基于动态安全模型的职业学校网络安全体系的构建

周 郁

（江苏省常熟职业教育中心校，江苏 常熟 215500）

摘要：当前智慧校园的建设正在很多职业学校中如火如荼地开展，智慧校园的建设不仅使得信息技术得到广泛应用，而且也提升了职业学校教育信息化的进程；但与此同时随着网络规模的扩大、各种应用系统的推广，校园网络安全的问题也日益突出，如何保证校园网络和业务系统正常运行成为亟须解决的新课题。本文基于P2DR2动态安全模型，对职业学校校园网络安全体系的构建进行了分析和研究，将有助于保障智慧校园的正常运行。

关键字：职业学校；网络安全； P2DR2模型

校园网是智慧校园的基础，是现代校园的主要组成部分之一，在学校的教学、管理和生活等方面发挥着举足轻重的作用。但随着智慧校园和教育新基建的深入建设，校园网络的体系结构也愈加复杂、规模也愈加庞大，同时网上教学、移动应用等各种应用的推广，面临的网络安全威胁和风险也不断增多。根据《中华人民共和国网络安全法》中相关条款的规定，学校亟须加强校园网络安全防御的主动性和准确性，并且提高定位网络攻击的效率，因此本文对职业学校网络安全体系的构建进行设计和研究，为智慧校园的正常运行提供保障。

一、智慧校园建设中面临的网络安全风险因素

（一）对网络安全问题的重视程度不足

在智慧校园的建设过程中，出于资金等方面的考虑，对于网络安全管理重视程度不够、投入不足，缺乏对病毒的主动防御和安全漏洞的分析系统，通常只是在校园网的边界部署防火墙来保护内部网络。另外在处理网络安全问题时，通常都是事后补漏，无法及时预判校园网络安全的态势。此外在职业学校中往往没有成立相应的网络安全管理机构，缺乏相应的安全管理制度和响应机制。通常情况下70%以上的信息安全问题是由管理不善造成的，而这些安全问题的95%是可以通过科学的信息安全管理制度来避免。

（二）病毒传播和黑客攻击的威胁

网络病毒的传播和黑客攻击是目前校园网络安全最大的安全威胁。当前种类和数量繁多的网络病毒往往与黑客攻击行为结合在一起，黑客通常利用病毒以及多样和频繁的攻击手段对目标对象进行攻击，而这些病毒会被植入黑客程序，当目标对象感染病毒后就会沦为黑客的肉鸡，黑客就可以远程控制这些肉鸡，对目标对象进行网络攻击，进而获取目前对象的重要信息，这对校园网络的安全构成了严重威胁。

（三）网站及各业务系统自身存在的漏洞风险

学校网站、各业务系统在设计过程中或者所采用的软件框架存在着未知的缺陷或者漏洞，而这些缺陷和漏洞会随着技术发展、系统的更新逐步被发现，这会给学校网站及各业务系统带来相应的安全风险。由于漏洞的产生，会加大病毒和网络攻击对系统的危害，因此，需要提高系统安全保护意识，将网络安全维护作为一项长期性工作。另外学校网站、业务系统所使用的服务器操作系统，也存在着缺陷和漏洞，为病毒传播和黑客攻击提供了机会。

二、P2DR2安全模型

P2DR2模型是目前被广泛采用的一种动态信息安全理论模型，它是在P2DR模型的基础上发展起来的。该模型基于企业网对象，以时间、策略为特征，包含五个元素：Policy安全策略、Protection防护、Detection检测、Response响应和Recovery恢复，在该模型中，以安全策略为核心，综合运用防护、检测、响应以及恢复等手段，形成一个完整的、动态的安全循环，构建了一个全方位、多层次的网络安全环境（图1所示）。

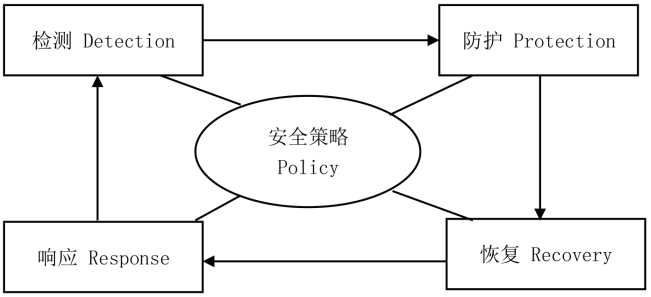

图1 P2DR2动态安全模型

在P2DR2模型中，设Pt为系统的防护时间，也就是入侵所需的时间，Dt为系统检测到入侵所需的时间，Rest为系统发现入侵的响应时间，Rect为系统恢复正常所需时间，Et为系统暴露给入侵的时间。针对防护的对象，若满足以下关系式：

Pt>Dt+Rest+Rect

则表示防护的时间大于检测、响应和恢复的时间之和，说明系统是安全的，该系统能在入侵发生之前进行处置。

若假设Pt=0，即在没有任何防护的条件下，应满足以下关系式：

Et= Dt+Rest+Rect

表示系统暴露给入侵者的时间为系统检测、响应和恢复的时间之和。从以上两个关系式可以知道：及时的检测、响应和恢复就是安全；提高系统的防护时间Pt、降低检测时间Dt和响应时间Rt，是加强网络安全的有效途径。

三、职业学校网络安全体系的构建

校园网络安全体系的建设是一个复杂的系统工程，本文基于P2DR2模型，综合运用多种技术和手段，并以安全策略为核心，构建了一个动态、多层次的校园网络安全体系。

（一）安全策略

在校园网络安全体系中，安全策略处于核心位置，防护、检测、响应以及恢复只有在安全策略的统一控制下，才能发挥最大的作用。

1. 建立校园网络安全管理制度体系

“三分靠技术、七分靠管理”是校园网络正常运行的法宝，建立全面的校园网络安全管理制度并贯彻执行则是网络安全的保障。自2017年6月《中华人民共和国网络安全法》正式实施以来，

学校成立了校园网络安全领导小组并制定了校园网安全管理的各项条例与制度，确保各项管理制度有效落实。规范了学校网站的建设原则，要求学校各类网站必须依托学校网站群系统进行建设和管理，并且遵循“谁发布谁负责”的原则规范网站信息的发布；规范了数据中心机房的安全管理、管理员的系统操作和维护的管理；建立了学校网络安全应急响应机制，确保校园网安全、可靠、稳定地运行。

2. 划分区域实施不同的访问控制策略

根据校园网中安全需求的不同，将整个校园网划分为网络出口区、核心汇聚区、服务子网区、网络接入区和客户机区，并实施不同的访问控制策略。

Internet 和校园网的边界是网络出口区，该区域的主要作用是防止非法用户访问校园网内部资源，规范校园网用户上网行为是该区域的主要访问控制策略。核心汇聚区，该区域汇聚接入层的数据，主要功能是进行路由寻址和高速的数据转发，该区域主要安全需求是对校园网进行 VLAN 划分和控制广播风暴。为校园网用户提供网络和信息资源服务是服务子网区的主要功能，该区域对网络的安全性要求比较高。该区域的主要访问控制策略是防止非授权的访问和非法的攻击，并且要保证服务器的安全，确保网络和信息资源的正常访问。为用户提供安全的网络访问服务，预防病毒的传播，并对传输的不良数据进行有效过滤是网络接入区的主要安全需求。校园网的主体所在的区域为客户机区域，该区域对校园网中的客户主机实施终端防护控制策略。

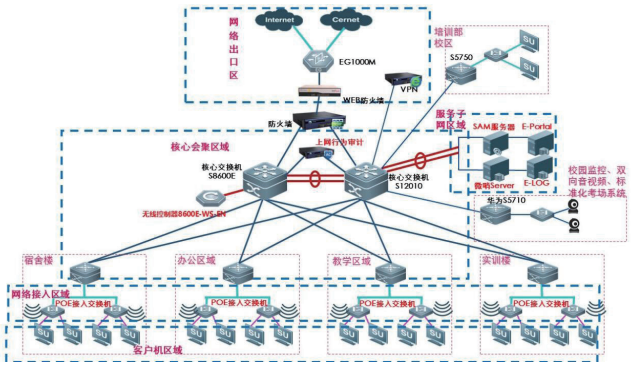

图 2 校园网区域图

（二）防护

在安全策略的统一控制下，根据校园网所采用的 TCP/IP 模型中物理层、网络层、传输层和应用层的不同功能和特性，分别采用不同的安全技术和部署相应的安全产品，实现校园网络的安全可靠运行。

1. 在物理层上，学校校园网络主干采用万兆互联和线路冗余技术，避免由于单点故障造成网络传输的中断；建立专门的备份服务器，用于重要信息系统的数据灾备，提高信息系统的可靠性。

2. 在网络层上，在网络出口与核心交换机之间架设高性能防火墙，根据“最小化访问”原则，实施“零信任 VPN 服务”，部署 VPN 设备，校园网出口网关默认不允许校外向校内访问只允许校内向校外单向访问，对外提供服务的服务器只映射所需的对应端口；主要的应用系统不对外提供服务，只能通过 VPN 进行访问；对于一些高风险的端口（如 3389、22、445、135、136、137、139 等）通过校内交换机配置 ACL（访问控制列表）进行访问隔离，可以起到过滤病毒端口，防止病毒传播的作用。

3. 在传输层方面，为了防止蠕虫病毒和 ARP 病毒对网络性能和安全的影响，对重要的服务器、网络设备的 IP 地址进行 MAC 地址绑定，防止信息被非法窃取。

4. 应用层安全防护上，为了强化对校园网用户的管理，便于对上网用户的行为审计，禁止非授权用户非法使用校园网资源，学校实行校园网用户接入实名制认证机制；学校部署上网行为管理系统，应用行为访问控制策略，屏蔽黄、赌、毒等不良的互联网信息，并对网络带宽进行合理管控，限制游戏、P2P 下载等行为，保证校园网中教学和管理业务的正常稳定运行；根据《中华人民共和国网络安全法》的要求，部署综合日志审计系统，保存用户上网行为、各种服务器、网络设备的日志，并对这些日志进行关联分析，便于事故发生后能精确回溯，满足监管部门的要求；为保证对外 web 服务的安全，学校采购部署了 web 应用防火墙，有效防御了常见的各种 web 网络攻击行为；在防病毒方面，学校部署了 EDR 终端管理平台，为学校各种终端提供了防病毒服务。

（三）检测

检测是对防护的补充，通过安全检测能及时发现现有校园网络中存在的问题与漏洞。利用防火墙的 IPS 功能，定期对校园网进行安全检测，找出网络中存在的安全隐患；同时利用综合日志系统中用户及设备的日志数据进行关联分析，实现对校园网络的安全态势感知与预警监控。

（四）响应

响应是指当网络发生异常或攻击行为后，可以触发相应机制自动或者人为来阻止该事件的发生。学校部署防火墙与终端管理平台 EDR 之间能进行协同响应，当防火墙等设备发现有外来攻击行为时，响应机制就可以记录该行为并通知管理员，使用联动 EDR 进行查杀，并阻止该行为，从而保障网络的安全。

（五）恢复

对学校主要应用系统、数据库定时进行备份，虚机定时生成快照，当系统由于某种原因不能正常工作时，系统管理员就可以利用备份机制快速迁移虚机，重建系统，保障学校业务连续性。

四、结束语

随着智慧校园建设和教育新基建的不断深入和推进，职业学校的教育信息化的水平也在不断提高。但网络安全仍是影响学校智慧校园持续发展的重要因素，基于 P2DR2 动态安全模型，从系统上规划和建设校园网络安全体系，利用多种网络安全技术及安全产品的功能互补性，在每个区域和层次上设置安全策略和安全产品，从而构建了一个多层次的安全协同防护体系，能够有效地保障智慧校园及其应用系统的安全运行，提升职业学校教育信息化的水平。但是威胁网络安全的因素是不断动态变化的，所以对于校园网络安全体系的构建需要不断地去完善和加固。

参考文献：

[1] 傅川，陈云 . 高校信息系统安全体系研究与实践 [J]. 中山大学学报（自然科学版），2009（S1）：26-27.

[2] 夏冬梅 . 基于智慧校园的网络安全保障体系建设 [J]. 智能城市，2019，5（19）：13-14.

[3] 李家春，李之堂 . 动态网络安全模型的研究 [J]. 华中科技大学学报，2003，31（3）：40-42