4.2 推动“下沉市场 + 新兴场景”全域深耕覆盖工作落地

市场覆盖率的持续提升并非简单的盲目扩张，而是需要充分聚焦增量市场，以市场覆盖质量以及效益双赢为抓手，大力促动全域覆盖格局形成。具体而言，一方面要有意识将重点放在下沉市场精细化深耕等工作上。县域以及农村等市场作为通信企业关键增量市场，其普遍具有地域广阔、人员分散等特征，传统粗放式营销渠道拓展模式可能难以顺利为继。因此需充分聚焦特点，大力采用差异化策略，助推下沉市场工作持续深耕。策略一：可加强与县域政府、农村村委会的合作，依托本土化资源，发展本地专用渠道合作伙伴，保障渠道本地化服务供给能力更强。策略二：可充分聚焦用户需求特点，推出高性价比通信套餐以及具体产品，通过一对一营销服务，化解用户信任危机，确保用户转化率更为理想。

另一方面，还要有意识关注新型场景的全方位战略渗透，真正做到新兴场景这一通信市场新增长级的统筹兼顾。具体而言，通信企业要积极作为，化被动为主动，快速对接新兴场景需求，通过指定营销渠道的拓展，为全方位渗透目标的顺利落地造势赋能。如针对智能家居场景，在售楼处以及家电卖场设置沉浸式体验区，并大力推广通信服务与智慧家居联合套餐。又如针对智慧办公场景，与服务平台合作，为其提供办公通信解决方案在线提供服务窗口，实现问题的一对一解决。总而言之，相信在新兴场景渠道的持续渗透作用下，势必能够顺利实现由个人用户向多维度用户群体覆盖的跨越转型，最大化挖掘新兴市场价值，给通信企业的持续性发展注入鲜活动力。

4.3 打造“技术驱动 + 精准赋能”的渠道运营体系

作为助推运营能力升级的重要策略，以营造技术驱动 + 精准赋能双赢格局为工作主线，全新打造渠道运营体系也势在必行。相信随着高品质渠道运营体系支撑作用的有效发挥，势必会助推营销渠道拓展以及市场覆盖率提升的成效更为显著。

其中，针对技术驱动维度，构建技术驱动精准运营体系，需积极引入大数据分析平台，利用大数据成熟算法，整合 CRM、ERP、SCM 等系统相关数据资源内容，构建渠道运营数据集约中心。紧接着，再借助数据挖掘算法，快速实现用户需求渠道表现以及未来市场趋势的有效洞察，为后续能够“因地制宜”完成营销方案制定提供可靠内容支撑。

针对精准赋能维度，考虑到渠道合作伙伴能力也直接决定着渠道服务质量与效率。因而，通信企业也要重视分级分类渠道赋能策略的构建，将合作伙伴合理分为三级，分别是①战略级②核心级③授权级。顺利完成分级后，在依据差异化赋能逻辑，完成整体的发展部署，从根本上保障渠道专属服务质量更佳。

与此同时，若条件允许的话，还要搭建合作伙伴深度赋能中心，提供产品知识、运营管理等更为系统化的培训服务，确保能够通过系列培训活动保障合作伙伴综合能力能够得到直线攀升，补齐发展短板，从根本上避免木桶效应出现。

4.4 夯实组织、人才多维度基础保障

对于通信企业而言，营销渠道的拓展以及市场覆盖率的提升属于长期工程，因此需要健全且完善的保障体系支撑，通过组织架构和人才培养等多方面工作的齐抓共管，助推“工程”稳健推进。其中组织架构，要自觉突破传统部门壁垒，打破交流孤岛，通过独立性较强的全渠道管理部门成立，真正做到线上、线下、行业渠道拓展与运营工作的统筹协调。不会因管理层级过多，而致使最终的渠道响应速度明显滞后。针对人才队伍建设工作，要重视内培外引。一方面加强对内部员工的培训，持续夯实其数字化运营、场景化营销以及精准化服务能力。另一方面与高校联动，从源头上引入人才，为后续工作的稳健推进持续注入新鲜血液。

结论：综上所述，数字经济深度发展的当下，通信企业化被动为主动，自觉拓宽营销渠道助力市场覆盖率提升已然成为推动可持续战略目标顺利落地的大势所趋之举。而本文以服务有效性提升为工作主线，而提出的针对性营销渠道拓宽与市场覆盖率提升策略，便可帮助通信企业快速突破传统模式粗放式扩张掣肘，真正通过渠道形态创新、覆盖维度拓展、运营能力提升、保障体系构建的多方面齐抓共管，构建新型全面发展网，助力持续发展目标落地。

参考文献

[1] 马冲.通信企业市场营销的渠道建设与管理扩展[J].中文科技期刊数据库(全文版)经济管理,2025(8):078-081.

[2] 沈小洪.企业管理中营销渠道拓展与市场覆盖率提高的路径研究[J].现代商业研究,2025,(02):118-120.

[3] 张双丽.通信企业市场营销的渠道建设与管理[J].中国市场,2021(24):59-60.

 DOI: https://doi.org/10.12349/iser.v7i1.9037

Research and Practice of Cybersecurity Attack and Defense Technologies

Zhe Li

Fujian Mindun Network Security Co., Ltd., Fuzhou, Fujian, 350001, China

Abstract

As a critical node in the cybersecurity assurance system, the classified protection assessment serves as a vital tool for identifying system security risks and evaluating the effectiveness of defensive measures. This paper, based on practical scenarios of classified protection assessments, focuses on typical categories and core methods of current cyber attacks. It provides an in-depth analysis of the underlying logic of attack behaviors and their threat pathways to information systems of varying classification levels. By incorporating real-world examples from assessment practices, the study explores targeted strategies for building and implementing a defense technical system that aligns with classified protection requirements. Special emphasis is placed on methods for validating the effectiveness of defensive measures and optimizing their direction. The findings offer practical references tailored to business realities, facilitating the efficient execution of classified protection assessments and the steady enhancement of information system security defenses, thereby helping information systems meet the corresponding security protection requirements.

Keywords

Level Protection Assessment; Cybersecurity Attacks; Defense Technologies; Security Protection; Practical Implementation

网络安全攻击与防御技术研究与实践

李哲

福建闽盾网络安全有限公司，中国 · 福建 福州 350001

摘　要

等级保护测评作为网络安全保障体系的关键节点，是辨别系统安全隐患、检验防御措施有效性的重要手段。本文依托等级保护测评实操场景，聚焦当前网络安全攻击的典型类别与核心方式，深刻解析攻击行为的底层逻辑与对不同等级信息系统的威胁路径，结合测评工作中的实际事例，有针对性地探究适配等级保护要求的防御技术体系搭建与落地策略，着重讲述防御措施的有效性验证办法与优化走向，为等级保护测评工作的高效开展、信息系统安全防护能力的稳步提升，提供贴合业务实际的实践参照，助力信息系统符合对应等级的安全保护要求。

关键词

等级保护测评；网络安全攻击；防御技术；安全防护；实操落地

1 引言

随着数字化转型的深入，信息系统已然成为各行业运作的核心载体，其安全稳定性直接关系到业务连续性与数据安全。等级保护测评作为我国网络安全保障的基础性制度，借助分级分类保护的准则，给不同重要程度的信息系统划定安全防护底线 [1]。当下，网络攻击手段不断更新升级，攻击路径更具隐蔽特性与针对性，给等级保护测评工作带来了新的难题。鉴于此，从等级保护测评角度出发，深入研究网络安全攻击的核心特点与防御技术的实操重点，明确攻击与防御的动态博弈联系，对提升测评工作精准度、增强信息系统安全防护能力具有重要现实意义。

【作者简介】李哲（1991–），男，中国福建闽侯人，本科，工程师，从事计算机科学与技术、网络安全研究。

2 等级保护测评下网络安全攻击的典型类型与核心特征

2.1 恶意代码攻击

恶意代码攻击是各等级信息系统均高频面对的攻击类型，亦是等级保护测评中重点核查的风险点。此类攻击通过植入病毒、木马、勒索软件等恶意程序，达成对系统的控制、数据窃取或破坏。和传统泛化攻击有别，当前恶意代码更具针对性，部分攻击团伙会针对特定行业的信息系统定制恶意代码，躲避常规杀毒软件的检测 [2]。在测评过程中察觉，低等级信息系统多面临常规病毒、蠕虫攻击，主要通过 U 盘、邮件附件等途径传播，攻击目的以破坏系统正常运行为主；高等级信息系统则容易遭遇定制化木马与勒索软件攻击，攻击者通过社工渗透获取系统入口，植入恶意代码之后控制核心业务模块，以加密数据索要赎金为主要目的，对系统的破

坏性质极强。除此之外，恶意代码的持久化驻留能力明显提升，部分恶意程序会修改系统注册表、创建隐藏进程，即便系统重启也难以彻底清除，给测评过程中的隐患排查带来了挑战 [3]。

2.2 网络渗透攻击

网络渗透攻击为攻击者冲破系统边际防护、非授权访问内部资源的核心方式，也是等级保护测评里对边界安全、访问管控有效性验证的关键切入点。此类攻击遵循“侦察—扫描—利用—提权—维持”的完整轨迹，实操特性极强。在侦察时期，攻击者借助端口扫描、信息搜集工具，获取目标系统的 IP 地址区段、开放端口、操作系统版本等基础信息，为后续攻击进行准备；在扫描时期则将焦点置于系统漏洞与弱口令，针对测评中常见的未修复高危漏洞、默认密码未调整、密码复杂度不足等状况实施精确突破；利用时期通过漏洞利用工具获取系统低权限访问权，再经由提权操作获取管理员权限，最终达成对系统核心资源的掌控。在高等级信息系统测评中，还察觉攻击者会采用“旁路渗透”策略，绕开核心防护装置，通过办公终端、无线网络等薄弱节点切入内部网络，此类攻击轨迹隐蔽性强，易于绕过常规边际防护举措，给测评带来了更大难题 [4]。

2.3 数据泄露攻击

数据作为信息系统的核心资产，是攻击者的主要目标之一，数据泄露攻击也成为等级保护测评中数据安全核查的核心内容。此类攻击的核心意图是窃取系统中的敏感数据，包含用户信息、业务数据、核心机密等，攻击手段呈现出“技术 + 社工”融合的特征。技术层面，攻击者通过 SQL 注入、XSS 跨站脚本等途径，利用系统数据交互接口的漏洞，非法读取、下载敏感数据；社工层面，通过钓鱼邮件、伪基站短信等方式，引诱系统管理员或普通用户泄露账号密码、验证码等关键信息，进而登录系统获取数据。

3 适配等级保护测评要求的防御技术体系搭建与实操要点

3.1 边界防护技术：筑牢系统安全首道防线

边界防护是等级保护测评中边界安全核查的重点，其核心目的是阻断非法访问，过滤恶意流量，保障网络边界的可操控性。针对不同等级信息系统，边界防护技术的配置需体现差异化。低等级信息系统可运用防火墙、入侵检测系统（IDS）搭建基础边界防护，防火墙需严格配置访问控制策略，仅开放业务必需的端口与协议，禁用不必要的服务，防止出现“宽进宽出”的情形；IDS 则用于实时监测边界流量，及时对异常访问行为发出告警。高等级信息系统需在基础防护之上，增设入侵防御系统（IPS）、下一代防火墙（NGFW），实现“检测—防御—阻断”一体化管控 [5]。

3.2 终端防护技术：增强末端安全防护能力

终端作为信息系统的末端节点，是恶意代码攻击、渗透攻击的主要入口，终端防护成效径直作用于体系整体安全，亦是等级保护测评中终端安全核查的关键内容。终端防护技术需聚焦“准入把控—实时防护—应急回应”全流程。准入把控方面，借助终端准入体系，对接入网络的终端开展身份验证与安全状态核查，仅准许契合安全要求（像安装杀毒软件、系统补丁完备）的终端接入，根绝不安全终端接入产生的风险；实时防护方面，布置终端安全管理体系，整合杀毒、恶意代码拦截、主机入侵检测（HIDS）等功能，定时更新病毒库与恶意代码特征库，对终端的文件操作、进程运行、网络连接等行为实施实时监测，及时处理异常行为。

3.3 数据防护技术：守住核心资产安全底线

数据防护是等级保护测评中数据安全与备份恢复核查的核心，需围绕数据“存储—传输—运用—销毁”全生命周期搭建防护架构，保障数据的机密性、完整性与可用性。存储层面，针对敏感数据运用加密存储技术，低等级信息体系可采用文件加密、数据库加密等途径，高等级信息体系需采用透明加密技术，在不干扰业务运用的前提下，达成数据自动加密存储，同时配备访问权限管控，细化不同角色的数据访问范畴；传输层面，对数据传输过程采用 SSL/TLS 等加密协议，规避数据在传输过程中被监听、篡改，特别是跨网络传输的敏感数据，必须经由加密通道传输；在备份恢复层面，依照等级保护测评要求，制定完善的数据备份策略，定时开展全量备份与增量备份，备份数据需存储于安全的离线介质或异地备份中心，同时定时开展备份恢复演练，验证备份数据的完整性与可用性，确保体系遭遇攻击后能迅速恢复数据与业务。

3.4 访问控制技术：构建精细化权限管理架构

访问控制是防范未授权访问、数据泄露的关键是技术，亦是等级保护测评中访问控制核查的核心要求，核心准则是“最小权限”与“权责对等”。低等级信息体系可采用基于角色的访问控制（RBAC）模型，依据用户的岗位职责分配体系权限，确保用户仅具备完成工作所需的最小权限，杜绝超权限访问；同时严格施行密码策略，要求密码具备足够复杂度，定期更换，禁止使用默认密码、弱密码。高等级信息体系需于 RBAC 模型架构之上，构建多因素认证（MFA）、权限审计等制度体系，多因素认证可联合密码设置、动态验证码生成、生物特征识别等形式手段，提升身份认证环节的安全系数，规避单一认证模式遭到破解；权限审计则需周期性对用户权限实施核查工作，清除冗余权限配置、休眠账号数据，对权限变动情形、超权限访问行为开展实时记录与预警操作。测评实践过程当中，需着重验证权限分配的合理程度、身份认证的有效状态，核查权限审计日志的完整情况，保障访问活动具备可追溯性、可管控性。

4 等级保护测评范畴内防御技术有效性验证及优化策略

4.1 防御技术有效性验证手段运用

等级保护测评实操场景下，防御技术有效性验证需采