数字信息

浅谈数字校园背景下的信息化安全防护

[1]裴文财 [2]高 振

（营口理工学院 辽宁省营口市 115014）

摘要：目前，各大高校经过这几年加大对信息化的建设，基本实现全校网络覆盖，安全防护的能力也已经达到“二级”合格标准。如站群系统、OA 系统、招生系统、教务系统、财务系统、科研系统、人事系统、学工系统、图书管理等信息系统也已基本建成，可以说这些应用系统覆盖了大部分的管理信息化领域，数字校园建设初具规模，信息化安全防护建设也应加快建设步伐。

关键词：信息化；数字校园；安全防护；

引言

各大高校现已建成的业务系统如：教务管理、办公自动化系统、财务系统、科研系统、人事系统、学工系统等已经基本能够满足学校的日常行政办公的要求。在方便了各业务部门进行业务处理的同时，也积累了各种业务、不同阶段的各类数据。而这些数据的积累，作为学校为下一阶段的数据决策和分析提供了有效的依据和支撑。

随着数字校园建设的推进，各大高校也加快了服务器虚拟化、云计算、数据中心平台的建设等，加强对核心数据的集中管控，提高核心数据的安全性。把各类数据进行集中管理，使得对信息安全的审计、数据资产的评估、平台运维等行为更加的简单，同时使得系统容错、高可用性和容灾恢复等的实现也变得简单易行，但带来方便快捷的同时也将带来新的挑战。

1、高校信息化安全防护现状

1.1 高校网站的安全防护有待加强

随着教育信息化的快速发展，互联网技术应用的普及，网络安全问题也正面临着诸多的挑战。很多高校的网站或信息系统存在很多高危的漏洞，例如敏感信息泄露、目录遍历漏洞、命令执行漏洞、文件包含漏洞、SQL 注入、反射跨站脚本、弱口令等。虽然大部分高校都已经部署了相应的安全防护设备，但由于平时疏于管理，安全防范意识不到位，防护的实效性差，就会影响安全防护的效果。总而言之，教育行业的网络与信息安全任重而道远，我们应做到及时的发现信息安全的漏洞，同时及时采取应对措施，防患于未然。

1.2 高校数据中心平台安全防护需引起高度重视

高校教育信息化建设的逐步深入，各大高校数字校园建设进行的如火如荼，高校对数据安全也越来越重视，学校建成的各类应用系统产生了大量的数据，而且数据积累也会越来越多，在对这些数据进行集中管控的同时，数据安全就显得尤为重要。近几年黑客通过网络攻击，成功破解成绩数据库，修改考试成绩，骗取认证证书等事件屡有发生，教育系统已经逐渐成为黑客关注的重点目标，高校数据中心的安全保障工作已经迫在眉睫，应当引起高度重视。

2、安全防护措施的自查与优化

高校应加强在防病毒系统建设、补丁管理体系建设、网页防篡改、门户网站防护、安全审计、信息发布审批、防泄密、防恶意信息、移动存储介质的保密存储、信息系统安全防护、安全域的划分、保密检查、计算机资产统计、网站备案、安全防范技术措施有效性核查等方面的安全防护措施的落实情况，对工作过程中存在不足的地方进行整改，使得安全防护的措施真正地落到实处。

3. 安全防护建设

3.1 新一代防火墙

现如今网络环境越来越复杂，所以我们就更应该寻找新的安全解决方案，以满足抵挡外部攻击以外的安全需求。以往，网络攻击的手段基本停留在 OSI 的网络层，现如今 web3.0 技术已经逐渐成熟，大多数的 web 应用都采用了 HTTP 和 HTTPS 协议，然而传统的防火墙只能根据数据包的源地址和目标地址的信息来检测流量，对于 HTTP 和 HTTPS 这些基于应用层协议的流量却是无可奈何。虽然现在各高校都部署了针对应用层的 IPS 设备，但是 IPS 无法识别具体的应用，用户想要对应用层实施精细的控制也就无法实现，所以就需要寻找新一代的防火墙技术来抵御复杂网络环境的潜在威胁。

3.2 上网行为管理系统

人们在享受互联网带来的巨大便利的同时，由其带来的负面影响和安全威胁也日趋严重。高校需要对校园内部网络实现上网行为的精细管控，同时还要达到国家监管单位的安全监管要求，如公安部 82 号、信息安全等级保护等，所以要从根本上提高自身网络信息安全保障体系，就需要对数据包进行深度的检测，能够按照协议对网络流量、应用识别，进行精准的控制，对用户的上网行为进行规范的管理，同时还需增加对日志的审计以及报表查看的功能，能够将当前网络中的各种报文流量实时的展示出来，从而达到对流量进行综合分析、对符合行为策略的事件进行实时告警并记录的效果，最终达到国家监管的要求。

3.3 网络安全审计系统

依据国家相关法律的规定，信息安全等级保护是我国信息安全保障的基本制度、基本策略、基本方法。开展信息安全等级保护工作，目的是要解决我国信息安全面临的威胁和存在的主要问

题，而等级保护包含数据安全、物理安全、应用安全、网络安全、主机安全。其中的网络安全与主机安全是重中之重，我们可以通过网络安全审计系统来保障网络和主机的安全，同时通过网络安全审计系统还可以内外部网络信息进行监管和控制，也能够详实的记录发生在网络内的各种网络活动，为发生网络安全事件时的追溯取证提供快速且有效的技术支持。

3.4 运维审计系统（堡垒机）

运维审计系统是利用虚拟机镜像技术，对各种应用平台进行细粒度的权限管控，可以对应用平台中虚拟机的生命周期进行管理，以第三方的身份对各种应用平台进行审计和管控，提供更加精准、可靠的权限管控与审计功能。在不改变原有应用平台管理方式的基础上，灵活地配置在各种应用平台上，与上层的应用进行无缝的对接，如对应用平台上运行的站群系统进行细粒度的权限管控，通过对用户权限进行细粒度的划分，是用户只能在其授权的权限内进行操作，同时对用户的操作进行录屏保存，当用户进行越权操作时，进行及时告警同时阻断其操作，以确保每次的操作均在可控制的范围内。通过历史访问回放，可以更直观更方便的审计用户的操作行为，使得对应用平台、服务器的管理更加安全可控。

4、结束语

综上所述，随着信息技术的不断发展，个人信息泄露、网络诈骗等信息安全问题层出不穷，信息安全问题也备受关注。在这个信息技术腾飞的时期，为了提高信息化安全防护水平，在提高专业技术人员业务水平的同时也要定期对信息系统进行安全维护、检查和修复漏洞，减少网络安全事件的发生。

参考文献：

[1]薛忠.探究信息化时代计算机网络安全防护技术[J].科学技术创新，2020（17）：107-108.

[2]翟丽.信息化时代计算机网络安全防护技术探索[J].产业与科技论坛，2018（12）：87-88.

[3]何平,丁成.构建高校网络意识形态安全机制措施[J].当代教育实践与教学研究,2019,(19).199200.

作者简介：

第一作者：裴文财(1987-),男,汉族,辽宁营口人,本科,工程师,研究方向：网络安全。

第二作者：高振(1986-),男,汉族,辽宁营口人,研究生,高级工程师,研究方向：网络安全,

项目来源 :营口理工学院 2021 年校级科研项目

基金项目:数字校园背景下的网络安全建设研究

项目编号：YBL202115