数字时代网络安全管理与防范探讨

高嘉阳　周晓俊　郭珂琪
北京计算机技术及应用研究所　北京　100854

摘　要：数字时代，网络空间为数字经济提供了虚拟的营商环境，也成为大国博弈的新战场，网络安全风险与威胁与日剧增。本文探讨了数字时代网络安全管理的重要性及紧迫性，分析了网络安全面临的新形势。为提升数字时代网络安全管理，提出了构建全面的网络安全框架、加强数据安全、应用内生安全等能力建设、加强API资产管控、建立快速应急机制、持续提升全员安全意识等策略。旨在构建安全、稳定的网络环境，保障数字经济的健康发展。

关键词：数字时代；网络安全管理；威胁防范

引言：二十大加快建设网络强国、数字中国提出了一系列的新要求，做出了一系列新部署。当今世界正处于新一轮科技革命和产业变革的关键时期，数字技术的快速迭代和深入应用，促进了数字经济的高速发展。在国家利益和经济利益的驱使下，网络攻击手段呈新特征，网络安全防护力量建设刻不容缓。本文旨在探讨数字时代网络安全管理与防范的重要性，分析网络安全面临的新形势，并提出有效的应对策略，为保障数字时代的网络安全提供参考。

1 数字时代网络定义

数字时代，又称数字化时代，是当今社会发展的重要阶段。在这个阶段，网络不仅是信息传递的主要渠道，更是数字时代经济社会发展的核心驱动力。它不再仅仅是传统意义上的计算机网络，而是涵盖了包括互联网、物联网、大数据、云计算等在内的多种数字化技术。这些技术相互交织、相互促进，共同构成了数字时代网络的复杂体系。互联网是数字时代网络的基础。人们可以通过互联网浏览新闻、学习知识、进行在线购物、观看视频。物联网则是数字时代网络的扩展。它将各种智能设备、传感器等连接到网络中，可以实时监控家居安全、智能控制家电设备、优化物流配送等，为人们的生产生活带来了极大的便利[1]。大数据和云计算则是数字时代网络的重要支撑。它们通过强大的数据处理和存储能力，为各种数字化应用提供了可靠的技术保障，为企业和个人提供了更加便捷的信息处理方式。在数字时代，网络已经成为连接人与人、人与物、物与物的重要桥梁，推动了社会的信息化进程。随着5G、人工智能等技术的不断发展，数字时代网络将进一步拓展其边界和功能，为人们带来更加丰富、智能、高效的数字化体验。网络安全问题也日益凸显，加强网络安全防护，保障数字时代网络的健康稳定发展，成为摆在我们面前的重要课题。

2 数字时代网络安全面临的新形势

数字时代对网络空间的依赖日益加深，国家利益和经济利益的驱使，使得数字时代网络安全的风险和潜在威胁与日剧增。

2.1 勒索攻击将成为新常态

勒索病毒，主要以邮件、程序木马、网页挂马的形式进行传播，利用在线系统的安全漏洞获取业务数据并实施加密，进而达到索要赎金的目的。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，性质恶劣，危害极大。2024年全球勒索病毒攻击事件近5000起，仅上半年敲诈赎金约合32.93亿元。下半年勒索软件团伙开始瞄准大型组织和关键基础设施提供商，他们专注于高调攻击并获得更大的回报。

2.2 开源软件将成为攻击新利器

随着数字化转型的开展，软件已经成为发展数字经济的重要基础设施。据VeraCode公司统计，大约30%-70%自主研发软件的代码都使用过第三方代码，并以开源组件、商业或外包共享库的形式存在[2]。大部分的软件的基本功能都是在源代码的基础上进行改造。2024年著名的xz utils供应链攻击事件，就是攻击者成为xz utils项目的维护者，在潜伏了长达2年半之后，于2024年3月，在XZ Utils源代码中植入后门，并通过极为隐蔽的手法将恶意代码伪装成正常的代码。一旦开发者使用该版本XZ Utils源代码进行软件开发并上线使用。攻击者就可以通过供应链攻击，远程控制服务器并执行恶意操作。当前第三方开源软件的安全问题尤为值得关注。

2.3 数据保护将成为新挑战

数据、流量作为数字时代一种特殊资源，时刻都在被采集、处理、加工、分析、共享和使用。随着大数据和人工智能技术的深度应用，基于数据开展的分析、预测、决

策的需求不断增加，售卖数据已经成为新的牟利方式，自数据产生到销毁的全生命周期的保护刻不容缓。

3 加强数字时代网络安全管理与威胁防范

3.1 构建全面的网络安全框架

在数字时代背景下，构建全面的网络安全框架是确保组织安全的关键。经过多年的发展，众多的网络安全架构被不断提出，并用于指导安全体系设计。以主动防护为核心的主动安全架构，对网络威胁采取主动措施，以防止潜在攻击并保护网络系统和数据安全；以检测能力和自适应为核心的动态安全架构，可持续性对安全威胁进行动态分析，从而适应不断变化的安全威胁；美国国土安全部提出的网络韧性架构，目标是使整个网络始终保持提供预期结果的能力，在遭遇安全灾难或受到攻击后，整个网络依旧可以正常运行。应通过基于合适的安全框架开展安全管理体系、安全技术体系、安全运营体系的深化设计，以安全可靠基础软硬件、密码基础设施等为安全基础支撑，以供应链安全检测、网络攻防对抗等新技术为抓手，构建供应链安全管控能力、内生安全保障能力、数据治理能力，形成安全有效的网络安全防护架构。同时融合人工智能、大数据分析等先进技术，提升安全威胁的预测、识别与响应速度，确保网络安全框架的智能化与前瞻性。通过持续优化与迭代，构建适应性强、防护全面的网络安全体系，为组织的数字化转型提供坚实的安全保障。从源头上防控勒索病毒等威胁的入侵与传播。

3.2 开展数据分类分级，做好数据加密与备份

开展数据资源分类，形成分类清单，并根据重要程度及其遭受窃取、篡改和破坏后造成的危害程度，拟定数据级别。通过建立数据安全管理机制，构建覆盖数据全生命周期的组织体系、制度体系和运营体系等，加强对数据从采集、传输、存储、使用、加工和共享等全过程的安全保护。聚焦核心业务、核心系统，加强风险识别和分析，及时化解风险。

在数据加密与备份时，应采用先进的国产加密算法，对敏感数据进行加密处理，确保数据在存储和传输过程中的安全性。建立多层次的备份体系，包括本地备份、异地备份和云备份，能够在数据丢失或损坏时迅速恢复，保障业务的连续性。数据加密还结合密钥管理策略，确保密钥的安全存储和分发，防止密钥泄露导致的数据安全风险。而备份体系则需定期测试恢复流程，确保备份数据的完整性和可用性，为业务提供可靠的数据恢复支持。建立完善的权限管理和访问控制机制，确保只有经过授权的人员和系统才能访问和操作数据。同时加强对数据使用情况的监控和审计，及时发现并处置任何异常或可疑的数据访问行为。通过这些措施，可以全面提升数据的安全性，保护企业的核心资产，为企业的稳健发展提供坚实的数据支撑。

3.3 推动应用安全再设计，做好开源代码检测

应用软件的安全管控应贯穿从设计到编码、上线、运维的全过程。通过建立有效的应用软件安全开发和管理机制，明确并规范安全开发的技术要求，结合应用软件安全工程实践方法，将安全的设计理念和要素同步融入应用软件全生命周期的管理制度和管控流程，最大限度的实现应用内生安全。特别为降低供应链安全威胁，建立开源软件准入和跟踪机制，开展对应用系统开发使用的第三方开源软件的资产发现、风险评估，及时规避开源软件造成的网络安全风险。推动应用安全再设计，加强对应用软件架构、代码逻辑、数据处理等方面的安全审查，确保应用在设计之初就具备足够的安全防护能力。

3.4 加强API资产的管控，防止敏感数据不当使用

随着数字化建设的深入和完善，越来越多的关键应用要实现业务融合、流程打通、数据共享及集成，API接口的数量与使用频率与日剧增。API接口中承载了大量重要数据和敏感信息。为了防止非授权使用和数据泄露，应通过API资产梳理，API规范编制，API接口异常行为监控，API异常访问监管、API接口风险评估等，建立API安全防护能力，满足对API接口的资产管理、攻击防护、敏感数据管控和访问行为管控等能力，确保API接口的安全可靠稳定运行。同时实施严格的权限管理和访问控制策略，对API接口的调用进行身份验证和授权验证，确保只有合法的用户和服务才能访问和使用API接口。此外定期进行API接口的安全审计和漏洞扫描，及时发现并修复潜在的安全隐患。通过这些措施，可以全面加强API资产的管控，有效防止敏感数据的不当使用，为企业的数字化转型提供坚实的安全保障。

3.5 建立快速有效的应急机制

在数字时代，安全问题更复杂、更隐蔽，建立健全网络安全事件应急工作机制，规范强化网络安全事件应急演练，有助于提高网络安全事件的应对能力，预防和减少网络安全事件造成的损失和危害。（1）快速响应与处置。一旦发生安全事件，立即启动应急响应，快速定位问题源头，开展先期处置，最大限度减少损失，并评估影响范围。（2）强化沟通与协调。建立有效的信息通报和沟通机制，确保与上级部门、相关单位以及用户之间的信息畅通无阻。在发生安全事件时，能够及时传递信息、协调各方行动，形成合力应对挑战。（3）做好事

后分析与总结。在安全事件处置完成后，应深入分析与总结，评估应急响应预案的有效性和不足之处，为今后的应急响应工作提供宝贵的经验和教训[3]。通过不断改进和完善应急机制，确保组织在面对网络安全挑战时能够从容应对、化险为夷。（4）持续监控与预警。建立常态化的网络安全监控体系，利用先进的安全监测工具和技术，对网络环境进行实时监控，及时发现并预警潜在的安全威胁。通过持续监控，确保组织能够提前采取措施，防范于未然，进一步提升网络安全防护的主动性和有效性。

3.6 提升全员安全意识与技能

提升全员安全意识与技能是构建网络安全体系的重要一环，确保全员具备高度的安全防范能力。（1）定期组织安全培训。紧跟最新的安全威胁和攻击手法，将密码管理、钓鱼邮件识别、社交媒体安全等融入培训课程，提醒员工注意保护个人隐私，避免在社交媒体上泄露过多个人信息，降低个人信息泄露的风险，提升员工的安全防范意识。（2）开展应急演练工作。通过模拟真实的安全事件，如勒索攻击、网络钓鱼攻击、恶意软件感染等，让员工在实战中学习和掌握应对策略，提升应急响应能力。（3）加强管理层的安全培训[4]。管理层在安全体系建设中起着关键作用，通过专门的安全培训，使他们了解企业面临的安全威胁，掌握安全管理的基本方法和技巧，能够正确决策，推动企业安全体系的不断完善。

3.7 强化合作与信息共享，构建网络安全生态

在数字时代，网络安全不再是单一组织或国家能够独立应对的挑战，而是需要全球范围内的合作与信息共享。为了构建更加稳固的网络安全生态，我们应积极寻求与业界、学术界、政府以及国际组织的合作。首先加强与网络安全厂商、安全服务提供商的合作，不断引入先进的安全技术和解决方案，提升组织的整体安全防护能力。同时与这些合作伙伴共同开展安全研究，探索新的安全威胁和防御策略，保持对网络安全领域的持续关注和更新。其次与学术界建立紧密的合作关系，利用高校和研究机构的科研力量，推动网络安全技术的创新和突破。通过设立联合实验室、开展科研项目等方式，促进产学研用深度融合，将科研成果转化为实际的安全防护能力。此外积极与政府及监管机构沟通协作，了解最新的网络安全政策和法规要求，确保组网络安全工作符合法律法规标准。同时主动参各项应急演练工作，提升组织的应急响应能力和协同作战能力。

结束语：数字时代网络安全管理与防范是一项复杂而艰巨的任务。通过构建全面的网络安全框架、加强数据安全、应用内生安全等能力建设、建立快速应急机制、提升全员安全意识，可以有效应对网络安全威胁，保障数字经济的健康发展。未来继续探索和实践更多有效的网络安全管理与防范策略。

参考文献

[1]刘亮.数字时代企业网络安全管理[J].数字技术与应用,2024,42(5):89-91.

[2]刘丽娜.数字时代企业网络安全管理研究[J].现代企业文化,2022(25):50-52.

[3]赵佩娜.数字化时代下企业现金流管理的创新策略[J].乡镇企业导报,2024(17):99-101.

[4]陈琴琴.数字经济时代企业管理策略优化探讨[J].投资与创业,2023,34(24):103-105.