 DOI: https://doi.org/10.12349/iser.v5i8.3248

Government Affairs Cloud Security and Confidentiality Risk Prevention Strategy in Digital Government Construction

Na Zhao

Shanxi Yunshidai Smart City Technology Development Co., Ltd., Taiyuan, Shanxi, 030032, China

Abstract

The construction of digital government has significantly accelerated the online speed of government services, provided more refined, intelligent and diversified services for the masses, and achieved higher online work efficiency. Among them, the government cloud is an important support for the construction of digital government, but in the process of operation, due to the large number of business, it faces many security risks. Therefore, in the construction of digital government, improve the attention to the government cloud, strengthen the construction of security and confidentiality risk prevention, and ensure the security of daily use. In view of this, in the research work of this paper, it mainly analyzes the potential security risks of government cloud, explores the construction ideas of government cloud, and puts forward several effective security risk prevention strategies for the reference of relevant personnel.

Keywords

digital government; government cloud; security risk

数字政府建设中政务云安全保密风险防范策略

赵娜

山西云时代智慧城市技术发展有限公司，中国 · 山西 太原 030032

摘　要

数字政府的建设使政府服务的线上速度明显加快，为群众提供了更加精细化、智能化、多元化的服务，线上办事效率更高。其中政务云是数字政府建设的重要支撑，但在运行的过程中，由于业务数量庞大，面临诸多安全风险。因此，数字政府建设时提高对政务云的重视，加强安全保密风险防范的建设，保障日常使用的安全性。鉴于此，在论文的研究工作中，主要分析政务云的潜在安全风险，探究政务云的建设思路，并提出几点有效的安全保密风险防范策略，以供相关人员参考。

关键词

数字政府；政务云；安全保密风险

1 引言

近些年信息技术水平的不断提升，为电子政务的基础建设提供了支持，促进政务云平台的建设，打造数字政府，为群众提供线上服务，也能提高政府的信息化水平和管理效率。但由于云平台本身存在开放性、分布式计算与存储虚拟性等诸多特点，因此也带来了安全保密风险隐患。因此，在开展政务云建设时，需要从风险隐患方面入手，加强虚拟机的安全建设，保护云数据的安全性，并做好运维管理，有效应对各类风险问题，保障政务云的安全稳定运行。

2 数字政府建设中政务云存在的潜在安全风险

2.1 虚拟机的安全风险

政务云平台中借助于虚拟化的平台开展电子政务系统的资源应用管理、拓展与迁移，从而提高信息化管理的效率。在这一过程中还存在一定的安全隐患，主要包括安全管理隐患、虚拟化软件隐患和资源被破坏隐患。安全管理风险主要指的是，政务云系统租用了远端云服务的工作模式是由供应商所提供服务，在这一过程中，供应商可以绕过安全机制直接访问后台数据，不需要进行安全确认，因此存在数据失窃丢失的风险[1]。通过虚拟化技术，整合云计算中的各种资源，在软件中进行数据共享和迁移的过程，容易增加数据泄露丢失的风险。电子政务资源包括计算机软件资源、数据资源、网络资源等。在云计算安全建设的过程中，安全标准并不统一，导致黑客病毒等攻击难度降低，存在资源被破坏的风险。

2.2 云储存系统的安全风险

政务云平台中包含了海量的数据信息，需要打造云存储系统，提高数据的存储效率，并为数据的利用提供服务空间。然而在具体的应用中，虽然云存储可以为客户带来便利，但也存在诸多的安全隐患。在存储的过程中，用户并不知道

【作者简介】赵娜（1986–），女，中国山西五台人，硕士，高级工程师，从事智慧城市、大数据研究。

使用如何的方式进行存储和管理、数据存在何处的信息，借助于软件虚拟化技术提供支持，但也存在隔离风险。

2.3 云数据的安全风险

云数据在使用的过程中存在一定的安全隐患。用户进行浏览器交互访问、App 交互访问时，向云平台传输或者下载数据，在这一过程中容易受到病毒干扰、木马植入等影响。虽然云服务商也提供了相应的杀毒和防木马的软件，但相关的安全保障技术还并不成熟，因此云数据使用时，依旧存在一定的风险隐患。

2.4 运维与管理风险

除了网络自身带来的安全风险以外，网络的运维管理也会影响政务云平台的运行情况。缺乏完善的安全风险防范机制，对其中的隐患难以识别、恶意篡改的代码和日志难以恢复这些问题，都会影响到政务云平台的日常运行。再加上缺乏足够人才的支持，运维人员的专业素养参差不齐，在很大程度上影响着平台的安全性，受到人为因素影响，带来一定的安全隐患。

2.5 Web 攻击的风险

政务云的用户在云端使用浏览器时访问云资源。而黑客会通过 Web 攻击，对电子政务系统造成一定的安全风险隐患。常见的攻击方式有跨站脚本、安全配置错误、注入攻击、失效的访问控制等。

2.6 网络安全风险

电子政务云平台是基于虚拟网络技术，将物理网虚拟成多个逻辑独立网络，从而提高网络资源的利用率。但这种连接方式也带来了网络安全隐患，物理虚拟网络结成的各个节点中，会通过虚拟交换机来完成通信，常规的网络防护手段已经失去了保护效率。云网络的安全运维的过程中，存在资源负载平衡、流量异常监控及审计等安全风险。

3 数字政府建设中政务云安全保密风险的建设思路

3.1 政务云安全管理的要求

开展数字政府的建设工作，打造高效的政务云平台，需要明确基本要求，加强安全管理建设，从有效规避风险保障政务云，平台的安全稳定运行。在建设时需要遵循三不变，一不出境的原则。第一，安全管理责任不变。安全管理的人不会随着服务外包而外包，与云服务平台的供应商建立合作关系，而安全管理责任是由党政部门来完成的。党政部门要提高重视，加强安全建设，保障数据和业务的精密性、完整性、可操作性等等。第二，数据归属关系不变。党政部门将各种数据设备等资源提供给云服务商，完成各方面的建设，在日常运行的过程中，筛析和收集产生的各项数据、文档的资源都属于党政部门，数据归属关系不会变。未经党政部门授权，服务商不得访问、修改、转让、利用、销毁党政部门的数据。第三，安全管理标准不变。在建设政务云平台时，需要参照党政信息系统开展安全管理工作，服务商要严格遵循相关的安全政策规定、安全技术标准等，要求完善安全防护体系的建设。第四，敏感信息不出境。为党政部门提供服务的计算平台需要设在境内，敏感信息不出境。

政务云的使用单位是系统及数据安全的第一责任方，因此要重视安全管理建设与各方网络攻击，保障了系统的连续性。同时还要充分把握数据资产的主权，在可控的范围内实现开放共享。

3.2 政务云平台的框架建设

基于云计算的电子政务体系的框架设计，包括物理资源层、虚拟管理层和云服务层。物理资源层主要包括网络资源、数据资源、存储资源和计算资源，整合在一个云资源区；虚拟管理层对物理资源进行虚拟化抽象，从而开展各项管理工作（见图 1）；云服务层面向电子政务用户提供 IaaS、SaaS、PaaS 三种模式 [2]。

为了保障政务云平台的稳定运行，需要加强安全体系架构的建设。主要包括安全评估、安全管理和安全运维，从而实现数据管理与利用的电子政务安全体系。政务云是共建安全的安全模型，通过与服务商共同承担安全责任，打造良好的安全体系，规避安全风险。服务商的责任主要包括云平台主机安全、云平台网络安全和基础设施安全，而租户的责任主要在于租户应用系统安全、虚拟机主机安全和虚拟机网络安全。因此构建了安全管理体系中，需要包括公共基础安全、管理层安全、应用服务安全和安全评估与运维。

图 1 政务云的安全管理架构

4 数字政府建设中政务云安全保密风险的防范策略

4.1 虚拟机的安全建设

政务云应用是虚拟机存在一定的安全风险，因此加强该方面的安全管理建设，应对各类风险。虚拟层会对物理层的各种资源抽象化，形成虚拟资源，开展管理和应用。在虚拟机发挥作用时，需要对虚拟机访问进行加密监控、行为认证和有效反馈，可以防止恶意攻击、虚假运行和非法通信等

多种风险。可以开展对虚拟机完整性检测工作，排查其中的安全隐患。配备防火墙，加强设备边界的安全管理，有效应对各种违法入侵和恶意攻击。

4.2 云储存的安全建设

在云平台的支持下，可以解决存储容量的问题，实现有效扩充、异地存储和分布式管理。为了有效应对云存储安全隐患，需要引入各种安全技术，对分布式系统开展数据加密和用户身份认证等，可以确保数据存储与访问的安全性。多项建设可以确保数据存储与访问的机密性与可控性。在云存储平台中可以进一步优化密钥分发机制，改进 PKI 体系，采用基于属性的加密方式，强化加密，减少泄漏风险。

4.3 云数据的安全

基于不同物理介质开展访问存储，利用数据工作会出现各种安全隐患，在这个过程中也要设置身份认证与访问、安全隔离、安全审计等各种有效的措施，可以强化安全风险。防范工作排除隐患，确保数据存储、使用、分享等各个环节更加安全可靠。开展云平台安全特征库集中管理工作，收集整理关于病毒、漏洞层的特征库，及时更新并升级检测能力。在这一过程中，云服务商应当实时跟踪最新安全警报、开源样本等攻击数据，推陈出新，应对最新特征推出相应的防范措施，有效保障云数据的安全性 [3]。

4.4 运维与管理的风险防范

云平台开展运维与管理安全建设，主要包括安全事件管理、运维管理和安全审计三个方面。安全事件管理是对平台和所承载业务进行风险分析、预警等一系列工作。安全运维管理主要是进行环境安全管理、变更管理备份与恢复管理等多方面的管理内容。而安全审计则是对各层面进行审计服务，包括网络行为审计、数据库审计等，通过统一独立的检验公共平台的各项行为活动，进行相应的评价，从而有效识别风险排除隐患。此外还要重视人才的培养，提供专业的运维与管理人员，并近期组织他们进行技术培训和考核工作，选拔优秀人才，提高综合素养，有效应对各种安全风险问题（见图 2）。

4.5 Web 攻击的防御

Web 攻击严重威胁到网络运行的安全性。在政务云平台建设时要考虑到这一特点，完善 Web 攻击防御建设。可以将漏洞扫描、流量监控、入侵检测安全认证等多项技术，应用于 Web 中，提升防御能力。在先进技术的支持下，开展全面安全部署和实时监控工作，精准地掌握各类应用端的流量，获得数据信息进一步剖析，及时发现其中存在的隐患因素，有效响应，保障政务云平台的安全稳定运行。

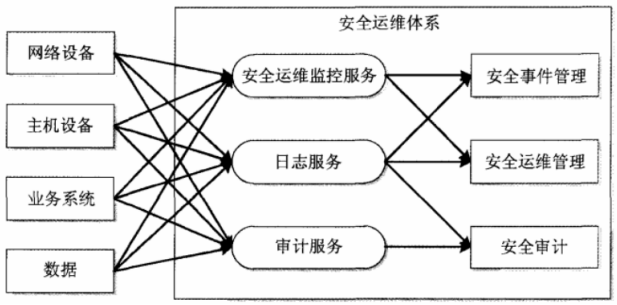

图 2 政务云的安全运维体系构成

4.6 网络安全认证建设

开展网络安全认证建设，保障网络运行的安全性，从而有效规避政务云使用中的安全风险隐患。借助 PKI 体系，加强安全认证。其中核心部分是 CA 认证中心。可以对用户身份进行认证，加强证书运营管理与维护。远程用户可以通过 VPN 专网访问器，保障通信过程中的安全性。根据安全等级进一步划分，包括业务网区和互联网区，采取物理隔离措施，设置跨网数据交换，从而实现数据的安全传输。通过划分一级二级三级等不同等级的保护区，分立其专属的网络防护体系，实现各个区域的安全隔离，保障电子政务云平台的网络安全性。

5 结语

综上所述，政务云在应用过程中存在诸多安全风险，因此，数字政府建设时要重视安全管理的建设要求，遵循原则，构建完善的框架，引进先进技术，从而加强虚拟机、云存储、云数据等各方面的安全建设，抵御风险，加强网络安全认证建设建立起完善的运维体系，有效保障政务云平台的安全性，提高安全保密风险的防范效果。

参考文献

[1] 陈春燕,赵弘洋,雷鹏炫,等.政务云安全风险分析与监管对策[J].电子质量,2024(2):1-5.

[2] 陈孝云,潘海华,王美子,等.电子政务云平台的安全风险与解决对策[J].通讯世界,2023,30(1):160-162.

[3] 张淑霞.浅析政务云安全潜在风险及应对措施[J].通讯世界,2022,29(11):31-33.