国企云安全风险分析与监管对策

罗碧林

广州市云享数据科技有限公司 广东 广州 510000

摘要：随着公共服务平台建设的不断推进，国企云作为关键基础设施，其安全性日益受到关注。本文深入分析了国企云面临的安全风险，包括云服务商与供应链安全、安全管理能力、数据安全、业务连续性、技术漏洞与网络攻击等方面。针对这些风险，本文提出了一系列监管对策，如完善国企云安全标准体系、强化网络安全等级保护制度、提升国企云安全管理能力、加强数据安全保护等。通过构建国企云安全域划分、强化接口安全管理等措施，旨在全面提升国企云的安全性，确保数据的安全合规与风险可控。本文的研究为国企云的安全防护提供了有益的参考，对于推动公共服务平台建设具有重要意义。

关键词：国企云；安全风险；监管对策

1 引言

在数字化转型的浪潮中，国企云作为公共服务平台建设的核心支撑平台，正发挥着越来越重要的作用。国企云不仅实现了数据的集中存储与处理，还促进了不同部门之间的信息共享与业务协同，极大地提高了服务效率和质量。然而，随着国企云应用的不断深入，其承载的敏感信息也日益增多，这使得国企云的安全性成为了关乎信息安全和服务公信力的重大问题。国企云的安全性不仅关系到数据的保密性、完整性和可用性，还直接影响到服务的连续性和稳定性。一旦国企云发生安全事件，不仅可能导致数据的泄露或被篡改，还可能引发服务的中断，进而对公众信任和服务形象造成不可估量的损害。因此，深入分析国企云面临的安全风险，并提出切实可行的监管对策，对于提升国企云的安全性、保障数据的完整与保密、维护服务的连续与稳定具有重要意义。本文旨在通过全面梳理国企云的安全风险点，结合当前的安全技术和实践，提出一系列针对性的监管对策，为国企云的安全防护提供有力的理论支撑和实践指导^[1]。

2 国企云概述

国企云，作为新时代公共服务平台建设的重要基石，是主导方推动、企业参与建设并运营的一种综合性服务平台。它不仅融合了云计算的先进技术，还承载着公共服务数字化转型的厚望与使命。

2.1 定义与功能

国企云，顾名思义，是由主导方推动，依托云计算技术构建，由专业企业负责建设运营的综合服务平台。其核心目标在于打破传统信息化建设中的“信息孤岛”现象，通过数据的共享互通与业务的高效协同，实现各部门

间的无缝连接。国企云不仅提供基础设施服务（IaaS）、平台服务（PaaS）和软件服务（SaaS）等一站式云计算解决方案，还致力于推动数据的开放共享，促进服务流程的优化与再造，从而大幅提升服务效能和水平。

2.2 发展现状

近年来，随着公共服务平台建设的加速推进，国企云在全国范围内得到了广泛应用。据统计，目前多地都已经完成了国企云的建设工作，这些云平台承载着数以千计的业务系统，成为日常运转不可或缺的重要支撑。国企云的普及不仅提升了信息化水平，还为数据的集中管理、高效利用提供了有力保障^[2]。

2.3 重要意义

国企云的建设与运营，对于推动数字化转型、提升服务效能具有深远意义。首先，国企云通过资源的集约化利用，有效降低了信息化建设的成本投入，提高了资金的使用效率。其次，国企云促进了数据的共享汇聚，为跨部门的数据交换与业务协同提供了坚实基础，有助于打破信息壁垒，提升决策的科学性和准确性。最后，国企云作为公共服务平台建设的重要驱动力，为服务的创新与发展提供了广阔空间，助力更好地服务于公众。

3 国企云安全风险分析

3.1 云服务商与供应链安全

云服务商的信誉与经营情况是国企云安全的首要考量因素。一个信誉良好、经营稳定的云服务商能够提供更可靠、更安全的云服务。然而，如果云服务商存在信誉问题或经营状况不佳，可能会因资金链断裂、技术支撑不足等问题导致云服务中断或数据丢失，从而对国企云的安全性构成威胁。此外，云服务商的人员背景和稳定性也是不可忽视的安全风险。人员流动频繁、外包

人员过多可能增加敏感数据泄露的风险。这些人员可能因缺乏足够的安全意识和培训,成为黑客攻击的目标或内部泄露的源头。同时,供应链的安全也是国企云安全的重要环节。缺乏统一的供应链管理制度,存在层层转包、供应链关系不清等问题,可能导致供应链中的某个环节成为安全漏洞,进而威胁到整个国企云的安全^[3]。

3.2 安全管理能力

云服务商的安全管理能力直接关系到国企云的安全水平。然而,部分云服务商在安全管理方面存在明显不足。例如,未建立有效的安全基线机制,导致云平台的安全配置和防护措施缺乏统一标准;未定期对云平台开展全面的安全检测,无法及时发现和修复存在的安全漏洞。这些安全管理上的缺失,使得国企云在面临黑客攻击或内部恶意行为时,难以有效抵御。此外,云平台资产不清、暴露面不明也是安全管理能力不足的体现。云平台上的资产包括服务器、数据库、应用程序等,如果这些资产的管理不善,存在漏洞的资产可能会直接暴露在互联网上,成为黑客攻击的目标。同时,数据可迁移性和便捷性也是国企云安全管理中需要关注的问题。在数据迁移过程中,如果缺乏有效的安全措施和监管机制,可能会导致数据泄露、篡改等风险。

3.3 数据安全

数据是国企云的核心资产,其安全性至关重要。然而,国企云在数据安全方面面临着多方面的威胁。首先,数据丢失或泄露是国企云面临的主要风险之一。当云服务商或运营商受到黑客攻击或自身存在安全漏洞时,信息可能面临丢失的风险。这些敏感信息的泄露不仅可能对服务形象造成损害,还可能对信息安全构成威胁。其次,数据被更改或删除也是数据安全的重要风险。运维人员在操作过程中可能因失误或恶意行为删除或篡改数据,导致数据丢失或失真。这种数据的篡改可能引发严重的法律后果和社会影响。此外,黑客拦截或盗取数据包也是数据安全的一大威胁。黑客通过拦截或盗取数据包,可以篡改文件内容、骗取受害人转账汇款等,从而对公众和个人造成经济损失和信息安全风险。

3.4 业务连续性风险

国企云作为业务运行的关键支撑平台,其业务连续性对于服务的正常开展至关重要。然而,当前国企云在应急响应和灾难恢复演练方面存在明显不足,这成为了影响业务连续性的重要因素。一方面,缺乏有效的应急响应计划。国企云在面对突发事件时,往往缺乏迅速、有效的应对措施。这可能导致在事件发生时,无法及时恢复业务运行,进而造成服务的中断,影响公众对服务

的信任和满意度。另一方面,灾难恢复演练的缺失也是一大隐患。国企云应定期进行灾难恢复演练,以检验其备份和恢复机制的有效性。然而,在实际操作中,这一环节往往被忽视。这使得在真正面临灾难时,国企云可能无法迅速恢复业务,导致长时间的服务中断。而且,云平台底层严重依赖开源软件,这也带来了业务连续性的另一大风险——开源软件安全隐患。开源软件虽然具有开放、共享的优势,但其安全性却难以得到完全保障。云服务商若不能及时跟踪、修复开源组件的漏洞,这些漏洞就可能被攻击者利用,进而威胁到国企云的安全稳定运行。

3.5 技术漏洞与网络攻击风险

国企云作为数字化服务的重要组成部分,其技术架构的复杂性和开放性也使其成为了网络攻击的重点目标。其中,拒绝服务攻击(DDoS攻击)是国企云面临的一种常见且严重的网络攻击。攻击者通过向国企云发送大量无效或高流量的请求,耗尽其网络资源,导致平台无法正常提供服务。这种攻击不仅影响服务的可用性,还可能引发公众对服务能力的质疑。除了DDoS攻击外,国企云还面临着传统安全策略失效的挑战。云计算技术的虚拟化、分布式等特性使得传统基于物理边界的安全策略和检测模型难以适应。攻击者可以利用云计算技术的这些特性,绕过传统的安全防御措施,对国企云进行渗透和攻击。并且,服务的互联互通也带来了安全保密监管的挑战。国企云需要与其他部门、机构进行信息共享和交互,这突破了传统的物理边界。然而,这种互联互通也增加了持续监管的难度和边界的不可控性。攻击者可能利用这一漏洞,对国企云进行恶意攻击或窃取敏感信息,进而威胁到信息安全和服务稳定。

4 国企云安全监管对策

4.1 完善国企云安全标准体系

为国企云的安全运营提供坚实的制度基础,需加快健全公共服务平台信息安全保密管理机制,制定并完善国企云安全保密的政策、法规与标准体系。这一体系应明确国企云平台的安全责任主体,确保系统建设单位与云服务提供商在安全管理上的协同配合。同时,加强数据分类分级管理,根据政务信息的敏感程度,科学设定访问权限,并对系统管理人员进行严格的信息审核与身份认证,确保数据的合规访问与使用。

4.2 强化网络安全等级保护制度

推动网络安全等级保护2.0在国企云环境中的有效落地,是提升国企云安全防护水平的关键。相关部门应及时出台建设标准和指导意见,为国企云平台的安全建设

提供明确的方向。同时,加强宣传与教育,提高主管领导及全体员工对等级保护制度的重视程度。通过强化内部和行业主管的监督,以及加大执法力度,确保等级保护制度得到切实执行,对不履行要求的违法行为依法进行处罚,形成有效的威慑力。

4.3 提升国企云安全管理能力

国企云的安全管理能力是其安全防护体系的核心。应建立全面的安全基线机制,包括上线前的安全检测与动态评估,确保云平台始终符合安全要求。加强运维管理,制定严格的运维管理制度,对运维活动进行精细化管理,严格控制运维变更,并加强运维终端的管控。同时,定期进行全面的安全检测,及时发现并堵塞安全漏洞,确保云平台的持续安全。此外,还应建立完善的安全事件应急响应机制,对检测发现的安全问题进行快速响应与处置,确保国企云的安全稳定运行。

4.4 加强数据安全保护

为确保数据在云环境中的安全,必须采取以下措施:首先,利用数据脱敏、加密传输等先进技术,对云服务数据进行加密存储和备份。这不仅能有效防止数据泄露,还能在数据传输过程中提供额外的保护层。其次,通过实时监测与溯源技术,对敏感数据进行全天候监控,及时发现并追踪政务系统中的异常行为,确保数据的安全性和完整性。最后,在电子政务信息资源共享过程中,应统一数据类型与格式,以确保数据的一致性和可互操作性,降低因数据格式不一致而引发的安全风险。

4.5 构建国企云安全域划分

国企云安全域划分是保障业务安全的重要手段。通过合理的安全域划分,可以有效隔离不同业务系统的安全风险,防止安全威胁的蔓延。具体而言,应在业务区和互联网区之间设置物理隔离,确保外部网络无法直接访问内部业务系统。同时,根据业务系统的安全保护等级,将国企云划分为不同的安全域,如高安全等级域、中安全等级域和低安全等级域。此外,还可以利用区块链网络架构的特点,如公共链、联盟链和私有链,来进一步划分安全域,实现数据的分布式存储和访问控制。最后,根据业务需求,对安全区域进行细致划分,如互联网区、应用服务区、安全接入区、安全交换区等,确保每个区域都有明确的安全边界和防护措施。

4.6 强化接口安全管理

接口是国企云与外部系统交互的重要通道,也是安全风险的高发区域。因此,加强接口安全管理至关重要。首先,应对所有接口进行全方位的安全检测,包括数据访问安全、数据存储与传输安全、数据共享安全等方面。通过定期的安全测试和漏洞扫描,及时发现并修复潜在的安全漏洞。其次,按需部署单向导入、隔离交换等安全交换和防护设备,利用云安全、安全监测、防火墙设置等技术手段,实时监测接口处的异常事件,防止恶意攻击和非法访问。最后,实现数据的动态防护,通过智能分析和实时响应机制,自动抵御网络恶意攻击,确保接口的安全性和稳定性^[4]。

5 结论

在公共服务平台建设的大背景下,国企云作为关键的信息技术基础设施,其安全性直接关系到公共服务的连续性和数据的保密性、完整性。本文通过对国企云面临的安全风险进行深入剖析,并针对性地提出了完善安全标准体系、强化等级保护制度、提升安全管理能力等监管对策,旨在构建一个全方位、多层次的国企云安全防护网。

经过上述分析与实践可以得出,国企云的安全防护是一项系统工程,需要服务管理方、云服务提供商以及社会各界共同努力。只有不断完善安全制度、强化技术防护、提升管理水平,才能有效应对日益复杂的安全挑战。展望未来,随着技术的不断进步和安全管理理念的持续创新,国企云的安全防护将迈向更高水平。我们应持续关注安全态势,及时调整和完善安全策略,确保国企云始终成为公共服务平台建设中的坚实基石。

参考文献

- [1]王锦.基于随机博弈的云平台安全性分析方法研究[D].中原工学院,2018.
- [2]宋瑞欣.社区风险防控云平台领域分析设计与实现[D].天津大学,2018.
- [3]孟凡帆.智慧城市生产安全云平台的领域分析、设计与实现[D].天津大学,2017.
- [4]王鸣.基于云计算的电子政务平台安全风险分析方法及应用研究[D].上海交通大学,2016.