中职学校网络安全现状及措施研究

谢瑜
武汉市仪表电子学校

摘　要：随着信息化教学方式的广泛应用，网络安全问题在中职学校中日益突出。此项研究旨在探究当前中职学校的网络安全现状，评估存在的问题，同时提出有效的解决方法，以解决网络安全的威胁，保护教育资源的安全可靠。本文通过对多所中职学校的实地调查和网络测评，提供了全面深入的网络安全现状述评。针对观察到的问题，如：网络设备的安全保障不足，网络使用的监管机制缺乏，学生的网络素质教育等，提出了一系列的解决方案，包括硬件设备的更新，监管制度的完善，以及网络素质教育的加强。希望通过实践运用，提升中职学校的网络安全水平，构建健康安全的网络教学环境。

关键词：中职学校；网络安全；解决措施；网络教学环境
【DOI】10.12252/j.issn.2096-6288.2022.05.073

引言

随着信息技术的广泛应用和互联网的普及，中职学校逐渐实现了教育信息化，通过网络为学生提供更加便捷、高效的学习和交流方式。然而，网络空间的开放性也给中职学校带来了一系列安全威胁。网络攻击、数据泄漏、信息泄漏等安全问题不断浮出水面，给学校和学生的利益造成了严重威胁。因此，加强中职学校网络安全的研究和措施的制定，对维护网络环境的安全与稳定具有重要意义。

一、中职学校网络安全现状

（一）网络攻击

网络攻击是指恶意个体或组织利用计算机网络的弱点和漏洞，对目标网络、系统或数据进行非法访问、损坏或篡改的行为。在中职学校网络安全中，网络攻击是一项严重的威胁。以下是一些常见的网络攻击类型。

病毒和恶意软件：病毒和恶意软件通过电子邮件附件、下载文件或恶意链接等方式感染计算机系统，造成数据丢失、系统崩溃和信息泄漏等问题。

电子邮件欺诈：网络攻击者通过伪造电子邮件，冒充合法机构发送虚假信息，诱导学校员工或学生提供敏感信息，从而获得非法利益。

DDoS攻击：分布式拒绝服务（DDoS）攻击通过发送大量请求占用网络资源，导致网络服务器过载，无法提供正常服务。

SQL注入：攻击者通过在网站的输入框中插入恶意命令，获取或修改数据库中的数据，导致数据泄漏或破坏。

（二）安全意识与培训

中职学校网络安全的现状受到安全意识和培训的影响。许多学校的教职员工和学生对网络安全问题的认识不足，缺乏基本的安全意识和正确的网络行为习惯。他们可能会轻信虚假的电子邮件，不小心点击恶意链接，泄漏个人账户信息等。此外，由于技术快速发展，网络攻击手法不断更新，中职学校需要定期进行网络安全培训，提高师生的网络安全素养。

（三）安全设施与系统

中职学校网络安全现状受到安全设施和系统的影响。目前，许多学校已经部署了一些基本的网络安全设施，如防火墙、入侵检测系统和反病毒软件等，以保护网络系统免受恶意攻击。然而，一些中职学校的网络设施仍存在漏洞和薄弱环节。例如，网络设备、服务器和软件的更新和维护不及时，存在安全漏洞。此外，一些学校的网络设备配置和管理不当，使得网络系统易受攻击。

综上所述，中职学校网络安全现状存在诸多问题。网络攻击类型繁多，从病毒和恶意软件到电子邮件欺诈和DDoS攻击，威胁着学校的信息安全。安全意识和培训不足导致教职员工和学生容易受到网络攻击。此外，安全设施和系统仍存在漏洞和薄弱环节，需要进一步加强更新和维护。中职学校应当认识到这些问题，并采取切实有效的措施来提高网络安全水平。下一部分将详细分析这些问题，并提出相应的解决措施。

二、存在的问题分析

（一）缺乏全面的安全策略

中职学校在网络安全方面存在缺乏全面的安全策略的问题。许多学校仅局限于基本的网络安全措施，如防火墙和反病毒软件，而缺乏整体的安全规划和策略。这导致学校在应对日益复杂的网络威胁时显得捉襟见肘，

容易被攻击者利用新的安全漏洞进行攻击。此外，缺乏综合的安全策略还使得学校在应急响应和安全事件处理方面缺乏统一的指导和流程。

（二）漏洞和薄弱环节

中职学校的网络系统中存在一些漏洞和薄弱环节。例如，网络设备、服务器和软件更新不及时或未及时修补已知的安全漏洞，容易被攻击者利用。此外，一些网络应用程序和网站的开发和部署存在安全漏洞，如弱密码策略、缺乏访问控制和输入验证等。这些漏洞和薄弱环节给攻击者提供了入侵和入侵目标的机会，从而导致数据泄漏、服务中断和系统崩溃等问题。

（三）安全意识和教育的不足

安全意识和教育的不足是中职学校网络安全现状的一个重要问题。许多教职员工和学生对网络安全的重要性和风险认识不足，缺乏基本的安全知识和技能。他们可能对网络攻击技术和常见的网络诈骗手段缺乏了解，容易受到钓鱼邮件、网络钓鱼网站和恶意软件的诱惑。同时，学校缺乏针对师生的定期网络安全培训和教育计划，无法提高他们对网络安全的警惕性和应对能力。

综上所述，中职学校在网络安全方面存在着一些问题。缺乏全面的安全策略导致学校难以应对复杂的网络威胁，容易受到攻击。漏洞和薄弱环节使得网络设备和应用易受攻击，导致数据泄漏和系统故障。另外，安全意识和教育的不足使得教职员工和学生容易成为网络攻击的目标。为解决这些问题，中职学校需要制定全面的安全策略，加强系统的漏洞管理和修复，并提供定期的安全意识教育以提高师生的网络安全素养。

三、措施研究

（一）建立完善的网络安全管理体系

为了应对中职学校网络安全的挑战，建立一个完善的网络安全管理体系是至关重要的。该体系应包括以下措施：

制定网络安全政策和规范：学校应制定明确的网络安全政策和规范，明确安全责任、权限和行为准则。这将为师生提供明确指导，确保网络使用符合安全标准。

建立网络安全团队：设立专职的网络安全团队负责网络安全管理和响应。该团队应具备网络安全技术和威胁情报分析的能力，及时发现和应对安全事件。

实施风险管理和评估：定期进行网络安全风险评估，识别潜在的安全威胁和漏洞。根据评估结果，采取相应的预防措施和修复措施，减少风险发生的概率和影响。

强化身份认证和访问控制：采用强密码策略、多因素身份验证和访问控制措施，确保只有授权人员才能访问关键系统和敏感数据。

（二）加强网站和服务器的安全防护

中职学校应加强对网站和服务器的安全防护措施，以减少恶意攻击的风险。

更新和维护：及时更新操作系统、应用程序和网络设备的安全补丁，修复已知的安全漏洞。定期检查和维护服务器和网站的安全配置，确保其符合最佳实践和安全标准。

防火墙和入侵检测系统：配置防火墙以监控和过滤网络流量，阻止潜在的攻击。部署入侵检测系统（IDS）和入侵防御系统（IPS）以实时检测和阻止网络攻击。

数据加密和备份：对敏感数据进行加密存储和传输，确保数据在存储和传输过程中的安全性。同时，定期备份数据，以便在发生数据丢失或损坏时能够及时恢复数据。

（三）提升网络安全意识和培训

提升中职学校师生的网络安全意识和培训是提高整体网络安全水平的关键所在。

定期安全培训：开展定期的网络安全培训，向教职员工和学生传授基本的网络安全知识和技能，提高他们识别和防范网络威胁的能力。

社交工程防范：教育师生警惕社交工程攻击，如钓鱼邮件、钓鱼网站和恶意广告等。提供实际案例和演练，帮助他们识别和避免社交工程攻击。

安全意识宣传活动：组织安全意识宣传活动，如举办网络安全讲座、举办安全意识竞赛等，增强广大师生对网络安全的重视和关注。

四、案例分析与实证研究

在这一部分，我们将通过案例分析和实证研究来深入研究中职学校的网络安全措施的有效性和实施情况。通过对真实案例的调查和分析，可以获得对问题的更深刻理解，并从中获得宝贵的经验和教训。

（一）某中职学校网络安全实施情况

我们选择一所中职学校进行网络安全实施情况的详细调查和分析。

第一，安全策略和规范。该中职学校已制定了一系列网络安全政策和规范，明确了师生对网络安全的要求和责任。政策要求教职员工和学生在使用学校网络时遵守一定的行为准则，包括保护个人账户信息、禁止非法

下载和分享文件，以及警惕网络诈骗等。这些政策和规范为学校网络安全提供了法规依据和指导。

第二，安全设施和系统。学校配备了一些基本的网络安全设施和系统，例如防火墙、入侵检测系统和反病毒软件。这些措施有助于阻止潜在的恶意攻击和病毒感染。此外，学校还进行了定期的设备和软件更新，以修补已知的安全漏洞，确保网络设施和系统的安全性。

第三，安全意识和培训。学校意识到安全意识和培训的重要性，定期开展网络安全培训和教育活动。教职员工和学生接受针对网络安全的培训，学习如何识别和防范网络威胁。此外，学校组织安全意识宣传活动，提高师生对网络安全的重视和意识。

通过对这所中职学校网络安全实施情况的案例分析，我们发现了一些成功的做法和为改进的方面。

首先，制定明确的网络安全政策和规范，为教职员工和学生提供了明确的指导和规范，保护了学校网络安全。其次，配备基本的网络安全设施和系统，如防火墙、入侵检测系统和反病毒软件，以保护网络设施和系统免受恶意攻击。再次，定期进行设备和软件的更新和维护，修补已知的安全漏洞，确保网络的安全性。最后，开展定期的网络安全培训和教育，提高教职员工和学生的网络安全意识和技能。

需要改进的方面可能包括，进一步加强安全设施和系统的完善性和覆盖范围，确保对潜在威胁的全面防护和加强安全意识和培训的广度和深度，包括针对最新网络攻击技术和趋势的培训，以保持师生的安全意识与威胁感知能力的更新。

（二）欧美国家中职学校网络安全措施的启示

为了获取对中职学校网络安全措施的进一步启示，我们可以进行欧美国家中职学校网络安全措施的比较研究。以下是一些可能的研究结果。

1.欧美国家中职学校强调综合的安全策略

许多欧美国家的中职学校注重制定综合的网络安全策略，旨在建立全面的安全管理体系。他们将安全政策、技术控制和员工培训相结合，形成一个协同工作的网络安全框架。

2.欧美国家中职学校高度重视持续监测和响应

为了及时发现和应对网络威胁，许多欧美国家的中职学校建立了实时监测和响应系统。他们通过使用先进的安全工具和威胁情报，监测网络活动，并采取相应的措施来应对安全事件。

3.欧美国家中职学校推动跨部门合作和信息共享

为了更好地应对网络安全挑战，许多欧美国家的中职学校积极推动教育、技术和政策部门之间的合作和信息共享。他们建立了合作机制，定期举行会议和工作坊，就共同关注的网络安全问题进行合作研究和交流。

通过对欧美国家中职学校网络安全措施的比较研究，我们可以从中学习到一些宝贵的经验和做法。这些经验和做法可以为中职学校制定和改进网络安全措施提供参考。

五、结论与展望

通过案例分析和实证研究，我们深入研究了中职学校网络安全措施的有效性和实施情况。我们发现了成功的实施案例和可改进的方面，并从欧美国家的经验中获得了启示。

总体而言，中职学校应制定明确的网络安全政策和规范，配备适当的网络安全设施和系统，并加强安全意识和培训。此外，中职学校可以借鉴欧美国家中职学校的经验，加强安全策略的制定、持续监测和响应能力的建设，以及跨部门合作和信息共享的推动。

未来的研究应继续关注中职学校网络安全的现状和演变趋势，以促进网络安全措施的持续改进和创新。中职学校需要不断适应新的网络威胁和技术发展，加强对师生的安全教育和培训，并与政府、技术机构和其他学校展开合作，共同应对网络安全的挑战。只有这样，中职学校才能确保网络环境的稳定和安全，营造良好的学习和工作环境。

参考文献

[1]肖波.中职学校计算机网络教学网络信息安全教育的渗透[J].中国新通信，2021，23（23）：121-122.

[2]王冰玉.中职学校网络安全教学策略[J].福建电脑，2021，37（08）：148-150.

[3]孙美玲.基于网络空间安全的中职计算机网络教学改革思考[J].造纸装备及材料，2021，50（02）：139-140.

[4]尚娟娟，刘明.将网络信息安全教育融入中职学校计算机网络教学中的策略探究[J].网络安全技术与应用，2020（11）：109-110.

[5]罗伊佑.中职学校校园网安全维护措施的探讨[J].网络安全技术与应用，2021（07）：103-104.

[6]徐丹.计算机网络安全技术在中职学校校园网中的应用[J].信息记录材料，2020，21（07）：99-100.