中小型企业网络安全问题及其解决方案探究

罗淇
云南金质信息技术服务有限公司，云南 昆明 650000
DOI: 10.61369/TACS.2025060012

摘　　要： 随着数字化转型推进，中小型企业对网络的依赖度持续提升，但网络安全防护能力未能同步跟进，成为网络安全风险的高发群体。本文从技术防护、管理体系、员工意识、资金投入及外部威胁五个维度，剖析中小型企业网络安全现存问题，深入梳理各类问题的表现形式与内在成因，旨在为中小型企业构建科学有效的网络安全防护体系提供思路，助力企业在数字化发展中规避安全风险，实现稳定运营。

关 键 词： 中小型企业；网络安全问题；解决方案

Exploration on Cybersecurity Issues and Their Solutions for Small and Medium-Sized Enterprises

Luo Qi
Yunnan Hi-Q Information Technology Service Co., Ltd, Kunming, Yunnan 650000

Abstract: With the advancement of digital transformation, the dependence of small and medium-sized enterprises (SMEs) on networks continues to increase, but their cybersecurity protection capabilities have not kept pace, making them a high-risk group for cybersecurity threats. This paper analyzes the existing cybersecurity issues of SMEs from five dimensions: technical protection, management systems, employee awareness, capital investment, and external threats. It also conducts an in-depth review of the manifestations and internal causes of various issues, aiming to provide ideas for SMEs to build a scientific and effective cybersecurity protection system. This will help enterprises avoid security risks in their digital development and achieve stable operations.

Keywords: small and medium-sized enterprises (SMEs); cybersecurity issues; solutions

引言

在数字经济蓬勃发展的当下，网络已成为中小型企业开展生产经营、对接客户资源、管理内部流程的核心支撑，其重要性不言而喻。然而，与大型企业相比，中小型企业在网络安全建设上存在明显短板，安全防护能力与网络应用需求之间的差距不断扩大，导致各类网络安全事件频发。这些安全事件不仅会造成企业直接的运营中断与财产损失，还可能损害企业长期积累的客户信任与市场声誉，对企业的可持续发展构成严重威胁[1]。因此，深入分析中小型企业网络安全现存问题，探索适配的解决路径，对保障中小型企业数字化转型成效、维护市场秩序稳定具有重要现实意义。

一、中小型企业网络安全现存问题

（一）网络安全技术防护薄弱

中小型企业在网络安全技术部署上普遍存在短板，多数企业仍在使用老旧的网络设备与软件系统，设备运行稳定性不足，且缺乏定期的维护与升级，导致设备自身存在的安全漏洞长期无法修复，为网络攻击提供了可乘之机。同时，企业缺乏专业的技术人员，难以搭建完善的安全防护体系，多数未部署有效的防火墙与入侵检测系统，对终端设备的安全管控也较为松散，无法及时识别恶意软件与非法访问行为[2]。此外，企业在数据安全保护上投入不足，数据加密与备份机制不完善，一旦遭遇数据丢失或篡改，难以快速恢复，进一步加剧了安全风险。

（二）网络安全管理体系不完善

中小型企业普遍缺乏系统化的网络安全管理体系，多数企业未制定明确的网络安全管理制度，安全责任划分模糊，往往由 IT 人员兼任安全管理工作，导致安全管理精力分散，难以专注于专业的安全防控工作。企业缺乏常态化的安全风险评估机制，无法定期排查网络环境中的安全隐患，对潜在风险的预判能力不足，常等到安全事件发生后才被动应对[3]。同时，应急响应机制缺失，一旦遭遇网络攻击，缺乏清晰的处置流程与恢复方案，导致事件

影响范围不断扩大，延长了业务中断时间，造成更大的损失。此外，企业未建立有效的安全审计制度，无法对网络操作行为进行全程监督，难以追溯安全事件的根源，也无法及时调整安全防护策略。

（三）员工网络安全意识淡薄

员工网络安全意识不足是中小型企业网络安全防护的重要薄弱环节，多数员工缺乏基础的网络安全知识，对钓鱼邮件、恶意链接等常见的网络攻击手段识别能力较弱，容易因误操作点击危险链接或打开恶意附件，为网络攻击提供入口。在日常工作中，员工存在诸多不安全操作习惯，如使用简单易破解的弱密码、随意共享账号权限、违规外接私人存储设备等，这些行为直接破坏了企业的网络安全防护屏障[4]。同时，企业对员工的网络安全培训重视不足，培训频率低且内容缺乏针对性，无法有效提升员工的安全意识与操作规范，导致员工在工作中难以落实企业的安全防护要求，进一步放大了网络安全风险。

（四）外部网络安全威胁

中小型企业正面临日益复杂的外部网络安全威胁，随着网络技术的发展，黑客攻击手段不断升级，攻击形式愈发隐蔽多样，对企业的网络安全构成严重挑战。当前，针对中小型企业的勒索软件攻击频发，攻击者通过加密企业核心数据索要赎金，直接导致企业业务中断，若无法满足勒索要求，甚至可能造成数据永久丢失。钓鱼攻击也呈现精准化趋势，攻击者通过伪装成企业合作伙伴或官方机构发送邮件，诱导员工泄露敏感信息[5]。此外，供应链攻击成为新的威胁形式，攻击者通过渗透企业上下游合作伙伴的网络，间接获取目标企业的访问权限，扩大攻击范围。这些外部威胁不仅会造成企业经济损失，还可能导致客户信息泄露，严重损害企业声誉，对中小型企业的生存与发展带来冲击。

二、中小型企业网络安全问题解决方案

（一）强化网络安全技术防护体系建设

中小型企业需从基础设备与核心防护技术两方面入手，构建分层、立体的网络安全技术防护体系。首先，应定期对老旧网络设备进行更新与维护，优先更换运行不稳定、存在已知漏洞的路由器、交换机等硬件，同时及时升级操作系统与应用软件的固件，关闭不必要的端口与服务，从源头减少安全隐患。其次，部署适配企业规模的防护系统，如新一代智能防火墙，实现对进出网络流量的实时监测与异常拦截；引入入侵检测与防御系统（IDS/IPS），精准识别恶意攻击行为并自动阻断，尤其针对常见的端口扫描、SQL 注入等攻击手段形成有效防护。此外，加强终端设备安全管控，为员工电脑、移动办公设备安装统一的杀毒软件与终端安全管理系统，限制违规外接存储设备的使用，防止恶意软件入侵与数据泄露[6]。在数据安全层面，需对核心业务数据进行分类分级管理，采用对称加密与非对称加密相结合的方式保护数据传输与存储安全，同时建立多副本、异地备份机制，定期开展数据恢复演练，确保遭遇勒索软件攻击或硬件故障时，能快速恢复数据与业务运行。

（二）健全网络安全管理体系

健全的网络安全管理体系是保障技术防护措施落地的关键，中小型企业需从制度、组织、流程三方面完善管理机制。首先，制定系统化的网络安全管理制度，明确网络接入、设备使用、数据管理、权限分配等环节的操作规范，例如规定员工账号密码的复杂度与定期更换要求，明确敏感数据的访问权限范围，禁止未经授权的网络访问行为，确保安全管理有章可循。其次，优化组织架构，根据企业规模设立专门的网络安全管理岗位或部门，若资源有限可由专人专职负责网络安全工作，避免 IT 人员兼任导致的精力分散，同时明确安全管理职责，将安全责任落实到具体岗位与个人，形成“全员参与、专人负责”的管理格局。再者，建立常态化的安全风险评估与应急响应机制，定期组织内部或委托第三方对企业网络环境、系统漏洞、数据安全等进行全面评估，及时发现并整改潜在风险；制定详细的网络安全事件应急处置预案，明确事件分级标准、响应流程、责任分工与恢复措施，一旦发生攻击事件，能快速启动预案，减少损失并缩短业务中断时间[7]。此外，完善安全审计制度，对网络操作行为、系统访问记录、数据传输情况等进行全程日志记录与定期审计，实现安全事件的可追溯，同时通过审计结果优化安全管理策略，形成“评估—整改—审计—优化”的闭环管理。

（三）提升员工网络安全意识与技能

员工是网络安全防护的“第一道防线”，提升员工安全意识与技能需从培训、宣传、考核三方面构建长效机制。首先，制定针对性的网络安全培训计划，根据员工岗位差异设计培训内容：对技术岗位员工重点培训漏洞扫描、攻击防御、应急处置等专业技能；对普通岗位员工则聚焦基础安全知识，如识别钓鱼邮件的特征（虚假发件人、诱导性链接、可疑附件）、弱密码的危害与设置方法、违规操作（如随意共享账号、外接私人设备）的风险等，确保培训内容贴合员工实际工作需求。其次，创新培训形式以提升效果，除传统的线下讲座、线上课程外，可引入案例教学，分享同行业中小型企业遭遇网络攻击的真实案例，让员工直观感受安全风险；开展模拟钓鱼演练，向员工发送仿真钓鱼邮件，测试员工识别能力并针对性辅导，帮助员工在实践中提升技能。同时，加强日常安全宣传，通过企业内部公告栏、工作群、邮件等渠道，定期推送网络安全小贴士、最新攻击手段预警等内容，营造“人人重视安全、时时关注安全”的氛围[8]。此外，建立培训考核与激励机制，将网络安全知识与技能考核纳入员工日常绩效评估，对考核优秀、及时发现安全隐患的员工给予奖励，对因违规操作导致安全风险的员工进行批评教育与再培训，通过正向激励与反向约束，推动员工养成良好的安全操作习惯，从根本上减少人为因素引发的安全事件。

（四）优化网络安全资金投入与配置

中小型企业需转变“重业务、轻安全”的投入观念，通过科学规划实现网络安全资金的高效利用。首先，明确资金投入的优先级，结合企业核心业务需求与安全风险评估结果，将资金优先投向关键领域：如保障核心业务系统的防护设备采购、客户数据与商业机密的加密技术研发、应急响应所需的备份系统建设等，

避免资金分散投入导致“面面俱到却处处薄弱”的问题。其次，探索性价比高的投入模式，针对中小型企业资金有限的特点，可优先选择云安全服务替代传统硬件采购，如云防火墙、云备份、云杀毒等服务，不仅能降低前期设备购置成本，还能减少后期维护费用，同时享受服务商提供的实时技术更新与威胁防护，实现“低成本、高防护”[9]。再者，合理分配资金结构，将安全资金分为硬件采购、软件升级、人员培训、第三方服务、应急储备等模块，避免单一模块过度投入，例如在人员培训上适度增加投入，可减少因员工操作失误导致的安全损失，形成“投入—防护—降损”的良性循环。此外，建立资金投入效果评估机制，定期分析安全资金的使用情况与防护效果，如通过对比投入前后的安全事件发生率、损失金额等指标，判断资金配置是否合理，及时调整投入方向与比例，确保每一笔资金都能发挥最大的安全防护价值，避免盲目投入与资源浪费。

（五）借助外部力量提升网络安全防护能力

中小型企业可通过整合外部资源，弥补自身技术、人员、资金的不足，构建多元化的安全防护支撑体系。首先，加强与专业第三方安全服务机构的合作，根据企业需求选择适配的服务类型：如委托机构开展定期的网络安全风险评估与漏洞检测，借助其专业工具与技术团队发现企业自身难以察觉的安全隐患；引入Managed Security Service Provider（MSSP，托管安全服务），由服务商提供7×24小时的实时安全监控、攻击拦截与应急响应服务，相当于为企业配备“外部安全运维团队”，解决内部技术人员不足的问题；在遭遇复杂攻击事件时，寻求第三方机构的应急支援，快速溯源攻击源头并恢复系统运行，减少事件影响[10]。其次，加入行业网络安全联盟或协会，参与行业内的安全信息共享与交流活动，及时获取针对本行业的最新攻击手段、威胁情报与防护方案，例如制造业企业可了解勒索软件对生产系统的攻击模式，服务业企业可掌握客户数据泄露的防范要点，通过行业协作提升整体防护水平。

在数字经济深入发展的背景下，中小型企业网络安全防护能力的强弱，直接关系其数字化转型成效与可持续发展。本文通过剖析中小型企业在技术防护、管理体系、员工意识、资金投入及外部威胁层面的核心问题，针对性提出 “技术筑基、管理提效、人员赋能、资金优化、外部协同” 的系统性解决方案。这些方案并非孤立存在，而是需相互衔接、形成闭环，方能构建适配中小型企业规模与资源的安全防护体系。唯有中小型企业切实重视网络安全建设，将安全理念融入经营全流程，才能有效抵御各类安全风险，为自身发展筑牢安全屏障，同时为数字经济的稳定运行注入微观动力。

参考文献

[1] 丁蓓蓓 . 加快推进中小企业数智化转型的实践要求与路径 [J]. 中国集体经济 , 2024, (07): 21-24.

[2] 谷彦章 . 我国中小企业网络安全建设面临的挑战与对策 [N]. 市场信息报 , 2025-01-27 (014).

[3] 王炳翔 . 中小企业网络安全管理模型研究 [J]. 网络安全技术与应用 , 2024, (11): 91-95.

[4] 冯前进 . 数字化背景下我国中小企业网络安全等级保护实现路径研究 [J]. 网络安全技术与应用 , 2024, (10): 101-103.

[5] 李茹 , 翟书颖 , 李波 . 中小企业网络安全防御体系研究 [J]. 微型电脑应用 , 2023, 39 (06): 1-3.

[6] 郝钢有 . 中小企业安全等级保护网络防护研究 [J]. 无线互联科技 , 2023, 20 (05): 151-154.

[7] 王韧 , 许豪 , 王中杰 , 等 . 异质性视角下中小企业网络安全防御的最优投资策略 [J]. 系统工程理论与实践 , 2023, 43 (02): 398-420.

[8] 李舒沁 . 欧盟中小企业网络安全风险应对与启示 [J]. 网络安全技术与应用 , 2022, (04): 132-134.

[9] 贵彩虹 , 曹新洲 . 大数据应用视角下中小企业智慧网络安全感知平台总体架构的构建 [J]. 信息系统工程 , 2021, (12): 20-23.

[10] 范渊 , 叶鹏 . 数字化转型背景下中小企业安全防护策略研究 [J]. 新型工业化 , 2021, 11 (10): 8-10.

