 DOI: https://doi.org/10.12345/bdai.v5i7.19735

Analysis of Computer Network Security Technology Based on Big Data Technology

Lei Gao

Liaoning Provincial Data Center, Shenyang, Liaoning, 110000, China

Abstract

Computer network security technology based on big data is very important in maintaining data and network security. This paper mainly discusses the connotation of cybersecurity and its importance in the information age, and then analyzes the threats faced by computer network security technologies in the context of big data, such as data leakage, tampering and abuse, malware and virus attacks, as well as phishing and social engineering attacks. Finally, based on big data technology, this paper proposes measures to strengthen network security detection, application firewall technology, data encryption technology protection, install system anti-virus software, and optimize network sharing resource management to deal with the above security threats and ensure computer network security.

Keywords

big data technology; computer; cybersecurity technology

基于大数据技术的计算机网络安全技术分析

高蕾

辽宁省数据中心，中国·辽宁 沈阳 110000

摘　要

以大数据为基础的计算机网络安全技术在维护数据和网络安全性方面非常重要。论文主要探讨了网络安全的内涵以及其在信息化时代的重要性，随后分析了大数据背景下计算机网络安全技术所面临的威胁，如数据泄露、篡改和滥用，恶意软件和病毒攻击，以及网络钓鱼和社交工程攻击等。最后，论文基于大数据技术，提出了加强网络安全检测、应用防火墙技术、数据加密技术防护、安装系统杀毒软件以及优化网络共享资源管理等措施，以应对上述安全威胁，保障计算机网络安全。

关键词

大数据技术；计算机；网络安全技术

1 引言

在数字化技术不断发展的时代，网络安全态势感知已经成为企业和机构保障信息资产安全的关键能力。网络环境的开放性是其固有特点，但同时也为各种风险隐患提供了滋生的空间。在这些风险当中，数据泄露尤为突出。在大数据技术的支持下，数据信息变得更容易被获取和滥用，不仅侵犯了人们的隐私权，还为网络诈骗、网络暴力等不法行为提供了便利。这些网络安全问题的存在不仅损害了个人和企业的利益，也对和谐社会建设造成了严重威胁。所以，在大数据时代，必须加强计算机网络安全技术研究，通过深入的技术研究和创新不断完善网络安全防护措施，提高计算机网络的抗攻击能力和自我修复能力。

【作者简介】高蕾（1983–），女，中国河北乐亭人，硕士，高级工程师，从事网络技术和网络安全研究。

2 网络安全的内涵及重要性

2.1 网络安全的内涵

网络安全是一个综合性的概念，涵盖了对计算机网络及其系统中信息的全面保护。在网络安全中，保密性是核心，可保证信息在传输和存储过程中不被未经授权的第三方获取；完整性是保障数据真实性的基础，主要是指信息在传输、存储和处理过程中保持未被篡改、破坏或丢失的状态；可用性则强调网络系统和信息资源的持续、稳定、可靠运行，保证授权用户能够在需要时及时访问和使用网络资源；可控性要求对网络系统中的信息和资源实施有效的管理和控制，防止非法访问和滥用；真实性则要求网络中的信息来源可靠，保证信息的真实性和可信度；抵抗赖性则是一种责任追溯机制，保证在信息安全事故发生时能够及时追查到相关责任方，防止其逃避责任[1]。

2.2 网络安全的重要性

在当今信息化时代下，网络安全的重要性日益凸显，

其中数据是网络安全的基础。在数字化浪潮当中，企业、政府和个人的重要数据均需要得到妥善保护，防止数据泄露、篡改和滥用，以维护正常的社会秩序和经济利益。在实际运行中，还需保证网络系统的稳定性，一旦系统遭受攻击或感染病毒，可能导致服务中断、数据丢失等严重后果，为个人和企业带来巨大的损失 [2]。同时，隐私保护在网络安全中占据重要地位，在互联网时代下，个人隐私信息容易暴露于风险之中，而加强网络安全防护则可有效保护个人隐私不被非法获取或利用，维护个人权益。除此之外，随着相关法律法规的不断完善，企业和机构需要遵循相应的网络安全标准和规范，保证业务运营符合法律法规要求，并采取先进的安全技术和管理措施及时发现和应对各种网络安全威胁，降低潜在风险的发生概率和影响程度。

3 大数据背景下计算机网络安全威胁

3.1 数据泄露、篡改和滥用

在数据爆炸的大数据时代，计算机网络安全面临着前所未有的严峻挑战，其中最严重的便是数据泄露。因计算机系统当中存储着海量如个人隐私、商业核心数据以及政府机密等敏感信息，黑客们通过攻击数据存储和传输的关键环节能够轻易窃取相关信息。一旦数据泄露，个体隐私将无处遁形，企业可能面临着金融损失和声誉损害，甚至国家的安全也可能因此受到威胁 [3]。除数据泄露外，数据篡改问题同样不容小觑。在大数据驱动下，数据是决策制定和商业运营的基石，但是一旦数据被恶意篡改，就可能导致出现决策失误甚至面临经济损失，严重时还会危及人们的生命安全。例如，在医疗、交通等关键领域，数据的准确性直接关系到人们的生命财产安全。与此同时，数据滥用这一问题也比较严重，不法分子主要利用非法获取的个人信息进行广告骚扰、电信诈骗等犯罪活动，严重侵犯了个体的合法权益。

3.2 恶意软件和病毒攻击

在大数据时代下，计算机网络安全所面临的威胁越来越严重，恶意软件和病毒攻击是其中比较严重的一项挑战。恶意软件主要是由不法分子精心设计的一种恶意程序，可将其看作网络世界的隐形杀手，潜伏在网络的每一个角落，随时都可能入侵计算机系统。恶意软件的目的明确，会试图窃取用户的敏感信息，导致系统无法正常运行，甚至还可能控制用户的计算机进行非法活动。恶意软件的传播途径多种多样，可能隐藏在看似无害的电子邮件附件中，也可能潜伏在恶意网站上，通过诱导用户点击的方式进行传播。除此之外，恶意软件还会借助广告和可移动储存设备进入用户的计算机，一旦被感染将会造成不堪设想的后果，甚至还可能将计算机纳入僵尸网格，成为发动大规模网络攻击的帮凶。在恶意软件当中，病毒是比较常见的一种形式，具有自我复制和感染其他计算机的能力，会在网络中迅速传播，造成大规模的数据丢失和系统崩溃。病毒攻击不仅会给个人和企业带来巨大的经济损失，还可能引发敏感信息泄露，甚至破坏关键基础设施，对社会和国家安全构成严重威胁。随着大数据的不断发展，网络规模越来越大，病毒和恶意软件的传播速度明显增加，海量的数据流动为其提供了更多的传播机会和渠道。

3.3 网络钓鱼和社交工程攻击

网络钓鱼和社交工程攻击是两种比较狡猾的欺诈手段，主要利用人们的信任心理巧妙伪装成可信任的实体或者是联系人，窃取用户的敏感信息。网络钓鱼攻击者通过模拟知名的网站、银行服务或者社交媒体平台，通过伪造邮件、短信或网页链接的方式，诱骗用户点击并提供个人信息、账户密码等关键数据。而社交工程攻击则更加的狡猾，攻击者会利用心理战术，冒充受害者信任的人或者机构，通过电话或者即时通讯工具进行诱导，使受害者主动泄露隐私信息或执行对自己不利的操作。上述两种攻击方式的共同点在于，不依赖于直接的技术漏洞进行入侵，而是巧妙地利用社会工程学原理，利用人类的心理弱点和社会信任关系来获取信息。在大数据时代，因为信息量激增，攻击者能够更精确地了解个人和组织的详细信息，进而更逼真地伪装自己，使这类攻击更具迷惑性和危险性。

4 基于大数据技术的计算机网络安全技术

4.1 加强网络安全检测

为有效防范大数据时代中计算机网络安全所面临的多重风险，首要任务在于提升整体的安全意识，这不仅意味着在日常操作中需要严格遵循相应规范和流程，还需强化网络安全检测能力。在实际检测中，可借助更加先进的技术手段，构建一个全面、高效的安全检测系统，并配备兼顾的防火墙以及多样化的检测软件，其可在计算机受到攻击时迅速识别并消除威胁，在最短时间内消除潜在的安全隐患。除此之外，还需对计算机系统进行定期的升级工作，保证系统可以应对最新的安全威胁。同时，对系统中存在的漏洞，需要及时打上补丁，防止攻击者利用这些漏洞进行入侵。在访问和操作系统时，权限验证非常重要，其保证了只有经过授权的用户才能够访问敏感数据或者执行关键操作。但是需要明确，打造一个稳固的计算机网络安全环境并不是一蹴而就的，而是一项需要长期投入和持续努力的工作，操作者必须始终保持高度的安全意识，不断进行隐患排查，并采取一切可能的措施减少甚至避免病毒和恶意攻击发生，保证在大数据时代下计算机网络能够安全、稳定地运行，为人们的生活和工作提供坚实的保障。

4.2 应用防火墙技术

防火墙技术在增强计算机网络安全方面具有至关重要的作用，通过构建防火墙，系统能够将潜在的漏洞进行隔离，进而将网络划分成公共网和内部网两个独立的部分。这种隔离机制允许用户在享受网络服务的同时，无需访问或获取系

统源代码的权限，不仅降低了用户不当操作的风险，也有效阻止了恶意攻击者通过系统漏洞进行渗透和破坏。防火墙技术的另一大优势在于其与网络管理系统的集成，通过将防火墙与网络管理系统相连，管理员可以实时监控和分析网络运行状况，及时发现潜在的安全隐患。这种实时监控能力使得管理员能够在安全风险升级之前，采取必要的防御和修复措施，有效减少网络系统的安全漏洞，最大程度降低用户面临的安全威胁。但是需要注意，防火墙技术并不是一劳永逸的解决方案，其需要定期更新和维护，同时用户还需增强安全意识，避免在公共网络上随意泄露个人信息和敏感数据，以免成为网络攻击的目标。

4.3 数据加密技术防护

数据加密技术不仅能够增强数据对各种潜在风险的抵抗力，还能够有效降低数据丢失和损坏的风险。随着技术的不断进步，数据加密技术已经十分成熟，并广泛应用于计算机网络安全的各个领域。数据加密技术的优势在于高度灵活性和适应性，可根据不同场景和需求进行定制化加密处理。对于重要数据，通过结合身份认证、数据库访问权限以及数字签名等多种技术手段，计算机操作者可为数据信息提供多重保护，进而有效保证数据的安全性和完整性。在信息传输过程中，数据安全性非常重要，为进一步提高数据传输的安全性，可采用信息隐藏技术结合数据加密处理。信息隐藏技术主要通过将数据隐藏在看似普通的文件中，使数据在传输过程中难以被检测和窃取，即时数据被截获，因为被隐藏，攻击者也无法轻易读取或篡改其中的内容，可有效保证信息的完整性和保密性。

4.4 安装系统杀毒软件

在用户计算机上安装杀毒软件可有效保证网络系统安全，其能够实时地监测计算机网络系统的安全状况，自主识别并警示恶意软件的安装企图，有效降低其对系统安全运行的威胁。通过安装杀毒软件，用户能够享受到更加安全、稳定的网络环境，减少潜在的风险。一旦杀毒软件安装并运行在系统内，其将开始自动进行实时监控，无论是隐藏在邮件附件、恶意网站还是通过其他途径传播的病毒，只要其试图对用户的计算机进行恶意攻击，杀毒软件都能够迅速发现并采取相应的防护措施，显著缩短问题处理的时间，并将病毒对系统的影响降至最低。但是，在选择杀毒软件时需要注意从正规渠道下载并安装，避免从非法或者不受信任的源获取软件，防止引入伪装成杀毒软件的恶意程序，进一步威胁系统的安全，甚至导致个人信息泄露。除了计算机本身的安全防护，用户还需要重视与外部设备相关的安全管理，如打印机、扫描机、计算机网络服务器等，也可能成为病毒和恶意软件的攻击目标。所以，用户必须定期对这些设备进行全方位、深层次的检查，排除潜在的安全隐患，保证整个网络系统的安全。

4.5 网络共享资源管理

在大数据背景之下，共享资源广泛使用增加了计算机网络安全隐患，政府部门需要发挥引领的作用，联合计算机网络行业协会共同发起一系列的网络净化活动，从源头上消除潜藏的风险隐患，提高网络共享资源的安全性。这些网络净化活动主要包括对各类信息共享平台的严格管理和控制，在实际工作时需要重点关注数据信息严格审核，保证所分享的内容合规、合法，并对发现的违规资源进行及时清理，为广大网络用户创造一个安全、可靠的共享环境，保护机器免受恶意内容的侵害。对于共享资源中存在的质量问题，一旦发现不合格、不合规的内容，需要立即采取措施进行整改和优化，采取零容忍的态度，有效维护网络共享环境的纯净和健康，保证所有用户都能够得到高质量的共享资源。与此同时，加强网络安全宣传工作也非常重要，通过提高用户的安全信息教育用户在使用共享资源的时候保持警惕，及时发现并举报潜在的安全隐患，在政府、行业协会、媒体以及广大网民的共同努力下，形成全社会共同维护网络安全的良好氛围。

5 结语

大数据技术为计算机网络安全提供了强有力的支持，通过分析海量数据，大数据可精准识别风险、预防攻击，有效保证网络环境的稳定和安全。随着技术的不断进步，网络安全将会越来越牢固，可为后续的数字生活提供坚实的基础。

参考文献

[1] 刘博.大数据背景下计算机网络信息安全技术与防范机制[J].办公自动化,2024,29(11):39-41.

[2] 王雪.大数据技术应用背景下计算机网络安全技术专业人才培养的探讨[J].电脑知识与技术,2024,20(9):148-150.

[3] 马鑫越.大数据背景下医院计算机网络信息安全技术的应用实践研究[J].科技资讯,2023,21(20):30-33.