

DB32

江苏省地方标准

DB32/T 5073.1—2025

政务“一朵云”安全管理体系规范
第1部分：安全运行监测

Security management system specification for the "cloud" of
government affairs—Part 1: Security operation monitoring

2025-02-21 发布

2025-03-21 实施

江苏省市场监督管理局 发布
中国标准出版社 出版

目 次

前言Ⅲ

引言Ⅳ

1 范围1

2 规范性引用文件1

3 术语和定义1

4 缩略语2

5 总体框架2

6 基本要求3

7 资产监测4

8 可用性监测4

9 风险监测5

10 安全事件监测.....6

11 重大保障与应急响应.....6

12 安全协同.....7

13 供应链安全.....8

14 安全检查.....9

15 运行效果评价10

16 安全审计10

17 安全监测管理11

参考文献13

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 DB32/T 5073《政务“一朵云”安全管理体系规范》的第1部分。DB32/T 5073 已经发布了以下部分：

- 第1部分：安全运行监测；
- 第2部分：密码应用技术要求；
- 第3部分：密码应用安全性评估。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏省数据局提出并组织实施。

本文件由江苏省数据标准化技术委员会(JS/TC 88)归口。

本文件起草单位：江苏省大数据管理中心。

本文件主要起草人：吴中东、忻超、黄敏、刘尧、杨扬、王文娟、刘鑫、蔡一凡、谷和启、周云龙、林玉波、俞黎斌。

引 言

为加强统筹规划,全面提升江苏省政务云服务能力和安全运行水平,促进政务信息基础设施建设可持续发展,根据《省政府关于加快统筹推进数字政府高质量建设的实施意见》《江苏省政务“一朵云”建设总体方案》的要求,建立健全江苏省政务“一朵云”安全保障体系,提升安全防护能力,制定本文件。

DB32/T 5073《政务“一朵云”安全管理体系规范》分为以下3个部分:

- 第1部分:安全运行监测;
- 第2部分:密码应用技术要求;
- 第3部分:密码应用安全性评估。

政务“一朵云”安全管理体系规范

第1部分：安全运行监测

1 范围

本文件规定了政务云安全运行监测工作的总体框架、基本要求、资产监测、可用性监测、风险监测、安全事件监测等内容。

本文件适用于政务云管理机构和使用单位开展安全运行监测工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.8 信息技术 词汇 第8部分：安全
GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
GB/T 25069 信息安全技术 术语
GB/T 29246 信息安全技术 信息安全管理体系 概述和词汇
GB/T 31168 信息安全技术 云计算服务安全能力要求
GB/T 37988 信息安全技术 数据安全能力成熟度模型
GB/T 39786 信息安全技术 信息系统密码应用基本要求
GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 25069—2022、GB/T 5271.8、GB/T 29246—2023界定的以及下列术语和定义适用于本文件。

3.1

安全监测 security monitoring

以信息安全事件为核心，通过对网络和安全设备日志、系统运行数据等信息的实时采集，以关联分析等方式，实现对监测对象进行风险识别、威胁发现、安全事件实时报警及可视化展现的过程。

[来源：GW0203—2014，3.1，有修改]

3.2

安全审计 security audit

对信息系统记录与活动进行独立评审和考查的行为，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程等方面提出改进建议。

[来源：GB/T 25069—2022，3.24，有修改]

3.3

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

[来源：GB/T 39204—2022，3.2]

3.4

政务云 e-government cloud

运用云计算技术,统筹利用机房、计算、存储、网络、安全、应用支撑等软硬件设备,发挥云计算虚拟化、高可靠性、通用性、高扩展性,以及快速、按需、弹性的服务等特征,为政务信息系统提供基础设施、支撑软件、运行保障和信息安全等的综合服务平台。

[来源:GB/T 34078.1—2017,2.1,有修改]。

注:用“机房、计算、存储、网络、安全、应用支撑等软硬件设备”取代“机房资源、计算资源、存储资源、网络资源、信息资源、应用支撑等资源”,用“为政务信息系统提供基础设施、支撑软件、运行保障和信息安全等的综合服务平台”取代“为各政务部门构建提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等服务的电子政务综合性服务平台”。

3.5

政务“一朵云”the "cloud" of government affairs

在省级行政区域统一建设和部署的政务云(3.4),依托电子政务外网和互联网,运用云计算技术和智能化工具,为该区域各类电子政务的业务应用系统提供计算资源、存储资源、服务支撑、安全保障等共性服务的新型信息基础设施。

4 缩略语

下列缩略语适用于本文件。

API:应用程序编程接口(Application Programming Interface)

APT:高级持续性威胁(Advanced Persistent Threat)

DC:数据中心(Data Center)

DDoS:分布式拒绝服务(Distributed Denial of Service)

IP:网际互连协议(Internet Protocol)

SLA:服务水平协议(Service Level Agreement)

5 总体框架

政务云安全运行监测框架基于政务“一朵云”安全架构进行设计,如图1所示。

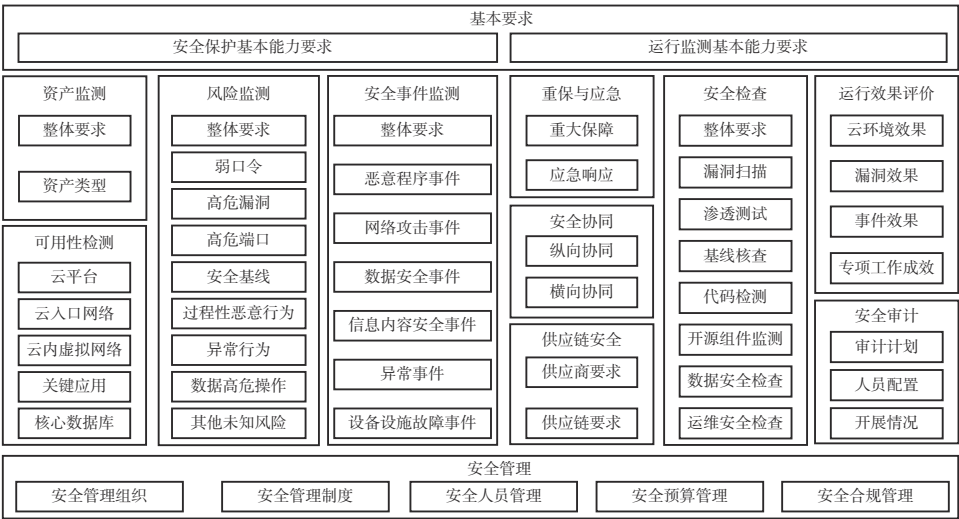


图1 政务云安全运行监测框架

6 基本要求

6.1 安全保护基本能力要求

6.1.1 整体要求

应按照 GB/T 22239、GB/T 31168 等相关要求建设安全保护基本能力,包括:

- a) 政务云运行管理机构负责政务云平台安全建设、运行及管理,开展政务云基础设施安全保护工作,构建技术、管理、运维等方面的安全能力体系,为安全运行监测工作开展提供基础能力支撑;
- b) 政务云使用单位负责本单位云上信息系统和数据的安全建设、运维、管理。

6.1.2 技术要求

技术要求包括:

- a) 政务云运行管理机构应建设政务云平台边界访问控制、云内访问控制、边界入侵防范、云内入侵防范、恶意代码防范、安全审计、身份鉴别、镜像和快照保护、数据加密、数据备份与恢复等安全防护能力;
- b) 政务云使用单位应充分利用政务云安全能力,按照相应网络安全等级保护级别的安全要求构建本单位云上信息系统安全防护体系。

6.1.3 管理要求

管理要求包括:

- a) 政务云运行管理机构应建立政务云基础设施管理制度、操作规程,形成由方针政策、管理制度、操作规程、记录表单等构成的安全管理制度体系。应设置指导管理安全工作的机构,设立安全岗位,明确岗位职责和能力要求,配备安全人员,建立并实施安全考核及监督问责机制;
- b) 政务云使用单位应落实本单位云上信息系统安全主体责任,指定系统安全负责人,报政务云运行管理机构备案。

6.1.4 运维要求

运维要求包括:

- a) 政务云运行管理机构应开展政务云基础设施安全运维工作,包括但不限于资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维服务商管理等;
- b) 政务云使用单位应开展本单位云上信息系统安全运维工作,包括但不限于资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维服务商管理等。

6.2 运行监测基本能力要求

6.2.1 政务云运行管理机构应围绕人员、工具、流程等开展运行监测,配备专职人员,构建平台工具,制定业务流程,建立主动防御机制,按要求开展资产监测、风险监测、可用性监测、安全事件监测、重保与应急、安全协同、安全检查、供应链安全、运行效果评价、安全审计、安全管理等工作。

6.2.2 政务云使用单位应按照相应网络安全等级保护级别的安全要求,开展本单位云上信息系统安全运行监测工作,包括但不限于资产监测、风险监测、可用性监测、安全事件监测、重保与应急、安全协同、安全检查、供应链安全、运行效果评价、安全审计、安全管理等工作。

7 资产监测

7.1 整体要求

7.1.1 监测范围应覆盖政务云平台、云边界、网络出入口、云上信息系统等。

7.1.2 应及时发现资产的上线、下线等变更情况,在72 h内完成资产清单更新。

7.1.3 应对多种来源的资产数据进行统一融合汇总,快速进行资产维度的风险评估、可视化展示、报表输出,挖掘资产安全问题。

7.1.4 应基于资产标识信息,及时通过资产和漏洞情报数据碰撞分析,快速评估漏洞影响资产范围。

7.2 资产类型

应能发现的资产类型,包括但不限于以下部分:

- a) 政务云平台资产,包括云主机、云存储、云网络、云安全组件、云数据库、操作系统、中间件、服务器、网络设备、安全设备等;
- b) 政务云边界资产,包括网络设备、通信设备、网络安全设备等;
- c) 政务云接入终端资产;
- d) 政务云使用单位云上信息系统资产,包括云主机、云网络、中间件、数据库、API接口等。

8 可用性监测

8.1 政务云平台

8.1.1 政务云平台应具备有效的容灾备份机制,包括但不限于主备容灾、双活容灾、多DC容灾等。

8.1.2 应监测政务云平台物理层和虚拟化层的资源可用性,对象包括但不限于计算处理能力、内存处理能力、硬盘处理能力等,使用率应不超过75%,同时应监测虚拟化软件的可用性。

8.1.3 应监测政务云平台的可用性,建立政务云平台SLA,关键节点全年可用率(全年可用时长/全年总时长)不低于99.99%。

8.2 政务云出入口网络

8.2.1 政务云出入口网络包括政务外网出入口、互联网出入口等,应具备有效的线路及核心设备冗余机制。

8.2.2 应监测政务云出入口网络的可用性,建立政务云出入口网络SLA,全年可用率(全年可用时长/全年总时长)不低于99.99%。

8.3 政务云内网络

8.3.1 政务云内网络应具备有效的核心设备及组件冗余机制。

8.3.2 应监测政务云内网络的可用性,应建立政务云内网络SLA,全年可用率(全年可用时长/全年总时长)不低于99.99%。

9 风险监测

9.1 整体要求

应监测政务云平台及云上信息系统的主要安全风险,包括但不限于弱口令、漏洞、高危端口、安全基线过低、过程性恶意行为、异常行为、数据高危操作、其他未知风险等,应在 24 h 内发现存在的隐患。

9.2 弱口令识别

应检测账号弱口令,包括但不限于内置规则、密码字典攻击、人工智能等检测方式。

9.3 漏洞监测

应识别高、中、低危安全漏洞。

9.4 高危端口监测

应探测高危端口对外暴露情况,包括但不限于数据库端口、远程桌面端口、FTP 服务端口等。

9.5 安全基线监测

应探测不合规基线及错误配置,包括但不限于身份访问控制、安全审计等方面。

9.6 过程性恶意行为监测

应发现过程性恶意行为,包括但不限于扫描探测、隐患利用、域名仿冒、钓鱼邮件、暴力破解等。

9.7 异常行为监测

应发现异常行为,包括但不限于高频登录尝试、异常时间登录等。

9.8 数据高危操作监测

应识别数据高危操作行为,包括但不限于违规外联、文件导出下载、非授信 IP 数据库绕行、超级管理员账号远程登陆、API 未授权访问、数据库导出、数据库高危操作等。

9.9 其他未知风险监测

应基于威胁情报,识别未知风险,包括但不限于 APT 攻击、勒索病毒等。

9.10 政务关键应用

9.10.1 政务关键应用应具备有效的容灾备份机制。

9.10.2 按要求对政务关键应用开展压力测试,基于测试结果优化资源分配。

9.10.3 应监测政务关键应用的可用性,应建立政务关键应用 SLA,全年可用率(全年可用时长/全年总时长)不低于 99.99%。

9.11 政务核心数据库

9.11.1 核心数据库应具备有效的容灾备份机制,包括但不限于主备容灾、双活容灾、多 DC 容灾等。

9.11.2 应监测核心数据库的可用性,应建立政务核心数据库SLA,全年可用率(全年可用时长/全年总时长)不低于99.99%。

10 安全事件监测

10.1 整体要求

应通过流量解析、日志分析等技术手段对政务云平台及云上信息系统进行7×24 h安全事件监测,及时发现安全事件。

10.2 恶意程序事件

应发现恶意程序事件,包括但不限于计算机病毒、网络蠕虫、特洛伊木马、僵尸网络、网页内嵌恶意代码、勒索软件、挖矿病毒等。

10.3 网络攻击事件

应发现网络攻击事件,包括但不限于DDoS攻击、域名解析异常、流量劫持、广播欺诈、主机失陷、APT攻击等。

10.4 数据安全事件

应发现数据安全事件,包括但不限于数据篡改、数据泄露、数据窃取、隐私侵犯等。

10.5 信息内容安全事件

应发现内容安全事件,包括但不限于反动宣传、暴恐宣传、色情传播等。

10.6 异常事件

应发现异常事件,包括但不限于访问异常、流量异常、高风险操作等。

10.7 设备设施故障事件

应发现设备设施故障事件,包括但不限于云平台硬件故障、软件故障、过载等。

11 重大保障与应急响应

11.1 重大保障

11.1.1 在春节、国庆等重要活动、会议期间,应设立专门负责加强安全响应的保障组织,开展专项活动,制定工作规范,确保政务云基础设施安全运行。

11.1.2 应将重大保障活动划分为准备阶段、实战阶段、总结阶段等环节,在各环节落实检查自查,及时通报预警安全隐患,处置安全事件,管理监测过程结果数据,落实报告管理、信息共享、舆情报送等工作。

11.1.3 应基于可视化态势大屏等工具平台开展专项安全监测和分析研判,及时预警可能造成重大影响的风险和隐患,重点部门、重点岗位保持24 h值班,及时发现和处置安全事件隐患。

11.1.4 应在重大保障期间组织协同技术支撑单位、政务云基础设施服务商、安全专家等,提升重大活动整体安全保障能力。

11.2 应急响应

11.2.1 应急管理

应明确应急管理组织、职责和工作机制等,包括:

- a) 应落实安全应急工作责任制,明确安全事件应急领导机构与职责,办事机构与职责,各单位部门职责,将责任落实到具体部门、岗位和个人;
- b) 应建立健全应急工作机制,制定安全应急管理规范,明确安全事件的预防、监测、报告和应急处置等的工作流程。

11.2.2 应急预案

应制定应急预案并开展预案培训与演练,包括:

- a) 应制定并管理安全突发事件处置场景预案,围绕政务云关键业务的可持续运行保障进行个性化预案编排和执行流程配置;
- b) 加强安全应急预案的培训,提高防范意识及技能,每年应至少组织1次预案培训;
- c) 定期组织演练,检验和完善预案,提高实战能力,每年应至少组织1次预案演练。

11.2.3 应急处置

应对安全事件开展应急处置,按要求进行事件上报、响应和总结调查,包括:

- a) 政务云安全事件发生后,应立即启动应急预案,实施先期处置并及时报送信息,属于较大、重大或特别重大安全事件的,应当于1 h内进行报告。
- b) 应按相关预案开展应急处置工作,加强技术手段运用,实现快速响应,及时将事态发展变化情况及应急处置结果上报。
- c) 应急结束后应组织调查处理和总结评估,总结调查报告应对事件的起因、性质、影响、责任等进行分析评估,提出处理意见和改进措施。总结调查工作应在应急响应结束后30 d内完成。

12 安全协同

12.1 纵向协同

12.1.1 应积极、主动配合上级主管单位的安管理工作,包括工作指挥、指令协同、安全检查、考核评估等。

12.1.2 应及时、准确向上级主管单位报告安全监测数据。

12.1.3 应及时、全面向上级主管单位报告较大及以上级别安全事件。

12.1.4 应及时向下级单位发布风险预警,进行日常通报,开展通报处置,包括:

- a) 针对潜在威胁事件,应向下级单位发布预警信息,预警发布内容宜包括事件性质、威胁方式、影响范围、涉及对象、影响程度、防范对策等信息,同时对预警的接收状态进行跟踪确认,确保预警信息被及时接收确认,达到主动预警防范的效果;
- b) 应持续获取预警发布机构的安全预警信息,按规定通报给相关人员和部门,分析、研判相关事件或威胁对政务云基础设施可能造成损害的程度,必要时启动应急预案;
- c) 应主动采取措施对预警进行协同响应,当安全隐患得以控制或消除时,执行预警解除流程;
- d) 应监测发现安全隐患、事件,通报至对应单位,推动开展暴露面收敛、隐患排查等主动防御工作,形成通报处置业务闭环。

12.2 横向协同

12.2.1 应落实安全监管要求,与网信、公安等主管部门建立沟通工作机制,配合开展安全检查工作。

12.2.2 针对潜在威胁事件,应向同级相关单位发布预警信息。

12.2.3 涉及跨区域安全事件时,应按需展开与同级单位的事件协查、分析研判、形成分析报告等。

13 供应链安全

13.1 供应商要求

13.1.1 应调查政务云基础设施供应商及人员背景、保密协议签订、安全教育培训等情况,包括:

- a) 应调查供应商类型应包括但不限于咨询、设计、集成、运维、测评、改进等各环节供应商;
- b) 应调查人员类型应包括但不限于项目经理、外派运维人员、实施人员、监理人员、开发人员、测评人员、设计人员等;
- c) 应调查保密协议签订情况,协议内容应包括但不限于安全责任、保密内容、保密期限、奖惩机制等。

13.1.2 应明确供应商安全责任和义务,包括但不限于加强对提供产品的设计、研发、生产、交付等环节的安全管理,声明不非法获取用户数据、不非法控制和操作用户系统和设备,不利用用户对产品的依赖性谋取不正当利益或迫使用户更新换代、无正当理由不中断产品供应或必要的技术支持服务等。

13.1.3 应对供应商人员加强账号权限管控、资源访问控制管理及操作行为监管。

13.1.4 供应商应对涉及的运维后门、特权账号重置及其他特权管理技术进行技术交底,并提供关闭方式。

13.1.5 对于被认定为关键信息基础设施的,应加强如下要求:

- a) 应建立和维护合格供应商目录。应选择有保障的供应商,防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险;
- b) 应强化采购渠道管理,保持采购的产品和服务来源的稳定或多样性。

13.2 供应链要求

13.2.1 应开展软件源代码安全检测、开源组件检测、容器镜像检测等,或由供应商提供第三方机构出具的相应检测报告,并在正式上线前进行漏洞检查。

13.2.2 采购和使用的产品和服务应符合国家相关标准要求。

13.2.3 使用的产品和服务存在安全缺陷、漏洞等风险时,应及时采取措施消除风险隐患,涉及重大风险的应按规定向相关部门报告。

13.2.4 按照《云计算服务安全评估办法》要求,对政务云服务商开展安全评估的情况进行监督核查。

13.2.5 对于被认定为关键信息基础设施的,应加强如下要求:

- a) 采购网络关键设备和网络安全专用产品目录中的设备产品时,应采购通过国家检测认证的设备和产品;
- b) 采购、使用的网络产品和服务,可能影响国家安全的,应通过国家网络安全审查;
- c) 应要求网络产品和服务的提供者对网络产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得10年以上授权,或在网络产品和服务使用期内获得持续授权;
- d) 应要求网络产品和服务的提供者提供中文版运行维护、二次开发等技术资料。

14 安全检查

14.1 整体要求

14.1.1 应制定安全检查计划,定期开展安全检查工作,并能根据重大保障等时期的实际情况进行调整。

14.1.2 应建立检查事项库,包括但不限于漏洞扫描、渗透测试、基线核查、代码检测、开源组件检测、数据安全检查、运维安全检查等。

14.2 漏洞扫描

14.2.1 应检查漏洞扫描工作开展情况,漏洞扫描的频率、覆盖范围、漏洞发现、修复、报送情况等。

14.2.2 漏洞扫描的频率应不低于每季度一次,范围应至少覆盖政务云平台、核心系统,执行时应不影响信息系统正常运行。

14.3 渗透测试

14.3.1 应检查渗透测试工作开展情况,渗透测试的频率、覆盖范围、漏洞发现、修复、报送情况等。

14.3.2 渗透测试的频率应不低于每半年一次,范围应至少覆盖核心系统,执行时应不影响信息系统正常运行。

14.4 基线核查

14.4.1 应检查基线核查工作开展情况,基线核查的频率、覆盖范围、配置缺陷发现及修复加固情况等。

14.4.2 基线核查的频率应不低于每半年一次,范围应至少覆盖政务云平台、核心系统。

14.5 代码检测

14.5.1 应检查代码检测工作开展情况,代码检测的覆盖范围、源代码缺陷检出及整改情况等。

14.5.2 政务关键信息系统上线及重大变更前应进行代码检测,范围应至少覆盖核心系统。

14.6 开源组件检测

14.6.1 应检查开源组件检测工作开展情况,开源组件检测的频率、覆盖范围、开源组件漏洞检出及整改、开源组件许可协议情况等。

14.6.2 开源组件检测的频率应不低于每年一次,范围应至少覆盖核心系统。

14.7 数据安全检查

14.7.1 应检查云上数据安全运行工作开展情况,安全检测的频率、覆盖范围、检出问题及整改情况等。

14.7.2 云上数据安全检测的频率应不低于每年一次,范围应至少覆盖核心系统、数据库及API接口。

14.8 运维安全检查

14.8.1 应检查运维安全工作开展情况,运维安全检查频率、覆盖范围、检出及整改情况等。运维安全包括但不限于机房环境、设备运行状态、设备维保期限、云平台运行状态、云平台资源管理、账号使用情

况、运维人员管理、告警监测分析与策略优化等。

14.8.2 运维安全检查的频率应不低于每季度一次,范围应至少覆盖政务数据中心服务器、网络设备及安全设备和信息系统检出问题整改情况。

15 运行效果评价

15.1 云环境效果

应核查云基础设施高危端口暴露、云平台边界违规外联等云环境安全效果情况,包括:

- a) 应核查政务云基础设施高危端口暴露情况,按季度进行汇总,并采取有效措施防范高危端口利用;
- b) 应核查政务云平台边界违规外联情况,按季度进行汇总,并采取有效措施阻断违规外联;

15.2 漏洞效果

应核查年度周期内政务云基础设施中危及以上漏洞数量、及时修复率等,涉及影响业务安全运行的漏洞应立即采取补救措施,包括:

- a) 应核查中危及以上漏洞发现数量等情况;
- b) 应核查中危及以上漏洞及时修复率,高危漏洞应在3 d内完成修复,及时修复率不低于98%,中危漏洞应在5 d内完成修复,及时修复率不低于95%,存在严重安全隐患且未按期修复时,政务云运行管理机构关闭系统对外网络策略,中止提供云资源服务。

15.3 事件效果

应核查年度周期内政务云基础设施发生一般、较大、重大、特别重大及国家通报的安全事件的次数:

- a) 应核查发生特别重大安全事件的情况,扼制损害程度和影响范围的扩大,确保不发生特别重大安全事故;
- b) 应核查发生重大安全事件的情况,扼制损害程度和影响范围的扩大,确保不发生重大安全事故;
- c) 应核查发生较大安全事件的情况,扼制较大安全事件发生率,开展有效处置,防范事件升级;
- d) 应核查发生一般安全事件的情况,扼制一般安全事件发生率,开展有效处置,防范事件升级;
- e) 应核查国家通报的本地区高危隐患和安全事件情况,确保不发生安全事故。

15.4 专项工作成效

应核查年度周期内政务云基础设施运行管理单位开展攻防演习、安全检查等专项工作情况。

- a) 应核查在政务云基础设施安全攻防演练中所发现问题的整改修复情况;
- b) 应核查在各种政务云安全检查中的表现情况、政务云基础设施的可用性情况。

16 安全审计

16.1 审计计划

应建立常态化安全审计机制,审计工作开展频率应不低于每月1次,范围至少应覆盖政务云平台、云上信息系统。

16.2 人员配置

16.2.1 应配备专职审计人员或采购安全审计服务。

16.2.2 应划分审计管理员、系统管理员、安全管理员等独立的运维管理角色,仅审计管理员具备审计权限,仅系统管理员具备日常管理权限,仅安全管理员具备账户管理权限。

16.3 开展情况

16.3.1 应建立统一的日志采集和存储工具,确保日志审计记录留存时间不低于6个月,应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。

16.3.2 应对安全策略及安全制度进行审查,对日志进行审计分析,对运维人员日常操作进行监督审计。

16.3.3 应对管理员账号的敏感操作行为进行审计,审计是否有对应的管理审批记录等,应对特权账号的使用情况进行审计。

16.3.4 应对可能影响政务云基础设施安全稳定运行的重大变更进行审计,审计是否符合流程规范要求,重大变更包括但不限于云配置变更、云数据库高危操作、云主机删除或重启、容器创建与销毁、API接口添加、核心路由配置修改、防火墙配置修改、账号权限提升等。

17 安全监测管理

17.1 安全管理组织

应建立和落实安全责任制,设立安全决策、管理、执行、监督的组织,成立网络安全和信息化领导小组,明确第一责任人和直接责任人。

17.2 安全管理制度

应制定安全工作总体方案,明确战略方针目标,建立数据安全、个人信息保护、商用密码应用、关键信息基础设施安全等相关的管理制度,明确机构、职责、负责人等。

17.3 安全人员管理

应配置专职安全工作人员,加强人员录用、离岗安全管理。针对全员开展经常性安全基础知识培训,频率不低于每季度一次;针对专业技术人员定期组织技能培训,确保取得安全专业资质人员在本单位安全工作人员中占比不低于30%。按需组建安全专家队伍。

17.4 安全预算管理

应统筹做好政务云安全建设预算管理,确保安全部分预算符合相关要求,保障日常运维、教育培训、安全加固、风险评估、系统升级、应急处置等安全工作经费落实。

17.5 安全合规管理

17.5.1 网络安全等级保护

应落实国家网络安全等级保护制度相关要求,定期开展云平台和信息系统的定级、备案、安全建设整改和等级测评等工作。

17.5.2 商用密码应用保护

应落实《中华人民共和国密码法》《商用密码管理条例》等相关要求,开展密码应用建设和改造工作。

建设政务云基础设施加解密、签名验签、时间戳、数字证书等配套密码应用保障能力,新上云政务信息系统按要求开展密码应用同步建设,已上云政务信息系统按要求进行密码应用改造,定期开展商用密码应用测评等。

17.5.3 关键信息基础设施保护

应落实政务关键信息基础设施保护合规要求:

- a) 政务关键信息基础设施的运营者应履行《关键信息基础设施安全保护条例》规定的安全保护义务;
- b) 按照 GB/T 39204 等要求,建立关键信息基础设施清单,落实关键信息基础设施边界防护、访问控制、容灾备份等保护措施。

17.5.4 数据安全保护

应落实政务数据安全保护合规要求:

- a) 应落实《中华人民共和国数据安全法》等相关要求,有效防范重要数据篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险。
- b) 参照 GB/T 37988 等要求,开展数据安全能力成熟度测评工作,保障重要数据安全。

17.5.5 个人信息保护

应落实政务信息系统个人信息保护合规要求:

- a) 应落实《中华人民共和国个人信息保护法》等相关要求,开展个人信息处理活动时应符合权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与等基本原则;
- b) 应按要求开展个人信息保护合规审计等。

参 考 文 献

- [1] 省政府关于加快统筹推进数字政府高质量建设的实施意见(苏政发〔2022〕44号)
 - [2] 江苏省政务“一朵云”建设总体方案》(苏政发〔2023〕36号)
-