

# 关于高校校园网安全管理和维护的研究思路构架实践

吕洋

(白城师范学院 信息化建设管理处 吉林 白城 137000)

摘要：在 21 世纪，计算机网络技术为高校教学管理工作和各方面服务工作提供了诸多便利，同时，计算机网络信息安全防护工作不容忽视。高校计算机网络管理人员应注意加强校园网安全管理，避免私密数据被窃取，防止信息泄露，不断优化高校网络结构，全面建立校园安全网络。本文将简单分析关于高校校园网安全管理和维护的研究思路，希望能为校园网络安全防护工作提供借鉴。

关键词：高校；校园网；安全管理

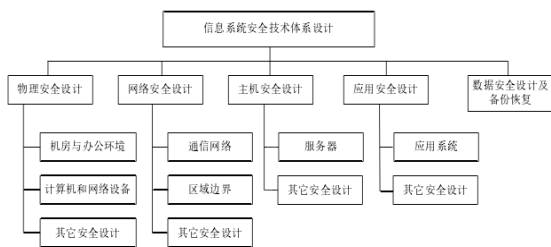
目前，各高校引入了各种先进的技术以加强校园网安全管理，抵御网络病毒攻击，维护信息安全。本文将简单介绍高校校园网信息安全管理特征，浅析高校计算机网络安全管理技术，并综合探讨校园网安全管理策略。

## 一、高校校园网络信息安全管理特征

21 世纪属于信息时代，高校教学管理工作和各项服务工作和计算机网络技术应用密不可分。当代高校校园网络计算机安全管理有五项基本特征：第一，校园网拓扑结构复杂。第二，高校计算机网络功能多样。第三，计算机网络安全设置涉及面广。第四，计算机网络安全维护应用人员多样。第五，计算机网络安全攻击来源具有多样。

从校园网安全建设内容来看，高校计算机网络安全建设有完整的安全技术体系，层次分明，信息安全管理功能良好。图一就是高校校园网络安全建设结构图。

图一 高校校园网络安全建设结构图



从图一可以看出，高校校园网络信息系统安全技术体系设计包括物理安全设计、网络安全设计、主机安全设计、应用安全设计、数据安全设计及备份恢复。其中，物理安全设计下设有机房与办公环境安全管理、计算机和网络设备安全管理、其他安全设计。网络安全设计分为通信网络安全设计、区域边界安全设计和其他安全设计。主机安全设计分为服务器安全设计和其他安全设计。应用安全设计包括应用系统设计和其他安全设计<sup>[1]</sup>。

## 二、高校校园网安全管理技术

### (一) 防火墙技术

对于高校校园网安全管理工作来说，安全防火墙并非实体墙，而是一种有特殊功能的安全访问控制设备，能够在本

校内部网络与 Internet 之间设置一道完整的安全屏障。在大数据时代，数据流在经过校园安全防火墙时会出现三种不同的结果：第一，允许。第二，拒绝。第三，丢弃。防火墙技术的主要功能是根据计算机网络系统的安全设置，对未经授权的数据流实施全面监控、安全限制、针对性选择与屏蔽，这样有助于维护本校网络信息数据的安全。当前校园网系统多种设备均配置了的防火墙功能，像路由器、交换机和无线基站等设备。与此同时，常用网络操作系统均嵌入了防火墙软件。必须注意的是，部署在出口网络上的硬件防火墙通常无法防预来自内网的攻击，因此，要进行必要的优化，对不安全服务进行科学控制，全方面保护容易受到攻击的服务，加强 IP 地址和协议端口等站点安全访问控制，科学采取集中式安全保护措施，定期实施安全防护扫描，防止 DDoS 和异常包等网络层的攻击。其次，要对站点资源的私有属性予以提升和强化，做好网络层日志的安全管理工作，加强其他安全控制。

### (二) 入侵检测与防御技术

入侵检测与防御系统技术的英文简称是 IDP 技术，该技术属于一种可以针对违规的网络行为进行自动辨识和采取主动防御措施的系统。安装该系统之后，能够自动做好重要数据的监控工作，识别数据信息内容，破坏恶意代码与记录侵入。一般情况下，在安全防火墙之前或者之后均可以按照 IDP 系统，该系统不仅能够对入侵的数据流进行及时响应，而且能自动拦截透过防火墙攻击计算机网络的数据流。对于在安装了 IDP 系统的校园局域网，必须在容易受到入侵攻击的计算机防火墙与服务器附近安装硬件设备。大多数入侵攻击均来自计算机网络出口，而位于防火墙和服务器附近的 IDP 系统可以对大量进出网络的数据流予以及时监控，并自动生成入侵检测报警日志，拦截病毒<sup>[2]</sup>。

### (三) 虚拟局域网技术

虚拟局域网技术简称 VLAN，英文全称是 Virtual Local Area Network，该技术属于一种虚拟的工作组，能够对校园局域网内的设备实施逻辑性划分，使其转变为多个网段。因

而,可以说 VLAN 技术的核心就是划分网段。在校园局域网内, VLAN 技术能根据不同的业务与相关安全等级,按照网段实施安全隔离,对于网段之间的互访予以严格的控制,从而有效阻隔网络非法入侵。

#### (四) 虚拟专用网技术

虚拟专用网简称 VPN, 英文全称 Virtual Private Net, 属于私有网络互联技术, 其在公共资源上组合了完整的架构体系, 运用加密技术和专用隧道能够实现数据信息的共享。VPN 技术的重要功能之一是为广大用户提供专用网络, 在专用网中所传输的信息均为私有信息。目前, VPN 技术主要是运用隧道、身份认证技术、加密技术和密钥来维护高校计算机网络信息的安全<sup>[3]</sup>。

### 三、校园网安全管理策略

高校在制定校园网络信息安全防护策略的过程中, 主要是从两方面入手, 一方面是结合本校的教学系统、科研系统、计算机应用系统、网络安全管理系统和生活等系统运行需求制定安全管理策略。另一方面则是立足于网络安全指导原则, 为本校核心网络与上网用户提供安全的网络环境, 运用各种安全管理技术防止防止网络病毒入侵, 避免用户个人信息泄露, 保护校园私密数据安全。与此同时, 高校秉承“管理先行”理念, 针对校园网信息安全与防护工作要求设置了信息化建设安全办公室, 在本校内部培养了一批高素质骨干技术人才, 由他们担任校园网络安全管理员, 为本校信息安

全管理工作奠定良好的人才资源, 使校园网络信息安全建设体系更完善。当前大多数高校均按照《信息系统安全等级保护基本要求》, 针对校园网络安全管理机构、计算机网络信息安全管理制度、人员、网络安全系统建设和计算机网络系统运维管理体系采取了相应的优化策略<sup>[4]</sup>。

#### 结束语:

综上所述, 全面做好高校校园网安全维护工作, 优化网络防护策略, 高校应重视提高校园网安全管理技术, 细化网络信息安全建设内容, 健全网络安全管理系统。

#### 参考文献:

- [1]王珍. 浅析高校校园网的安全管理及测试维护对策[J]. 价值工程,2018,33(25):244-245.
- [2]刘宇波. 高校校园网安全管理和维护[J]. 信息技术与信息化,2019,(04):147-148.
- [3]封冰. 探讨高校校园网的管理和维护[J]. 信息通信,2018,(06):150-151.
- [4]王金火. 规范校园安全管理工作 维护高校校园安全稳定[J]. 科技视界,2019,(03):63-64.

作者简介: 吕洋, 白城师范学院, 1979年1月出生, 男, 汉族, 籍贯: 吉林白城, 硕士学历。职称: 高级实验师, 研究方向: 网络工程