DOI:10.13657/j.cnki.gxkxyxb.2013.02.004

2013,29(2):89～91,102
Vol. 29, No. 2 May 2013

一个基于等级保护的高校数据中心信息系统安全方案*

A Scheme for Information System Security of College Data Center based on Classified Protection

李 茜
LI Qian

(广西经济管理干部学院,广西南宁 530007)
(Guangxi Economic Management Cadre College, Nanning, Guangxi, 530007, China)

摘要:针对国家信息系统安全等级保护体系中第三等级的所提出的关键技术要求,结合某高职院校数据中心在网络环境、主机服务、应用程序和数据管理等方面的实际情况,提出一个基于等级保护的高校数据中心信息系统安全体系设计方案。

关键词:信息安全 数据中心 等级保护 网络安全
中图法分类号:TP309 **文献标识码**:A **文章编号**:1002-7378(2013)02-0089-03

Abstract: According to the key technical requirements of the third grade national information system security and combined with the actual situation of the network environment, hosting services, applications, and data management in the vocational colleges data centers, a design scheme based on classified protection for university data center information system security is proposed.

Key words: information security, data center, classified protection, network security

高校教育服务的各个业务环节正向数字化、网络化、智能化方向快速发展,所产生的海量信息资源和应用程序服务日益向数据中心集中。与其他领域一致,高校数据中心已经从传统意义上的纯粹物理基础设施变成了集基础设施、数据、应用程序、服务行为于一体的综合性信息服务体系。由于高校数据中心综合性信息服务体系的特性,使得其信息安全保护已经成为高校教育信息化建设中一个重要课题。高校数据中心信息安全的最终目的是保护自身的信息资源被合法用户安全使用,并禁止非法用户、入侵者、攻击者和黑客非法盗窃、使用信息资源。高校数据中心信息安全保护必须从物理环境、软件应用及开发技术、网络技术和数据管理技术等方面进行"体系化"的综合保护。本文根据信息系统安全等级保护方法[1～6],讨论并规划高校数据中心的信息安全保护方案。

1 数据中心信息安全体系架构

1.1 体系架构设计

根据"一个中心、三重防护(安全管理中心、计算环境安全、区域边界安全、通信网络安全)"的架构设计理念,高校数据中心信息安全体系结构如图1所示。

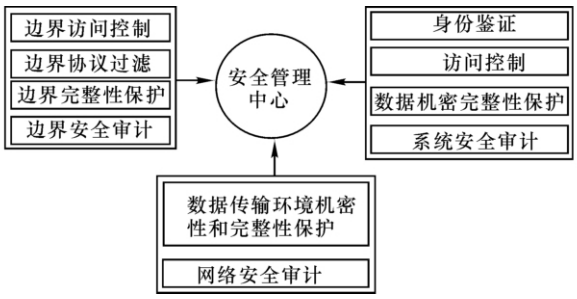

图1 高校数据中心信息安全体系架构

图1中,安全管理中心针对系统、产品、设备、信息安全事件、操作流程等的统一管理。计算环境安全从系统应用级的身份鉴别、访问控制、安全审计、数据机密性及完整性保护、客体安全重用、系统可执

收稿日期:2013-03-01
修回日期:2013-03-16
作者简介:李 茜(1980-),女,硕士,讲师,主要从事计算机应用技术研究。
*广西壮族自治区教育厅科研项目(编号:201010LX700)资助。

行程序保护等方面开展相应的安全保护。区域边界安全从加强网络边界的访问控制粒度、网络边界行为审计以及保护网络边界完整等方面，提升网络边界的可控性和可审计性。通信网络安全从保护网络间的数据传输安全、网络行为的安全审计等方面保障网络通信安全。

1.2 分层安全设计

分层设计是对物理层、网络层、主机层、应用层和数据层分别进行安全设计。(1)数据中心的物理层是由机房环境系统提供的，主要在于保障通信线路、物理设备和整体机房的安全可靠，不受供电、火灾、水灾、地震和人为物理入侵导致的破坏等。(2)网络层包括冗余网络结构；对网络设备访问控制；设备、用户和流量安全审计；边界完整性检查、定位和阻断；边界入侵防范；恶意代码防范；设备用户身份鉴别权限分离等。网络层安全设计按照信息系统业务处理过程将系统划分成计算环境、区域边界和通信网络三部分，构成由安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的三重防护体系结构(图 2)。安全管理中心统一实施对计算环境、通信网络和区域边界的安全策略管理，确保整个安全系统的配置完整和可信，确定不同的用户所具备的操作权限，全程实施审计追踪；区域边界对进入和流出应用环境的信息流进行安全检查和访问控制，确保不会有违背系统安全策略的信息流经过边界；通信网络设备通过对通信双方进行可信鉴别验证，建立安全通道，实施传输数据密码保护，确保其在传输过程中不会被窃听、篡改和破坏。(3)主机层包括主机结构安全；主机系统安全加固；主机防病毒体系；主机审计；主机入侵防范。(4)应用层包括安全漏洞检测和修补后的运行环境安全；及时发现各种非授权行为与攻击行为，并且入侵检测提供协议还原的功能；为安全事件提供审计依据；不同安全域间的隔离防护。(5)数据层是指数据完整性的要求，系统管理数据的传输完整性和安全性。能够检测数据破坏和进行恢复；实现系统管理数据、鉴别信息和要求业务数据的传输和存储的保密性；本地完全数据备份。

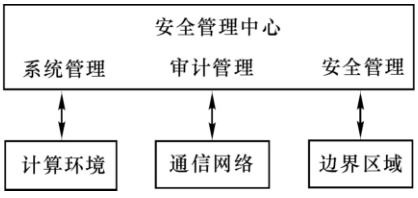

图 2 网络层安全体系结构

2 数据中心信息系统安全方案

2.1 整体安全模型结构

将数据中心系统结构(图 3)划分为普通安全服务应用区、核心计算存储区域、服务管理区域和存储备份区域，分别部署防火墙、安全隔离与信息交换系统、入侵检测系统、入侵防御系统、防病毒网关、网络安全审计系统、数据库安全审计系统、终端管理系统、漏洞扫描系统、数据库安全增强套件和 CA 认证组件的等级化安全保护系统，建设形成的物理拓扑结构如图 4 所示。

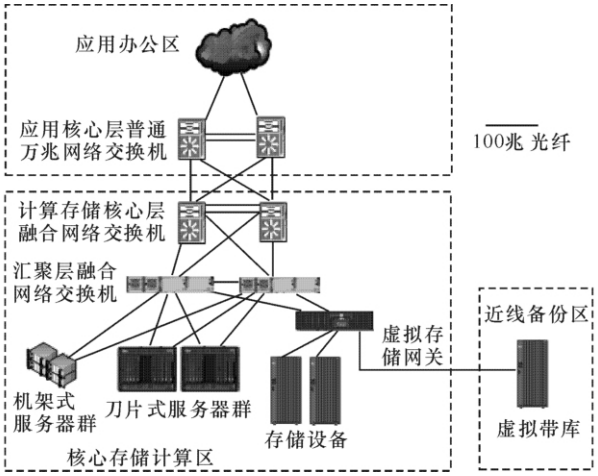

图 3 数据中心系统结构

2.2 安全设计方案

根据整体安全模型结构，用图 4 表示不同安全区域部署的安全服务以及配属的设备，以形成本文的安全方案设计。

(1)安全区域划分。整个系统安全区域按照功能和需求划分为普通安全服务应用区、核心交换区、核心计算存储区、广域网接入区和安全服务管理区域等五个安全区域。

(2)层次化的安全设计。按照信息系统安全等级保护的技术要求，分别针对网络层、主机层、应用层和数据层，以及他们所覆盖的五个安全区域进行安全设计。

网络层包括普通安全服务应用区、核心交换区、核心计算存储区、广域网接入区和安全服务管理区等全部 5 个安全区域，是最基础的安全层次。在这个区域里部署的设备及其功能如下：①防火墙。部署在普通安全服务应用区、核心交换区、核心计算存储区和广域网接入区，可以是单台设备，也可以是冗余设备，采用多端口分配给不同区域的模式，划分不同的安全区域。主要实现的服务为不同安全域之间

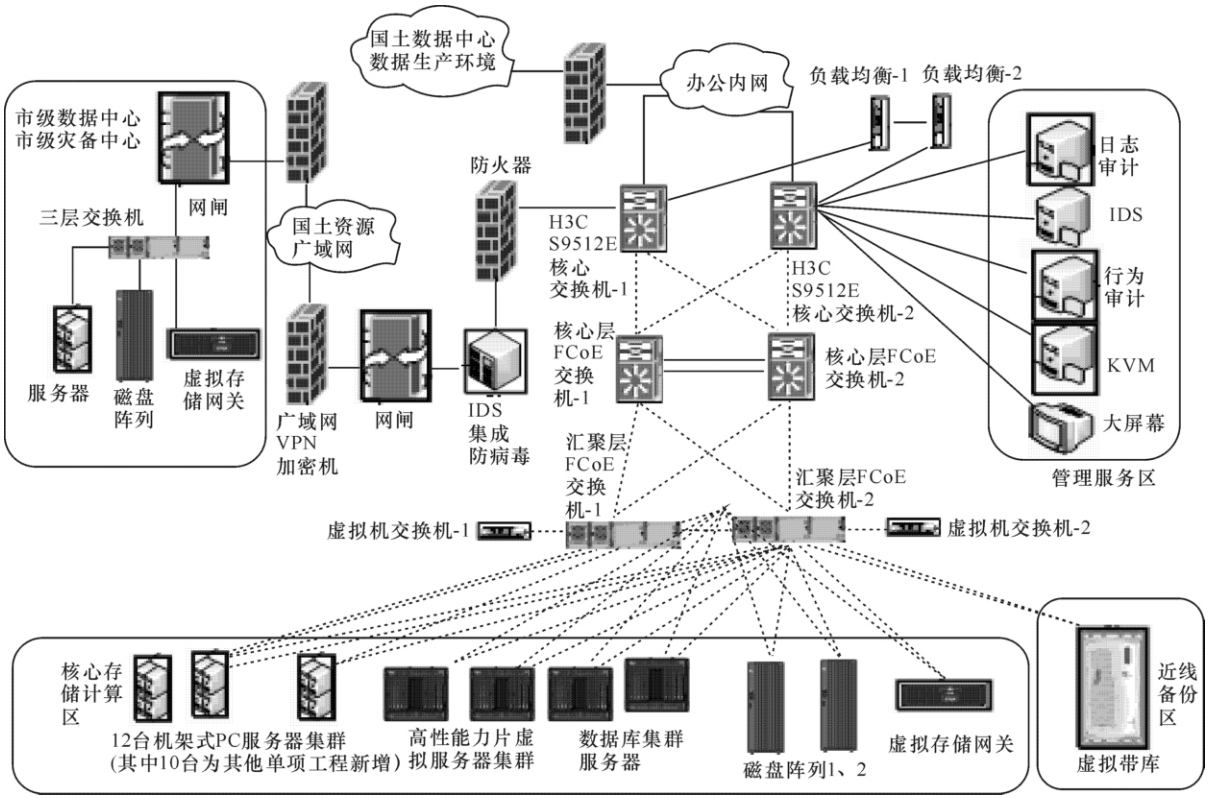

图 4　基于等级化保护的高校数据中心信息系统的物理拓朴结构

的边界进行访问控制,防范黑客,阻止未经授权的非法访问。②入侵检测系统。部署在安全服务管理区域。主要实现的服务为实时监控的各种数据包和网络行为,提供及时的预警和应急机制。实现病毒攻击和黑客入侵的监测,实时监控整个网络的安全运行状态。③入侵防御系统。部署在核心计算存储区域。主要实现的服务为分析过滤网络流量,并设置的检测和隔离策略;阻止异常的攻击和可疑流量对IT资源的访问。④网络安全审计系统。部署在安全管理服务区域。主要实现的服务为监控数据库的网络应用,完整的数据记录的各种信息和用户的起始地址以及所有的操作。⑤漏洞扫描设备。部署在安全服务管理区域。主要实现的服务是对应用系统,网络设备的漏洞进行扫描,并开展安全性评估。

主机层包括广域网接入区域和安全服务管理区域、普通安全服务应用区。在这个区域里部署的设备及其功能如下:①防病毒系统。部署在广域网接入区域的入口路由器后。主要实现的服务为以网关过滤的形式,对病毒和恶意代码、木马等进行扫描和服务器主机保护。②终端管理系统。部署在安全服务管理区域和普通安全服务应用区,其中客户端部署在后者,服务器端部署在前者。主要实现的服务为监控主机资源,部署安全策略管理和控制计算机主机;普通客户端计算机访问网络资源和托管服务。部署访问控制管理,安全策略管理和控制主机终端活动。

应用层包括核心计算存储区。在这个区域里部署的设备及其功能如下:防病毒软件。主要实现的服务为,对终端设备的病毒和恶意代码、木马等进行扫描主机应用程序防注入保护。

数据层包括安全服务管理区域。在这个区域里部署的设备及其功能如下:①数据库安全增强组件,部署在安全服务管理区域。主要实现的服务为增强数据库的安全性,如加密,身份验证等;②数据库审计设备。部署在安全服务管理区域。主要实现的服务为审计访问到数据库服务器的用户和IP;审计用户的数据库访问行为,记录关键系统资源的使用和重要的系统安全事件;记录审计事件,事件类型,主要标志(帐户),对象识别;审计行为记录,审计记录和过程保护等。

3　结束语

近年来,随着国内外信息安全形势的剧烈变化,境外敌对势力和境内有组织的犯罪活动对我国科

(下转第 102 页)

等景观分割，形成廊道的效果，从而导致整体景观破碎化程度加深。

目前利用遥感影像进行景观分类是景观格局研究技术方面的发展方向，但是遥感影像分类中对景观类型的划分精度比较低，因此，我们结合实地调查的东兴市森林资源调查和土地利用调查资料进行景观类型划分，能够将景观类型划分得更加精细，边界把握得更加准确，提高了研究的准确性。但是，在研究过程中，我们无法收集到当地社会经济发展的数据，因此本文还没有能够对东兴市海岸带景观格局变化的原因进行定量分析，今后还需要对研究区域的社会现状进行调查，收集当地社会经济发展方面的实际数据，以弥补对驱动力未能进行定量分析的不足。

参考文献：

[1] 张健，濮励杰，陕永杰. 海岸带土地开发利用及生态环境效应研究简述[J]. 长江流域资源与环境，2012，21(1)：36-42.

[2] 刘厚田. 湿地的定义和划分[J]. 生态学杂志，1995，14(4)：73-77.

[3] 丁晶晶，王磊，刑伟，等. 基于 RS 和 GIS 的盐城海岸带湿地景观格局变化及其驱动力研究[J]. 江苏林业科技，2009，36(6)：19-21.

[4] 曹林，韩维栋，李凤凤，等. 雷州湾红树林湿地景观格局演变及驱动力分析[J]. 林业科技开发，2010，24(4)：19-23.

[5] 高义，苏奋振，孙晓宇，等. 珠江口滨海湿地景观格局变化分析[J]. 热带地理，2010，30(3)：218-226.

[6] 候西勇，徐新良. 21 世纪初中国海岸带土地利用空间格局特征[J]. 地理研究，2011，30 (8)：1371-1379.

[7] 王瑾. 典型海岸带综合管理模型及其管理对策研究[D]. 北京：北京化工大学，2005：72.

[8] 冯厚文. 东兴市近 45 年气候变化统计特征[J]. 广西气象，2006(7)：64.

[9] 宋国利，李玉宝，付春雷，等. 基于 RS 和 GIS 的乐清湾湿地景观格局变化分析[J]. 东北林业大学，2010，38(12)：81-83.

[10] 张绪良，张朝晖，徐宗军. 莱州湾南岸滨海湿地的景观格局变化及累积环境效应[J]. 生态学杂志，2009，28(12)：2437-2443.

[11] 张继平，常学礼，李健英，等. 基于 3S 的呼和浩特市土地利用变化及其生态效应[J]. 生态学杂志，2008，27(12)：2184-2189.

[12] 申怀飞. 基于 3s 的豫西黄河流域景观格局变化研究[D]. 开封：河南大学，2007.

（责任编辑：邓大玉）

（上接第 91 页）

研、教育领域等非政府非涉密目标的窥探热情日趋高涨，手段也越发先进，“孤岛化”、“单一化”的安全技术保障手段已经不能满足新形势下的安全要求。本文主要针对信息系统安全等级保护体系中第三等级的技术要求，提出一个高校数据中心的信息系统安全体系设计方案。该信息安全防护方案已经在一个高职院校实际应用，目前运行良，对该校的信息安全起到了很好的保护作用。该信息安全防护体系可以推广应用。

参考文献：

[1] GB/T 22239－2008. 信息安全技术 信息系统安全等级保护基本要求[S]. 2008.

[2] GB/T 25070－2010. 信息安全技术 信息系统等级保护安全设计技术要求[S]. 2010.

[3] 贾非. 数据中心网络安全攻防[J]. 信息安全，2011(7)：30-36.

[4] 王大川，王永书，林红. 浅议计算机信息系统安全等级保护[J]. 中国公共安全：学术版，2009(3)：4-10.

[5] 陈雪秀，任卫红，谢朝海. 信息安全等级保护中的两大基本问题研究[J]. 信息安全与通信保密，2009(3)：36-39.

[6] 池仁隆，张超，张春柳. 信息系统安全等级保护建设与测评方法简析[J]. 软件产业与工程，2012，2(14)：44-47.

（责任编辑：邓大玉）