文章类型：论文| 刊号（ISSN）：3082-8295(O) / 2630-4759(P)

云安全审计视角下数据泄露原因及预防机制研究

王璐瑶
西京学院
DOI:10.12238/ej.v8i1.2217

[摘　要] 随着云计算技术的广泛应用,数据泄露和信息安全问题日益凸显,成为企业面临的重大挑战。本文以上海市某科技公司发生的数据泄露擅自删库事件为例,从云安全审计的视角出发,深入探讨了数据安全、云用户和云供应商所处的位置与作用,分析数据泄露的原因,提出针对性的风险防范措施和建议,即建立完善的云审计机制,引入先进加密技术,强化员工责任意识,制定完善的数据泄露应急预案,为云审计在数据安全领域的应用提供了有益的参考和借鉴。
[关键词] 云安全审计；数据泄露；预防机制
中图分类号：F239　文献标识码：A

Research on data leakage reasons and prevention mechanism from the perspective of cloud security audit

Luyao Wang
Xijing university

[Abstract] With the wide application of cloud computing technology, data leakage and information security problems have become increasingly prominent, which has become a major challenge for enterprises. In this paper, a data leakage of Shanghai technology company delete library event, for example, from the perspective of cloud security audit, deeply discusses the data security, cloud users and cloud suppliers of position and role, analyze the cause of the data leakage, and put forward targeted risk prevention measures and Suggestions, namely establish the cloud audit mechanism, introducing advanced encryption technology, strengthen the employee responsibility consciousness, develop perfect data leakage emergency plan, for cloud audit application in the field of data security provides a useful reference and reference.
[Key words] cloud security audit; data leakage; prevention mechanism

引言

随着云计算技术的迅猛发展和广泛应用,越来越多的企业选择将业务和数据迁移到云端,以提高效率、降低成本。然而,云环境的开放性和复杂性也带来了前所未有的数据安全和隐私保护挑战。近年来,数据泄露事件频发,不仅给涉事企业带来了巨大的经济损失和声誉损害,也对整个社会的信息安全和信任体系构成了严重威胁。云计算技术与审计工作的结合创造了“云审计”的概念[1]。云安全审计是一个全面评估云计算环境中的安全控制、数据保护、访问权限和合规性要求的过程。如何通过云安全审计加强数据安全和隐私保护是减少数据泄露的重要步骤。

1 数据泄露概述及影响

数据泄露通常包括企业业务数据泄露和企业客户个人信息泄露,从而丧失了数据原有的保密状态。目前,我国学界主流观点习惯性地将数据泄露理解为保密数据以非法方式对外传输和公布[2]。数据泄露事件近年频发,不仅揭示了当前云环境下数据泄露和信息安全问题的严峻性,也暴露了部分企业在数据安全管理方面的缺失和不足。信息的非法披露和滥用可能会引发一系列的严重后果,不仅涉及敏感信息的非法获取和利用,而且可能导致严重的经济损失,甚至招致法律责任[3]。

2 上海市某科技公司数据泄露并擅自删库案例回顾

2022 年 10 月，上海市某科技公司安装配置了一台Elasticsearch数据库服务器,用于搜集多个应用系统的业务日志。该公司主要从事为保险类企业提供互联网通信服务,在Elasticsearch数据库服务器中存储了包含用户姓名、身份证号码、手机号在内的大量个人信息。2023年10月,上海市科技局在工作中发现,该公司相关数据库存在未授权访问漏洞,部分数据泄露并被传输到境外IP。此外,该公司未健全全流程数据安全管理制度,未采取相应的技术措施和其他必要措施保障数据安全。上海市网信办将相关情况通报涉事企业并要求立即核查整改,

但该科技公司无视数据安全保护责任,未进行及时有效整改且擅自将涉事数据库一删了之,意图逃避处罚。针对以上违法情况,上海市网信办依据《数据安全法》第二十七条、第四十五条,对该科技公司作出责令改正,给予警告,并处人民币8万元罚款的行政处罚;对公司直接责任人员作出罚款人民币1万元的行政处罚。

如今,数据泄露问题已经渗透到社会各个行业,近一半的数据泄露事件会发生二次泄露,造成直接和潜在的损失达到万亿美元级,并威胁到数十亿人的数据信息安全。在云计算广泛应用的今天,云环境中的数据和资源面临更多元的访问路径和潜在的安全漏洞,数据泄露的风险进一步加剧。面对这一挑战,加强云安全审计显得尤为重要。云安全审计不仅是对云用户、云供应商和数据安全的全面检查和评估,更是构建云安全防线的重要一环。通过云安全审计,可以及时发现并修复潜在的安全隐患,防止数据泄露事件的发生。

3 云安全审计视角下数据泄露原因

3.1数据安全审计不足,未健全全流程数据安全管理制度

数据安全审计是确保数据安全的重要手段。由于各组织机构的数据机密性与隐私保护均不到位,数据泄露事件频发。对于企业,存在数据泄露问题的大多是提供互联网通信服务的信息科技公司,这类企业的门槛较低,未制定严格的数据管理制度、未采取加密措施,导致数据的使用、存储和传输过程缺乏规范。其次,企业存在未授权访问漏洞,导致系统容易受到攻击和数据泄露。数据安全审计目前主要问题在于：未充分应用加密技术数据在传输过程中或存储于云端时容易被非法获取和解析；用户身份授权与验证不合格,未能有效防止未授权用户访问敏感数据；第三方服务具有安全隐患。

云供应商和云用户尽管强调对数据安全管理制度的审核和评估,但是制度不完善,未覆盖数据生命周期的各个环节。涉事企业和机构未制定明确的数据安全政策、访问控制策略、数据加密措施等,这些措施的执行情况的评估也未做到定期审计。如果不能及时建立健全全流程数据安全管理制度,完善身份验证机制以及用户身份授权与验证机制,审查和更新就无法得到保障,使得未经授权的人员能够轻松访问系统并窃取数据,增加了数据泄露的风险。

3.2云用户安全审计的技术防护措施不足

数据泄露事件通常是由于安全漏洞、人为错误、系统配置不当或恶意攻击等原因导致的,这进一步凸显了加强云用户安全审计的必要性。技术防护措施是防止数据泄露的关键手段。在案例中,企业由于技术防护措施不足或存在漏洞,未充分应用加密技术数据在传输过程中或存储于云端时容易被非法获取和解析,导致数据被泄露。当加密技术未得到充分应用或安全漏洞未能及时被发现和修复时,数据在传输或存储过程中将缺乏足够的保护。这意味着攻击者能够利用这些技术上的薄弱环节,绕过安全防护措施,非法获取和解析数据,从而导致数据泄露事件的发生。这种技术上的疏忽和缺陷带来了严重的安全风险,使得敏感信息容易被窃取和滥用。

3.3云供应商安全审计人员责任和法律意识淡薄

现有关于云供应商的审计研究大多以事前审计(对云供应商安全状态的检验与评估)与事后审计(取证问责云供应商)为主[4]。数据泄露不发生的前提是操作合规,这就要求云供应商安全审计人员严格进行,以确保云供应商遵守相关法规要求,避免因违规操作而引发的数据泄露事件。然而,云供应商安全审计人员责任和法律意识不足。涉事企业因员工违规操作或泄露敏感信息而导致数据泄露,如果员工缺乏对数据安全的重视,不遵守相关规定和操作流程,就会进行违规操作,极大地增加了数据泄露的风险。因此,加强员工的安全培训和法律意识教育,提高他们对数据保护的认识和重视程度,是预防数据泄露的关键措施之一。

3.4应急响应与危机管理策略有效性低

数据泄露事件发生时,应急响应和危机管理的能力对于减轻损失和恢复声誉至关重要。然而,当组织缺乏有效的应急响应机制和危机管理策略时,数据泄露的风险会显著增加。根据近年数据泄露事件,观察到部分企业由于未能迅速识别并应对数据泄露事件,导致敏感信息被长时间暴露于风险之中,损失进一步扩大。云供应商作为数据存储和传输的关键环节,其事后审计和取证问责的能力也直接关系到数据泄露事件的处置效果。如果云供应商在数据泄露事件发生后无法提供充分的证据和协助,那么企业将面临更大的挑战,难以准确评估损失并有效应对危机。因此,建立健全的应急响应机制和危机管理策略,并加强对云供应商的监管和审计,是降低数据泄露风险、减轻损失和恢复声誉的关键措施。

4 数据泄露预防机制

4.1扩大数据保护“围城”,建立完善的云审计机制

云数据泄露预防机制的主要作用是识别潜在的数据泄露风险并采取措施加以预防,切实保障数据安全[5]。虽然现已提出了很多云审计方案,但大多数方案都假设个人和企业在使用云存储系统的整个过程中,用户及其公私钥始终不变,且不能高效地对数据进行实时动态更新[6]。针对数据泄露事件频发,需要实施云审计,建设云审计平台,扩大数据保护“围城”,并建立完善的云审计机制[7]。具体而言,涉事企业和机构应制定清晰、具体的数据安全政策,明确数据访问控制策略,实施有效的数据加密措施,并确保这些措施的执行情况得到定期审计和评估。同时,身份验证机制和用户身份授权与验证机制也应得到加强和完善,确保只有经过授权的人员才能访问敏感数据,降低数据泄露的风险。为确保这些措施的有效执行,建议建立完善的云审计机制,应包括对云服务提供商的定期安全评估、数据保护策略的合规性检查以及对数据访问和使用情况的监控和审计。通过这一机制,可以及时发现并纠正潜在的安全隐患,确保数据的完整性和安全性。

4.2引入先进加密技术,建立完善的用户身份认证机制

引入先进加密技术是保护数据安全的基础。通过引入先进

的加密算法和密钥管理技术，确保数据在传输和存储过程中的机密性和完整性。加密技术能确保数据在传输和存储过程中的机密性，即使数据被非法获取，攻击者也无法轻易解析出其中的敏感信息。因此，应采用最新、最安全的加密算法，对重要数据进行加密处理，并确保加密技术的正确实施；定期更新加密算法和密钥，防止因技术过时而导致的安全风险。其次，建立完善的用户身份认证机制是防止未经授权访问的关键。通过实施严格的身份验证和访问控制策略，可以确保只有经过授权的人员才能访问敏感数据。这包括采用多因素认证技术，如密码、指纹、面部识别等，以增加身份验证的复杂性和安全性。最后，还应定期审查和更新用户权限，确保离职员工或不再需要访问敏感数据的员工无法继续访问系统，从而显著提升数据的安全性，降低数据泄露的风险，并保护敏感信息不被窃取和滥用。

4.3重视人员队伍建设，强化员工责任意识

为了有效预防数据泄露事件，必须重视和加强人员队伍建设。第一，应定期进行全面的数据安全培训，确保员工充分理解数据安全的重要性，并掌握基本的数据保护知识和技能。培训内容应包括数据安全法规、公司数据安全政策、数据泄露案例分析等，以便员工能够深入理解数据安全风险及其后果。第二，建立责任追究机制，对违反数据安全规定的行为进行严肃处理。鼓励员工积极参与数据安全管理和监督工作，及时发现和报告潜在的安全风险，共同维护企业的数据安全。第三，建立激励机制，对在数据安全工作中表现突出的员工给予表彰和奖励，激发员工对数据安全工作的积极性和热情。从“一味利用数据”，转变到“合理善用数据”，积极配合国家对于数据安全保护的整体方针。

4.4加强危机防范和风险意识，制定完善的数据泄露应急预案

制定有效的应急响应与危机管理策略，能够很大程度上减小数据泄露造成的风险，降低成本与损失。加强事后审计，建立专门的数据安全团队或指定专人负责数据安全的监督和管理，确保数据泄露事件得到及时、有效的处理。制定完善的数据泄露应急预案同样至关重要。预案应明确数据泄露事件的识别、报告、处置和恢复等各个环节的具体操作流程和责任分工，确保在事件发生时能够迅速、有序地应对。预案还应包括与云供应商等合作伙伴的协同配合机制，确保在事件处置过程中能够得到充分的支持和协助。在制定预案时，应充分考虑各种可能的数据泄露场景和风险因素，确保预案的针对性和实用性。同时，应定期组织预案的演练和评估，不断完善和优化预案内容，提高组织的应急响应能力和危机管理水平，为组织机构的长期发展提供坚实的安全保障。

5 结束语

在数据泄露事件频发的当下，利用云安全审计来保证云服务的安全显得尤为重要。云用户和云供应商需要共同努力，构建更加安全、可靠的数据环境，为组织机构的长期发展提供坚实的安全保障。

[参考文献]

[1]傅静.云计算下的审计风险分析与防范[J].现代企业,2020,(04):161-162.

[2]周瑞珏.数据泄露风险治理中网络安全保险的介入路径[J].北方法学,2024,18(02):76-90.

[3]晏庆,崔浩贵,刘冰,等.大数据时代下计算机信息网络安全问题研究[J].无线互联科技,2024,21(17):102-104+115.

[4]陈希晖,侯良格.云安全审计及相关文献述评[J].商业会计,2021,(14):24-28.

[5]池淑玲.基于机器学习算法的云数据泄露检测与预防机制研究[J].华东科技,2024,(08):99-101.

[6]韩静,李艳平,禹勇,等.用户可动态撤销及数据可实时更新的云审计方案[J].软件学报,2020,31(02):578-596.

[7]魏祥健.云计算环境下的云审计系统设计与风险控制[J].会计之友,2015,(01):101-105.

作者简介：

王璐瑶(2000--),女,汉族,河南省郑州市人,西京学院硕士研究生,研究方向：信息系统审计。