

简析制定高校网络安全事件专项应急预案的重要性

王明宇

(黑龙江林业职业技术学院信息工程学院,黑龙江 牡丹江 157011)

摘要:高校网络安全运营是保障高校教育、教学工作正常进行的基础。随着网络安全法的颁布,保障网络安全也成为网络运营部门的义务。本文结合两个遭受攻击的案例,对网络遭受攻击后如何快速处置及预案的制定进行了探讨。

关键词:网络安全;应急预案

[DOI]10.12231/j.issn.1000-8772.2021.02.295

计算机网络系统和信息系统的大量应用对高校办学质量的提高起到了重要的基础作用。高校中的信息系统主要分为五大类:(1)行政管理类,如OA办公自动化系统、人事管理、财务管理等;(2)教学管理类,如教务系统、督导系统、师资管理系统、科研管理系统、各种网络教学平台等;(3)学生管理类,如学工、宿舍系统;(4)消费管理类,如一卡通等;(5)网络设备管理类,如上网认证计费管理、云平台管理、网站群管理、WEB VPN管理等。随着高校软件系统应用增多,对网络安全要求也越来越高。

近年来,网络高度发展带来便利的同时,网络安全事件频发,为网络安全运营带来了前所未有的挑战。尤其在教育系统,网络安全隐患多,主要体现在:系统多、漏洞多、威胁攻击多、投入不足(资金不足、人员不足)。教育系统网络安全防护薄弱,为国内外不法分子提供了可乘之机,信息泄露、网站被黑客攻击等事件频发。

2017年《中华人民共和国网络安全法》颁布,明确规定了网络运营者不履行网络安全保护义务要承担的法律后果。网络安全法的颁布引起了各网络运营单位的重视,各高校加大了网络安全建设的投入。然而仅仅只是重金购买网络安全设备并不能保证网络的安全。高校网络安全是一个系统性的安全,高校网络安全的系统要素包括:人、组织、IT系统。人是操作主体,组织是管理和责任主体。在网络遭受攻击时,如何快速反应,将危害降到最低是网络管理者的重要任务。

网络安全法第二十五条规定:网络运营者应当制定网络安全事件应急预案,及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;在发生危害网络安全的事件时,立即启动应急预案,采取相应的补救措施,并按照规定向有关主管部门报告。

高校网络运营管理部门大多都按照各行业网络安全事件应急预案模板制定了《网络安全事件应急预案》,规定了组织机构与责任、应急处置流程、调查与评估等内容。由于应用系统众多,各系统遭受的工具方式各异,应急处置方案也不尽相同,所以不能只有一部《网络安全事件应急预案》,还要针对不同的应用系统和不同的突发事件制定《专项应急预案》,保证事件的快速处理、降低事件的影响范围。

以本人经历的两个不同应用系统遭受攻击处置方法为例:

(1)一卡通被植入木马事件

在日常服务器巡检过程中,发现一卡通身份前置机服务器账户异常,突然增加了一个用户账户。由于一卡通虽然与校园网络共用一条光纤,但VLAN不同,防火墙设置了安全策略,一卡通网络与办公、教学网络不能互访,一卡通网络也不能访问外网,所以立即断开一卡通核心数据库服务器线路,断开一卡通交换机与校内核心交换机连接,保障数据安全。此时没必要切断全校网络,影响正常的教学管理。事件分析后查明是一卡通服务人员私自通过U盘拷贝程序致使服务器中了木马病毒。

(2)WEB VPN被植入挖矿病毒事件

安全感知平台报警,WEB VPN设备被植入了挖矿病毒。由于WEB VPN提供师生校外访问校园网服务,立即切断WEB VPN设备与校园网的连接,启动终端检测响应平台对服务器进行扫描。事件分析后查明是WEB VPN厂家调试后,遗留弱密码账户,被黑客工具扫描破解植入病毒。

从以上两个网络安全事件可以看出,不同的系统应急处置方法不同,需要制定专项的网络安全事件应急预案,按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级,并规定相应的应急处置措施。

高校编制本单位网络安全事件专项应急预案可以参考教育系统网络安全应急预案架构。主要要点包括:组织机构及职责、事件级别及事件类型、事件响应流程、预警措施、调查与评估。

教育系统网络安全事件分为四级:特别重大网络安全事件-I级、重大网络安全事件-II级、较大网络安全事件-III级、一般网络安全事件-IV级。直观的判断网络安全事件等级可以参考下表

表 1

事件等级	直观判断	报送单位	指挥处置主体
一级事件	跨省的影响严重事件	部网络安全应急办、中央网信办	部网信领导小组
二级事件	不跨省的影响严重事件	部网络安全应急办	地方省级教育行政部门或教育部
三级事件	单位的严重事件	省级教育行政部门	本单位
四级事件	一般事件	本单位自行处置	本单位

以高校《门户网站网络安全事件专项应急预案》为例,说明事件响应流程的制定:

(1)事发紧急处置:断网、保护现场、上报本单位安全到任人和主要负责人。

(2)事中情况报告与处置:掌握损失、分析原因、修复漏洞、恢复功能、配合调查、事件报告的填写。

(3)事后整改报告与处置:总结教训、排查隐患、加强管理和防护。事件报告的填写。

在日常的网络管理中,高校应制定完善相关的专项应急预案和配套的管理制度,建立完善的应急管理体制机制,按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施,做好网络安全核查、风险评估和容灾备份,加强信息系统的安全保障能力。

参考文献

[1]中华人民共和国网络安全法.2017.

[2]中央网信办.国家网络安全事件应急预案.2017.

课题:本论文是黑龙江省高等职业教育教学改革研究项目《网络安全等级保护2.0制度下智慧校园网络安全防护措施与制度建设研究》的研究成果;课题编号: SJGZZ2019030