校网络安全存在的问题及对策研究[J].科技资讯,2019,17(18):22-23.
[5] 祝新宇.构建网络空间命运共同体的问题与路径研究[D].北京:北京邮电大学,2021.
[6] 曾辉.江西地方政府应对网络舆情的对策研究[D].南昌:江西财经大学,2019.
[7] 崔金生,丁霞,刘明,等.网络安全事件应急响应策略体系研究[J].计算机应用与软件,2009,26(7):274-277.