校园网络安全风险的防范与控制研究

曹立明
（天津生物工程职业技术学院，天津 300000）

摘要：随着信息化时代的发展，智慧校园在不断建设与完善，网络信息成为支持学校教育发展的关键技术，不仅为师生提供了便捷的资源，而且改变了教学方式，提升了课堂效率。但是在校园网络建设的过程中，也面临着诸多安全风险，成为影响学校、师生信息、身心、财务安全的关键因素。本文即通过分析当前校园网络安全面临的危险，进而提出校园网络安全风险的防范与控制手段和策略。

关键词：校园网络；安全风险；防范；控制

当今是以信息化为核心技术的时代，而学校的教育发展与建设必须依靠计算网络的服务与承载，因此构建一个高效完善的校园网络体系就成为学校发展进程中的不可或缺的基础设施，对于教师教学以及学生学习具有重要的辅助作用。但是在网络建设过程中，也会带来大量的安全风险，为保证学校工作的稳定、安全开展，还需要进一步深化校园网络的安全防范问题，为学校与师生提供良好的保障。

一、当前校园网络安全面临的问题

（一）黑客攻击

网络黑客是网络世界中存在的一些角色，他们为了达到一定的目的或利益，而借助网络工具对目标用户或网络体系进行攻击，进而对目标网络中的信息数据等内容进行盗取，不仅会导致目标用户的信息泄露，面临更大的风险，而且还会出现严重的利益损失。

对于学校来说，黑客的攻击可能会导致校园网络体系出现漏洞，从而导致其网络中的数据信息被泄露，尤其教务系统中具有大量的师生信息以及学校机密，一旦泄露就可能会影响到学校的正常工作开展。

（二）电脑病毒

计算机病毒是一种具有特殊作用的程序，尤其在网络的便捷传输作用下，计算机病毒成为影响网络安全的关键因素，不仅具有潜伏期，会在特殊时期引起计算机系统甚至网络体系的崩溃，而且还具有更大的安全风险，比如盗取信息数据等，造成更大的利益损失。对于校园网络体系而言，病毒程序的入侵不仅对师生个体产生影响，还会造成教务体系、教学设备的应用问题。

（三）安全漏洞

对于高校校园网络体系而言，由于其本身建设过程中可能存在的不规范行为，导致其系统中也会存在相应的安全漏洞，同时计算机系统、服务器、浏览器等各类系统与软件中，也会存在安全漏洞的问题，不仅可能为黑客等不法分子提供了可乘之机，而且还可能造成数据的泄露与丢失，造成较大的损失。

（四）网络缺陷

网络本身具备共享与传播的功能，因此其网络体系也必然存在安全缺陷，对于校园计算机网络而言，即使在 TCP、IP 协议下运行，也存在一定的缺陷与隐患，导致网络系统面临各种安全威胁。

甚至校园网络中的部分协议还缺少完善的安全服务，比如电子邮件就是以SMTP协议为基础，但该协议却存在认证机制的空白，这就导致垃圾邮件特别多，甚至还会携带病毒等程序附件。此外，远程登录系统中的 telnet 协议会将未经加密的用户名与密码直接传输，这就导致用户信息极其容易被盗取。

（五）管理问题

除了网络相关的问题之外，在学校制度建设与管理方面也存在一定的问题。

1. 在制度设计方面存在缺陷

制度保障是维持校园网络安全稳定的基础所在，但是大多数高校却缺乏相应的规章制度，导致学校职工、学生以及教师在运用网络时存在态度或认知上的问题，比如没有安装杀毒软件、进行了违规操作等，从而造成了安全隐患。

2. 高校网络安全保护系统还需要进一步升级

一方面学校需要更新网络安全保护方面的软硬件设备，另一方面则需要建立专业的安全部门，对学校网络的安全问题负责，定期开展网络检查与维护。

3. 对于学生健康上网的安全教育存在缺陷

由于网络信息的便捷性，导致各种内容都能通过网络传播，学校应进一步加强对学生的教育引导，从根本上杜绝学生的违规操作，避免不良信息数据传入校园网络之中。

二、校园网络安全风险的防范与控制

（一）优化技术服务，提升安全性能

为保证校园网络体系的安全，首先要通过技术的优化与升级实现安全性能的提升。

1. 充分发挥交换机的 VLAN 技术

应全面利用VLAN技术，尤其在网络安全风险的防控环节中，要充分发挥交换机的 VLAN 技术，由此实现将网络中不同端口的计算机设备进行独立划分，建立一个虚拟局域网段落，以此阻碍不同网段之间用户的自由访问，一定程度上将学校内部的网络与外界进行了隔离。

2. 要全面使用接入式网络设备

目前高校使用的大多数网络系统为共享式网络设备，而这就导致网络的共享为设备安全提高了风险，因此在进一步维护与优化校园网络体系时，可以采取接入式设备，以保证各个设备之间的独立，同时也强化了网络运行的稳定性。

3. 要善于运用 VPN（虚拟专用网）技术

该技术是借助公用网络建立临时稳定且安全连接的有效技术，不仅可以穿越混乱的网络环境，还能保证网络的独立性，尤其在为学校的财务管理、人事管理等方面服务时，可以保障其数据传输的稳定性与安全性。

4. 要及时更新与升级网络设备

一方面，学校应定时更新网络设备与软件，通过增加网络设备中的容量，进一步满足师生对网络的需求；另一方面也要尽快对设备进行升级，比如 RIP 等在升级或更换为 OSPF 路由器后，可以进一步完善路由协议 RIP 中的缺陷，提升安全性能力。

5. 要强化校园网络信息传输的加密性

加密传输是网络安全保障的重要手段，在网络信息传播过程中，很多信息数据容易被拦截盗取，从而造成信息的泄露，对此可以通过加密系统的设备服务，比如将系统口令、密码以及用户账号等信息进行加密处理，一定程度上可以提升关键数据的保密性，即使出现截获问题也可以保证安全。

6. 应控制服务端口

尤其在校园网络服务器建设中，应关闭不常用的协议与端口号，比如文件服务、邮件服务等系统，选择性的关闭一些服务端口，比如 HTTP、FTP、RLOGIN 等，进而实现降低安全风险的效果。

7. 学校还应安装入侵检测系统

一方面在配置设置上，学校应选取最新的网络攻击手段对应的信息代码，进而针对性的建立监管与记录体系；另一方面则要针对相应的问题建立阻断与预警服务，在网络接受到攻击企图后，即可自动防御并发出警告，以提醒网络使用者隔绝安全侵袭，保证网络的稳定。

（二）应用大数据技术，建立安全体系

随着大数据技术的普及应用，在网络安全方面也表现出重要的作用，因此学校还应围绕大数据建立相应的安全体系。

1. 应建立安全基准态势

即通过大数据对网络威胁的分析与统计，将一些特定的网络日志、用户行为等数据集制定为安全基准态势，即一旦出现该问题，即可立即反馈是否出现异常问题，并根究反馈制定解决方案。

2. 要建立智能处理方案库

仍然以大数据为基本体系，通过对算法、机器学习等方面的挖掘，生成各种网络安全问题的自动防御与保护方案，并将其纳入数据库，一旦出现相应的问题，即可自动调取解决方案应对，同时通过不同的调用与服务，还能通过机器学习机制不断完善方案，达到更有效的安全保护作用。

3. 应建立大数据检测平台

针对网络中的数据进行感知、判断与分析，一旦发现异常，可由平台系统从方案库中自动调取对应的解决策略，并通过截断数据流的方式停止侵害。

4. 应创建安全事故处理预案

由于网络威胁是客观存在而无法避免的，因此学校还应借助大数据建立预处理分析系统，即通过大数据系统模拟各类网络安全事故，并根据系统对应的结果进一步提出有效可靠的方案与恢复计划，尽快让受到攻击的网络系统还原稳定状态，以此尽可能降低网络风险对学校及师生利益的影响。

5. 还应进一步加强对数据信息的过滤，并及时更新和优化防火墙技术

高校一方面要根据学校自身的网络使用需求与习惯，制定特殊的信息过滤系统，将对学校、学生以及教师职工有害的信息直接过滤阻拦，保证网络环境的清洁。另一方面则要在互联网及学校内网间安装防火墙，以此建立一道可靠的安全屏障，既可以抵制非法入侵，保护内网之中的信息安全，又可以借助监控系统隔离内外网，并实现对网络安全事件的跟踪与审计功能。

（三）强化风险管理，提升重视程度

在学校管理方面，同样需要进一步提高对网络安全的重视。

1. 要依据学校自身的网络特征，建立完善的安全应急处理机制

在各个院系及职能部门之中应建立相应的安全管理员职位，通过管理人员之间的协同与合作，对学校整体网络的安全问题进行监控与监测，一旦发现问题即可展开联动作用，立即切断安全威胁与其他网络的连接，在控制其影响的前提下快速消除隐患。

2. 要进一步增加网络建设的投资预算

通过对软硬件设施的升级与完善，构建网络安全防护办公室，对学校网络的安全性进行定期检测与评估，并及时发现漏洞进行维护与解决。

3. 要进一步完善相应的网络安全管理制度

由于高校学生人数众多，而校园网络中的用户数量更为庞大，因此用户管理成为重要的问题，学校应建立内部网络实名制、责任制管理等机制，并设置相应的安全规范与惩处守则，比如《校园网络安全管理制度》《用户备案制度》等，由此可以快速找出运用破坏网络安全的责任人，针对违规用网的学生进行相应的处罚，同时还进一步提高网络安全管理的宣传作用，让学校师生能够进一步重视安全问题。

4. 学校还应进一步推动网络安全使用的宣传力度

通过学校的讲座、广播、宣传栏、新媒体等多种途径，向学生普及安全使用网络的方法、注意事项以及遇到网络安全问题时的及时处理方案，由此进一步提升学生的网络安全认知，从自身行为上杜绝大多数安全风险。

三、结语

综上所述，在当前的社会背景下，学校面临的网络安全风险具有各种形态与特征，对网络信息、人身安全、财务利益等有着重大的威胁，为保证学校机构的正常运营、保护全校师生与职工的信息与财务安全，必须进一步增强网络安全风险的防范与控制，通过对相关技术的升级优化以及大数据系统的应用，可以建立起更加完善的网络安全防控机制，同时借助学校制度建设、学生管理、设备升级等方式，也可以从宏观层面提升网络的安全性能，由此构建一个安全而又稳定的校园网络体系。

参考文献：

[1] 董彦斌 . 校园计算机网络安全风险的防范与控制 [J]. 网络安全技术与应用，2019（06）：64-65.

[2] 白天瑰 . 校园计算机网络安全风险防范与控制研究 [J]. 科学技术创新，2019（27）：90-91.

[3] 刘素军 . 大数据技术在高职院校校园网络安全中的应用 [J]. 计算机产品与流通，2020（02）：194.