ISSN 1002－4956
CN11－2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第28卷 第6期 2011年6月
Vol. 28 No. 6 Jun. 2011

高校信息安全体系建设与实践

孟坛魁，梁艺军

（中国人民大学 网络与教育技术中心，北京 100872）

摘 要：随着信息化校园建设的逐步深入，信息安全体系建设已经提上日程。该文以某大学信息安全体系建设的过程为案例基础，简要介绍了当前学校的信息安全现状、面临的问题，介绍了信息安全体系建设思路和建设过程，及已经完成的重点工作和未来展望。

关键词：安全体系；信息安全；校园网

中图分类号：TP309 文献标志码：B 文章编号：1002-4956(2011)06-0122-03

Practice of construction of information security system

Meng Tankui, Liang Yijun

(Network and Educational Technology Center, Renmin University of China, Beijing 100872, China)

Abstract: With the further advance of the E-campus construction, the construction of the information security system has been put on the agenda. This article describes the actual process of construction of the information security system in a university. It introduces the present situation, the existing problem, the construction style of the information security system in the university. In addition, the finished tasks and the future perspectives are given in the latter part.

Key words: security system; information security; campus network

当前，全国高校的信息化校园建设正在向纵深发展，高校的教学、科研和管理工作越来越依赖于各类信息系统的稳定运行[1-2]，这就给信息部门带来了安全保障上的挑战。国内外信息安全保障的技术和理念也在不断发展变化中[3-5]，从最初面对数据信息的产生、传输、存储、使用过程的保障，到后来面向整个业务系统的保障，随着各类业务系统的不断整合，当前的信息安全保障理念也随之逐步朝着面向服务的方向发展。

本文以中国人民大学经多次讨论和组织专家论证、逐步开始全校层次上的信息安全保障体系建设工作的案例为基础，简要介绍一些信息安全体系建设经验和体会。

1 现状与问题

1.1 信息安全现状

随着信息化建设的推进，我校信息化建设初具规模，软硬件设备配备完成，运行保障的基础技术手段基本具备。网络中心技术力量雄厚，承担网络系统管理和应用支持的专业技术人员达20余人；针对重要应用系统采用了防火墙、IPS/IDS、防病毒等常规安全防护手段，保障了核心业务系统在一般情况下的正常运行，具备了基本的安全防护能力[6]；日常运行管理规范，按照信息基础设施运行操作流程和管理对象的不同，确定了网络系统运行保障管理的角色和岗位，初步建立了问题处理的应急响应机制。

由网络中心进行日常管理的主要有六大业务应用系统，即网络通信平台、认证计费系统、校园一卡通、电子校务系统、网站群、邮件系统。

网络通信平台是大学各大业务平台的基础核心，是整个校园网的基础，其他应用系统都运行在高校的基础网络环境上；认证计费系统是针对用户接入校园网和互联网的一种接入认证计费的管理方式；校园一卡通系统建设在物理专网上，主要实现学生校园卡消费管理，校园卡与大学网络有3个物理接口；电子校务系统是大学最重要的业务应用系统，系统中存储着重要的教务工作数据、学生考试信息、财务数据等重要数据信息；大学主页网站系统为大学校园的互联网窗口，起到学校对外介绍宣传的功能；邮件系统主要为大学教师与学生提供邮件收发服务，目前邮件系统注册用户超过5万。

收稿日期：2010-10-12

作者简介：孟坛魁(1980－)，男，河北邢台，工学硕士，工程师，研究方向为网络运行管理和信息安全体系建设.

E-mail: mengtk@ruc.edu.cn

1.2 面临的主要问题

通过等级保护差距分析和风险评估，目前大学所面临的信息安全风险和主要问题如下：

（1）高校领域没有总体安全标准指引，方向不明确，缺少主线。

（2）对国际国内信息安全法律法规缺乏深刻意识和认识。

（3）信息安全机构不完善，缺乏总体安全方针与策略，职责不够明确。

（4）教职员工和学生数量庞大，管理复杂，人员安全意识相对薄弱，日常安全问题多。

（5）建设投资和投入有限，运维和管理人员的信息安全专业能力有待提高。

（6）内部管理相对松散，缺乏安全监管及检查机制，无法有效整体管控。

（7）缺乏信息安全总体规划，难以全面提升管理与防护水平。

（8）缺乏监控、预警、响应、恢复的集中运行管理手段，无法提高安全运维能力。

2 建设思路

2.1 建设原则和工作路线

学校信息安全建设的总体原则是：总体规划、适度防护，分级分域、强化控制，保障核心、提升管理，支撑应用、规范运维。

依据这一总体原则，我们的信息安全体系建设工作以风险评估为起点，以安全体系为核心，通过对安全工作生命周期的理解，从风险评估、安全体系规划着手，并以解决方案和策略设计落实安全体系的各个环节，在建设过程中逐步完善安全体系，以安全体系运行维护和管理的过程等全面满足安全工作各个层面的安全需求，最终达到全面、持续、突出重点的安全保障。系统流程见图 1。

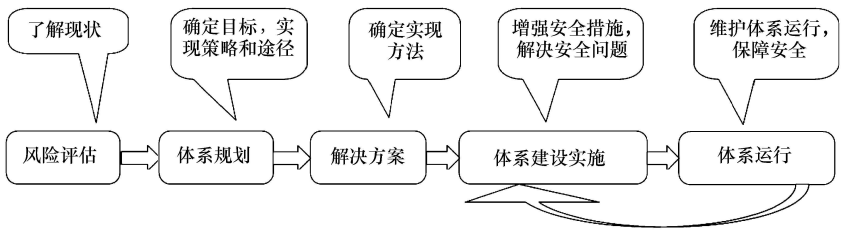

图 1 信息安全体系建设流程图

2.2 体系框架

信息安全体系框架依据《信息安全技术 信息系统安全等级保护基本要求》GBT 22239-2008、《信息系统等级保护安全建设技术方案设计要求》（征求意见稿），并吸纳了 IATF 模型[7] 中“深度防护战略”理论，强调安全策略、安全技术、安全组织和安全运行 4 个核心原则，重点关注计算环境、区域边界、通信网络等多个层次的安全防护，构建信息系统的安全技术体系和安全管理体系，并通过安全运维服务和 ITSM[8] 集中运维管理（基于 IT 服务管理标准的最佳实践），形成了集风险评估、安全加固、安全巡检、统一监控、提前预警、应急响应、系统恢复、安全审计和违规取证于一体的安全运维体系架构（见图 2），从而实现并覆盖了等级保护基本要求中对网络安全、主机安全、应用安全、数据安全和管理安全的防护要求，以满足信息系统全方位的安全保护需求。

（1）安全策略：明确信息安全工作目的、信息安全建设目标、信息安全管理目标等，是信息安全各个方面所应遵守的原则方法和指导性策略。

（2）安全组织：是信息安全体系框架中最重要的安全管理策略之一，明确了大学信息安全组织体系及各级组织间的工作职责，覆盖安全管理制度、安全管理机构和人员安全管理 3 个部分。

（3）安全运行：是信息安全体系框架中最重要的安全管理策略之一，是维持信息系统持续运行的保障制度和规范。主要集中在规范信息系统应用过程和人员的操作执行，该部分以国家等级保护制度为依据，覆盖系统建设管理、系统运维管理 2 个部分。

（4）安全技术：是从技术角度出发，落实学校组织机构的总体安全策略及管理的具体技术措施的实现，是对各个防护对象进行有效地技术措施保护。安全技术注重信息系统执行的安全控制，针对未授权的访问或误用提供自动保护，发现违背安全策略的行为，并满足应用程序和数据的安全需求。安全技术包含通信网络、计算环境、区域边界和提供整体安全支撑的安全支撑平台。该部分以国家等级保护制度为依据，覆盖物理层、网络层、主机层、应用层和数据层 5 个部分。

（5）安全运维：安全运维服务体系架构共分两层，实现人员、技术、流程三者的完美整合，通过基于 ITIL[9] 的运维管理方法，保障基础设施和生产环境的正常运转，提升业务的可持续性，从而也体现了安全运维与业务目标保持一致的核心思想。

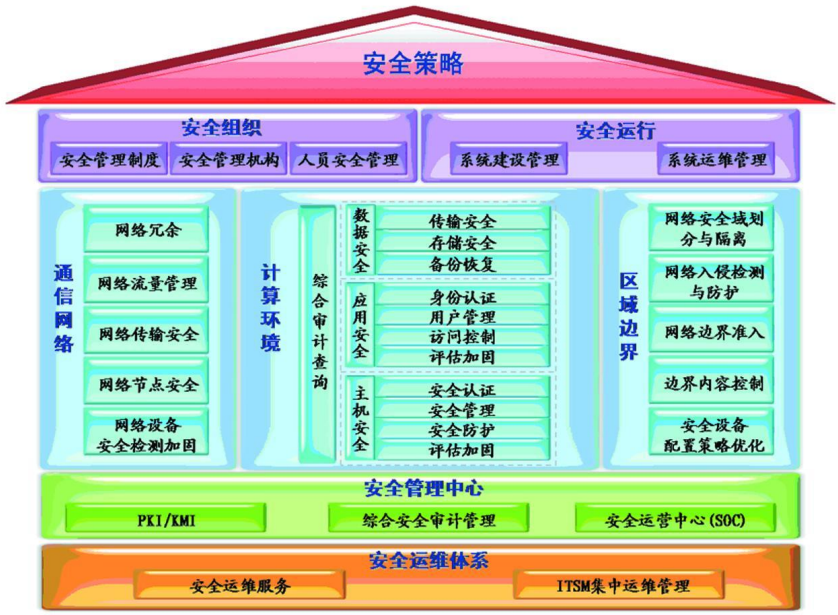

图 2 大学信息安全体系框架

3 重点建设工作

3.1 安全渗透测试

2009 年 4 月，学校对 38 个网站、2 个关键系统和 6 台主机系统进行远程渗透测评。通过测评，全面、完整地了解了当前系统的安全状况，发现了 20 个高危漏洞，并针对高危漏洞分析了系统所面临的各种风险，根据测评结果发现被测系统存在的安全隐患。

渗透测试主要任务包括：收集网站信息、网站威胁分析、脆弱性分析和渗透入侵测评、提升权限测评、获取代码、渗透测评报告。

3.2 风险评估和安全加固

2009 年 5 月，依据安全渗透测试结果，对大学的六大信息系统进行了安全测评。根据评估结果得出系统存在的安全问题，并对严重的问题提出相应的风险控制策略。主要工作任务包括：系统调研、方案编写、现场检测、资产分析、威胁分析、脆弱性分析和风险分析。通过风险评估最终得出了威胁的数量和等级，表 1、表 2 为威胁的数量和等级统计。2009 年 6 月和 9 月，基于风险评估结果，对涉及到的网络设备(4 台)和主机设备(14 台)进行了安全加固工作。

3.3 安全体系规划

根据前期对全校的网络、重要信息系统及管理层面的全面评估和了解，整理出符合大学实际的安全需求，并结合实际业务要求，对学校整体信息系统的安全工作进行规划和设计，并通过未来 3 年的逐步安全建设，满足学校的信息安全目标及国家相关政策和标准的要求。

表 1 现有信息系统安全威胁等级统计

严重程度	数量	严重程度	数量
最高	4	中等	88
高	95	较低	15

表 2 现有信息系统安全威胁数量统计

威胁类别	数量	威胁类别	数量
误用	85	恶意代码和病毒	36
信息收集	27	溢出攻击	19
信息截取	39	物理损坏	3
拒绝服务攻击	36		

学校依据国际国内规范及标准，参考业界的最佳实践 ISMS[10]（信息安全管理体系），结合我校目前的实际情况，制定了一套完整、科学、实际的信息安全管理体系，制定并描述了网络与信息安全管理必须遵守的基本原则和要求。

通过信息安全管理体系的建立，使学校的组织结构布局更加合理，人员安全意识也明显提高，从而保证了网络畅通和业务正常运行，提高了 IT 服务质量。通过制度、流程、标准及规范，加强了日常安全工作执行能力，提高了信息安全保障水平。

4 未来展望和下一步工作

4.1 安全防护体系

根据网络与信息系统各节点的网络结构、具体的应用以及安全等级的需求，可以考虑使用逻辑隔离技术（VLAN 或防火墙技术）将整个学校的网络系统划

（下转第 129 页）

[2] 锁志海. 基于信息技术的高校学术会议资源整合研究[J]. 科研管理, 2007(4): 51-54.
[3] 于晓娜, 张竞志. 信息化: 高校科研管理工作的有效方法[J]. 辽宁医学院学报: 社会科学版, 2008(6): 77-79.
[4] 刘沐, 谢素萍, 申艳菊. 论高校科研管理信息系统在大学评估中的应用[J]. 中国教育信息化.
[5] 李世收, 仲伟俊, 孙宙, 等. 高校科研信息化模型研究[J]. 河海大学学报: 哲学社会科学版, 2008(10): 85-88.
[6] 刘沐, 马振伟, 宿芬. 信息化是促进高校科研管理工作的有效手段[J]. 东北师大学报: 自然科学版, 2009(7): 255-256.
[7] 顾小清, 李雪. 信息化科学研究及其教育应用综述[J]. 开放教育研究, 2008(14): 15-20.
[8] 杨俊平. 信息网络化对高校科研管理的影响[J]. 合肥工业大学学报: 社会科学版, 2008(22): 57-59.
[9] 杨庆, 李志恒, 高全福, 等. 高校科研信息系统的研究与实现[J]. 甘肃科技, 2006(22): 91-93.
[10] 吴静. 学术会议对构建高校学术氛围的意义的探讨[J]. 科研管理, 2008(10): 104-106.
[11] 张喜爱, 曾庆平, 韩晶. 浅论高校科研管理信息化中的问题和对策[J]. 科技管理研究, 2008(9): 262-264.

(上接第 124 页)

分为 3 个层次的安全域: 第一层次安全域包括整个学校网络信息系统; 第二层次安全域将各应用系统从逻辑上和物理上分别划分; 第三层次安全域主要是各应用系统内部根据应用人群的终端分布、部门等划分子网或子系统。

公钥基础设施包括: CA 安全区: 主要承载 CA Server、主从 LDAP、数据库、加密机、OCSP 等; KMC 管理区: 主要承载 KMC Server、加密机等; RA 注册区: 主要承载各院所的 RA 注册服务器, 为各院所的师生管理提供数字证书注册服务。

应用安全支撑平台为各信息系统提供应用支撑服务、安全支撑服务以及安全管理策略, 使得信息系统建立在一个稳定和高效的应用框架上, 封装复杂的业务支撑服务、基础安全服务、管理服务, 并平滑支持业务系统的扩展。主要包括: 统一身份管理、统一身份认证、统一访问授权、统一审计管理、数据安全引擎、单点登录等功能。

4.2　安全运维体系

ITSM 集中运维管理解决方案面对学校日益复杂的 IT 环境, 整合以往对各类设备、服务器、终端和业务系统等的分割管理, 实现了对 IT 系统的集中、统一、全面的监控与管理; 系统通过融入 ITIL 等运维管理理念, 达到了技术、功能、服务三方面的完全整合, 实现了 IT 服务支持过程的标准化、流程化、规范化, 极大地提高了故障应急处理能力, 提升了信息部门的管理效率和服务水平。

根据终端安全的需求, 系统应建设一套完整的技术平台, 以实现由管理员根据管理制度来制定各种详尽的安全管理策略, 对网内所有终端计算机上的软硬件资源、以及计算机上的操作行为进行有效管理。实现将以网络为中心的分散管理变为以用户为中心集中策略管理; 对终端用户安全接入策略统一管理、终端用户安全策略的强制实施、终端用户安全状态的集中审计; 对用户事前身份和安全级别的认证、事中安全状态和安全行为的监控、事后安全状态和安全行为的审计。

定期安全检测, 内容包括定期的安全风险评估、安全加固、安全应急响应和安全巡检。

4.3　安全审计体系

综合安全审计平台可以跟踪记录谁操作了我们重要的数据, 记录谁复制了机密文件, 谁访问了数据库等等, 并且从数月累积的庞大审计记录中分析和获得异常现象, 为安全管理制度提供参考。通过建立相应的网络审计模块、主机审计模块、数据库审计模块和安全设备审计模块等, 建立定期针对某些事件信息数据进行安全审计的机制, 确保目前信息系统安全控制的有效性, 集中发现网络行为的合规性, 根据既定策略识别非授权访问、入侵等现象, 并进行分析。通过对受控对象的活动进行安全审计, 为网络、系统与应用安全管理人员及高层管理人员提供一个监督、检查当前信息系统运行状况的有效手段。

参考文献(References)

[1] 蒋东兴, 宓咏, 郭清顺. 高校信息化发展现状与政策建议[J]. 中国教育信息化: 高教职教, 2009(15): 27-30.
[2] 刘臻. 从美国大学看高校信息化中的深化应用和改革创新[J]. 中国教育信息化: 高教职教, 2010(11): 4-6.
[3] 吴海燕, 苗春雨, 蒋东兴. 美国高校信息安全管理情况分析与启示[J]. 实验技术与管理, 2009, 26(5): 169-172.
[4] 李西明, 鹿海涛. 高校信息安全管理探讨[J]. 中国教育信息化: 高教职教, 2010(1): 20-22.
[5] 阎春平, 刘飞, 郭风. 数字化企业的信息安全体系及实施方案[J]. 重庆大学学报, 2010, 33(2): 37-41.
[6] 梁艺军. 中国人民大学: 异地容灾保护 99% 的校园资源[J]. 中国教育网络, 2010(1): 66-67.
[7] National Security Agency Information Assurance Solutions Technical Directors. Information Assurance Technical Framework, IATF Release3. 1[R]. Maryland: National Security Agency, 2002.
[8] ITSM. IT Service Management[EB/OL]. [2010-09-19]. http://en.wikipedia.org/wiki/IT_service_management.
[9] ITIL. Information Technology Infrastructure Library[EB/OL]. [2010-09-19]. http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.
[10] ISO/IEC 27001: 2005 Information technology - Security techniques - Information security management systems Requirements[S]. Geoeva: ISO/IEC, 2005.