 DOI: https://doi.org/10.12349/iser.v7i5.10527

Research on Network Information Security Protection System and Data Backup Collaborative Mechanism

Lei Zhang

Xinjiang Uygur Autonomous Region Data Resources and Government Service Center, Urumqi, Xinjiang, 830000, China

Abstract

Against the backdrop of increasingly diversified cyberattack methods and the continuously rising value of data assets in network information systems, this study addresses the issues of delayed response and compounded risks caused by the separation of traditional security protection and data backup operations.From the perspective of system coordination, it systematically examines the mechanisms of network information security protection and data backup.By analyzing the structural composition and operational logic of the security protection system, and integrating data backup strategies, recovery mechanisms, and disaster recovery pathways, a coordinated technical framework for security protection and data safeguarding is established.On this basis, focusing on key aspects such as risk identification, anomaly response, and dynamic recovery, an integrated operation model of security monitoring and backup systems is proposed.Furthermore, encryption control, automated operation and maintenance, and intelligent scheduling technologies are introduced to achieve unified optimization of protection and recovery capabilities.The study provides systematic technical support for enhancing overall information system security and ensuring business continuity.

Keywords

network information security; security protection system; data backup; coordination mechanism; disaster recovery

网络信息安全防护体系与数据备份协同机制研究

张磊

新疆维吾尔自治区数据资源和政务服务中心，中国·新疆 乌鲁木齐 830000

摘要

围绕网络信息系统面临的攻击手段多样化与数据资产价值持续提升的现实背景,针对传统安全防护与数据备份分离运行所导致的响应滞后与风险叠加问题,从体系协同视角对网络信息安全防护与数据备份机制进行系统梳理.通过分析网络安全防护体系的结构构成与运行逻辑,结合数据备份策略,恢复机制及容灾技术路径,构建安全防护与数据保护协同联动的技术框架.在此基础上,围绕风险识别,异常响应及动态恢复等关键环节,提出安全监测与备份系统融合运行模式,并引入加密控制,自动化运维与智能调度等技术手段,实现防护与恢复能力的统一优化.相关研究为提升信息系统整体安全性与业务连续性提供了系统化技术支撑。

关键词

网络信息安全；安全防护体系；数据备份；协同机制；容灾恢复

1 引言

随着信息技术的快速发展,网络系统在各类业务运行中的核心支撑作用不断强化,数据资源逐渐成为组织运行与决策的重要基础。在复杂网络环境与高强度攻击态势下,信息安全风险呈现出隐蔽性强,传播速度快及影响范围广等特征,传统以单一防护为主的安全模式已难以满足现实需求.同时,数据备份作为保障业务连续性的关键手段,在实际运行中往往与安全防护体系缺乏有效联动,导致在突发事件发生时恢复效率受限,甚至出现数据完整性与可用性受损问题.在此背景下,将安全防护与数据备份纳入统一框架,通过机制协同与技术融合,实现风险防控与数据恢复能力的同步提升,已成为信息系统安全管理的重要发展方向.围绕体系结构优化与运行机制重构,对协同模式与关键技术路径进行系统分析具有现实必要性与应用价值。

2 网络信息安全防护体系的结构构成与功能定位

网络信息安全防护体系以分层架构为基础,由网络边界层,主机终端层,应用服务层与数据资源层构成,形成覆盖全链

【作者简介】张磊（1989–），男，中国河南周口人，本科，工程师,从事政务数据中心运维管理,政务数据安全和数据备份恢复等研究。

路的防护结构.网络边界层侧重于流量控制与访问过滤,通过部署防火墙,入侵检测与入侵防御系统实现对外部威胁的拦截与识别;主机终端层通过安全加固,补丁管理及终端检测响应系统实现对内部节点的持续监测;应用服务层依托身份认证,权限控制及安全审计机制保障业务系统运行安全;数据资源层围绕数据分类分级,加密存储与访问控制实现数据资产保护.在功能定位上,该体系兼具防御,检测与响应能力,能够在威胁发生前形成阻断能力,在威胁发生过程中实现实时感知,在事件发生后提供溯源分析与恢复支撑,从而构建多维度协同运行的安全防护格局[1]。

3 网络信息安全防护与数据备份协同机制构建

3.1 安全防护与数据备份协同运行逻辑设计

安全防护与数据备份协同运行以数据可用性与系统连续性为目标,将安全监测与备份策略进行融合设计.在系统运行过程中,通过安全信息事件管理平台对网络流量,主机行为及应用日志进行实时分析,当检测到异常行为时触发备份策略调整机制,对关键数据执行即时快照或增量备份.备份系统采用全量备份,差异备份与增量备份相结合的策略,并结合存储分层技术将数据分布在本地存储与远程存储节点,实现数据冗余.通过与安全防护系统的数据接口对接,使备份策略能够根据风险等级动态调整,实现防护与备份的协同运行。

3.2 基于风险识别的数据保护与备份联动机制

基于风险识别的数据保护与备份联动机制以风险评估模型为核心,通过对资产价值,威胁概率及脆弱性进行量化分析确定数据保护等级.在高风险场景下,对关键业务数据采用实时复制与同步备份技术,实现数据在主备系统间的同步更新,在中风险场景中采用定时增量备份与周期性全量备份相结合的方式降低存储压力.通过数据防泄漏技术对敏感数据进行监测与控制,并结合访问行为分析识别异常操作,触发备份系统执行数据隔离与保护策略.结合存储虚拟化与分布式备份架构,使数据在不同节点间实现冗余存储，提高数据可靠性与抗风险能力[2]。

3.3 异常事件响应与数据恢复协同处置机制

异常事件响应与数据恢复协同处置机制以快速恢复业务运行能力为核心,通过建立自动化响应流程实现安全事件与恢复操作的联动.当安全系统检测到勒索软件,恶意入侵或数据篡改行为时,通过终端隔离,网络封禁及进程终止等技术手段控制风险扩散,同时启动灾难恢复系统进行数据回滚操作.数据恢复过程依托备份索引与版本管理技术,从最近的有效备份点进行恢复,并通过校验算法确保数据完整性.结合容灾架构中的热备与冷备机制,在主系统失效情况下实现业务切换与快速重建,通过自动化编排工具实现恢复流程的标准化与可执行化,从而提升系统在异常事件中的恢复效率与稳定性，图1为网络安全事件响应与处置流程。

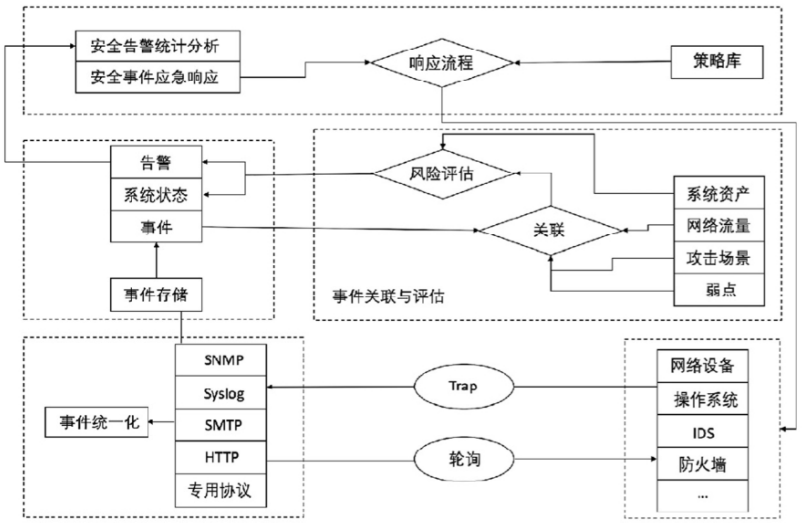


图1网络安全事件响应与处置流程图

4 协同机制下的关键技术支撑体系优化

4.1 数据加密与访问控制技术协同应用模式

数据加密与访问控制的协同应用围绕“数据可控,访问可审”的目标展开,通过密码算法与权限管理机制形成闭环控制。数据存储环节采用AES-256对称加密算法对核心数据进行加密处理，密钥长度256 bit，配合密钥管理系统实现分级管理与周期轮换，密钥更新周期一般控制在90 d以内。传输环节采用TLS1.3协议建立安全通道，握手时间控制在1ms级别以内，数据完整性通过SHA-256摘要算法进行校验，误码检出率达到10^-12量级。访问控制采用基于角色的访问控制模型与属性访问控制模型相结合的方式,对用户,设备及应用进行多维授权,权限粒度细化至字段级与接口级,访问响应时间控制在50 ms以内。结合多因素认证技术，通过口令,动态令牌与生物特征实现身份校验,认证成功率保持在99.9%以上。通过日志审计系统对访问行为进行实时记录与分析,日志采集频率达到每秒5000条以上,实现异常访问行为的快速识别与阻断,使加密机制与访问控制形成协同防护体系。

4.2 网络监测与备份系统联动分析技术路径

网络监测与备份系统的联动分析依托流量采集,行为分析与数据同步机制实现协同运行.网络侧通过流量镜像技术对关键链路数据进行采集，采样带宽可覆盖10 Gbps以上,结合深度包检测技术对协议特征与行为模式进行解析,识别准确率达到95%以上.安全信息事件管理平台对来自防火墙,入侵检测系统及主机日志的数据进行集中处理,单节点处理能力可达每秒10000条事件，通过关联规则与机器学习模型对异常行为进行识别.备份系统通过与监测平台的数据接口进行对接,在检测到异常流量或异常操作时自动触发数据保护策略,对关键数据库执行快照备份或日志备份，备份时间控制在30 s以内。数据同步采用块级复制与增量传输技术，传输效率提升至80%以上，网络带宽占用控制在30%以内。通过建立监测结果与备份策略之间的映射关系,实现基于实时风险的动态备份调整,使监测系统与备份系统形成数据驱动的联动分析机制[3]。

4.3 自动化运维与智能调度技术集成机制

自动化运维与智能调度技术通过平台化集成实现安全防护与数据备份的协同管理.运维系统基于自动化脚本与编排工具对安全策略部署,补丁更新及备份任务执行进行集中控制，任务执行成功率稳定在98%以上，平均执行时间控制在60 s以内。监控系统对网络设备、服务器与存储系统的运行状态进行实时采集，指标采集周期为10 s，异常响应时间不超过5 s。智能调度模块通过分析系统负载、网络带宽与存储利用率等参数,对备份任务与安全扫描任务进行动态分配，使资源利用率提升至75%以上。调度算法采用基于优先级与权重的模型,对关键业务任务设置高优先级,确保其响应时间控制在100 ms以内.通过引入容器化与虚拟化技术,实现运维环境的快速部署与弹性扩展,节点扩展时间控制在2min以内.结合自动告警与自愈机制,在系统出现异常时自动执行故障处理脚本,实现运维效率与系统稳定性的同步提升。

5 网络信息安全与数据备份协同机制实施路径

5.1 组织架构与运行机制协同优化模式

组织架构优化围绕安全管理与数据管理协同运行需求进行设计,通过设立信息安全管理中心与数据运维中心形成双核心架构,并通过统一指挥平台实现资源调度与信息共享.安全管理岗位负责威胁监测与策略制定,数据管理岗位负责备份执行与恢复验证,两类岗位通过标准接口进行信息交互,数据交换延迟控制在1 s以内。运行机制通过建立跨部门协同流程,使安全事件处置与数据恢复操作在同一工作流中完成，事件响应时间缩短至15 min以内。通过配置集中管理平台，实现对1000台以上终端设备与50 TB级数据资源的统一管理.岗位职责通过权限划分与操作审计进行约束，审计覆盖率达到100%。通过定期演练机制提升协同处置能力，演练周期设定为每季度1次，使组织架构与运行机制在实际运行中保持高效协同状态[4]。

5.2 制度流程与标准体系一体化构建路径

制度流程与标准体系构建以规范化与可执行性为核心，通过制定安全防护标准,数据备份规范及应急响应流程实现一体化管理.安全防护标准涵盖网络访问控制,终端安全加固与日志审计要求，配置合规率需达到98%以上。数据备份规范明确备份周期,备份类型及存储位置,关键数据每日执行增量备份,每周执行全量备份,数据保留周期不少于180d。应急响应流程通过流程引擎进行固化，包含事件识别,风险评估,处置执行与恢复验证等环节,流程执行时间控制在30min以内。通过引入国际标准与行业规范,对制度体系进行对标与优化,使各项技术措施具备可量化指标.结合流程监控与绩效评估机制,对执行效果进行持续跟踪,使制度与流程在运行过程中保持稳定性与适应性。

5.3 持续评估与动态优化运行机制设计

持续评估与动态优化机制依托数据分析与反馈调整实现系统性能提升.评估体系通过采集安全事件数量,响应时间,数据恢复成功率及系统可用性等指标进行量化分析,系统可用性目标设定为99.99%，恢复成功率保持在99%以上。评估周期一般设定为每月一次,通过对历史数据进行趋势分析识别潜在风险点.动态优化机制基于评估结果对安全策略与备份策略进行调整,如在异常事件频发区域增加监测频率，将采集周期由10 s缩短至5 s，对高风险数据提高备份频率至每小时一次.通过引入机器学习算法对运行数据进行建模,对系统负载与风险变化进行预测,预测准确率达到90%以上[5].结合自动化调整工具对策略进行实时更新,使系统在运行过程中具备自适应能力,实现安全防护与数据备份协同机制的持续优化与性能提升。

6 结语

网络信息安全防护体系与数据备份协同机制的构建,是提升信息系统安全性与业务连续性的关键路径.通过将安全防护,数据保护与恢复机制纳入统一框架,实现风险识别,实时响应与快速恢复的闭环运行,可显著降低系统运行中的不确定性与数据损失风险.依托加密控制,监测分析及自动化运维等技术手段,协同机制在实际运行中展现出良好的适应性与扩展能力.随着网络环境复杂程度持续提升,强化协同机制的动态优化与技术迭代,将有助于进一步提升整体防护水平与系统稳定性。

参考文献

[1] 李静.网络环境的计算机信息安全防护体系研究[J].信息技术与信息化,2026,(02):123-126.
[2] 张路,纪惠强.物联网时代下计算机网络信息安全防护体系的构建[A].《水资源保护》创刊40周年学术交流会暨2025（第十三届）水生态大会论文集[C].河海大学:2025:586-597.
[3] 陈宠,顾强.中国移动5G网络切片技术下的信息安全防护体系构建[A].第九届工程技术管理与数字化转型学术交流会论文集[C].广西网络安全和信息化联合会:2025:324-326.
[4] 李宪伟,陈静.基于计算机网络技术的网络信息安全防护体系建设[J].长江信息通信,2025,38(04):144-146.
[5] 郭金龙.网络信息安全防护体系中信息管理技术的应用研究[J].中国管理信息化,2025,28(08):156-158.