信息化背景下企业网络安全风险及对策研究

李 旗 周云飞
河北方维网络技术有限公司 河北 石家庄 050000

摘 要：在信息化深度融入企业运营的背景下，网络安全已成为企业发展的关键保障。本文聚焦企业网络安全领域，首先阐述保护数据资产、保障业务连续性与提升客户信任三大核心重要性，随后从外部攻击、内部管理、技术漏洞三方面剖析风险，最后对应提出加强外部威胁防护、防范内部威胁、完善安全管理体系的策略，为企业应对网络安全挑战、构建稳固安全防线提供理论与实践参考。

关键词：信息化背景下；企业网络；安全风险；对策研究

引言：当前，信息化技术推动企业实现业务数字化、运营高效化，但也使企业暴露于复杂多元的网络安全风险中。数据泄露、业务中断等安全事件频发，不仅造成巨大经济损失，还损害企业声誉与客户信任，甚至威胁行业稳定与社会安全。在此背景下，深入研究企业网络安全风险，探索科学有效的应对策略，成为企业可持续发展的迫切需求。围绕信息化背景下企业网络安全的重要性展开，系统分析现存风险类型，针对性提出解决对策，旨在为企业提升网络安全防护能力、应对数字化时代安全挑战提供助力。

1 信息化背景下企业网络安全的重要性

1.1 保护数据资产

信息化浪潮下，数据成为企业发展的关键驱动力，涵盖客户偏好、市场趋势、产品研发等核心内容。企业网络安全如同忠诚卫士，为数据资产构筑起坚固防线。一旦网络安全失守，数据可能被窃取、篡改或破坏。竞争对手若获取关键数据，能精准模仿企业策略，抢占市场份额；内部核心数据泄露，会使企业多年研发成果付诸东流。而完善的网络安全体系，能通过加密、访问控制等技术，防止数据非法访问，确保数据完整性和保密性，让企业在激烈竞争中凭借独特数据优势稳步前行。

1.2 保障业务连续性

信息化时代，企业业务高度依赖网络，从日常办公到生产流程，从线上销售到客户服务，都离不开网络支撑。若网络安全出现问题，如遭受恶意攻击或系统故障，业务将瞬间停滞。比如，电商企业网络中断，无法处理订单，客户流失严重；制造企业网络受阻，生产设备失控，造成巨大经济损失。而强大的网络安全能实时监测网络状况，提前预警潜在风险，快速响应并解决安全事件，确保网络稳定运行，保障企业业务不间断，维持正常运营秩序。

1.3 提升客户信任

在信息化社会，客户与企业交互频繁，会提供大量个人信息和交易数据。客户十分在意这些数据的安全，若企业网络安全薄弱，数据泄露风险高，客户便会对企业望而却步。反之，企业若重视网络安全，采用先进技术保护客户数据，如加密存储、安全传输等，能让客户感受到企业对他们的尊重和负责[1]。

2 企业面临的网络安全风险分析

2.1 外部攻击风险

2.1.1 网络钓鱼攻击

网络钓鱼攻击是企业面临的常见外部风险。攻击者常伪装成合法机构或可信人员，通过邮件、短信、社交平台等渠道，向企业员工发送看似正规的信息，诱导其点击恶意链接、下载带毒文件或泄露敏感信息。一旦员工中招，攻击者就能获取企业账号、密码等关键数据，进而渗透企业网络，窃取重要资料、破坏系统或进行其他恶意活动。企业需加强员工安全意识培训，提升其对钓鱼手段的识别能力，同时部署先进的邮件过滤和安全防护系统，降低此类攻击的成功率。

2.1.2 勒索软件攻击

勒索软件攻击对企业危害极大。攻击者利用系统漏洞、恶意邮件附件等方式，将勒索软件植入企业网络。一旦触发，软件会迅速加密企业重要文件和系统，使企业业务陷入瘫痪。随后，攻击者会索要高额赎金，否则将永久删除数据或公开敏感信息。企业为恢复业务，往往面临艰难抉择，支付赎金可能助长攻击者气焰，不支付则可能遭受巨大损失。

2.1.3 供应链攻击

供应链攻击是一种隐蔽且危险的外部攻击方式。企业的供应链涉及众多供应商和合作伙伴，攻击者会瞄准其中安全防护薄弱的环节，通过植入恶意代码、篡改软

件或硬件等方式，将威胁渗透到企业网络。由于供应链的复杂性和相互关联性，一旦某个环节出现问题，可能引发连锁反应，影响整个企业的安全。

2.1.4 利用生成式AI技术的攻击

随着生成式AI技术的发展，其被用于网络攻击的风险日益凸显。攻击者可利用AI生成高度逼真的钓鱼内容，如仿冒的邮件、语音或视频，迷惑企业员工，使其难以分辨真伪，从而更容易上当受骗。此外，AI还能自动化扫描企业网络漏洞，快速发起大规模攻击，提高攻击效率和成功率。

2.2 内部管理风险

2.2.1 员工行为不当

员工行为不当是企业内部管理的一大隐患。部分员工安全意识淡薄，可能会随意在不可信的网站下载文件、使用弱密码，甚至将企业敏感信息外传。还有些员工因情绪或利益问题，故意泄露机密、破坏系统。这不仅会使企业数据面临泄露风险，还可能扰乱正常业务秩序。

2.2.2 权限过度开放

权限过度开放是常见的内部管理风险。企业为方便工作，有时会赋予员工超出其职责范围的权限，这使得员工能访问大量敏感数据和关键系统。一旦员工账号被盗用或员工心怀不轨，就可能利用这些权限进行非法操作，如篡改数据、窃取机密等。

2.2.3 忽视安全风险

忽视安全风险会给企业带来严重后果。一些企业管理层和员工对网络安全重视不足，认为攻击不会降临到自己头上，从而在日常工作中忽视安全防护措施。比如不安装安全补丁、不进行数据备份等。这使得企业在面对外部攻击和内部失误时，毫无抵御能力，极易遭受数据丢失、系统瘫痪等损失。

2.3 技术漏洞风险

2.3.1 软件漏洞

软件漏洞是技术漏洞风险的常见来源。软件在开发过程中，由于代码编写错误、逻辑缺陷或未充分考虑安全因素，会留下可被攻击者利用的漏洞。这些漏洞可能存在于操作系统、应用程序、中间件等各类软件中。攻击者一旦发现并利用这些漏洞，就能绕过安全防护，窃取数据、篡改系统或植入恶意程序。

2.3.2 网络架构漏洞

网络架构漏洞会给企业网络安全带来严重威胁。不合理的网络架构设计，如缺乏隔离、访问控制不严格、网络设备配置不当等，都可能成为攻击者的突破口。例如，内部网络与外部网络没有有效隔离，攻击者可轻易进入内部系统；网络设备存在弱口令，易被暴力破解[2]。

3 应对企业网络安全风险的策略

3.1 加强外部威胁防护

3.1.1 提升安全意识

提升员工安全意识是抵御外部威胁的基础防线。企业应定期开展网络安全培训，内容涵盖常见攻击手段如网络钓鱼、恶意软件等，让员工了解其危害与防范方法。通过模拟攻击演练，如发送模拟钓鱼邮件，检验员工应对能力并针对性强化训练。同时，制定安全手册，明确日常操作规范，如不随意点击不明链接、使用强密码等。管理层要以身作则，将安全意识融入企业文化，使员工从思想上重视网络安全，形成全员参与的安全防护氛围，有效降低因人为疏忽导致的外部威胁入侵风险。

3.1.2 部署安全防护系统

部署先进的安全防护系统是应对外部威胁的关键举措。企业需构建多层次防护体系，包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等。防火墙可过滤非法网络流量，阻止外部未经授权访问；IDS实时监测网络异常行为并报警；IPS则能主动阻断攻击。此外，安装防病毒软件和反恶意软件工具，及时查杀潜在威胁。利用安全信息和事件管理（SIEM）系统，集中收集、分析安全日志，快速发现和响应安全事件。定期更新系统规则和病毒库，确保防护系统始终具备强大的防御能力。

3.1.3 强化供应链管理

强化供应链管理能有效降低外部供应链攻击风险。企业要对供应商进行全面安全评估，审查其安全策略、技术措施和合规情况。在与供应商签订合同时，明确安全责任和要求，如要求供应商及时通报安全漏洞、采用安全开发流程等。建立供应商安全监控机制，定期对供应商的产品和服务进行安全检测。同时，减少对单一供应商的依赖，分散风险。加强与供应商的信息共享和协作，共同应对安全挑战，确保供应链各环节的安全稳定，保障企业网络不受供应链漏洞的影响。

3.1.4 应对生成式AI威胁

应对生成式AI威胁需采取综合策略。企业要利用AI技术构建智能防御体系，通过机器学习算法分析网络流量和行为模式，精准识别生成式AI生成的恶意内容，如深度伪造的钓鱼信息。采用内容验证和溯源技术，对接收的信息进行真实性和完整性验证，防止虚假信息传播。加强数据保护，对敏感数据进行加密和匿名化处理，避免被AI恶意利用。与行业组织和安全机构合作，共享生成式AI威胁情报，及时了解最新攻击手法和防范措施。

3.2 防范内部威胁

3.2.1 加强权限管理

加强权限管理是防范内部威胁的重要环节。企业应遵循最小权限原则，依据员工岗位需求精准分配系统访问权限，避免权限过度开放。例如，普通员工无需访问核心财务数据，就不应赋予其相关权限。同时，建立权限审批流程，任何权限变更都需经过严格审核与记录。定期审查权限分配情况，及时回收离职员工或岗位变动员工的冗余权限。利用身份认证和访问管理（IAM）系统，实现权限的集中管理与动态监控，确保只有授权人员能在合适时间访问特定资源，有效降低内部人员滥用权限带来的安全风险。

3.2.2 改进员工行为

改进员工行为对防范内部威胁至关重要。企业要制定明确的员工行为准则和安全操作规范，涵盖数据使用、设备操作、信息共享等方面。通过定期培训和宣传，让员工清楚知晓哪些行为是允许的，哪些是禁止的。建立监督机制，利用技术手段监测员工操作行为，及时发现异常活动并预警。对于违规行为，要依据规定严肃处理，起到警示作用。此外，营造积极的安全文化氛围，鼓励员工主动报告安全问题和可疑行为，形成全员参与、共同维护企业网络安全的良好局面。

3.2.3 提升安全意识（内部威胁部分）

提升内部员工安全意识是防范内部威胁的基石。企业应开展针对性的安全意识培训，内容不仅包括常见的网络安全威胁，如数据泄露、恶意软件感染等，还要强调内部人员违规操作可能引发的严重后果。采用多样化的培训方式，如线上课程、线下讲座、案例分析、模拟演练等，提高员工参与度和学习效果。定期组织安全知识考核，检验员工对安全知识的掌握程度。

3.3 完善安全管理体系

3.3.1 制定安全策略

制定全面且细致的安全策略是完善安全管理体系的核心。企业需结合自身业务特点、数据敏感程度及合规要求，明确网络安全目标与原则。涵盖数据保护策略，规定数据的分类、存储、传输和销毁方式；访问控制策略，确定不同用户和系统的访问权限；还有应急响应策略，设定应对安全事件的流程和责任分工。安全策略要具有可操作性和动态性，随着业务发展和技术变化及时更新。

3.3.2 建立安全组织

建立专门的安全组织是保障安全管理体系有效运行的关键。企业应成立跨部门的安全管理团队，成员包括信息技术、法务、人力资源等部门代表，确保从不同角度审视安全问题。明确各成员职责，如安全专员负责日常安全监测与维护，法务人员处理合规与法律事务。同时，设立安全决策层，负责重大安全决策和资源调配。安全组织要定期召开会议，评估安全状况、制定改进措施。

3.3.3 引入安全认证

引入安全认证是提升企业安全管理水平和公信力的重要途径。常见的安全认证如ISO27001信息安全管理体系认证，它为企业提供了一套全面的信息安全管理框架和最佳实践。通过引入此类认证，企业需按照标准要求建立、实施、运行、监控、评审和改进信息安全管理体系。认证过程能促使企业梳理现有安全流程，发现并弥补安全漏洞。获得认证后，不仅能向客户和合作伙伴展示企业对信息安全的重视和保障能力，还能在市场竞争中获得优势，增强客户信任，促进企业业务的健康发展[3]。

结束语

在信息化浪潮席卷的当下，企业网络安全风险呈现出多元化、复杂化与隐蔽化的特征，外部攻击、内部管理疏漏以及技术漏洞等问题时刻威胁着企业的稳定运营与数据安全。然而，通过加强外部威胁防护，如提升安全意识、部署防护系统；防范内部威胁，像强化权限管理与改进员工行为；完善安全管理体系，包括制定科学策略、建立专业组织及引入权威认证等综合对策，企业能够有效应对各类网络安全挑战。未来，企业需持续关注网络安全动态，不断优化安全措施，以筑牢网络安全防线，在信息化时代稳健前行，实现可持续发展。

参考文献

[1]陈小辛.数字化转型下企业网络安全管理战略调整路径[J].金融科技时代,2024,(10):52-56.

[2]药丹.数字化转型背景下企业网络安全管理现状及优化路径[J].中国管理信息化,2024,27(17):114-116.

[3]李卓智.企业网络安全防护体系建设研究[J].网络安全技术与应用,2024,(07):108-110.