企业大数据网络安全防护思路

杨家全
浙江信网真科技股份有限公司　浙江　杭州　310051

摘　要：在大数据时代的浪潮下，企业迎来了数据安全的全新考验。大数据如同一把双刃剑，既赋能企业高效运营与精准决策，又潜藏着不可忽视的安全风险。面对这一挑战，企业必须高度重视大数据网络安全，警觉数据泄露、非法入侵等威胁。为此，我们需深入剖析现存问题，从多个层面出发，打造立体化的安全防护网。通过综合施策，确保企业在享受大数据红利的同时，也能守住网络安全的底线。

关键词：大数据安全；网络安全；企业数据保护；防护

引言

在大数据的浩瀚海洋中，企业如同勇敢的航海者，探寻着商业的宝藏。然而，这片富饶的数据之海，亦暗藏着无数的风险与挑战。数据的机密性、完整性和可用性，如同航海中的指南针，指引着企业安全前行的方向。在这个信息爆炸的时代，如何守护这些宝贵的数据资产，确保它们在风浪中安然无恙，已成为企业发展的关键。本文将深入剖析大数据网络安全的重要性及其面临的挑战，并探寻加强防护的有效思路。

1 企业大数据网络安全的重要性

在数字化转型的时代背景下，大数据技术的快速发展和广泛应用为企业带来了巨大的商业价值和发展机遇。然而，与此同时，大数据网络安全问题也日益凸显，成为企业不得不面对的重要挑战。大数据网络安全对于企业的重要性不言而喻，它直接关系到企业的商业机密保护、客户信任度以及业务连续性等多个关键方面。首先，大数据网络安全关乎企业的商业机密保护。在大数据分析中，企业会收集和存储大量的商业数据，包括产品信息、市场趋势、竞争策略等。这些数据对于企业的运营和发展具有极高的价值，一旦被泄露或被竞争对手获取，将可能导致企业遭受重大损失。保护大数据网络的安全，就是保护企业的核心竞争力和商业利益。其次，大数据网络安全影响客户信任度。在数字化经济中，客户数据是企业进行精准营销和提供个性化服务的基础。然而，如果企业的大数据网络存在安全隐患，客户的个人信息就可能被泄露，进而引发客户对企业的不信任感。这种不信任感不仅会损害企业的品牌形象，还可能导致客户流失，对企业的长期发展造成不利影响。最后，大数据网络安全关乎业务连续性。在现代企业中，大数据已经渗透到业务的各个环节，从市场调研、产品研发到供应链管理、客户服务等。如果大数据网络遭受攻击或出现故障，将可能导致业务中断，甚至引发连锁反应，影响整个企业的运营。所以，确保大数据网络的安全稳定运行，对于保障企业业务的连续性至关重要[1]。

2 企业大数据网络安全存在的主要问题

2.1 数据泄露风险

在大数据环境中，数据泄露风险尤为突出。大数据中蕴含着大量敏感信息，这些信息包括但不限于客户资料、交易数据、市场分析报告、产品研发细节等。这些信息一旦泄露，不仅会对企业的商业利益造成直接损害，还可能危及客户的个人隐私，甚至导致法律责任。数据泄露的具体表现有多种，（1）不安全的存储和传输。如果大数据存储在未加密或加密强度不足的服务器上，或者在传输过程中未采用安全的通信协议，那么数据就很容易在传输或存储过程中被截获。（2）内部人员泄露。有时数据泄露并非来自外部攻击，而是由于内部员工的不当行为或疏忽；例如，员工可能将敏感数据泄露给未经授权的第三方，或者在非安全的环境下讨论敏感信息。（3）供应链风险。在大数据处理过程中，可能涉及到多个供应商和合作伙伴；如果供应链中的某个环节存在安全隐患，那么整个大数据系统都可能受到威胁。

2.2 数据篡改与破坏

数据篡改与破坏是大数据网络安全的另一大威胁。恶意攻击者可能会通过网络入侵、恶意软件植入等手段对数据进行篡改或破坏，以达到混淆视听、误导决策或破坏企业运营的目的。数据篡改与破坏的具体表现包括：（1）恶意注入虚假数据。攻击者可能向大数据系统中注入虚假数据，以干扰企业的正常分析和决策过程；例如，在金融领域，虚假的交易数据可能导致企业做出错误的投资决策。（2）数据删除或破坏。除了篡改数据外，攻击者还可能直接删除或破坏关键数据，使企业无

法正常使用这些数据进行分析和决策；这种破坏可能是有针对性的，也可能是随机的。（3）勒索软件与加密货币挖矿。近年来，勒索软件和加密货币挖矿活动日益猖獗；这些恶意软件可能会感染大数据系统，对数据进行加密或破坏，并以此为要挟向企业索取赎金。

2.3 非法访问与滥用

非法访问与滥用大数据资源是网络安全领域的一个常见问题，在大数据环境中，未经授权的访问和滥用可能导致严重的后果，如企业资产损失、知识产权泄露以及法律纠纷等。非法访问与滥用的具体表现有：（1）越权访问。攻击者可能利用系统漏洞或弱密码等手段获取不应有的访问权限，从而浏览、复制或修改敏感数据；这种越权访问可能是有意的，也可能是无意的。（2）数据滥用。即使访问是合法的，但如果数据被用于不当目的或未经授权的方式，也构成数据滥用；例如，员工可能将客户数据用于个人目的，或者将敏感信息泄露给竞争对手。（3）账号共享与盗用。在某些情况下，员工可能共享自己的账号给他人使用，或者账号被盗用。这种情况下的非法访问和滥用往往更难追踪和防范。

2.4 系统脆弱性与漏洞

大数据系统本身可能存在脆弱性和漏洞，这些安全隐患如不及时发现和修补，将给攻击者留下可乘之机。系统脆弱性与漏洞的具体表现包括：（1）软件缺陷与漏洞。大数据系统通常建立在复杂的软件架构之上，这些软件中可能存在未被发现的缺陷和漏洞；攻击者可以利用这些漏洞绕过安全措施，直接访问或篡改数据。（2）配置错误。大数据系统的配置可能非常复杂，一旦配置错误，就可能导致安全漏洞；例如，错误的访问控制设置可能允许未经授权的用户访问敏感数据。（3）硬件和基础设施风险。除了软件层面的风险外，硬件和基础设施也可能存在安全隐患；例如，物理服务器的安全防护不足、网络通信设备的漏洞等都可能成为攻击者的突破口[2]。

3 加强企业大数据网络安全的防护思路

3.1 强化访问控制与权限管理

建立完善的访问控制机制和权限管理体系是大数据网络安全的首要防线。这一体系的建立，能够确保数据只被那些经过明确授权的人员访问，从而大大降低数据泄露或被滥用的风险。（1）用户身份验证是这一体系的基础。传统的用户名和密码验证方式虽然简单易行，但在安全性方面存在不足。为了提高安全性，多因素身份验证被越来越多地采用。这种方式结合了两种或更多的验证手段，如手机短信验证、生物识别等，确保了只有真正的用户才能通过验证，大大提高了账户的安全性。（2）基于角色的访问控制（RBAC）为企业提供了一种更为灵活和高效的权限管理方式。在大型企业中，员工众多，职责各异。RBAC允许企业根据员工的角色和职责来为其分配相应的数据访问权限。这样，不仅可以确保每个员工都能够获取到完成工作所需的数据，还可以防止他们访问到与其工作无关的数据。这种精细化的权限管理方式，既满足了员工的工作需求，又确保了数据的安全性。（3）审计跟踪是这一体系中不可或缺的一部分。通过详细记录用户对数据的每一次访问和操作，企业可以在数据出现异常或被非法访问时迅速作出反应。这些记录不仅可以帮助企业快速定位问题的根源，还可以为后续的法律追责提供有力的证据。

3.2 数据加密与隐私保护

企业大数据网络安全的防护思路中，数据加密与隐私保护是两大关键支柱；这两者相辅相成，共同构建了企业数据安全的坚固屏障。（1）数据加密，作为一种基础的安全措施，其重要性不言而喻。在这个信息化的时代，数据就如同企业的生命线，一旦泄露或被非法利用，后果不堪设想。通过数据加密，即使是最敏感的信息，也能在传输和存储过程中得到强有力的保护。不同的加密方式，如对称加密、非对称加密或混合加密，都各有其特点和应用场景。企业应根据自身的实际情况，选择最适合的加密方法。而密钥的管理同样不容忽视，一个完善的密钥管理体系能确保密钥的安全性、完整性和可用性，从而避免因密钥泄露而引发的安全风险。（2）隐私保护在大数据时代显得尤为重要。随着数据分析技术的日益精进，如何在挖掘数据价值的同时保护用户隐私，成为了一个亟待解决的问题。差分隐私技术的出现，为这一难题提供了有效的解决方案。通过向数据中注入适量的噪声，既保护了用户隐私，又不影响数据的统计分析。这种微妙的平衡，正是差分隐私技术的魅力所在。而联邦学习等技术则更进一步，它们能在不共享原始数据的情况下进行模型训练，这无疑为企业提供了一种全新的数据安全和隐私保护思路[3]。

3.3 安全监测与应急响应

（1）安全监测是预防安全威胁的第一道防线。利用安全信息和事件管理（SIEM）系统，企业可以实时地收集和分析网络中的各类安全日志和事件信息。这些日志和事件信息如同大数据网络中的“脉搏”，能够实时反映出网络的安全状况。通过设定合理的规则阈值，SIEM系统可以在发现任何异常行为或潜在威胁时，立即触发警报，使企业能够在第一时间做出响应。（2）制定详尽的应急响应计划。该计划应明确在发生不同类型的安全

事件时，应采取的处置流程、责任人以及预期的恢复时间等；这样的计划，企业在面对安全事件时就不会手忙脚乱，而是能够有条不紊地进行应对。（3）为了提高应急响应的效率和准确性，企业需要组建专门的应急响应团队，并定期进行培训和演练。这样不仅可以提升团队的实战能力，还可以确保在真实的安全事件中，团队能够迅速进入状态，有效地进行处置。（4）与专业的网络安全机构建立合作关系也是非常重要的。这些机构可以为企业提供最新的安全情报、技术支持以及应急响应的协助，从而大大提升企业应对安全威胁的能力。

3.4 安全培训与意识提升

在网络安全领域，技术固然重要，但人的因素同样不容忽视；再先进的技术也无法完全防止人为的失误。（1）定期开展网络安全培训活动是企业提升员工安全意识和技能的有效途径。这样的培训应该涵盖网络安全的各个方面，从密码安全、社交工程防范，到钓鱼邮件的识别与处理等。密码安全是网络安全的基础，一个强密码能大大增加攻击者的破解难度。社交工程则是近年来网络安全领域出现的新型威胁，员工需要学会识别并防范各种社交工程手段，避免在不知不觉中泄露企业敏感信息。（2）模拟演练和案例分析也是非常实用的教学方法。通过模拟网络攻击场景，员工可以在一个相对安全的环境中体验真实的网络威胁，从而更深刻地理解安全的重要性。案例分析则可以让员工从实际的安全事件中汲取教训，了解各种安全威胁的具体形式和防范措施。（3）提升员工安全意识还需要持续的努力。企业可以通过内部宣传、定期的安全知识竞赛等方式，不断强化员工的安全意识。更重要的是，企业应将网络安全纳入企业文化建设中，让员工从入职开始就明白网络安全的重要性，并在日常工作中时刻保持警惕[4]。

3.5 技术创新与持续改进

（1）网络技术不断进步，企业需要密切关注最新的网络安全技术和趋势。新的防护手段和工具不断涌现，为企业提供了更多的选择。例如，近年来兴起的人工智能和机器学习技术，在大数据网络安全领域具有广阔的应用前景。这些技术可以对大数据网络进行实时监控和分析，通过数据挖掘和模式识别，及时发现潜在的安全威胁，从而提高安全防护的主动性和准确性。（2）除了引入新技术，企业还需要定期对现有的安全策略进行评估和调整。网络安全是一个动态的过程，没有一劳永逸的解决方案。因此，企业需要定期进行模拟攻击测试、渗透测试等，以检验现有防护措施的有效性；通过这些测试，企业可以发现安全策略中的漏洞和弱点，并及时进行调整和加强。（3）积极参与网络安全相关的行业交流和合作活动也是提升企业安全防护能力的重要途径。通过与其他企业和机构的交流，企业可以及时了解最新的安全情报和技术支持，以便更好地应对未知的安全威胁。同时，通过共同研发新技术、分享经验等方式，企业还可以促进行业整体的安全水平提升，形成共赢的局面。

结语

在数字化转型的征途上，企业大数据网络安全如同一座坚固的灯塔，指引着企业在数据海洋中稳健前行。通过构建多层次、多维度的安全防护体系，我们能够抵御外部威胁，确保数据的纯净与安全。未来，随着技术的不断进步，我们应继续加强网络安全的防范与创新，让大数据成为企业发展的强大引擎，而非潜在的风险源。只有如此，我们才能在数字化的浪潮中乘风破浪，开创更加辉煌的未来。

参考文献

[1]朱芃璇.大数据时代企业网络安全防护策略分析[J].数字通信世界,2020(9):114-115.

[2]赖显凌.大数据时代企业网络安全防护策略分析[J].电脑迷,2021(35):34-36.

[3]靳峰.大数据时代背景下企业网络信息安全问题及防护探讨[J].现代工业经济和信息化,2022,12(2):124-125,129.

[4]加永次仁.企业网络安全管理问题浅析[J].通讯世界,2020,27(1):81-82.