大数据时代计算机网络信息安全与防护策略分析

尹毕成 程芳

中国电子科技集团公司第十五研究所信息产业信息安全测评中心，中国·北京 100083

摘要：本次研究立足大数据时代网络运行特性，深度剖析计算机网络信息安全面临的各类核心风险，梳理数据流转、攻击手段、权限管控、合规监管层面的隐患成因，结合场景需求搭建分层分类的防护体系，提出针对性防控举措，为各类主体化解网络安全隐患、规范数据管控流程、规避合规风险提供切实可行的实践参考。

关键词：大数据时代；计算机网络；信息安全

Analysis of Computer Network Information Security and Protection Strategies in the Big Data Era

Yin Bicheng, Cheng Fang

Information Technology Security Testing and Evaluation Center, The 15th Research Institute of China electronic technology group Corporation, China Beijing 100083

Abstract: This study, based on the operational characteristics of networks in the big data era, deeply analyzes the core risks faced by computer network information security, sorts out the causes of hidden dangers in data flow, attack methods, permission control, and compliance supervision, builds a hierarchical and classified protection system in combination with scene requirements, and proposes targeted prevention and control measures, providing practical and feasible references for various entities to resolve network security risks, standardize data control processes, and avoid compliance risks.

Keywords: Big data era; Computer network; Information security

0 引言

大数据技术的深度应用重构了计算机网络数据的流转模式，海量信息跨域采集、传输、共享与存储成为行业常态，网络信息安全的防护范畴不断延伸，传统单一防护手段难以适配复杂场景需求，数据泄露、智能攻击、权限失管等问题持续凸显。当下网络安全管控面临技术与管理的双重挑战，隐私保护与行业合规的压力逐步加剧，本次研究深挖安全风险根源，探寻适配大数据环境的防护路径。

1 大数据时代网络信息安全的核心风险

大数据时代网络信息安全的核心风险，集中体现在数据流转场景变复杂、防护触点增多后，安全隐患的扩散速度和破坏力度大幅提升。当下数据不再局限于单节点封闭存储、内部单向传输，而是跨部门、跨环节汇聚流转，涵盖业务办理、公共服务、内部管理等各类敏感信息，各类安全风险相互交织、随时变化，常规防护手段很难全面覆盖，处置难度远高于传统网络环境。

1.1 数据泄露与窃取风险加剧

当前数据大多采用分布式存储、多节点协同对接的模式，从前端采集、链路传输到内部共享、外部调用，全流程都存在防护薄弱点。黑客常抓住传输漏洞、存储节点弱密码、接口权限管控不严等漏洞，精准盗取核心数据；内部人员私自拷贝、非授权导出数据的行为，也缺乏实时拦截和预警手段。数据泄露一旦发生，不会局限在单个终端，会顺着流转链路快速蔓延，轻则泄露群众隐私、单位核心业务信息，重则波及公共资源数据，造成难以挽回的损失。即便只是零散数据片段泄露，也能通过关联分析还原完整信息，进一步扩大危害范围[1]。

1.2 网络攻击手段智能化升级

大数据技术为攻击方提供了精准画像、流量模拟、漏洞挖掘的技术支撑，传统零散式、粗放式攻击逐步演变为协同化、智能化的高级持续性威胁，分布式拒绝服务攻击借助海量傀儡节点发起规模化流量冲击，可轻松突破常规带宽防护阈值，瘫痪网络服务链路。精准钓鱼攻击依托用户行为数据、业务场景数据定制诱饵内容，能够绕过基础身份验证环节，此类攻击具备极强的伪装性与针对性，常规防御规则无法实现精准识别，而且攻击溯源、源头阻断的技术难度呈指数级提升，攻击响应的滞后性极易引发大规模安全事故。

1.3 数据管理与权限管控漏洞

大数据平台多采用跨部门、跨系统的模块化架构搭

建，数据调用场景复杂且频次较高，权限划分往往缺乏精细化维度界定，未结合数据敏感等级、岗位职能边界设置动态权限阈值，平台内置的监管模块存在监测盲区，无法实时捕捉异常访问、非合规调用等行为。此外，部分平台未建立权限联动机制，账号权限与岗位变动脱节，闲置账号、冗余权限长期留存，违规操作、越权访问等行为极易引发数据篡改、非法调取问题，直接形成安全管控的真空地带，为恶意行为提供可乘之机[2]。

1.4 隐私保护与合规管控压力

用户隐私数据作为大数据挖掘与分析的核心资源，在采集、处理、流转环节易出现过度收集、未经授权共享、违规挖掘的问题，隐私数据的边界界定与管控难度大幅提升。除此之外，行业数据合规条例对数据处理全流程提出严苛的约束要求，企业若未建立配套的合规审核、风险排查机制，不仅会触发隐私数据滥用引发的权益纠纷，还会触碰监管红线，衍生行政处罚、法律诉讼等多重风险，安全防护落地与合规标准执行的双重压力，成为大数据环境下网络信息安全的突出难题。

2 大数据环境下网络安全防护核心策略

2.1 构建全方位数据安全防护体系

2.1.1 数据采集传输加密防护

依托端到端加密技术搭建全链路加密屏障，针对前端采集终端部署硬件加密模块与数据校验算法，对采集的原始数据进行即时脱敏预处理，剔除冗余无效信息的同时锁定核心敏感字段，杜绝采集环节的数据裸奔风险。传输链路选用国密标准的对称加密与非对称加密组合方案，针对跨域传输、外网调用等场景增设加密隧道，对传输数据包进行分片加密与完整性校验，同时部署链路监听阻断模块，实时拦截非法窃听、数据篡改等链路攻击行为[3]。

2.1.2 数据存储脱敏备份管理

按照数据敏感等级划分存储层级，将核心涉密数据、普通业务数据、公开数据进行分区隔离存储，针对高敏感数据采用专用加密存储介质，搭配访问白名单机制限制存储节点的接入范围。落地数据动态脱敏规则，针对结构化数据采用掩码替换、字符扰动等脱敏方式，非结构化数据通过特征提取、内容模糊化处理实现隐私屏蔽，且脱敏操作全程留痕，便于后续核查追溯。建立多级异地备份机制，区分实时热备份、定时增量备份与全量冷备份模式，针对核心业务数据设置双活备份架构，确保主存储节点故障时可快速切换备用节点，同时定期开展备份数据完整性校验与恢复演练，排查备份链路的断点隐患，避免数据丢失后无法复原的问题。

2.1.3 数据销毁合规流程管控

制定覆盖全场景的数据销毁标准流程，针对过期数据、废弃数据、冗余数据区分销毁方式，电子存储数据采用多次覆写、物理消磁等不可逆销毁手段，杜绝数据碎片被技术还原的可能，纸质涉密数据则通过专业粉碎设备进行无害化处理。建立数据销毁审批与核验机制，销毁前需完成数据用途核查、备案登记，销毁过程由专人全程监督并留存操作记录，销毁后开展残余数据检测，确认无信息残留后方可完成闭环。同时，对接数据全生命周期管理平台，将数据销毁节点纳入平台管控范围，自动预警超期未销毁数据，避免闲置数据长期堆积形成安全漏洞，并且针对跨平台流转的数据，同步联动各关联节点完成销毁操作[4]。

2.2 升级智能化网络安全防御技术

2.2.1 智能入侵检测系统搭建

融合机器学习与深度流量分析算法搭建智能入侵检测框架，突破传统规则库的识别局限，对网络流量的特征维度、行为轨迹进行实时解析，精准识别异常访问、端口扫描、漏洞利用等隐蔽入侵行为，同时针对高级持续性威胁建立特征画像模型，通过历史攻击数据训练算法，提升未知威胁的预判能力。系统部署采用分布式节点布局，覆盖网络边界、核心服务器、终端设备等多个防护触点，实现入侵行为的全域监测，并且联动边界防火墙实现威胁的即时阻断，缩短入侵行为的扩散时长。

2.2.2 网络安全态势感知部署

整合全网安全设备、服务器、终端的运行数据与告警信息，搭建可视化态势感知平台，实现网络安全状态的全局呈现与动态监测，平台具备风险关联分析能力，可将零散的安全告警进行整合研判，定位风险根源与扩散路径，避免单一告警信息遗漏核心隐患。依托大数据分析技术对网络流量、用户行为、漏洞分布等数据进行深度挖掘，生成风险趋势研判报告，为防御策略调整提供数据支撑，同时针对高风险区域、高危漏洞进行重点标注，触发分级预警机制。与此同时，打通态势感知平台与各防护模块的数据接口，实现监测数据的实时共享，打破各安全设备之间的信息孤岛。

2.2.3 攻击应急响应机制优化

建立分级分类的攻击应急处置流程，根据攻击类型、影响范围、破坏程度划分响应等级，针对不同等级制定标准化处置步骤，明确各岗位的操作职责与协同流程，避免

应急处置过程中的混乱推诿。优化应急响应的联动机制，实现态势感知、入侵检测、防火墙等模块的自动联动，高危攻击发生时自动启动隔离、封堵、溯源等操作，压缩攻击响应的时间窗口。同时，搭建应急处置知识库，收录各类新型攻击的处置方案与修复措施，为应急操作提供专业指引，并且定期开展应急演练，模拟真实攻击场景测试流程落地效果，排查处置环节的漏洞短板[5]。

2.3 完善权限管理与内部监管机制

2.3.1 精细化身份认证体系构建

推行多维度身份认证模式，结合账号密码、生物特征、硬件令牌、环境校验等多重因素完成身份核验，摒弃单一密码认证的薄弱环节，针对核心数据访问、高权限操作场景增设二次认证环节，提升身份验证的安全性。基于最小权限原则划分访问权限，结合岗位职能、数据敏感等级、操作场景设定权限阈值，杜绝权限过度分配与越权授权，同时细化权限颗粒度，区分数据查看、调取、修改、导出等不同操作权限，实现权限的精准管控。另外，建立身份认证日志全记录机制，留存每一次认证的时间、终端、操作内容等信息，便于异常身份访问的追溯核查，并且针对外部合作方、临时访客设置专属认证通道与临时权限，限定访问范围与有效时长，避免外部接入带来的权限风险。

2.3.2 全流程操作审计监督

搭建数据操作全流程审计平台，对数据采集、传输、存储、调用、销毁等各环节的操作行为进行无死角记录，细化操作主体、操作时间、操作内容、操作终端等核心信息，形成完整的操作轨迹链条，确保所有数据操作均可追溯、可核查、可追责。优化审计数据的分析能力，通过异常行为算法识别违规操作、非授权访问、批量导出等可疑行为，实时触发预警并阻断后续操作，同时定期开展审计数据复盘，排查隐性违规操作与管控漏洞。与此同时，规范审计日志的存储与管理，采用加密存储方式保障日志数据的完整性与不可篡改性，设定日志留存期限以满足监管核查要求，并且开放分级审计权限，允许管理人员按职责范围查阅对应审计数据，兼顾监管需求与信息保密原则。

2.3.3 内部人员权限动态调整

建立账号权限全生命周期管理机制，将人员入职、调岗、离职、离岗等变动信息与权限管理平台实时联动，入职时按岗位精准分配初始权限，调岗时同步回收原有冗余权限并配置新岗位所需权限，离职或离岗时立即注销所有系统账号与访问权限，杜绝闲置账号、越权账号长期留存。定期开展权限梳理核查工作，对现有账号权限进行全面排查，清理无效账号、重复权限与超额权限，修正权限分配偏差，同时结合业务调整与岗位变动，动态更新权限配置，保持权限与岗位职责的高度匹配。

2.4 强化安全意识与合规体系建设

2.4.1 全员安全意识常态化培训

结合岗位特性制定差异化安全培训内容，针对运维人员侧重攻防技术、应急处置、设备操作等专业技能培训，针对普通员工侧重数据保密、钓鱼识别、终端防护等基础常识培训，摒弃同质化培训模式，提升培训内容的实用性。采用常态化宣教与专项培训结合的方式，通过内部宣讲、线上课程、案例解读等多种形式开展安全宣教，将网络安全知识融入日常工作流程，潜移默化提升人员风险防范意识。同时，定期开展安全考核与实操测试，检验人员的安全技能掌握情况，针对考核不合格人员进行二次培训，并且建立安全奖惩机制，对违规操作行为予以惩戒，对主动规避安全风险的行为予以激励，倒逼人员落实安全操作规范。

2.4.2 健全安全管理制度规范

完善适配大数据环境的网络安全管理制度，细化数据管控、权限管理、设备运维、应急处置等各环节的操作规范，明确各岗位的安全职责与工作标准，杜绝管理层面的权责模糊。制度内容贴合实际业务流程，兼顾可操作性与管控力度，避免制度与实操脱节形成形式化管控，同时根据网络环境变化、技术升级与监管要求，定期迭代更新制度条款，确保制度的时效性与适用性。另外，建立制度执行监督机制，安排专人负责制度落地情况的核查，及时纠正违规操作行为。

2.4.3 数据合规监管落地执行

对标国家网络安全法律法规、行业数据合规标准与隐私保护条例，搭建全流程合规管控框架，将合规要求嵌入数据采集、处理、流转、存储、销毁的每一个环节，从源头规避违规操作风险。建立常态化合规自查机制，定期开展数据合规风险排查，重点核查数据收集合法性、隐私保护落实情况、权限管控规范性等核心内容，对排查出的合规隐患建立台账并限期整改。

3 结语

综上所述，本次研究厘清了大数据时代计算机网络信息安全的核心风险脉络，搭建了技术防御、权限管控、合规约束相结合的多维防护框架，突破了传统被动防护的局限，贴合数据全生命周期管控逻辑优化防控模式。研究未针对细分行业的特殊场景做差异化适配，在未来研究中应

该结合不同领域的业务属性细化防护细则，同步跟进技术迭代与制度完善。

参考文献：

[1] 张妍，肖志勇. 大数据时代计算机网络信息安全与防护策略[J]. 数字通信世界，2025(1): 89-91.

[2] 孙式河. 大数据时代计算机网络信息安全与防护策略[J]. 数码设计，2025(2): 112-114.

[3] 关文涛. 大数据时代计算机网络信息安全与防护策略[J]. 数码设计（上），2020, 9(9): 20.

[4] 冯庆亮. 大数据时代计算机网络信息安全与防护策略研究[J]. 企业科技与发展，2020(1): 94-95,98.

[5] 于柯实. 探讨大数据时代计算机网络信息安全及防护策略研究[J]. 信息系统工程，2023(9): 130-133.

作者简介：尹毕成（1994-），男，汉族，北京市人，工程师，学士（本科），研究方向：网络安全。