网络安全维护中计算机网络安全技术的应用

刘晓松
中石油昆仑燃气有限公司海南分公司　海南　海口　570125

摘　要：本文探讨网络安全维护中计算机网络安全技术的应用，阐述基础防护技术在边界、终端及网络节点的具体实施，分析数据安全保障技术在加密、备份及生命周期管理方面的应用，介绍网络安全维护技术的日常、专项及智能化实施方式，以及主动防御与应急响应技术的应用，展示不同技术的协同作用，为网络安全维护提供参考。

关键词：网络安全维护；计算机网络安全技术；基础防护；数据安全；主动防御

引言：网络安全是保障网络稳定运行的关键，计算机网络安全技术在维护中发挥重要作用。随着网络威胁日益复杂，单一防护技术难以应对。研究各类安全技术在基础防护、数据保障、维护实施及防御响应中的应用，结合技术特性与应用场景，对构建全面的网络安全防护体系，提升网络安全维护水平意义重大。

1 基础防护技术的应用

1.1 边界安全技术

防火墙技术需配置访问控制策略，划分网络区域权限，限制非必要端口开放。数据包过滤规则区分协议与地址，拦截不合规数据包，减少无效通信。内外网隔离机制通过逻辑划分，使不同安全级别网络保持可控交换，防止外部威胁直接渗透核心区域[1]。入侵检测技术分析网络流量识别异常模式，捕捉非典型传输行为，发现潜在攻击。攻击行为特征匹配需更新特征库，对比流量与已知攻击模式，定位威胁来源。实时告警触发机制在检测到可疑行为时提示，明确等级与影响范围，为响应提供指引。虚拟专用网络技术搭建加密传输通道，用加密算法处理内容，确保公共网络传输不被窃取。身份认证流程结合多种验证方式，确认访问者身份，防止未授权接入。访问权限分级按角色分配操作权限，限制敏感资源访问，降低泄露风险。

1.2 终端安全技术

操作系统安全加固需定期修补漏洞，消除隐患。账户权限管理区分管理员与普通用户权限，避免风险扩散。安全配置优化关闭不必要服务与端口，调整参数增强防护，减少被攻击可能。终端防护软件需查杀恶意代码，扫描文件与进程，清除病毒木马。实时行为监控跟踪程序启动与网络连接，识别异常并拦截。主机入侵防御监控系统调用与注册表修改，阻止未许可更改，维护终端稳定。移动设备管理实施接入认证，检查设备安全状态，不合规设备无法接入。数据加密存储处理敏感信息，防止设备丢失后泄露。远程擦除功能在设备失控时启动，清除重要数据，避免信息被非法利用。

1.3 网络节点安全防护

路由器与交换机需启用端口安全策略，限制连接数与接入设备，防止端口被恶意占用。路由协议认证验证发送者身份，确保路由表更新合法，避免路由欺骗。冗余链路加密处理备用链路，保证主链路故障时传输安全不降级。服务器安全加固需精简端口，关闭无关端口，减少攻击入口。日志审计功能记录操作行为，包括登录与配置更改，为追溯事件提供依据。安全模块加载适配防护组件，增强对特定攻击的抵御能力，提升安全等级。物联网设备防护需修补嵌入式系统漏洞，按运行环境调整补丁安装，避免影响工作。通信协议加密处理设备间传输内容，防止指令被篡改或窃取。接入权限管控明确接入范围与权限，防止未授权设备干扰通信。

2 数据安全保障技术的应用

2.1 数据加密技术

对称加密与非对称加密结合应用需完善密钥管理机制，确保密钥生成、分发、存储全过程的安全，避免密钥泄露导致加密失效。加密算法选择依据数据敏感度与应用场景，高敏感数据采用强度更高的算法，平衡安全性与运算效率[2]。两种加密方式配合使用，对称加密处理大量数据提升效率，非对称加密用于密钥传递增强安全性。数据传输加密需做好传输协议安全配置，禁用存在漏洞的旧版本协议，启用具备加密与身份验证功能的协议。加密通道建立流程需在通信初始阶段完成身份验证，协商加密算法与密钥，确保通道建立后的数据传输全程处于加密保护状态，防止传输中途被拦截篡改。数据存储加密需对存储介质进行整体加密，防止介质丢失后数据被直接读取。敏感字段加密处理针对数据库中的身份证号、银行卡号等信息单独加密，即使数据库整体被攻破，敏感信息仍能保持安全。加密过程需与应用系

统适配，不影响数据的正常查询与使用。

2.2 数据备份与恢复技术

备份策略制定需结合全量备份与增量备份，全量备份完整保存数据状态，增量备份记录两次全量备份间的变化数据，减少备份所需存储空间与时间。备份周期规划根据数据更新频率确定，更新频繁的数据缩短备份间隔，确保数据丢失时能恢复至较近状态，降低损失。异地容灾部署需设计合理的数据副本存储架构，将数据备份至与主系统地理隔离的区域，避免因自然灾害等导致主备数据同时受损。跨区域数据同步机制需保证数据传输的及时性与一致性，采用压缩与加密技术减少同步过程中的数据泄露与传输延迟。恢复验证机制需定期进行恢复流程测试，模拟数据丢失场景执行恢复操作，检查恢复过程的顺畅性与耗时。数据完整性校验方法通过哈希值比对等方式，确认恢复后的数据与备份数据一致，无损坏或遗漏，确保恢复数据可正常使用。

2.3 数据生命周期安全管理

数据分类分级防护需对数据进行敏感程度标记，按级别实施差异化保护策略。高敏感数据采取加密存储、严格访问控制等措施，低敏感数据可适当简化防护流程，在保障安全的同时提高数据使用效率。保护策略需随数据敏感程度变化动态调整，确保防护措施始终适配。数据流转监控需记录数据传输路径，明确数据在各系统间的流转轨迹，便于追溯数据去向。访问操作留痕详细记录用户对数据的查看、修改、删除等操作，包括操作时间、账号、IP地址等信息，为异常操作审计提供依据。共享权限动态调整根据用户角色变化与数据使用需求，及时增减共享权限，避免权限长期不变导致的风险。数据销毁技术需对不再使用的存储介质进行彻底清除，采用多次覆写技术消除逻辑删除后的数据残留，防止数据被恢复。物理销毁合规操作针对硬盘、U盘等介质，通过粉碎、焚烧等方式确保数据无法复原，销毁过程需符合环保要求，避免对环境造成污染。不同类型介质选择适配的销毁方式，平衡销毁效果与操作成本。

3 网络安全维护的技术实施

3.1 日常维护技术应用

防护规则更新需确保防火墙策略定期适配网络环境变化，根据业务调整新增或移除访问控制条目，保证策略与实际需求匹配。入侵检测特征库需及时同步最新威胁特征，纳入新型攻击的识别标识，提升对未知攻击的发现能力。病毒库实时升级接收病毒样本与查杀规则更新，确保终端防护软件能识别近期出现的恶意代码，减少感染风险[3]。设备状态巡检需监测网络设备负载，跟踪路由器、交换机的CPU占用率与内存使用情况，避免因过载导致的性能下降。终端漏洞扫描定期检查操作系统与应用软件，发现潜在漏洞并记录位置与影响范围。加密密钥有效性核查验证密钥的时效与完整性，对即将过期或可能泄露的密钥进行替换，保障加密机制持续有效。日志审计分析需汇总系统操作日志，整合网络设备、服务器、终端的操作记录，形成完整的审计数据集。异常登录记录筛查通过分析登录时间、地点、设备等信息，识别非规律登录行为，如异地登录、非常规时段登录等。数据访问轨迹追溯跟踪敏感数据的调用与流转路径，关联用户操作与数据变化，为异常访问事件提供调查线索。

3.2 专项维护技术实施

漏洞管理需调度全量漏洞扫描，覆盖网络中的服务器、终端、网络设备等所有节点，确保无扫描盲区。风险等级评估结合漏洞的利用难度、影响范围等因素，划分风险级别，明确处理优先级。补丁部署优先级排序根据漏洞风险等级与业务系统重要性，确定补丁安装顺序，先修复高风险漏洞与核心系统，减少漏洞暴露时间。配置合规性检查需将设备配置与安全基线比对，识别偏离基线的设置项，如开放的非必要端口、宽松的访问权限等。非授权配置识别通过自动化工具监测系统参数与软件设置的变更，发现未经过审批的配置调整。自动修复脚本执行针对常见的不合规配置，运行预设脚本进行一键修复，提高合规性整改效率。应急维护演练需模拟典型攻击场景，如勒索病毒感染、数据泄露等，检验防护系统的拦截效果。响应流程验证按预定步骤执行应急操作，检查各环节的衔接顺畅度与处理时效。维护工具效能测试评估应急过程中所用到的检测工具、清除工具的响应速度与处理能力，确保工具在实际应急中可靠有效。

3.3 智能化维护技术融合

自动化维护脚本可实现批量配置下发，同时对多台设备推送统一的安全策略，减少重复操作。定期检测执行按设定周期自动运行漏洞扫描、配置检查等任务，无需人工触发。异常自动告警触发在监测到指标超限时立即发出通知，附带异常详情与初步分析，缩短故障发现时间。维护状态可视化通过设备安全指数仪表盘直观展示各设备的安全评分，用颜色标识风险等级。维护任务进度追踪实时更新各项维护工作的完成情况，显示延迟任务与责任人，便于进度管控。风险趋势图谱以曲线或柱状图呈现风险指标的变化趋势，帮助识别风险上升的设备或系统，提前采取干预措施。预测性维护模型通过

分析历史故障数据识别故障模式，总结设备故障前的特征表现。维护周期动态调整根据设备运行状态与故障概率，延长低风险设备的维护间隔，缩短高风险设备的检查周期。潜在风险提前预警基于模型预测结果，在故障发生前提示可能出现的问题，如硬件老化、策略失效等，为主动维护提供依据。

4 主动防御与应急响应技术的应用

4.1 主动防御技术

蜜罐技术需搭建逼真的诱捕环境，模拟真实系统的服务与数据，吸引攻击者将精力投入其中。攻击行为分析通过记录攻击者的操作步骤与使用工具，解析其攻击思路与手法。威胁情报收集从攻击行为中提取新的攻击特征与IP地址等信息，丰富威胁数据库，为其他防御系统提供支持[4]。沙箱技术将可疑程序置于隔离环境中运行，限制其对真实系统的访问权限，观察程序的文件操作、网络连接等行为。行为特征提取捕捉程序的异常活动，如创建后门、加密文件等，形成独特的行为标签。恶意代码判定结合行为特征与已知恶意代码库比对，确定程序是否具有恶意属性，避免其对正常系统造成破坏。威胁情报技术需拓展情报收集渠道，从开源信息、安全厂商共享、自身监测数据等多方面获取情报。威胁特征库更新将收集到的情报转化为可识别的特征，及时纳入防御系统。预警机制建立在发现新威胁时迅速发出提示，明确威胁类型与可能影响的系统，为提前防御争取时间。

4.2 动态防御策略调整

防御规则自适应更新需跟踪攻击模式变化，当发现新的攻击手段时，自动调整拦截策略，增加相应的检测规则。实时优化检测阈值根据网络环境的正常流量波动，动态调整异常检测的敏感度，减少误报与漏报情况。资源弹性调度根据威胁等级变化分配防护资源，高威胁时集中资源强化核心系统防护，低威胁时适当缩减资源投入。优先级调整响应能力让关键业务系统获得更快的防御响应速度，确保核心功能不受攻击影响。虚假信息部署需伪造系统节点信息，在网络中散布虚假的IP地址与端口开放情况。误导攻击路径使攻击者在探测过程中进入错误方向，浪费其时间与精力。增加攻击探测难度通过模糊真实系统结构，让攻击者难以准确掌握网络拓扑，延缓攻击进度。动态调整网络标识信息，随时间变换设备命名与端口映射关系，进一步混淆攻击目标识别。

4.3 应急响应技术

安全事件检测与分析需精准识别异常行为，如流量突增、权限异常提升等，标记潜在安全事件。事件根源追溯通过分析日志与网络数据包，查找攻击发起的源头与利用的漏洞。影响范围评估确定受事件波及的系统与数据，划分受影响等级，为后续处置提供依据。快速处置技术需迅速阻断攻击源，通过防火墙或入侵防御系统屏蔽攻击IP与端口。受影响系统隔离将被入侵的系统从网络中分离，防止攻击扩散至其他节点。漏洞临时修复对发现的漏洞采取紧急补丁或配置修改等措施，暂时阻止攻击继续利用。事后恢复与加固需遵循系统重建流程，格式化受感染的存储介质，重新安装操作系统与应用程序。安全策略优化根据事件原因调整访问控制与检测规则，弥补防御漏洞。防御机制升级引入更先进的防护技术，增强系统对同类攻击的抵御能力，避免类似事件再次发生。

结束语

网络安全维护需综合运用多种计算机网络安全技术。从基础防护到数据保障，从维护实施到主动防御与应急响应，形成完整的防护链条。这些技术的应用能有效抵御网络威胁，保障网络安全。未来需持续优化技术应用，细化实施流程，适应网络环境变化，为网络安全提供更可靠的保障。

参考文献

[1]周燕彬.网络安全维护中计算机网络安全技术的应用探讨[J].科技创新与生产力,2023(1):75-77.

[2]于鑫,王婷婷.计算机网络安全技术在网络安全维护中的应用[J].通信电源技术,2024,41(3):167-169.

[3]陈洁.计算机网络安全技术在网络安全维护中的应用分析[J].通信电源技术,2023,40(17):193-195.

[4]黄涛.计算机网络安全技术在网络安全维护中的应用[J].电子元器件与信息技术,2023,7(6):187-190.