

计算机数据库安全管理研究

胡 斌 杨 勤

航宇救生装备有限公司规划发展部 湖北 襄阳 441003

摘要: 计算机数据库系统,是指以计算机系统为平台而形成的数据处理空间,重点在于为程序所生成的数据进行保存、调动等。从中可以看出,数据库系统中存储了用户程序使用的所有信息,而其中也可以涉及个人的财务信息,甚至还有组织机关的商务机密,所以保证数据安全是计算机数据库系统管理人员的基本责任。

关键词: 计算机;数据库;安全管理

引言:计算机数据库系统的安全性问题,已变成了当前计算机技术发展中必须面对的主要课题之一,数据库系统既要确保信息的共享性,也要有相应的安全。所以,为保证计算机数据库系统可以更好的为大家服务,应该针对数据库系统目前所出现的缺陷,积极采取相应的对策,持续加以改进与完善,保证计算机系统的安全。

1 计算机网络数据库安全管理的必要性

由于计算机技术的飞速发展,计算机早已成为了现代社会中不可或缺的重要组成部分。在这个信息时代,数据和信息已经成为了企业和个人最宝贵的财富。然而,随着网络技术的普及和应用,网络安全问题也日益严重。数据库作为企业的核心数据存储和管理平台,其安全性对企业的正常运营和信息安全具有重要意义。因此,加强计算机网络数据库安全管理具有重要的必要性。保障企业核心数据的安全。数据库中存储着企业的核心数据,如客户信息、财务数据、生产数据等。这些数据的安全性直接关系到企业的竞争力和发展。一旦数据库遭受攻击,可能导致数据泄露、篡改或丢失,给企业带来巨大的经济损失和声誉损害。通过加强数据库安全管理,可以有效防止这些风险的发生,确保企业核心数据的安全。维护企业的商业利益。在市场竞争激烈的环境下,企业需要通过各种手段获取竞争优势。如果企业的数据库安全无法得到保障,竞争对手可能会利用黑客技术窃取企业的商业秘密,从而削弱企业的竞争力^[1]。通过加强数据库安全管理,可以有效防止商业秘密泄露,维护企业的商业利益。保护用户的隐私权益。随着互联网的普及,越来越多的用户将自己的个人信息存储在网络数据库中。这些信息包括姓名、身份证号、电话号码、家庭住址等。如果数据库安全管理不善,这些敏感信息可能会被泄露,给用户的隐私权益带来严重威胁。加强数据库安全管理,可以有效保护用户的隐私权益,提高用户对网络服务的信任度。共同构建一个安全、健康、有序

的网络环境。

2 计算机数据库安全管理现状

随着信息技术的飞速发展,计算机数据库已经成为了企业、教育等各个领域的核心应用系统。然而,数据库安全问题也日益凸显,成为制约数据库应用发展的重要因素。从技术层面来看,数据库安全技术已经取得了很大的进步。传统的数据库安全技术主要包括访问控制、加密技术、备份与恢复等。随着技术的发展,数据库安全技术也在不断创新。数据库防火墙、数据泄露防护(DLP)等新型安全技术应运而生。这些技术的出现,大大提高了数据库的安全性能,降低了安全风险。从管理层面来看,数据库安全管理意识逐渐提高。越来越多的企业和组织开始重视数据库安全问题,制定了一系列严格的数据库安全管理制度。例如,定期进行安全审计、建立安全应急响应机制等。这些措施有助于及时发现和处理数据库安全隐患,降低安全风险。尽管数据库安全管理取得了一定的成果,但仍然存在一些问题。数据库安全技术的普及程度不高。许多企业在实际应用中,仍然采用传统的安全技术,如用户名和密码登录、SQL注入攻击等。这些技术在面对高级攻击时,往往显得力不从心。部分企业对数据库安全管理的重视程度不够。只有不断创新,才能使数据库安全技术更好地适应不断变化的安全威胁;提高企业和组织的数据库安全意识,加强安全管理制度建设^[2]。通过定期进行安全培训、演练等活动,提高员工对数据库安全的认识,形成良好的安全文化;加强数据库安全人才培养。企业应加大对数据库安全人才的培养力度,提高人才队伍的整体素质;加强国际合作与交流。通过与国际同行的合作与交流,学习借鉴先进的数据库安全管理经验,提升我国数据库安全水平。计算机数据库安全管理虽然取得了一定的成果,但仍然面临着诸多挑战。我们需要从技术、管理、人才等多方面入手,全面提升数据库安全管理水

平, 确保数据库安全稳定运行。

3 计算机数据库安全管理策略

3.1 加强访问控制

随着信息技术的飞速发展, 计算机数据库已经成为了企业和个人存储、管理和处理数据的重要工具。然而, 数据库安全问题也日益凸显, 如何确保数据库的安全性和完整性成为了亟待解决的问题。用户身份认证是指通过验证用户的身份信息来确定用户是否具有访问数据库的权限。为了保证数据库的安全, 应该采用强密码策略, 要求用户设置复杂且不易猜测的密码。还可以采用多因素身份认证技术, 如短信验证码、指纹识别等, 以提高安全性。访问控制是指对用户数据库的操作进行限制和管理, 包括对用户的登录、查询、更新、删除等操作进行权限控制。在实现访问控制时, 可以采用基于角色的访问控制(RBAC)模型, 将用户分配到不同的角色中, 根据角色的权限来限制用户的访问范围。还可以通过设置数据访问权限来限制用户对特定数据的访问, 防止未经授权的数据泄露和篡改。审计是指对数据库的各类操作进行记录和分析的过程, 通过对审计日志的分析, 可以发现潜在的安全隐患和违规操作。企业和组织应该定期开展数据库安全培训, 提高员工的安全意识和技能。培训内容应包括数据库安全的基本知识、常见的安全威胁和防范措施、安全操作规范等。通过培训, 员工可以更好地了解数据库安全的相关知识, 提高自身的安全防护能力。加强计算机数据库安全管理策略, 需要从多个方面入手, 包括建立完善的用户身份认证机制、实现对数据库的访问控制、加强对数据库操作的审计和监控以及加强数据库安全教育和培训等。只有这样, 才能有效地保障数据库的安全和完整性, 为企业和个人提供可靠的数据支持。

3.2 完善安全审计

随着信息技术的发展, 数据库已经成为企业的核心资产之一, 其安全性直接关系到企业的生产经营和声誉。因此, 制定并实施有效的数据库安全管理策略至关重要。明确安全审计的目标和范围。安全审计的主要目标是评估数据库的安全性, 发现潜在的安全隐患, 为企业提供改进措施。审计范围应涵盖数据库的各个方面, 包括硬件、软件、网络、人员等。通过对这些方面的全面审计, 可以确保数据库在各个方面都达到了预期的安全标准。建立完善的审计制度和流程。企业应制定详细的数据库安全审计制度和流程, 明确审计的目的、方法、周期、责任人等内容。要确保审计工作的独立性和客观性, 避免因人为因素导致的误判。还应定期对审计

制度和流程进行审查和更新, 以适应不断变化的安全环境。加强审计人员的培训和素质提升。数据库安全审计是一项专业性很强的工作, 需要具备一定的专业知识和技能。企业应加强对审计人员的培训, 提高其对数据库安全的认识和理解^[3]。要关注审计人员的心理素质和职业道德, 确保其在执行审计任务时能够保持客观、公正的态度。利用先进的技术手段提高审计效率。随着信息技术的发展, 越来越多的先进技术被应用于数据库安全审计领域。完善计算机数据库安全管理策略需要从多个方面入手, 包括明确审计目标和范围、建立完善的审计制度和流程、加强审计人员的培训和素质提升、利用先进技术提高审计效率以及加强与其他部门的合作与沟通。通过这些措施的实施, 可以有效地提高数据库的安全性, 保障企业的生产经营和声誉。

3.3 加强物理安全

计算机数据库安全管理策略是确保数据安全和完整性的关键。除了加强物理安全外, 还有一些其他的策略可以采取来保护数据库免受未经授权的访问和恶意攻击。实施强密码策略是保护数据库的重要措施。密码应该足够复杂, 包含字母、数字和特殊字符, 并且定期更换密码。还可以使用双因素身份验证来增加账户的安全性。限制对数据库的访问权限也是必要的。只有经过授权的人员才能访问数据库, 并且他们只能访问他们需要的数据。通过角色基础的访问控制(RBAC)可以有效地管理用户权限, 确保只有合适的人员能够访问敏感信息。备份应该定期进行, 并且存储在安全的地方, 以防止数据被破坏或丢失。还可以使用灾难恢复计划来应对意外事件, 如硬件故障或自然灾害。加密数据库中的数据也是保护数据安全的有效方法。可以使用加密算法对敏感数据进行加密, 确保即使数据被盗取或泄露, 也无法被未经授权的人读取和使用。通过监控数据库的活动并记录日志, 可以及时发现异常行为或潜在的威胁。这些日志可以用于追踪和调查任何未经授权的访问或数据泄露事件。员工应该了解如何创建强密码、避免点击可疑链接或下载未知附件等常见的网络攻击方式。通过提供培训和教育, 可以提高员工对数据库安全的认识, 减少人为错误和疏忽导致的安全漏洞。通过实施强密码策略、限制访问权限、定期备份、加密数据、监测和审计以及培训员工等措施, 可以全面保护数据库免受未经授权的访问和恶意攻击。

3.4 加密存储数据

计算机数据库安全管理策略是确保数据安全和完整性的关键。其中, 加密存储数据是一种有效的保护手

段,可以防止未经授权的访问和篡改。加密存储数据可以提供数据的保密性。通过使用加密算法,可以将原始数据转换为密文,只有拥有密钥的人才能解密并读取数据。这样即使数据被窃取,黑客也无法直接获取有用的信息。加密存储数据可以提供数据的完整性。在数据传输过程中,如果数据被篡改,接收方可以通过加密算法验证数据的完整性。只有当数据未被篡改时,接收方才能确认数据的可靠性。加密存储数据还可以提供数据的可用性。即使数据被删除或损坏,只要密钥存在,就可以通过解密恢复数据。这样可以保证数据的可用性和持久性。加密算法的选择和管理需要专业知识和经验。错误的选择和管理可能导致安全性下降。密钥的管理和保护也是一个重要的问题。密钥泄露可能导致数据被攻击者解密和篡改。必须采取适当的措施来保护密钥的安全。为了实现加密存储数据的安全性,可以选择合适的加密算法。不同的算法有不同的特点和适用场景,应根据实际需求选择适合的算法。采用安全的密钥管理方法。可以使用密钥生成器生成随机密钥,并将其存储在安全的地方。同时,定期更换密钥以增加安全性。实施访问控制策略。只有授权的人员才能访问和操作加密的数据,以防止未经授权的访问和篡改。加密存储数据是一种有效的计算机数据库安全管理策略。它可以提供数据的保密性、完整性和可用性,同时也可以防止未经授权的访问和篡改。然而,加密存储数据也面临一些挑战和风险,需要采取适当的措施来保护数据的安全可靠性。

3.5 合理运用安全管理模式

在现代信息化社会,数据已经成为企业和个人的核心资产,因此,采取有效的安全管理模式至关重要。建立健全的安全防护体系。建立完善的网络安全规定,明确网络安全责任和义务,加强对网络安全的监管。同时,企业应建立专门的网络安全部门,负责数据库安全管理工作。企业应实施严格的访问控制策略,确保只有授权用户才能访问数据库。这包括对用户身份的验证、权限的管理以及对数据的加密保护。企业还应定期审查

访问权限,防止未经授权的用户获取敏感数据。采用先进的加密技术。加密技术是保护数据安全的有效手段。企业应采用先进的加密算法,对数据库中的数据进行加密存储和传输。企业还应定期对加密密钥进行更新,以防止密钥泄露导致的数据泄露风险。加强数据备份和恢复能力^[4]。企业应定期对数据库进行备份,确保数据的完整性和可恢复性。企业还应制定详细的数据恢复计划,以便在发生数据丢失或损坏时能够迅速恢复正常运行。提高员工的安全意识。定期开展网络安全培训,提高员工的安全意识和技能。员工是数据库安全的第一道防线,只有提高员工的安全意识,才能有效防范内部攻击和泄露风险。计算机数据库安全管理策略的实现需要企业从多个方面入手,包括建立健全的安全防护体系、加强访问控制、采用先进的加密技术、加强数据备份和恢复能力以及提高员工的安全意识。通过这些措施的实施,可以有效保障数据库的安全运行,为企业的发展提供有力支持。

结语

数据库技术从简单到复杂,功能从单一到多元极大地带动了相关技术的发展与变革,促成了相关技术体系的建成。计算机数据库管理系统是实现数据库管理的有效技术形式,是便利计算机数据库管理的有效途径,因而我们应对其管理和安全切实加强研究。

参考文献

- [1]李楠,王晓峰,王瑞,等.云数据库的安全管理技术研究[J].计算机科学与探索,2020,014(003):491-498.
- [2]马小军,杨庆红,王欣.人工智能在数据库安全领域的应用与发展[J].现代计算机(下旬刊),2021, No.394(07):6-9.
- [3]张亚飞,王民,孟庆余.基于区块链技术的数据库安全保障体系研究[J].现代电子技术,2022,045(001):39-42.
- [4]陈显彤,王卫星,王振宇.多维视角下数据库安全保障体系研究[J].计算机科学与探索,2020,v.14; No.395(03):317-324.