网络安全风险管控策略研究

宣俊
中核第七研究设计院有限公司，山西 太原 030012
DOI: 10.61369/TACS.2026010022

摘　　要： 新时代下，信息技术迅猛发展，数字化转型不断深入，网络安全成为国家关键基础设施、企业运转和个体隐私保护的坚实保障。针对当前主流的网络威胁类型，即计算机病毒、系统漏洞、黑客攻击、网络欺骗等，从技术原理和管控策略两个方面进行分析，在此基础上提出多层次、多维度的网络安全风险管控策略。全面防控并创建起“预防—监测—响应—恢复”一体化的安全治理体系，提升组织整体网络安全韧性，削减安全事件出现的几率和影响程度，对推动网络安全体系现代化有着现实意义。
关 键 词： 网络安全；风险；问题；攻击类型；管控策略

Research on Cybersecurity Risk Management Strategies

Xuan Jun
China Nuclear No.7 Research and Design Institute Co., Ltd., Taiyuan, Shanxi 030012

Abstract: In the new era, with the rapid development of information technology and the deepening of digital transformation, cybersecurity has become a solid guarantee for national critical infrastructure, enterprise operations, and personal privacy protection. Targeting the current mainstream types of cybersecurity threats—including computer viruses, system vulnerabilities, hacker attacks, and phishing attacks—this paper conducts an analysis from two aspects: technical principles and management strategies. On this basis, it proposes a multi-level and multi-dimensional cybersecurity risk management strategy. Comprehensive prevention and control are implemented to establish an integrated security governance system of "Prevention - Monitoring - Response - Recovery", which enhances the overall cybersecurity resilience of the organization, reduces the probability and impact of security incidents, and has practical significance for promoting the modernization of the cybersecurity system.
Keywords: cybersecurity; risk; problems; attack types; management strategies

引言

近年来，全球范围内的重大网络安全事件频频发生，显示出现有网络安全防御体系存在不足。我国网络安全法、数据安全法等法律相继出台，网络安全治理也从国家战略的高度被提到了议事日程上。但是，由于攻击手段越来越智能化、攻击目标越来越精准、攻击后果越来越连锁，传统的边界防御模式已经不能应对新型复合式威胁。因此，急需从风险识别、评价、处置到复盘的全过程角度来创建动态的、协同的、智能的风险管控体系。本文立足于当前网络安全形势，对典型的网络安全风险源进行梳理，研究出科学有效的综合防控措施，为相关研究和实践提供理论支持和操作指南。

一、网络安全风险与问题

网络安全存在着诸多风险和问题，严重危及网络环境的稳定以及用户的权益。网络作为信息传播的平台，其高速、广泛的传播特点被不法分子利用，用来散布不良信息甚至从事非法活动。此类内容传播速度快、影响范围广，对青少年身心健康造成严重危害，产生不良社会后果，给网络监管带来巨大压力[1-3]。其次，网络病毒属于恶意程序，依靠网络传播，破坏性极强，容易造成用户系统崩溃、数据丢失并且难以恢复，严重影响正常使用。第三，信息库的安全存在很大风险，不法分子利用非法手段进入数据库盗取、篡改、删除或者破坏用户的重要个人信息，既侵犯了隐私权，又造成巨大的经济损失和信任危机。网络安全威胁不单是软件、数据层面的，还会对硬件设施造成实质性损害。计算机病毒在感染的过程中会干扰服务器、路由器等网络设备的正常运行，造成设备功能异常或者物理损坏，从而影响整个网络系统的稳定性与可用性[4]。网络安全问题包含信息内容、软件系统、数据资产、硬件设施等各个方面，需要依靠技术防护、制度建设、用户教育等多方面措施来应对，从而构建出更加安全、健康的网络

环境。

二、常见的网络攻击类型分析

（一）病毒

计算机病毒具有自我复制的能力，属于一种恶意程序，它会依附于合法程序或者文件，在某些情况下被激活，从而执行预设的破坏性或者干扰性操作。病毒大多经由网络传播、移动存储设备或者软件下载等方式传播，一旦入侵到目标系统当中，就会引发数据遭到破坏，系统效能变差，信息泄露，或者完全瘫痪等状况。从理论上讲，病毒运行机制要依靠宿主程序的执行环境，它的代码结构一般包含引导模块、传播模块、触发模块，分别完成启动、复制、恶意行为实施等工作。病毒的隐蔽性、变异性使得传统的安全机制很难彻底识别和清除病毒，多态、变形技术的发展又使得病毒可以动态改变自身的特征码来逃避检测。病毒不仅对个体终端构成直接的威胁，而且由于它的传播性而给整个网络生态的安全稳定造成系统性的风险 [5]。

（二）系统漏洞

系统漏洞是指操作系统、应用程序或者网络协议在设计、实现或者配置过程中存在的缺陷或者疏漏，这些缺陷可以被攻击者利用来获取未授权访问、提升权限或者执行任意代码。漏洞的本质就是软件开发周期中没有对安全性进行考虑，即逻辑错误、边界条件处理不当、输入验证缺失等。理论上任何复杂的系统都存在着潜在的漏洞，漏洞的危害程度是由漏洞的可利用性、影响范围、修复难易程度决定的。漏洞可以分为已知漏洞和未知漏洞，已知漏洞可以依靠补丁或者配置调整来解决，而未知漏洞则叫零日漏洞，它缺乏防御措施，更加危险。另外漏洞的生命周期管理包含发现、披露、修复、验证等各个环节，任何一个环节的滞后都会使系统暴露于风险的时间窗口变长。因此系统漏洞不但是技术层面的安全隐患，也是贯穿软件工程全生命周期的安全治理问题。

（三）黑客与网络欺骗

黑客攻击是指具备较高技术水平的个人或者组织为了达到非法目的，突破系统防护，进行网络攻击的行为，其动机有信息窃取、服务中断、经济勒索、政治目的等。网络欺骗属于黑客常用的一类战术，它会假扮身份、篡改通信内容或者创建虚假的服务环境，从而引导用户或者系统作出非预期的反应。此类攻击利用的是人机交互中信任机制的缺陷、协议设计中的认证盲区 [6]。中间人攻击依靠通信双方没有端到端验证，钓鱼攻击则用社会工程学原理操纵用户行为。黑客与网络欺骗的核心就是伪装、误导，其成功与否取决于目标系统身份鉴别强度、用户安全意识水平、防御体系的纵深程度。

三、网络安全风险管控策略

（一）建立健全安全治理体系

网络安全风险的有效控制首先要有一个结构清晰、职责明确的安全治理体系。该体系应包含组织架构、制度规范、流程机制、监督问责等各个方面。企业或者机构应当设立专门的网络安全管理部门，明确首席信息安全官的职责，并把安全责任层层分解到各个业务单元。另外还应建立覆盖全生命周期的安全管理制度，包括资产识别、风险评估、事件响应、合规审计等环节，保证安全策略同业务目标高度契合。治理框架还要加入国家以及行业标准，从而提高合规性以及国际互认度。定期开展内部审计、第三方评价可以及时发现治理的盲区并促使持续改进。更重要的是，高层管理者要把网络安全当作战略问题而不是单纯的技术问题，用资源投入、文化建设、绩效考核等方式营造全员参与、全程可控的安全生态 [7-8]。只有制度保障和组织协同才能使系统性风险由被动防守变为主动治理，从根本上降低风险。

（二）强化技术防护纵深防御

面对日益复杂的网络攻击手段，单一的防线已经不能应对高级持续性威胁、零日漏洞利用、供应链攻击等风险。因此要建立多层次、多维度的纵深防御体系。该体系要覆盖网络边界、终端设备、应用系统、数据存储和传输等主要部分。在网络层部署下一代防火墙、入侵检测和防御系统，在终端侧实施端点检测和响应方案，结合行为分析识别异常活动，在应用层面采用 Web 应用防火墙、代码审计、安全开发实践，在数据层面采用加密、脱敏、访问控制、数据防泄漏技术来保障敏感信息不被非法获取 [9]。另外，零信任架构已经成为主流趋势，它的主要思想就是“永不信任，始终验证”，用身份认证、最小权限原则、动态访问控制大大压缩了攻击面。技术防护还要和自动化响应机制联动，SOAR 平台可以威胁发生时快速隔离、溯源、修复。只有依靠技术手段的立体化部署和智能协同，才能在攻防对抗中占据主动。

（三）推进常态化风险评估与监测

网络安全风险具有动态性、隐蔽性，不能用一次性的评估来满足长期的防护需求。因此必须建立常态化的风险评估、实时监测机制。风险评估应定期开展，以资产重要性、威胁情报、脆弱性扫描、业务影响分析等为量化风险等级和优先级处置计划的依据。同时要使用威胁建模的方法，预测出潜在的攻击路径，提前对薄弱环节进行加固。在监测上需要部署安全信息与事件管理系统，将日志、流量、用户行为等多源数据整合起来，用机器学习和关联分析技术来实现对异常活动的早期预警。威胁情报共享平台的接入可以使得组织及时了解新型攻击手法以及恶意 IP、域名等指标，从而加强前瞻性防御。风险评估不能只考虑 IT 系统，还要考虑供应链、第三方合作方和云服务环境，防止由于外部依赖而产生未知风险。通过评价、监测、反应、改善的闭环管理，组织可以不断地感知到风险态势的变化，动态地调整防护策略，由“事后补救”转变为“事前预防”。

（四）加强人员意识培训与应急演练

技术再先进，如果人员安全意识差，仍然会成为攻击的弱点。全球又超过80% 的安全事件是由人为失误造成的，如点击钓鱼邮件、使用弱密码或者违规外发数据等等。因此必须把人员当作风险控制的重要环节 [10]。一方面要开展分层级、场景化的安全意识培训，面向普通员工普及基础防护知识，面向开发人员强

化安全编码规范，面向管理层强调合规责任和决策风险。培训形式可以有多种多样，如在线课程、模拟钓鱼测试、案例复盘等，以提高参与感和实效性。另一方面要创建完备的网络安全应急预案，定时开展实战演练，检测响应流程是否可行以及团队协作水平如何。演练之后要开展复盘总结工作，对预案的细节加以优化，保证在真实的事件出现时，可以迅速遏制损失并恢复业务。还应该建立举报和奖励制度，鼓励员工举报安全隐患。只有把“人”纳入到整体防御体系中，形成技术、制度、文化三者并重的防护格局，才能真正筑牢网络安全的最后一道防线。

四、结论

综上所述，网络安全风险是不可控的，通过对病毒传播机制、系统漏洞利用方式、黑客社会工程学等攻击手段的分析，发现目前网络安全防护体系存在的薄弱环节。在此基础上提出的综合性风险管控策略是“人防、技防、制防”三者结合，即防火墙、入侵检测、加密认证等技术屏障的加强，安全管理制度的完善，等级保护要求的落实，员工安全意识培训的加强，快速响应和灾备恢复机制的建立，从而提高组织在遭受攻击后的韧性与恢复能力。未来网络安全风险管控会越来越智能、越来越主动。

参考文献

[1] 刘欣 . 基于危险理论的数字电网网络安全风险预警研究 [J]. 自动化技术与应用 ,2024,43(02):102-106.

[2] 梁业裕 . 基于 IPv6 资产测绘的企业网络安全风险评估分析 [J]. 电子技术 ,2024,53(02):258-259.

[3] 刘妍君 . 面向公路信息化建设的网络安全风险管理框架设计 [J]. 运输经理世界 ,2024,(02):71-73.

[4] 张宏 . 大数据时代计算机网络安全风险与控制策略探究 [J]. 信息与电脑 (理论版),2024,36(01):217-219.

[5] 吴树芳 , 高梦蛟 , 朱杰 . 基于三级编码的智能城市网络安全风险评估体系构建研究 [J]. 情报杂志 ,2024,43(03):198-207.

[6] 黄琼 .IP 架构在广播电视制播领域的应用和网络安全风险防范 [J]. 电视技术 ,2023,47(12):182-185.

[7] 施雪清 . 基于人工智能技术的计算机网络安全风险评估系统设计 [J]. 信息与电脑 (理论版),2023,35(23):199-202.

[8] 徐波 , 王昕 . 数字孪生水利工程网络安全风险分析和保障体系 [J]. 人民长江 ,2023,54(11):242-250.

[9] 杨倩晨 . 基于知识图谱的舰船通信网络安全风险评价研究 [J]. 舰船科学技术 ,2023,45(21):189-192.

[10] 刘旭东 , 周琳娜 , 任婷 .ChatGPT 带来的网络安全风险挑战及应对举措 [J]. 工业信息安全 ,2023,(02):73-78.

[11] 卜哲 , 叶帅辰 . 基于五维指标体系的网络安全风险值评估及预测 [J]. 无线互联科技 ,2023,20(07):144-150+157.

[12] 郭荣华 , 许世平 , 刘喆 , 等 . 装备软件供应链网络安全风险分析与对策 [J]. 信息安全与通信保密 ,2023,(03):103-112.

[13] 常杰 , 董蕴萌 , 刘硕 , 等 . 基于 PFWA 算子的层次化网络安全风险量化评估方法 [J]. 河北电力技术 ,2023,42(01):62-65.

[14] 顾磊 . 建立中国石化网络安全风险管控和处置机制研究 [J]. 信息安全研究 ,2022,8(11):1141-1144.

[15] 汪全胜 , 宋琳璘 . 我国未成年人网络安全风险及其防范措施的完善 [J]. 法学杂志 ,2021,42(04):91-100.

