大数据时代高校计算机网络安全分析

郭艺 孟令媛

（郑州西亚斯学院 451150）

摘要：随着大数据时代的到来，高校计算机网络安全面临着新的挑战。本文对大数据时代高校计算机网络安全进行了分析。首先介绍了大数据时代对高校计算机网络安全的重要性和影响。其次，探讨了高校计算机网络面临的两个主要问题与威胁，包括数据隐私保护与泄露风险以及弱点发现与漏洞修复挑战。然后，提出了保障高校计算机网络安全的两个关键策略与措施，包括综合安全策略与技术措施以及威胁检测与应急响应机制。最后，强调了加强安全教育和培训的重要性，并呼吁高校建立安全意识和技能的培养体系。本文的研究成果对高校计算机网络安全管理和实践具有指导意义，有助于保护高校计算机网络免受安全威胁的侵害。

关键词：大数据时代；高校；计算机网络安全

引言

随着信息技术的快速发展和大数据时代的到来，高校计算机网络的重要性日益突显。计算机网络不仅是高校教学、科研和管理的基础设施，也是各种敏感数据和知识的储存和传输渠道。然而，随之而来的是网络安全问题的日益严重。面对日益复杂的网络威胁和攻击，高校计算机网络安全变得更加紧迫和重要。本文旨在分析大数据时代下高校计算机网络安全的现状、问题和威胁，并提出相应的策略与措施。通过对大数据时代高校计算机网络安全的综合分析和策略探讨，可以为高校网络安全管理和实践提供有益的参考和指导。

一、大数据时代高校计算机网络安全

（一）网络规模的扩展

在大数据时代，高校计算机网络规模的扩展是一项重要的挑战。随着科研和教学的发展，高校网络连接的终端设备数量不断增加，包括学生的个人电脑、移动设备、科研实验室的服务器等。这些设备的增加导致了网络流量和数据量的急剧增加，网络的带宽和吞吐量需求也不断提升。因此，高校计算机网络需要扩展其规模以适应这一趋势。

高校需要考虑网络设备的部署和管理，随着网络设备数量的增加，高校需要建立完善的设备管理机制，确保设备的正常运行和及时维护。这包括设备的安装、配置、监控和更新等方面的工作。高校可以使用自动化的网络管理工具来简化和优化这些任务，提高网络设备的效率和可靠性。

高校需要加强网络基础设施的建设，随着网络规模的扩大，高校需要增加网络的带宽和容量，以满足大数据传输和处理的需求。这包括升级网络交换机、路由器和服务器等核心设备，以及增加网络存储和计算资源。同时，高校还应考虑使用高速网络技术，如光纤网络和高速无线网络，来提供更快速和可靠的网络连接。

高校需要关注网络安全问题，随着网络规模的扩展，网络安全威胁也变得更加严峻。高校需要加强网络安全防护措施，包括入侵检测系统、防火墙、访问控制和加密技术等。同时，高校还需要加强对网络用户的安全教育和培训，提高用户的安全意识，防止恶意软件、网络钓鱼和社交工程等攻击。[1]

（二）网络架构的复杂性

在大数据时代，高校计算机网络架构的复杂性是一个重要的挑战。传统的中心化网络架构已经无法满足大数据处理和分析的需求，因此高校采取了分布式系统、云计算、边缘计算等新兴技术来构建更复杂的网络架构。以下是网络架构复杂性带来的挑战和应对措施

网络拓扑的复杂性增加，在传统的中心化网络架构中，网络拓扑相对简单，通常是一个层级结构，有限的网络节点和连接。然而，大数据时代的高校网络涉及到多个网络节点和互联设备，包括数据中心、服务器、存储设备、边缘计算节点等。这些节点之间的连接变得更加复杂，需要考虑网络拓扑的设计、路由算法和数据传输策略，以确保数据能够高效地传输和处理。

不同网络架构之间的协同工作，在大数据时代，高校可能同时采用传统的本地网络、云计算平台和边缘计算设备来支持教学和科研活动。这些不同的网络架构需要进行协同工作，以实现数据的流动和共享。这就需要高校建立跨网络的互联机制和协议，确保数据能够在不同网络之间无缝传输，并保证数据的安全和一致性。

网络安全的挑战也随着网络架构的复杂性而增加，复杂的网络架构意味着更多的网络节点和连接，增加了网络攻击者入侵和渗透的机会。高校需要采取综合的安全策略和技术措施，包括网络防火墙、入侵检测系统、身份认证和访问控制等，以保护网络的安全和数据的完整性。

二、高校计算机网络安全面临的问题与威胁

（一）数据隐私保护与泄露风险

在大数据时代，高校计算机网络中包含大量的敏感信息，如学生和教职工的个人身份信息、研究数据、教学资料等。保护这些数据的隐私和机密性成为高校网络安全的重要任务之一。然而，数据隐私保护与泄露风险是一个复杂而严峻的问题，需要高校采取一系列措施来确保数据的安全性。

1.高校应建立严格的数据访问控制机制：通过限制数据访问权限，确保只有授权人员可以访问敏感数据，从而减少数据泄露的风险。这可以通过身份认证、授权管理和访问审计等手段来实现。高校可以使用多因素身份认证技术，如密码加令牌、生物特征识别等，以提高身份认证的安全性。

2.高校应加强数据加密保护：对于存储在高校计算机网络中的重要数据，如个人身份信息和研究成果，应使用强大的加密算法进行加密。这样即使数据被非法获取，也难以解密和使用。同时，在数据传输过程中，采用安全的传输协议，如 SSL/TLS，保障数据在传输过程中的机密性和完整性。

3.高校应制定严格的数据备份和恢复策略：定期备份数据，并将备份数据存储在安全可靠的位置，以防止数据丢失或损坏。在数据泄露或意外情况发生时，高校可以通过备份数据快速恢复，并减少对高校的影响。

4.高校还需要加强员工和用户的安全教育和意识提升：高校网络中的数据泄露往往是由于员工或用户的不慎操作或安全意识薄弱导致的。因此，高校应定期组织安全培训和教育活动，提高员工和用户对数据隐私保护的认识和重视程度。教育他们如何创建强密码、识别恶意链接和附件、安全使用网络等，以减少数据泄露的风险。[2]

（二）弱点发现与漏洞修复挑战

在大数据时代，高校计算机网络面临着日益复杂的安全威胁和攻击手段。为了保障网络安全，高校需要及时发现和修复网络中的弱点和漏洞，以防止恶意攻击者利用这些漏洞侵入系统并造成损失。然而，弱点发现与漏洞修复面临着一些挑战。

1.高校计算机网络的规模庞大且复杂：高校通常拥有大量的计算机和网络设备，包括服务器、交换机、路由器等。这些设备涉及多个厂商和多个操作系统，存在着不同的安全漏洞和弱点。因此，要全面发现和修复网络中的弱点和漏洞需要进行全面的安全扫描和评估，覆盖各个方面。

高校计算机网络的运行是一个持续的过程，网络设备、操作系统和应用程序等都需要进行更新和升级，以修复已知的漏洞和弱点。然而，对于庞大的高校网络来说，及时更新和升级是一个巨大的挑战。因为需要保证在更新过程中不影响网络的正常运行，并且要确保所有的设备和系统都得到更新，以免遗漏导致安全风险。

另外，高校计算机网络的漏洞修复需要综合的技术和资源支持。修复一个漏洞不仅仅需要技术人员的专业知识和技能，还需要合适的工具和平台来辅助识别和修复漏洞。高校需要投入足够的资源来建立和维护一个强大的漏洞修复团队，同时采用先进的漏洞扫描工具和漏洞管理平台，以加快漏洞修复的速度和效率。

此外，高校计算机网络的弱点和漏洞是不断变化的。新的安全威胁和攻击手段不断出现，新的漏洞和弱点也不断被发现。因此，高校需要建立起持续的弱点发现和漏洞修复机制。这包括与安全厂商和社区的合作，获取最新的漏洞情报和安全补丁，及时进行漏洞修复。

三、保障高校计算机网络安全的策略与措施

（一）综合安全策略与技术措施

为了应对大数据时代高校计算机网络安全的挑战，高校需要制定综合的安全策略并采取相应的技术措施来保障网络安全。[3]

高校应制定适应自身情况的安全策略，安全策略应考虑高校的网络规模、网络拓扑结构、用户需求等因素，制定相应的安全政策和控制措施。例如，限制网络访问权限，确保只有授权人员可以访问敏感数据；制定密码策略，要求用户设置复杂密码并定期更新；建立网络使用规范，明确用户的网络行为规范等。安全策略应与高校的整体信息化战略相一致，形成一个全面的安全框架。

高校需要采取技术措施来支持安全策略的实施，技术措施包括网络安全设备和软件的部署和配置，以及安全管理和监控系统的建立。例如，高校可以配置防火墙、入侵检测系统（IDS/IPS）等安全设备，用于检测和阻止网络攻击；采用虚拟专用网络（VPN）技术，保障远程访问的安全性；使用数据加密技术，确保敏感数据的保密性等。此外，高校还应建立安全事件管理系统，及时监测和响应安全事件，加强对网络安全的实时监控和管理。

高校应加强网络安全的风险评估和漏洞管理，定期进行风险评估，评估网络的安全性和弱点，确定安全风险的优先级和紧急程度。同时，建立漏洞管理系统，及时跟踪和修复网络中的漏洞。漏洞管理包括漏洞扫描、漏洞评估、漏洞修复等环节，通过定期的漏洞扫描和修复，降低网络遭受攻击的风险。

（二）威胁检测与应急响应机制

在大数据时代，高校计算机网络面临着各种复杂的安全威胁和攻击。为了及时发现和应对这些威胁，高校需要建立威胁检测和应急响应机制，以保障网络安全。

1.高校应部署威胁检测系统：威胁检测系统可以通过实时监控网络流量和日志记录，识别异常的网络活动和安全事件。高校可以使用入侵检测系统（IDS）和入侵防御系统（IPS）等技术来检测和阻止网络攻击。这些系统可以分析网络流量、检测攻击特征和行为模式，并及时发出警报或采取防御措施，以防止攻击者入侵和破坏网络。

2.高校应建立安全事件响应团队:安全事件响应团队由安全专家和技术人员组成，负责处理网络安全事件和应急响应工作。团队成员应具备丰富的安全知识和技能，熟悉各种安全工具和技术，能够快速响应和处置安全事件。团队应建立完善的应急响应流程和标准操作规程，以确保在安全事件发生时能够迅速、有效地应对和处理。

3.高校应定期进行安全事件演练和模拟攻击:通过模拟真实的攻击场景和安全事件，可以测试威胁检测和应急响应的效果，并发现和弥补安全漏洞。演练和模拟攻击还可以提高安全团队的应急响应能力和协同配合能力，使其能够快速、准确地应对各种安全威胁。[4]

4.高校应建立安全事件信息共享机制:安全事件的信息共享可以加强高校与其他组织和安全厂商的合作，共同应对安全威胁。高校可以参与安全信息共享平台，获取最新的安全威胁情报和攻击事件的分析报告，以便及时了解当前的威胁形势和趋势。同时，高校还应主动分享自身的安全经验和应急响应实践，以促进整个社群的安全提升。

结语

在大数据时代，高校计算机网络安全面临着日益复杂的挑战和威胁。为了保护数据隐私、防止泄露风险，高校需要采取综合的安全策略和技术措施。同时，弱点发现与漏洞修复是确保网络安全的重要环节，需要全面评估网络的安全性并及时修复漏洞。另外，威胁检测和应急响应机制的建立对于及时发现和应对安全威胁至关重要。高校应加强威胁检测系统的部署和安全事件响应团队的建设，通过安全事件演练和信息共享，提升网络安全的应急响应能力。只有通过综合的安全措施和紧密的合作，高校才能在大数据时代有效保护计算机网络安全，确保教学、科研和管理等各项工作的顺利进行。

参考文献：

[1] 金国望.大数据时代高校计算机网络安全分析[J].数码世界,2021:2(250-251).

[2] 邓熊平.大数据时代高校计算机网络安全分析[J].网络安全技术与应用,2017

[3] 黎闻华.大数据时代的计算机网络安全分析[J].现代工业经济和信息化,2019:82-83.

[4] 王展.大数据时代的计算机网络安全分析[J].信息与电脑(理论版),2020:3.

项目：河南省教育厅2020年民办普通高等学校学科专业(计算机科学与技术)建设资助项目（教政法[2020]162号）