ISSN：3078-8994
EISSN：3104-4492

面向新型攻击的等级保护测评与密码应用加固研究

文瑞阳 [1,2]　王宇博 [1,2]　佘帅彦 [1,2]　佘瑾南 [1,2]

1. 中国联合网络通信集团有限公司，北京 100033

2. 联通数字科技有限公司，北京 100031

摘　要：随着信息技术的飞速发展，网络安全面临的威胁日益复杂，尤其是新型攻击手段的出现，极大挑战了传统的安全防护体系。等级保护作为我国网络安全的重要管理措施，在应对新型攻击中扮演着至关重要的角色。本文探讨了新型攻击背景下等级保护测评存在的问题，并提出了相应的优化对策。通过加强测评标准的动态更新与自适应性、整合人工智能与大数据技术优化测评与防护、提升测评结果的可操作性与针对性，本文旨在为提升等级保护体系的有效性和应对能力提供理论支持与实践指导。

关键词：新型攻击；等级保护；测评标准；人工智能

0. 引言

伴随网络攻击方式越来越繁复，信息系统的安全防护遇到严峻考验，特别是高级持续性威胁（APT）、零日漏洞等新型攻击手段带来的风险，传统防护措施大多显得力不从心，等级保护是我国网络安全的重要基础制度，要求按照信息系统的核心程度执行分级防护 [1]。现行的等级保护测评标准在面对新型攻击时存在一定挑战，如何通过技术手段精进测评标准，增强其灵活性和针对性，成为提升信息系统防护能力的重要课题。本文将探讨通过技术创新优化等级保护测评与防护体系，提升应对新型攻击的能力。

1. 新型攻击对信息安全的挑战及等级保护的应对重要性

1.1 新型攻击对信息系统安全的威胁

随着科技持续进步，新型的攻击手段变得越来越复杂和难以察觉，因此，传统的防护措施可能不能全面地应对高级持续性威胁（APT）和零日漏洞等新兴威胁。如何增强现有防护体系适应性与反应能力已成为信息系统安全防护工作的关键。比如借助软件漏洞、社会工程学、钓鱼攻击等手段，攻击者可以避开传统防火墙、入侵检测系统等防护措施，继而引发严重的安全问题，物联网、云计算等新方向上，攻击范围持续扩展，信息系统防护承受全新压力，伴随网络攻击技术持续升级，攻击者不再满足于单纯的数据窃取，而是转向谋求对系统的全面掌控，甚至凭借恶意篡改数据和破坏核心基础设施，干扰社会运行以及国家安全。所以找到应对新型攻击的有效防护手段，已变成信息安全方面急切需要处理的难题。

1.2 等级保护在应对新型攻击中的作用

等级保护制度是我国网络安全法框架下的核心安全措施，核心思想是依照信息系统的特性和安全级别实行分层次管理和防护，该体系借助为不同级别的信息系统制定对应的安全要求，建立了一种灵活且高效的防御方式，面对新型攻击，等级保护不只能在系统架构设计时顾及潜在风险因子，还能根据攻击特点实行有针对性的加强。等级保护体系凭借细致分析信息系统的安全风险，帮助发现系统薄弱点，继而设计并执行一系列防护手段，特别是在高等级保护要求的系统里，除了对信息数据本身实行加密防护外，还增强了物理、网络等多方面的安全措施，明显加强了系统应对新型攻击的能力。伴随网络环境和攻击方式的持续变化，等级保护体系可以快速优化防护方法，然后有效减少安全风险，保证信息系统平稳运行 [2]。

1.3 等级保护的动态适应性和持续更新机制

新型攻击的不断进化需要等级保护体系具有动态适应能力与持续更新机制来应对复杂多样的安全威胁。等级保护体系可通过适时更新标准与规范以及增强对新兴威胁实时监控与反应等措施来持续增强对新攻击行为的反应。信息安全漏洞找到后，系统可借助自动补丁管理机制迅速修复，避免攻击者利用漏洞发起攻击，加入人工智能以及机器学习等技术，能让系统在察觉异常行为时快速检测和响应，防止攻击造成大范围损害，凭借及时识别与应对新型攻击，等级保护可以增进防护体系的灵活性和成效，让信息系统适应变化中的安全形势。

2. 新型攻击下等级保护测评存在的问题

2.1 现有测评标准难以应对复杂攻击手段

面对新型攻击手段，传统的等级保护测评

ISSN：3078-8994
EISSN：3104-4492

标准可能在应对复杂威胁时有所局限。为了提升测评标准的适应性，建议加强对未知攻击方式的检测与响应，尤其是在 APT 攻击、勒索病毒和零日漏洞等新型威胁的识别能力上。现有标准一般无法快速更新，跟不上攻击技术的转变速度，致使面对新威胁时显得迟缓。

现有标准中，攻击复杂性、持续性以及攻击深度的分析较为薄弱，许多标准更依赖人工设定的安全阈值与定期检查流程，这致使面对未知、突发的攻击手段时缺乏适应性与灵活性，攻击者一直研发创新技术，上述技术不光能突破传统防御措施，还能绕开现有安全检测机制。如今的攻击更依赖社会工程学、智能化手段以及云计算、物联网等新兴技术，传统测评标准没能跟上变化，比较难给予有效防御方法 [3]。

2.2 安全防护和测评环节脱节

安全防护以及测评环节的脱节是目前等级保护测评中的一个突出问题，很多信息系统里，安全防护措施与等级保护测评一般处于不同阶段，互动和协同不足，等级保护测评意在检验信息系统的安全防护能力，但实际操作中，防护手段和测评结果的反馈大多没能形成有效闭环。具体表现为，测评中发现的安全问题没有及时修补成实际防护手段，而一些理论借助的系统，面对冗杂攻击时却没能有效抵御，这一种脱节现象让测评结果的真实性和成效大幅减少。

防护措施和测评环节的脱节体现在测评标准和防护方案匹配度不高，系统设计以及防护期间，很多安全策略未顾及测评要求，或实行时忽略结果中的潜在风险，测评可能指出某个系统有特定的安全漏洞或缺陷，但防护方略实际执行时，总是因为缺乏反馈机制，致使漏洞没能及时修复或加强。安全防护的动态更新与测评环节同步性差，系统在更新防护方针时未经过全面分析，增加了新型攻击威胁的风险，所以只有加强安全防护和测评环节的密切配合，才能保证系统应对越来越繁复的安全威胁时具备足够能力。

2.3 测评结果的可操作性差

目前等级保护测评可以检测出系统存在安全漏洞，但是为了增强实际操作性可以进一步强化报告漏洞修补建议及执行步骤，保证了测评结果更具有可操作性，有利于有关部门快速采取有效的加固措施。测评结果不够实用，企业以及机构不容易依据报告制定加固方针或安全精进方案。测评结果一般偏理论，缺少详细技术细节和实践参照，实际操作人员面对报告时不知怎样下手，不容易将结果转化为详细技术行动 [4]。

测评结果一般缺少针对不同系统和应用场景的具体操作方向，特殊需求的系统难以获得定制化解决办法，管理员与安全人员只能参照通用修复方法，忽略了系统的独特性和复杂性，不同的系统环境以及攻击模型，需要不同的防护方案。不过现有测评标准没有顾及这样的差别，致使实际使用时不容易增强系统的安全性，所以增强测评结果的实用性，让其能在具体操作中实行，已变成增进等级保护成效的重要环节。

3. 新型攻击下的等级保护优化对策

3.1 加强测评标准的动态更新与自适应性

新型攻击手段的快速演化要求等级保护测评标准可以及时更新，同样具备较强的自适应能力，为了跟上信息技术的变化，等级保护的测评标准需要定期修订，保证可以体现最新的安全威胁和防护技术，新的网络攻击方式、恶意软件变种以及攻击者繁复的手法，都要求测评标准增加新的检测维度。为此可以设立一个灵活的标准更新机制，借助对新型威胁的跟踪与分析，快速优化测评指标、检测方法和安全防护要求，这一类机制不光需要政府或行业的标准化组织发挥作用，还应助推企业以及学术界加入标准改良工作，保证测评标准可以应对最新的攻击手段。

测评标准需要有一定的自适应特点，面对不同的信息系统和使用场景时，可以灵活改变关注点和方式，信息系统的复杂性与多样性要求测评标准避免“一刀切”，而是融合系统实际状况实行有针对性的测评，针对云计算环境以及传统数据中心的安全要求差异，测评标准需要有所区分，特别是在防护机制和漏洞检测方面应体现详细的适应性。凭借使用依据场景的测评方式，可以增进测评结果的关联性和实用性，让测评标准灵活应对各种繁复攻击形态及环境变化。

动态更新和自适应性的增强需要靠着技术助力，特别是借助大数据以及人工智能等技术实现快速捕捉新型攻击趋势，分析历史攻击数据后，可以推测可能出现的攻击方式，并提前设定到测评标准里，定期开展安全审查和系统漏洞检测，为测评标准的精进给出依据，保证紧跟时代变化。凭借此类手段，测评标准不只能更高效地检测和防御新型攻击，还能为后续防护加固给出更准确的方向。

3.2 整合人工智能与大数据技术优化测评与防护

人工智能和大数据技术的融合，为等级保护测评和防护开辟了全新的优化方式，人工智能技术，特别是机器学习与深度学习，可以助力解析海量的安全日志以及事件数据，发现隐藏的安全隐患及攻击行为，借助对网络流量、系统调用、用户行为等各类信息的即时解析，

ISSN：3078-8994
EISSN：3104-4492

人工智能可以提前发出预警，并迅速执行防御措施。这一类预测性防护比传统规则防御更高效，人工智能能发现新未知攻击形式，突破了仅依赖已知攻击的限制。

大数据技术处理海量信息、识别冗杂攻击形式时，作用十分重要，借助对系统日志、网络流量及用户行为等数据的实时存储与分析，这项技术有利于发现攻击形式和检测安全漏洞，借助大数据平台，安全团队可以迅速开展跨系统、跨区域的安全分析，找出可能的攻击途径和漏洞，提前修复问题。靠着这一些技术方法，等级保护的检测可以更准确地发现安全隐患，同样为企业给予更高效且合理的防护方案，帮助防护手段更好地应对冗杂攻击方式。

防护环节里，人工智能和大数据联手能让安全防护更智能、更自动，比如人工智能能用来自动修复漏洞，凭借实时查看系统运行情况，找出潜在问题，优化安全策略，大数据则借助攻击趋势的分析，帮企业推测可能的安全隐患，提前做好应对准备。整合这两种技术，不只可以加强等级保护的检测准确性，还能大幅增强系统的防护能力，保证信息系统面对新型攻击时，快速反应且有效阻止。

3.3 提升测评结果的可操作性与针对性

增进等级保护测评结果的实用性和准确性，是保证测评成果可以有效增强系统安全性的核心举措，目前测评结果一般以报告形式表现，内容较为抽象，缺少实际操作的具体办法，为了增强测评结果的实用性，需要对测评报告的结构和内容加以优化。报告中应包含详细的安全漏洞解析、修复方法以及操作步骤，同样贴合系统特性，为不同级别的用户给出有针对性的解决办法，针对高风险漏洞，报告需说明优先处理的方式；而对较低风险漏洞，则可提出定期巡查与监控的方法。上述详细的修复步骤和方法可以协助企业或机构依据测评结果实行系统加固，减少因报告内容不明确引发的安全风险 [5]。

增强可操作性时，测评结果的表现方式需要更直观易懂，传统测评报告可能过于技术化，非技术人员比较难理解，所以要用图表、数据分析等形式，让决策者更好掌握安全状况，报告中需清楚说明每项安全加固措施的实行顺序，保证执行者能依照报告内容有效完成改良。借助此类方法，可拉近检测结果和实际操作的距离，增进信息系统防护的实际效果。

更深一步增强测评结果的准确性，还需顾及不同系统的详细需要，不同等级的信息系统，防护要求以及安全需求差异明显，所以测评报告应融合系统特性给予专属的加固方案，核心基础设施或涉及敏感信息的系统，需优先增加安全防护水平，同样给出更贴合实际的加固方向。借助融合系统的业务特性、技术架构以及运营环境，制定更有针对性的测评方案，能更高效地发现并修复潜在的安全漏洞，针对新型攻击的防护措施也应变成报告的重点，保证方略随时更新，应对目前威胁最大的攻击方式，凭借增强测评结果的实用性与准确性，不只能加强防护效果，又能减少安全事件的发生可能。

4. 结论

新型攻击的产生为传统的等级保护体系带来更多需求，促进测评标准动态更新及自适应性增强，并结合人工智能及大数据技术实现测评及防护的最优化，通过提高评估结果的实用性和精确度，等级保护体系的防护性能将得到明显的增强。在网络攻击手段不断发展的同时，等级保护测评也需不停地优化与精进，以确保能应对新安全威胁。在这一进程中，不断更新测评标准，强化实时威胁监测和增强系统自动化响应能力将是今后的一个重要方向。本研究对强化等级保护体系效果给出切实可行的思路，并提出具体技术路径，以期对后续研究及实践提供宝贵理论依据及操作框架。通过不断地创新和运用技术手段，可以有效地提高我国信息系统面对复杂攻击的防护能力以及应对水平，促进我国网络安全防护体系不断地改进和优化。

参考文献：

[1] 范仲伟，杨丹，曹德宇，等．基于属性攻击图的等级保护整体测评方法和系统．CN202211052954.8[2025-10-29].

[2] 王昊宇．渗透测试在网络安全等级保护测评中的应用探讨 [J]. 信息产业报道，2024(11):0190-0192.

[3] 张雨竹．网络安全等级保护测评项目管理系统的设计与实现 [D]. 西南大学，2023.

[4] 克金超，李威，姜传喜，等．DCS 系统的等级保护测评系统：CN202311081461.1[P]. CN116866083A[2025-10-29].

[5] 何飞，葛巍．基于网络安全等级保护下数据安全治理探讨 [J]. 2024(7):68-70.

作者简介：文瑞阳（2001.5—），男，汉族，陕西咸阳，本科，研究方向：网络安全；信息安全。