大数据时代下计算机网络安全及防范措施

孙莹莹
新疆天山职业技术大学　新疆　乌鲁木齐　830017

摘　要：随着信息技术的迅猛发展，大数据时代已全面来临，数据成为核心资源。然而，这一变革也带来了前所未有的网络安全挑战。个人隐私泄露、企业数据被盗、信息安全受威胁等问题频发，迫使我们必须正视并解决这些难题。本文旨在探讨大数据时代下的计算机网络安全现状，分析潜在威胁，并提出有效防范策略，以期构建更加安全的网络环境。

关键词：大数据时代；计算机；网络安全；防范措施

引言：大数据时代下，计算机网络安全问题日益严峻，涉及个人隐私、企业机密及国家安全。本文分析了大数据时代面临的网络安全挑战，包括黑客攻击、恶意软件、网络钓鱼、系统漏洞及数据泄露等风险，并提出了防范措施，以保障大数据环境下的网络安全。

1 大数据时代下计算机网络安全的重要性

随着信息技术的飞速发展，大数据时代已经悄然而至。在这个时代，数据成为新的资源和资产，其价值和意义日益凸显。然而，与此同时，计算机网络安全问题也日益严重，成为了制约大数据应用和发展的重要因素。因此，探讨大数据时代下计算机网络安全的重要性，对于推动大数据的健康发展具有深远的意义。在大数据时代，计算机网络安全的重要性首先体现在保护个人隐私方面。随着互联网的普及和社交媒体的兴起，个人的生活轨迹、行为习惯、兴趣爱好等都被数字化并存储在计算机系统中。如果这些信息被不法分子窃取或滥用，将对个人隐私造成极大的侵犯。加强计算机网络安全，防止个人信息泄露，是维护个人隐私权益的重要手段。其次，计算机网络安全对于保护企业机密和商业秘密也具有重要意义。在大数据时代，企业的运营数据、客户信息、产品研发等敏感信息都存储在计算机系统中。如果这些信息被泄露或被竞争对手获取，将对企业的商业利益和市场竞争力造成严重的损害。因此，企业必须高度重视计算机网络安全，采取有效的防护措施，确保企业机密和商业秘密的安全。最后，计算机网络安全对于促进大数据的健康发展也具有重要意义。在大数据时代，数据的价值在于其应用和创新[1]。然而，如果计算机网络安全问题得不到有效解决，那么数据的应用和创新将受到严重的制约。只有加强计算机网络安全，才能为大数据的应用和创新提供有力的保障，推动大数据产业的健康发展。

2 大数据时代下的计算机网络安全挑战

2.1 黑客攻击

在大数据时代，黑客攻击成为计算机网络安全领域最为突出的问题之一。黑客通过网络入侵系统，窃取数据、破坏网络服务等手段，给用户和企业带来了巨大的损失。其中，拒绝服务攻击（DDoS）和SQL注入攻击是两种典型的黑客攻击方式。（1）拒绝服务攻击（DDoS）是一种通过发送大量无用的请求，使服务器过载而无法提供正常服务的攻击方式。这种攻击方式如同洪水般汹涌而来，让服务器无法承受，从而导致服务不可用。对于依赖网络服务的企业和个人而言，DDoS攻击无疑是一场灾难。（2）SQL注入攻击则是通过注入恶意SQL代码，绕过身份验证，直接访问或操作数据库，从而窃取或篡改数据库中的数据。这种攻击方式利用了数据库系统的漏洞，以非法手段获取敏感信息，对个人隐私和企业机密构成了严重威胁。

2.2 恶意软件传播

除了黑客攻击外，恶意软件传播也是大数据时代计算机网络安全的一大挑战。计算机病毒、木马、蠕虫等恶意软件在网络中肆意传播，感染其他设备，破坏系统和窃取敏感信息。这些恶意软件如同网络世界的“病毒”，不断变异、进化，其数量、种类和功能都在不断提升，对网络安全构成了严重威胁。恶意软件的传播方式多种多样，如通过电子邮件附件、下载链接、社交媒体等渠道进行传播。一旦用户不慎点击或下载了恶意软件，就可能导致系统被感染，进而引发数据泄露、系统崩溃等严重后果。

2.3 网络钓鱼和社交工程攻击

网络钓鱼和社交工程攻击是大数据时代计算机网络安全的又一挑战，黑客通过伪造合法的网站或伪装成信任的实体，如银行、社交媒体等，诱骗用户点击恶意链

接、泄露密码等敏感信息，从而达到攻击目的。这些攻击手段利用了社会工程学原理，具有较高的隐蔽性和欺骗性。网络钓鱼攻击往往通过发送看似合法的电子邮件或消息，引诱用户点击恶意链接或下载恶意附件。而社交工程攻击则更注重利用人性的弱点，如好奇心、信任等，来诱骗用户泄露敏感信息。这些攻击手段不仅难以防范，而且一旦成功，往往会给用户和企业带来巨大的损失。

2.4 系统漏洞

计算机软件在开发过程中或多或少都存在一些系统性漏洞，这些漏洞如同黑客的“后门”，为黑客攻击提供了便捷途径。黑客可以通过这些漏洞入侵系统，窃取或破坏敏感信息。因此，系统漏洞也是大数据时代计算机网络安全的一大挑战。系统漏洞的存在往往是由于软件开发过程中的疏忽或错误导致的。这些漏洞可能隐藏在软件的各个角落，难以被发现和修复。而黑客则利用这些漏洞，通过精心构造的攻击代码，轻松入侵系统，获取敏感信息或破坏系统。

2.5 数据泄露风险

随着大数据技术的广泛应用，数据的价值日益凸显。然而，与此同时，数据泄露风险也随之加大。一旦网络安全措施不到位，大量个人和企业的敏感数据很容易遭到泄露，导致隐私泄露、商业机密泄露等严重后果。因此，数据泄露风险也是大数据时代计算机网络安全的一大挑战。数据泄露可能发生在数据的收集、存储、传输、处理等各个环节。例如，黑客可能通过攻击数据库服务器获取敏感信息；内部人员可能因疏忽或恶意行为导致数据泄露；恶意软件也可能窃取并传输敏感数据。这些泄露事件不仅会给个人和企业带来经济损失和声誉损害，还可能对国家安全和社会稳定造成严重影响。

3 计算机网络安全防范措施

3.1 强化身份验证

为了有效抵御恶意用户的攻击，我们必须采用更为复杂且难以破解的密码策略。这意味着，密码不仅需要足够长，包含字母、数字和特殊字符的组合，还应避免使用容易被猜测的个人信息，如生日、名字等。除了传统的密码验证方式，多因素身份验证（MFA）技术的应用为数据安全提供了额外的保障层。通过结合指纹识别、面部识别、动态口令等多种验证方式，即使密码被破解，恶意用户也难以绕过其他身份验证环节，从而极大增强了数据的安全性。企业和组织在制定密码策略时，应明确要求用户定期更换密码，并禁止使用弱密码或常见密码[2]。此外，还应通过定期的安全培训和意识提升活动，加深员工对密码安全性的认识，确保他们遵循最佳实践，有效降低密码被破解的风险。

3.2 使用加密技术

面对日益增长的数据量和复杂多变的网络威胁，我们必须依赖先进的加密技术来确保敏感数据的安全性。通过对敏感数据进行加密处理，我们可以构建起一道坚固的安全屏障，使得数据在传输过程中即使被不法分子截获，也无法被轻易解读和利用。为了实现有效的数据加密，企业和个人应当采用可靠的加密算法和工具。这些算法和工具应当经过广泛验证，能够抵御各种已知和未知的攻击手段。还需要定期更新加密算法和密钥，以适应不断变化的网络威胁环境。过时的加密算法和密钥可能会成为安全漏洞，被攻击者利用来破解加密数据。除了采用先进的加密技术，我们还应该关注加密数据的管理和保护。加密数据的存储和访问应当受到严格控制，只有授权人员才能够访问和使用这些数据。此外，我们还应该建立完善的密钥管理机制，确保密钥的安全性和可用性。

3.3 安装防火墙和反病毒软件

防火墙是计算机网络的第一道防线，它通过设置一系列规则，对进出网络的数据包进行检查和过滤，从而阻止未经授权的访问。防火墙还能监控网络流量，及时发现并阻止潜在的攻击行为，确保网络的安全稳定。而反病毒软件则是计算机系统的守护神。它能够定期扫描系统，发现并清除潜藏的病毒、木马和其他恶意软件。在大数据时代，恶意软件的种类繁多，传播速度极快，反病毒软件的实时防护和定期更新功能显得尤为重要。通过不断更新病毒库和扫描算法，反病毒软件能够有效应对新型威胁，保护系统免受侵害。为了确保防火墙和反病毒软件的有效性，我们需要定期进行更新和升级。还需要合理配置防火墙规则，既要有效阻止恶意访问，又要确保正常的网络通信不受影响。这需要我们对网络流量进行深入分析，了解各种应用的通信特点，从而制定出既安全又高效的防火墙策略。

3.4 定期备份数据

在数字化时代，数据已成为企业和个人的核心资产，无论是企业还是个人，都应将此视为数据安全策略的关键环节。通过定期备份，我们可以在数据遭遇意外删除、硬盘故障或恶意软件攻击时，迅速恢复数据，确保业务的连续性和个人生活的正常进行。（1）制定合理的备份计划。这包括确定备份的频率、选择适当的备份介质和存储方式，以及确保备份数据的完整性和可用性。企业可以考虑采用云备份解决方案，以实现数据的

远程存储和快速恢复。个人用户则可以选择外部硬盘或网络存储设备，定期将重要数据备份至其中。（2）还应关注备份数据的安全性。在备份过程中，应采用加密技术保护数据安全，防止敏感信息在传输和存储过程中被窃取或篡改[3]。此外，定期测试备份数据的恢复过程也是至关重要的，以确保在真正需要时能够顺利恢复数据。

3.5 构建完善的数据信息安全体系

构建完善的数据信息安全体系是确保计算机网络安全的核心任务，尤其在大数据时代，数据已成为企业和社会发展的重要资产。为了全面保障数据信息的安全，我们必须对数据的传输和共享全过程实施严格的监管控制。这意味着，我们需要建立一套机制，能够实时监测和识别潜在的危险行为，一旦发现风险，立即采取措施予以制止，防止数据泄露或被恶意利用。加密技术是保护数据信息安全的重要手段，通过对传输的数据信息进行加密，即使数据在传输过程中被截获，也无法被轻易解读，从而有效维护了数据的机密性。我们还需要采用先进的访问控制机制，确保只有授权的用户才能访问特定的数据，防止数据被非法访问或篡改。除了加密和访问控制，我们还需要制定严格的数据安全策略和标准。这些数据安全策略应明确数据的分类和敏感级别，以便对不同级别的数据采取不同的保护措施。还需要确保数据的完整性和可用性，防止数据在传输或存储过程中被篡改或丢失。最后，加强数据备份和恢复能力也是构建完善的数据信息安全体系的重要一环。通过定期备份数据，并在数据丢失或遭到破坏时能够及时恢复，我们可以确保业务的连续性和数据的完整性，从而进一步提升数据信息安全体系的可靠性和有效性。

3.6 引入智能化防御技术

在大数据时代，网络攻击手段日新月异，传统的防御技术已难以全面应对各种复杂的网络威胁。因此，我们必须积极探索并引入新的智能化防御技术，以更有效地保障计算机网络的安全。智能化防御技术的核心在于利用实时监测技术、行为分析算法和机器学习等手段，对网络环境进行全面、深入的地监控和分析。通过这些技术手段，我们可以快速发现和识别网络攻击行为，及时响应和处置威胁事件，从而大大降低网络攻击对系统和数据造成的损害。

此外，智能化防御技术还具备对网络流量、日志文件等进行深度分析的能力[4]。通过自动识别和分类安全威胁，我们可以更准确地判断网络环境的安全状况，并采取有针对性地防御措施。这不仅提高了防御的准确性，还极大地提升了防御效率，使我们能够更有效地应对大数据时代的计算机网络安全挑战。

3.7 持续投入研发与创新

面对大数据时代的计算机网络安全挑战，持续投入研发与创新显得尤为关键。为了有效应对这一挑战，政府和企业必须共同加大在网络安全技术研发方面的投入力度。这不仅仅意味着资金的支持，更包括政策引导、人才培养等多个维度的全面投入，共同为网络安全技术的发展创造一个良好的环境。在这个过程中，鼓励创新型人才和团队开展网络安全技术研究与应用是至关重要的。这些人才是推动技术进步的重要力量，他们的创新思维和实践能力将为网络安全领域带来新的突破和解决方案。因此，我们应该积极为他们提供必要的支持和资源，包括研究资金、实验设备、数据资源等，以激发他们的创新潜力，并促进他们的研究成果在实际中得到应用和推广。通过持续投入研发与创新，我们可以不断提升网络安全技术的水平和能力，有效应对大数据时代带来的网络安全挑战。

结语

综上所述，大数据时代下的计算机网络安全是一项复杂而艰巨的任务，需要政府、企业和个人共同努力。通过实施严格的身份验证、数据加密、加强数据备份、引入智能化防御技术并持续研发投入，我们能够有效应对各种网络安全挑战，保护个人隐私、企业利益和国家安全。未来，随着技术的不断进步和国际合作的加强，我们有信心构建一个更加安全、可信的大数据环境。

参考文献

[1]敬甫盛.大数据时代下计算机网络安全及防范措施探究[J].网络安全技术与应用,2022(3):66-67.

[2]马浩.计算机网络安全面临的威胁及其防范措施[J].数字通信世界,2020(4):107,121.

[3]曾志勇.计算机网络安全在大数据系统的应用[J].技术与市场,2019,26(5):124-125.

[4]张万强.大数据时代计算机网络安全防范策略分析[J].百科论坛电子杂志,2020(15):61.