加强校园网络管理，保证中职院校网络安全

潘慧军
桂林技师学院

摘　要：在信息技术快速发展的背景下，当前我国的各级职业院校都积极进行了校园网建设，力求通过校园网的成功建设储存具有可利用价值的信息资源，提高整体校园的信息化水平，让院校拥有良好的发展基础。对现阶段的中职院校校园建设来讲，信息化建设是核心工作内容。对教学管理、组织等多样化活动来讲具有重要价值和作用。但是，网络的开放性特点致使计算机病毒、非法入侵等安全问题频繁出现。如何加强校园网络安全管理已经成为学校各级领导以及教育工作者重点钻研的问题。基于此，本文立足中职院校背景，对校园网络安全管理展开探讨，希望能为中职院校校园网络安全管理提供有效参考。

关键词：中职院校；校园网络安全；管理
【DOI】10.12252/j.issn.2096-627X.2023.11.201

引言

互联网技术发展日渐成熟，推动了我国各个行业的信息化网络发展速度，校园网也迎来了良好的发展机会，促进了教育管理的智能化发展。网络安全不仅与学校未来发展息息相关，还与学生的成长、成才具有密切关联。而且，重点加强校园网络安全管理，能有效提高学校的整体利益。当今，我国各大校园的网络中都储存了丰富的信息内容，多数工作的开展也需要得到网络的支持。如果网络安全存在问题，将会导致信息传输不及时，或者信息内容被篡改、盗用等一系列情况的出现，致使学校面临难以弥补的损失。因此，为了让中职生的未来发展和成长得到保障，使中职院校的整体效益得到提高，应加强校园网络管理，保证校园网络安全。

一、计算机网络安全定义

网络安全主要指的是网络中的信息安全，利用系统中的硬件、软件进行信息保护，减少外界因素以及恶意攻击造成的信息泄漏等问题，使系统正常、安全地运行，保证网络服务的连续性。从广泛的角度上来讲，设计网络信息安全性、保密性等技术和理论隶属网络安全研究领域。

二、加强中职院校校园网络安全管理的必要性

重点加强中职院校校园网络安全管理是非常必要的，不仅能帮助院校形成良好的形象，还会影响学校的整体效益。当前，不同级别、类型的学校网络中储存了大量的信息内容，如果网络安全出现问题，将会造成信息泄漏、丢失、更改等问题的出现，使学校面临着无法弥补的损失。因此，在校园网络建设过程中，应高度重视网络安全管理，减少负面影响，维护信息安全。

三、中职院校校园网现状

（一）用户数量庞大，用户较为活跃

目前，我国中职院校的网络用户群体数量相对较多。而且，群体的人员结构比较复杂，表现得非常活跃。繁忙的网络、时段规律较为明显，白天网络的利用率相对比较低，下午到夜间的网络利用率逐渐提升，这对中职校园网络来讲属于沉重的负担。而且，在网络技术的全面推广下，人们的网络利用方式越来越丰富，庞大的数据上传、下载对校园网来讲都是“不堪重负”的，不仅会让校园网的响应速度越来越慢，还会使大量病毒隐藏在文件中，最终进入校园网，使服务器受到病毒的攻击和侵害。

（二）系统管理复杂，管理难度较大

校园网的用户群体多数为校内人员，以学生为主。多数中职学生都是寄宿制，学生会将自己的计算机设备带进校园，设备的类型、型号各不相同，不同型号、类型的计算机设备对系统、网络的要求不同。而且，部分师生并不具备良好的信息辨别能力。所以，在进行信息下载的过程中，可能会将网络中的病毒下载到设备中，当计算机与网络连接时，病毒趁虚而入，在设备中自动启动，甚至进行大范围传播，侵蚀服务器，导致与校园网连接的服务器设备受到病毒侵害。此外，不同型号的计算机设备系统差异明显。因此，在进行系统管理时无法实现统一管理，导致管理难度不断增加，让系统管理变得更加复杂。

（三）频繁遭受攻击，威胁网络安全

在连接特殊性的影响下，校园网经常会受到不同类型的攻击[1]。局域网所遭受的主要攻击源于局域网内部，次要攻击源于局域网以外，攻击类型分为两种，即DDoS攻击，通过软件的开发和利用对校园网的服务器进行信息轰炸，这样的行为会让网络服务器过载，从而出现瘫痪的问题。DNS劫持，通过缓存的方式进行病毒加载，或者劫持网站的DNS，然后进行指向性攻击。这两种攻击的危险性极强，一旦校园网遭受这两种类型的攻

击，将会造成极为严重、恶劣的负面影响。

（四）软件管理困难，维护工作受阻

从学校的角度上来讲，校园网络交换设备主要安装在建筑物内部，呈分散式。所以，监管人员无法全天、全面地进行监控、维护工作。而在应用的过程中，设备可能会出现故障，影响用户使用，还会在天气、人为等因素的影响下出现其他问题，而这些情况的出现导致硬件设备维护工作开展受到阻碍。

四、校园网络安全问题的表现形式

学校的主要工作核心就是教学活动[2]。因此，网络安全问题的类型多样化，具备的特点不同，主要表现形式如下：

（一）传播不良信息

在校园网和广域网有效连接的基础上，学校内的师生可以利用校园网进入互联网。而互联网上的信息较为丰富，且类型多样。关于暴力、色情等相关内容的网站并不少见。这些具有侵害性的信息对人的价值观、思想观会产生不良影响，对正在树立正确思想观念的学生来讲影响更深远。如果忽视此方面的安全管理，将会使不良信息在校园网中进行大范围传播，从而对学生身心、思想观念造成不可磨灭的损害和影响。

（二）病毒侵害

网络的快速发展和逐渐深入，使网络中传播的病毒类型越来越多样化，其传播速度范围并不是单机病毒可以比拟的，具备较强的破坏性、侵害性。在互联网中下载的软件程序、邮件都有可能携带病毒，这些病毒的存在不仅会损毁硬盘数据，还会清除主板芯片的内容，导致设备无法正常使用。当学校接入广域网后，学生会在下载软件发送邮件时，进行病毒传播，这些病毒是用户无法发现的。所以，必须加强校园网病毒安全管理工作。

（三）恶意破坏

网络设备主要包含服务器、路由器、工作站等多个关键组成部分。而且，这些组成部分分布在整个校园的不同区域中，某些人员可能有意、无意地进行破坏。另一方面，部分学生会通过黑客技术的运用对网络系统进行蓄意攻击，更改学校网站中的重要信息，修改网站主页，攻击服务器，这些行为均会使网络陷入瘫痪。

（四）口令入侵

通过实际调查结果分析得知，学校会为上网的教师、学生提供IP地址以及相关的账号信息及密码，以此用于管理和计费。每一个账户权限是不同的。因此，部分网络用户为了得到高权限才能获取的信息资料，会利用不正当的手段进行口令窃取，将网络费用转移给他人，而这也是网络监控的缺陷所在。网间隔离具备保护边缘器的作用，能有效预防内部的攻击行为。从多个角度上来讲，内部攻击与外部攻击相比前者更加致命。而且，学校中的计算机设备数量相对比较多，部分计算机设备是具有合法IP地址的。但在实际操作中，并不是所有计算机设备都有合法的IP地址。所以，会出现没有IP地址的用户冒充他人IP地址的问题和情况，进而使内部地址形成冲突，使合法用户的使用权益被侵害。基于此，必须积极建立完善的网络监控机制，加强对信息资源的保护，通过网络监控进行数据信息搜集、提炼和统计，针对网络安全进行风险评估。

五、中职院校校园网络安全管理策略

（一）采用安全认证防范技术

不合法的IP地址会对校园网的安全产生威胁。因此，校园内的用户必须进行使命认证，绑定个人的真实信息。具体方法有两种：第一，针对校园内部师生进行真实的身份绑定；第二，外部用户需要申请临时账号，并严令禁止非法进入。根据当前情况分析，网络的接入方式多样化，主要为MAC认证、WEB认证以及802.1X认证。其中，802.1X认证属于一种新型的认证方式，具备良好的安全性，符合国家相关标准，逐渐受到重视和关注，得到多家运营商的“注目”，将来也会得到更多设备、技术的支持。因此，中职院校可以尝试应用该认证方式，提升校园网络安全管理质量。

（二）安装入侵防御系统

传统的网络安全管理中，维护网络系统减少故障出现的主要方法就是安装入侵监测系统。通过网络传输过程的细致观察和分析，一旦发现不良传输，通过警报提醒，采取有效措施制止不良行为，阻止恶劣活动的发生，从而保证系统的安全性。虽然，这种方式能有效解决部分安全问题。但是，该方法具有明显的被动性特征，极其容易受到黑客的攻击以及病毒的侵害。因此，为了让该方法得到优化、创新和完善，“入侵防御系统”就此诞生。IPS的主动性较强，能在发现攻击的第一时间进行反攻，避免恶意侵入，更好地保护系统安全。这一系统与“网桥式防火墙”具有明显的相似之处，但多项功能都得到了优化和创新，能快速提取防火墙无法过滤的攻击行为，并做到及时制止，阻止攻击进入，从而更有效地保证系统安全。

（三）引用防火墙技术

防火墙是一种有效的病毒防侵入技术手段。主要指的是，在某一规则的基础上，严格监控管理信息交换过程，避免专门网络与互联网之间进行不良的信息传输，阻止不良网络通信。防火墙技术的应用能有效保护校园

网安全，未经过身份认证的用户无法进入校园网，如果强行进入会引发警报。同时，还能对用户的网站访问、浏览等进行实时监控。

现阶段，应用效果良好、广泛的防火墙技术为“隐蔽智能网关”。该项技术较为复杂，安全性能良好，不容易遭到破坏，隐蔽性较强。因此，管理人员应立足实际情况，定期进行防火墙安全的维护管理。比如，定期进行端口扫描，了解非法侵入的情况，掌握系统反映的信息，扫描所有网络主机，分析扫描结果，一旦发现问题，采取有效措施解决问题。此外，维护人员应根据校园网的应用情况，制定网络安全管理方案，明确网络安全管理目标，制定完善的规则条例，实施安全过滤，坚决防范非法攻击，使防火墙有效地保护网络信息安全，从而实现安全管理目标。

（四）应用Vlan技术

Vlan技术属于网络分段技术，该技术的应用，能将网络分成不同段，且分段依据为安全等级、业务范围，针对不同段的访问进行及时、有效地管控，阻止不具备访问权限的用户跨段访问。在校园网的安全管理中，应有效利用Vlan技术进行分段管理。尤其对于利用交换式局域网的学校来讲，要重点应用Vlan技术。网络分段的具体情况为：

物理分段。针对网络的物理层、数据链路层进行分段处理，让不同的段无法进行交互。

逻辑分段。在网络层上进行分段处理。以“TCP/IP”网络为例，将网络划分成不同的网段，如果网段需要交互，必须通过中间设备控制，中间设备为路由器、防火墙等。在网络的安全管理中，分段技术的应用效果良好。

（五）备份重要数据

校园网中储存的信息量相对来讲比较庞大。所以，应定期进行信息备份，优化校园网功能，及时恢复遗失的信息，有效开展数据备份工作，备份包含重要的信息数据，以及关键的设备信息，当校园网发生故障时可以利用备份线路，维持校园网的正常运行。与此同时，要想保证校园网络的安全，必须做好应急预案的制定，一旦校园网出现故障，可以通过应急预案的实施减少外部因素的负面影响，避免人为破坏的情况出现。

（六）加强设备管理

为了保护校园网的信息安全，减少外界的入侵和破坏。管理人员应定期对分散在校园不同区域的网络设备进行监管和维护，避免设备受到攻击和破坏，最关键的要保证机房网络线路的正常运行。鉴于此，管理人员应立足校园网的实际运行情况，建立完善的管理机制，组建优秀专业的管理队伍，针对员工进行岗前培训，提高管理人员的专业能力和水平，组织新生参与网络安全知识学习。信息时代的背景下，网络技术的快速发展使校园网的建立逐渐得到认可，应用更加广泛，其地位非常关键，但随之而来的还有各式各样的安全问题。而且，软件系统的局限性较强，计算机网络是开放的，所以不论防护措施多么严格、有效，也无法从源头上解决网络安全问题。立足这一背景，应从自身做起，重点增强用户的安全防范意识，避免无权限用户的网络访问，减少黑客的攻击，抵御病毒的侵害，让校园网更加安全。

（七）重点管理机房

中职院校的计算机机房规模庞大，上机人数比较多，计算机设备数量充足，应用频率相对较高。而且，机房的计算机在投入使用之前统一安装了操作系统，并设置了还原软件，开机之后能将系统盘，硬盘进行自动还原。但是，这样的方法无法消除蠕虫病毒的侵害，会使计算机反复感染，成为校园网的“病毒源头”，进而导致校园网崩溃、瘫痪。除此之外，部分学生比较喜欢利用实验室中的计算机玩一些网络游戏，甚至还会插入自己的U盘，利用实验室计算机读取U盘资料、下载U盘信息。这样行为很容易将病毒带进计算机，使其在网络中快速传播，严重危害校园网的安全。基于此，管理人员必须重点进行机房管理，落实单独监控措施，对机房内网、校园外网进行路由管理，要求学生上机登录自己的用户名，运用“方竹”软件监控学生的计算机应用情况，一旦发现威胁，第一时间处理。

结语

依上所述，在网络信息时代环境下，加强中职院校校园网络安全管理是必然举措。而且，要保证网络技术的先进性、安全性。在校园网管理期间，必须时刻掌握网络技术的发展情况和方向，立足实际情况，采取科学、有效的举措实施校园网安全管理，减少网络攻击、信息泄漏等问题的出现，提高校园网的安全性。同时，校园网络的安全特征为动态化、整体性，其涉及的内容包含系统、物理、应用安全等，需要应用数据保密、防火墙等先进技术，并配备专业能力较强的管理人才，只有这样，才能保证校园网络安全、正常运行。

参考文献

[1]毕双海.基础教育中网络信息安全教育与行为引导——评《校园行为安全管理探究》[J].安全与环境学报，2023（10）：3793-3794.

[2]肖承望.大数据技术在中职院校校园网络安全中的应用探讨[J].网络安全技术与应用，2021（12）：84-85.