

# 关于中职院校校园网络安全的思考

苏秦

(佛山市华材职业技术学校 广东 佛山 528000)

**摘要:** 随着信息技术、网络技术的不断发展进步,为中职院校教学工作的开展提供了极大的便利,丰富了教学资源,但同时,因为网络环境较为复杂,其中含有大量的不良信息、病毒以及隐藏在暗处的黑客,对院校校园网络的安全运行造成影响,针对网络环境中存在的安全隐患应当加强思考,并采取相应措施加以防范。

**关键词:** 中职院校; 校园网; 安全性

## 引言

本文以中职院校校园网络安全为核心展开讨论,首先简要分析中职院校校园网络安全存在隐患,然后提出中职院校提升校园网安全措施,为相关院校提升校园网络安全性提供参考。

### 1 中职院校校园网络安全存在隐患

#### 1.1 病毒入侵和网络漏洞

现阶段,多数中职院校所使用的操作系统为 Windows,其操作系统、服务器、防火墙以及 TCP/IP 协议均存在一定的安全问题,并且随着使用时间的不断增加,系统中存在的漏洞也将不断增多,为病毒入侵提供了条件。当前,多数病毒均是通过操作系统存在的漏洞传播,如果没有及时更新系统,将导致漏洞逐渐增多。

#### 1.2 网络攻击

当校园网和互联网连接,便增加了遭受网络攻击几率。黑客多通过网络环境对校园网服务器进行攻击,窃取重要信息。同时,因为中职院校对内部网络结构、应用模式较为了解,当其掌握相关理论知识和技能水平,校园网便成为其攻击的首选对象,有意无意对校园网进行攻击,对其安全运行产生影响。

#### 1.3 滥用网络资源

中职院校校园网应用中,大部分的互联网访问和工作无关,有些学生借助校园网观看视频,下载软件,更有甚者连接校园网后访问暴力、色情网站,大量的垃圾邮件和非法内容出入,占用网络宽带,导致流量堵塞,引发网络较慢等情况,同时,不良网站中潜藏着大量的病毒,当学生在校园网环境中浏览相关网站极有可能成为病毒攻击对象,导致网络崩溃,并对青少年身心健康成长造成影响。

#### 1.4 网络管理缺陷

多数中职院校对于网络系统的建设多注重硬件

设置的投入,忽略软件作用,过于注重系统的运行,忽略管理。究其原因,相关人员对于网络安全认识程度不足,把网络系统视作纯技术的工程,未制定相应的管理方案,管理人员工作的开展也仅是围绕 IP 申请分配、服务器日常维护、账户维护、日志审查、网络规范和调整方面,并没有对网络环境安全状态发展变化、防范措施、入侵方式以及安全机制加以研究,增加校园网被病毒、黑客攻击几率<sup>[1]</sup>。

### 2 中职院校提升校园网安全措施

#### 2.1 物理防范

首先,科学规划设计校园网,并对硬件设施的建设加以完善,确保稳定、安全运行。其次,应当配置专业人员管理校园网络,定期开展技术培训工作,确保管理人员具备足够的知识储备和技能水平,对网络环境中存在的漏洞及时发现,并采取相应的措施加以防范,为校园网安全、稳定运行提供技术支持<sup>[2]</sup>。管理人员应当借助安全策略提升校园网络的安全性,例如网络访问、审核策略、账户设定、安全设定等,有效防御病毒入侵,并对系统的运行情况进行监测,避免黑客攻击。最后,中职院校应当构建安全责任机制,构建使用台账,当校园网受到攻击后,追究个人责任,通过责任机制对人员使用校园网络行为加以约束,提升其以及管理人员责任意识。构建容灾机制,数据安全备份是属于重要的数据信息,增强数据云服务。

#### 2.2 系统防范

应当定期对操作系统进行维护。前文提到,中职院校所使用的计算机操作系统为 Windows 系统。因此本文以 Windows 系统为例,阐述系统安全管理相关内容。首先,需要都对系统账户加以管理。通常情况系统安装后可以建立 Administrator 账户和 Guest 账户,账户安全对策为,禁止使用 Guest 账户,并拒绝匿名进行访问。对 Administrator 账户进行更

改,并对密码设置加以强化,限制网络访问,杜绝非法网络的访问。并通过“管理”工具建立不同权限用户账号。具体操作步骤为:首先点击计算机管理,找到系统工具,本地用户和组或直接使用 Compmgmt.msc 命令创建新的用户账号<sup>[3]</sup>。之后在设置有控制器服务器中建立存在权限差异账号。通过身份认证,有效避免没有得到授权的用户进入。现阶段,较为常用身份认证方式为口令认证,管理人员账户可以设置强密度,同时不定期对口令密码进行更换,多数用户使用操作系统时并未设置密码或者密码比较简单,很容易就被破解。另外,为确保中职院校校园网安全性,应当通过第三方软件加强防护,对网络线系统运行中存在的漏洞加以及时地发现。例如,防火墙,通过防火墙能够有效阻止病毒入侵和黑客恶意访问,通过防火墙对外来访问、连接甄别,管理人员可选择阻止/取消阻止,将校园网受网络攻击的几率降低。将不必要服务端口关闭,增强远程访问的控制设置。操作步骤为点击网上邻居-属性-本地连接-属性-TCP/IP协议-属性-高级-TCP/IP筛选-属性添加、关闭操作端口。

#### 应用防范

#### 2.3 应用防范

通过展开网络安全教育,强化管理引导,应用技术屏蔽,拒绝不良信息传播。另外,需要对校园网数据、系统加以分类分级,明确使用等级,并定

期开展安全培训工作,让学生认识网络安全防护的重要性,从而对学生校园网使用行为加以约束和规范。例如,当前阶段,新媒体技术快速发展进步,中职院校可以通过微信公众号进行教育工作,始终提醒学生应当重视网络安全防护,并掌握一定的防范手段,减少学生不良使用导致病毒入侵、黑客攻击校园网络。

#### 总结

综上所述,中职院校为确保校园网络安全、稳定使用运行,应当设置分层架构、容灾机制以及信息过滤等因素,在对外部网络价值资源加以充分利用的同时做好内部网络的安全防范工作,有效管控网络安全,通过开展网络安全教育培训工作,提升全体师生安全意识,规范其校园网使用行为,构建安全、绿色、高效的校园网络,为老师教育教学和学生搜集学习资料提供安全保障。

#### 参考文献

- [1] 蒋会军. 县域中职学校校园网络安全现状分析与对策[J]. 科技经济导刊, 2020(07):150.
- [2] 张猛. 中职校园网络安全管理的措施与策略[J]. 信息安全与技术, 2016, 7(02):12-13+23.
- [3] 徐宁. 中职学校网络信息中心网络安全问题的研究[J]. 信息周刊, 2019(004):1.

作者简介: 苏秦, 1988.11, 男, 汉, 陕西渭南, 大学本科, 网络工程中职初级教师, 网络安全方向