大数据背景下数据治理的网络安全措施

李福峰
深圳市福利彩票发行中心　广东　深圳　518000

摘　要：在大数据背景下，数据治理的网络安全措施是保障数据安全的关键。数据分类和标记可以帮助更好地管理和保护数据的安全性。恶意行为检测和预防可以及时发现和阻止恶意行为的发生。安全漏洞管理与修复可以识别和修复系统中的安全漏洞。这些网络安全措施的实施将提高数据治理的安全性和有效性。

关键词：大数据；数据治理；安全措施

1 大数据背景下的数据治理

大数据背景下的数据治理是组织中不可或缺的一环，它涉及到数据的整个生命周期，包括数据的收集、存储、处理、分析和利用。随着数据量的不断增长，数据治理的难度和挑战也随之增加。本文将探讨大数据背景下的数据治理及其重要性。大数据时代的到来，使得组织中数据的产生和利用方式发生了巨大的变化。组织需要收集并处理大量的数据，以支持决策制定、提高业务效率和客户满意度。然而，随着数据量的增加，数据的复杂性和多样性也相应提高，这给数据治理带来了新的挑战。数据治理是指组织中数据的战略规划、管理、监督和控制的系统化过程。这个过程需要遵循一定的原则和标准，以确保数据的合规性、安全性和可靠性。在大数据背景下，数据治理变得更加重要，因为它可以帮助组织解决以下问题：（1）数据质量：大数据背景下，数据的质量是数据治理的核心问题之一。由于数据来源的多样性，数据的完整性、准确性和一致性可能存在问题。通过数据治理，组织可以识别并解决这些问题，从而提高数据的质量。（2）数据安全：大数据时代也带来了数据泄露和隐私保护的挑战。数据治理可以帮助组织建立完善的安全机制，包括数据加密、访问控制和权限管理等，以确保数据的安全性和隐私保护[1]。（3）数据利用：在大数据背景下，数据的利用变得更加重要。通过合理的数据治理，组织可以更好地利用数据进行决策制定、市场分析和业务优化等。总之，大数据背景下的数据治理对于组织的成功至关重要。通过建立完善的数据治理体系，组织可以更好地管理和利用大数据，提高业务效率和客户满意度，从而获得更大的竞争优势。

2 大数据环境下的网络安全威胁

大数据环境下的网络安全威胁是日益严重的挑战。随着组织对大数据的依赖程度不断增加，网络安全问题也变得越来越突出。（1）数据泄露和黑客攻击：大数据包含着大量的敏感信息，如个人数据、财务数据和业务数据等。黑客可以通过各种手段，如恶意软件、钓鱼攻击和社交工程等，获取这些数据并将其用于不良目的。组织必须采取有效的安全措施来保护数据，避免遭受泄露和黑客攻击。（2）高级持久性威胁：一些黑客组织和大公司之间存在雇佣关系，他们会利用各种技术手段来入侵组织系统，并长期潜伏在其中，等待合适的时机进行攻击。这些威胁行为通常很难被检测和防御，组织需要采取更加先进的安全技术来应对。（3）数据滥用：在大数据环境下，数据的价值越来越高，但也存在着被滥用的风险。一些组织可能会将数据用于不道德或非法的目的，如身份盗用、网络诈骗等。组织必须建立完善的数据管理制度，确保数据的合法使用和保护。（4）拒绝服务攻击：一些黑客组织通过大量的请求来攻击服务器，使其无法正常响应合法请求。这种攻击通常会导致组织的服务中断和业务中断，给组织带来严重的损失。组织需要建立有效的防御机制，避免遭受这种攻击的影响[2]。

3 网络安全在数据治理中的重要性

网络安全在数据治理中扮演着至关重要的角色。随着组织对大数据的依赖程度不断增加，网络安全问题也变得越来越突出。第一，保护数据安全：网络安全可以保护数据免受未经授权的访问、修改或泄露。通过加密、访问控制和身份验证等安全措施，组织可以确保数据的机密性和完整性，避免数据泄露和黑客攻击。第二，保障业务连续性：网络安全可以帮助组织保障业务的连续性。在遭受攻击或故障时，组织可以通过备份和恢复措施快速恢复数据和系统，确保业务的正常运行。第三，遵守法规要求：随着对数据保护的法规不断增多，组织需要遵守各种法规要求来保护个人隐私和敏感信息。网络安全可以帮助组织遵守相关法规，确保数据的合规性和合法性。第四，提高组织声誉：网络安全可以保护组织的声誉不受损害。如果发生数据泄露等安全

事件，这可能会对组织的声誉和客户信任度产生负面影响。因此，保障网络安全可以帮助组织维护良好的声誉和客户信任度[3]。第五，降低风险和成本：网络安全可以帮助组织降低风险和成本。通过预防安全事件的发生，组织可以避免遭受潜在的损失和罚款等成本。如果发生安全事件，有效的网络安全措施可以帮助组织快速响应并减少损失。总之，网络安全在数据治理中扮演着至关重要的角色。通过建立完善的安全管理体系和采用先进的安全技术，组织可以保护数据的安全、保障业务的连续性、遵守法规要求、提高组织声誉并降低风险和成本。因此，组织必须重视网络安全在数据治理中的重要性，并采取有效的措施来保障数据的机密性、完整性和安全性。

4 大数据背景下数据治理的网络安全措施

4.1 数据分类和标记

在大数据背景下，数据治理的网络安全措施是组织中不可或缺的一环。其中，数据分类和标记是保障数据安全的重要措施之一。数据分类是指将数据进行归类和分组，以便更好地管理和保护数据。通过对数据进行分类，组织可以更好地了解数据的性质和用途，并为不同类型的数据制定不同的安全策略。例如，将敏感数据进行单独的分类，并为其制定更加严格的访问权限和控制措施，可以更好地保护个人隐私和组织机密。数据标记是指为数据添加标签或标识，以便更好地识别和管理数据。通过数据标记，组织可以记录数据的来源、用途、敏感程度等信息，并为数据的处理、存储和传输提供更加准确和可靠的管理依据。例如，在数据传输过程中，可以使用加密算法对数据进行加密，并在数据接收端进行解密，以确保数据的安全性和完整性[4]。

4.2 数据加密保护

数据加密是一种将数据转化为不易被他人理解的形式的过程，只有持有特定密钥的人才能解密和理解原始数据。在大数据环境下，数据加密可以应用于数据的存储、传输和使用的整个生命周期，以保障数据的机密性和完整性。

在实施数据加密保护的过程中，组织需要采取以下措施：根据数据的重要性和敏感性，确定需要对哪些数据进行加密，以及需要采取哪种加密算法和密钥管理方案。选择适合其数据特性和加密需求的加密算法。常用的加密算法包括对称加密算法（如AES-256）和非对称加密算法（如RSA）。密钥是数据加密的关键因素之一，因此组织需要采取有效的措施确保密钥的安全性和保密性。这包括使用密码保护密钥、将密钥存储在安全的密钥管理系统中，以及定期更换密钥等。根据确定的加密需求和选择的加密算法，实施相应的加密方案。这包括对数据进行加密、解密、加盐哈希等操作[1]。建立监控和检测机制，及时发现和处理任何异常或潜在的攻击行为，以确保数据加密保护的有效性和安全性。

4.3 访问控制和身份验证

随着数据量的增加和数据的重要性，确保只有经过授权的用户可以访问和操作数据成为一项重要任务。访问控制是通过制定合理的权限策略和访问规则，控制用户对数据的访问权限。可以基于用户身份、角色、需求和数据敏感性等因素来设计和管理访问控制策略。通过实施细粒度的访问控制和权限管理，可以确保只有合法授权的用户能够访问和操作数据，有效地防止未经授权的数据泄露和滥用。身份验证是确认用户身份的过程，用于确保用户所提供的身份信息是真实有效的。常用的身份验证方式包括密码、指纹识别、人脸识别等。在大数据环境下，为了加强身份验证的安全性，可以采用多因素身份认证，结合多个因素来验证用户身份，提高身份验证的可靠性和安全性。通过访问控制和身份验证的措施，可以有效保护数据的安全性和隐私性。只有合法的用户能够访问和操作数据，降低了非授权访问和滥用的风险[2]。同时，通过多因素身份认证等技术，可以提高身份验证的准确性和可靠性，避免伪造和冒用身份。

4.4 恶意行为检测和预防

随着数据的快速增长和复杂性，恶意行为对网络安全构成了严重的威胁。为了保障数据安全，需要采取有效的措施来检测和预防恶意行为。恶意行为检测是指利用各种技术手段来识别和监测潜在的威胁和攻击。在大数据环境下，可以利用数据挖掘、机器学习和行为分析等技术，分析海量的数据，识别异常行为和恶意活动。通过对网络流量、用户行为、系统日志等数据的实时监测和分析，可以及时发现并预警各种网络攻击、数据泄露和恶意程序等问题。恶意行为预防是指利用各种措施和策略，主动防止和阻止恶意行为的发生。其中包括以下几个方面：（1）统一访问控制管理：建立统一标准的访问控制策略，监控和管理用户对数据和系统的访问权限，防止非法的访问和篡改[3]。（2）机器学习与数据分析：应用机器学习算法和数据分析技术，建立模型来识别恶意行为的特征，并实时检测和预防潜在的威胁。（3）实时监控和预警系统：建立实时监控和预警系统，对网络活动和用户行为进行监测和分析，并能够及时发出警报和采取应对措施。（4）快速漏洞修复机制：及时更新和修补系统漏洞，防止黑客利用漏洞进行攻击和入侵。

4.5 安全漏洞管理与修复

随着大数据规模的增长和复杂性的提高，安全漏洞可能导致数据泄露、系统瘫痪、恶意攻击等严重后果。因此，及时发现、管理和修复安全漏洞至关重要。定期对系统、应用程序、数据库等进行漏洞扫描，识别潜在的安全漏洞。可以利用安全审计工具、漏洞扫描工具和安全信息和事件管理系统等，对系统进行全面的安全评估。通过对扫描结果的分析和评估，确定需要修复的重要漏洞。建立一套快速反应、快速修复的机制，及时修复系统中发现的安全漏洞。修复措施可以包括修补漏洞、升级安全补丁、安装补丁、强化访问控制等。关键是要及时响应漏洞修复的请求，并确保修复措施的有效性。加强员工的安全意识教育和培训，让员工了解常见的安全漏洞和攻击手段，如社会工程学攻击、恶意软件、钓鱼等。同时，提供实时的安全动态和建议，帮助员工及时处理和修复安全漏洞[4]。建立持续监控机制，及时发现安全事件和漏洞，并采取相应的措施进行修复。同时，跟踪和了解最新的安全漏洞信息和防护措施，及时更新和升级现有的防护措施，提高数据治理的安全性。

5 未来网络安全与数据治理的发展趋势

随着科技的不断发展和大数据时代的到来，网络安全和数据治理面临着新的挑战和机遇。未来，网络安全和数据治理将继续发展和演变，以应对日益复杂和智能化的网络威胁。（1）人工智能与机器学习的应用：未来，人工智能和机器学习将在网络安全和数据治理领域扮演越来越重要的角色。通过利用机器学习算法和人工智能技术，可以自动化地分析和识别潜在的网络攻击、异常行为和安全威胁。同时，也可以实现智能化的数据治理，提高对数据质量、隐私和合规性的管理和保护。（2）区块链技术的应用：区块链技术的出现为网络安全和数据治理带来了新的机遇。区块链的分布式和去中心化特性能够提高数据的安全性和可信度，防止数据篡改和伪造。未来，区块链技术有望应用于身份验证、数据交换、数据溯源等方面，为网络安全和数据治理提供更加安全和可靠的解决方案。（3）数据隐私和合规性的保护：在大数据时代，隐私和合规性保护成为网络安全和数据治理的重要议题。未来，将对个人数据的收集、存储和使用等方面提出更加严格的要求。数据隐私保护的技术和法规将进一步完善和发展，例如差分隐私技术、数据保护法规等，以确保数据的隐私权和合规性[1]。（4）边缘计算与边缘安全：随着物联网的迅速发展，边缘计算和边缘安全将成为未来网络安全和数据治理的热点。边缘计算将数据的处理和存储推向网络边缘，减少了数据传输的延迟和网络风险。同时，边缘安全将边缘设备和传感器与安全系统结合起来，加强对边缘网络的安全保护。

结束语

在大数据时代，数据已经成为组织的核心资产之一，因此数据治理的网络安全措施是组织不可或缺的一部分。通过采取有效的数据治理措施，组织可以保护数据的安全性和完整性，提高业务的正常运行和可靠性。同时，组织还需要不断更新和优化网络安全措施，以应对不断变化的网络安全威胁和挑战。总之，大数据背景下数据治理的网络安全措施是组织成功的重要保障之一。

参考文献

[1]赵广磊.大数据背景下的计算机网络信息安全及防护措施[J].电子世界，2018（15）：43+45.

[2]邓辉.大数据背景下的计算机网络信息安全及防护措施[J].通讯世界，2018（07）：58-59.

[3]王晓栋,郁文娟.大数据环境下的数据安全治理研究[J].信息通信技术与政策,2021(3):58-63.

[4]王海燕,张华.大数据时代下数据治理的隐私保护[J].信息通信技术与政策,2021(2):69-73.

[5]杨柳青,王晓琳.大数据背景下的网络信息保护与治理研究[J].软件工程,2021(1):18-24.