企业信息化建设中网络安全问题探析

张 凯
中铁一局集团新运工程有限公司 陕西 咸阳 712000

摘 要：随着企业信息化建设的不断推进，网络安全问题日益凸显，成为制约企业信息化发展的重要因素。本文对企业信息化建设中面临的网络安全问题进行深入探析，从外部环境、内部管理、技术防护等方面分析问题产生的原因，并提出相应的防护措施和建议。通过本文的阐述，旨在为企业提供一个清晰的网络安全问题认识框架，引导企业加强网络安全防护，保障企业信息化建设的顺利进行。

关键词：企业信息化；网络安全；风险分析；防护策略

1 企业信息化建设与网络安全概述

企业信息化建设指的是企业在生产、经营、管理各个环节中，采用现代信息技术，如计算机、网络、数据库等，以提高企业的运营效率、降低成本、增强市场竞争力。随着信息技术的快速发展，企业信息化已经成为提升企业核心竞争力的关键手段。企业信息化建设不仅涉及到硬件设施的投入，更包括软件系统的开发与应用、业务流程的优化与重组、数据资源的整合与管理等多个方面。然而，在企业信息化建设的过程中，网络安全问题不容忽视。网络安全是指保护企业信息资产不受未经授权的访问、篡改、破坏或泄露的能力。由于信息技术应用的普及和互联网的广泛使用，企业的数据资源越来越丰富，网络安全威胁也日益复杂多变。这些威胁可能来自于外部的黑客攻击、病毒传播、恶意软件感染，也可能来自于内部员工的不当操作、误操作或泄露敏感信息。因此，企业在进行信息化建设的同时，必须高度重视网络安全工作[1]。一方面，企业需要建立完善的网络安全管理体系，包括制定网络安全政策、明确安全责任、加强安全培训、实施安全审计等；另一方面，企业需要采取多种技术手段，如防火墙、入侵检测、威胁发现、防病毒、数据加密、访问控制等，来保护企业的信息资产免受威胁。同时，企业还需要定期进行安全风险评估和应急演练，以应对可能发生的网络安全事件。

2 企业信息化与网络安全的关系

企业信息化与网络安全之间存在着紧密而复杂的关系。企业信息化是推动企业现代化、提升竞争力的关键路径，而网络安全则是保障这一进程顺利进行的基石。两者相互影响，互为支撑，共同构成了企业信息化建设的完整框架。网络安全是企业信息化的前提和保障，随着企业信息化程度的加深，企业的运营、管理、决策越来越依赖于信息系统和数据资源。如果网络安全得不到保障，企业的信息资产就可能面临泄露、篡改、破坏等风险，进而影响到企业的正常运营和市场竞争力。因此，网络安全是企业信息化的必要条件和重要支撑。

3 企业信息化建设中网络安全问题分析

3.1 内部网络安全问题分析

在企业信息化建设的进程中，内部网络安全问题同样不容忽视。内部网络安全问题主要源于员工操作失误、内部恶意行为、系统漏洞以及管理制度的不完善等多个方面。首先，员工操作失误是一种常见的内部网络安全问题，由于缺乏足够的网络安全意识或技能，员工可能在进行日常工作时，不经意间泄露敏感信息、使用未经安全检测的存储设备、下载未经授权的软件或点击恶意链接，这些行为都可能给企业的网络安全带来严重威胁。其次，内部恶意行为也是一个潜在的隐患，虽然大多数员工都是忠诚的，但总有一些员工可能出于个人利益或其他动机，对企业信息系统进行非法访问、篡改数据或传播病毒，这些行为不仅可能导致企业数据泄露，还可能造成系统瘫痪，给企业带来重大损失。此外，系统漏洞也是内部网络安全问题的一个重要方面，由于企业信息系统的复杂性，很难保证每个系统组件都是完美无缺的[2]。一旦存在漏洞，黑客或恶意用户就可能利用这些漏洞进行非法入侵，窃取数据或破坏系统。最后，管理制度的不完善也是导致内部网络安全问题的一个重要原因，如果企业没有建立完善的网络安全管理制度，或者制度执行不力，以及网络安全事件违规处罚措施不严，那么即使员工有良好的网络安全意识，也可能因为缺乏有效的制度约束而做出损害网络安全的行为。

3.2 外部网络安全问题分析

在企业信息化建设的道路上，外部网络安全问题同样不容忽视。这些问题主要来自于网络环境的不确定性、外部攻击者的恶意行为、合作伙伴或供应链中的安

全隐患等方面。网络环境的不确定性是外部网络安全的一个重要挑战，随着互联网和全球化的快速发展，企业越来越依赖于外部网络进行数据传输和资源共享。然而，外部网络环境的复杂性和不可预测性使得企业面临着各种安全威胁，如网络钓鱼、恶意软件、勒索软件等。这些威胁可能导致企业数据泄露、系统瘫痪或财务损失[3]。外部攻击者的恶意行为也是外部网络安全问题的一个重要方面，黑客或敌对势力可能出于经济利益、政治目的或破坏企业声誉等动机，对企业信息系统进行攻击。这些攻击可能包括DDoS攻击、SQL注入、跨站脚本攻击等，其目的可能是窃取数据、破坏系统或制造混乱。合作伙伴或供应链中的安全隐患也可能对企业的外部网络安全造成威胁，企业与合作伙伴或供应商之间的数据交换和共享是常态，但如果这些合作伙伴或供应商存在安全漏洞或被攻击，那么企业的数据也可能面临泄露的风险。

4 企业信息化建设中网络安全防护策略

4.1 增强员工安全意识与培训

提升员工的安全意识是网络安全防护的基石，企业应通过定期的安全意识教育活动，如安全知识讲座、安全知识答题竞赛、安全文化周等，使员工充分认识到网络安全的重要性，并理解自己在维护网络安全中的角色与责任。同时，通过实际案例分析，让员工了解网络威胁的严重性，并学习如何识别和避免潜在的安全风险。建立完善的培训机制是提升员工安全技能的关键，企业应根据员工的不同角色和职责，设计针对性的培训课程，确保员工掌握必要的网络安全知识和技能。培训内容可以包括网络安全意识、账号密码管理、电子邮件安全、社交媒体使用准则、防病毒和防恶意软件措施等。同时，通过模拟演练和实际操作，让员工在实践中学习和提升安全应对能力。为了持续监测和评估员工的安全意识和技能水平，企业应建立定期的安全考核和反馈机制。通过考核，可以发现员工在网络安全方面存在的问题和不足，并及时进行针对性的培训和指导。

4.2 完善内部管理制度与流程

在企业信息化建设的进程中，完善内部管理制度与流程是确保网络安全的关键一环。这些制度与流程不仅为企业提供了明确的安全操作指南，还为员工提供了行为规范，从而确保企业信息系统的稳定和安全。企业应制定全面的网络安全制度和标准，这些制度和标准应明确企业对于网络安全的基本要求、原则和目标，并为员工提供清晰的指导。同时，这些制度和标准还应包括对于敏感数据的保护、秘密级别、访问控制、密码管理、安全审计等方面的具体要求。建立完善的网络安全管理流程是保障制度执行的关键，这些流程应涵盖网络安全规划、风险评估、事件响应、安全审计等各个环节，确保企业在面对安全威胁时能够迅速、有效地作出响应。通过定期的安全审计和风险评估，企业可以及时发现和修补安全漏洞，不断提升网络安全防护能力。加强内部沟通与协作也是完善内部管理制度与流程的重要一环，企业应建立跨部门的安全协作机制，促进不同部门之间在网络安全方面的信息共享和协同工作。通过加强沟通与协作，企业可以及时发现和解决潜在的安全风险，确保企业信息系统的整体安全。持续监督和改进是确保内部管理制度与流程有效性的关键，企业应定期对网络安全管理制度和流程进行审查和更新，以适应不断变化的网络安全威胁和业务需求。通过定期的培训和考核，确保员工对制度和流程的理解和遵守[4]。

4.3 强化技术防护与系统安全

面对日益复杂的网络威胁和攻击手段，企业必须采取切实有效的技术措施，筑牢网络安全防线。强化技术防护是保障企业信息系统安全的基础，企业应部署先进的安全设备和系统，如防火墙、入侵检测系统、态势感知系统、威胁发现系统、病毒防护系统、上网行为管理系统、安全事件信息管理平台等，以实时监控和防御来自外部和内部的网络攻击。采用VPN和加密技术保护敏感数据的传输和存储，确保数据在传输过程中不被窃取或篡改。加强系统安全是确保企业信息系统稳定运行的关键，企业应定期对信息系统进行安全漏洞扫描和风险评估，及时发现和修补安全漏洞。建立完善的备份和恢复机制，确保在发生安全事件时能够迅速恢复系统正常运行，减少损失。强化访问控制和身份认证是保护企业信息系统的重要措施。企业应对不同级别的数据和资源设置相应的访问权限，并实施严格的身份认证机制，确保只有授权用户能够访问敏感信息。随着人工智能、云计算、大数据、物联网等新技术的不断涌现，企业应积极应用这些先进技术提升网络安全防护能力。例如，通过人工智能机器学习和深度学习技术，可以在身份识别、社会工程学防御、入侵检测等方面加强安全管理；通过云计算的弹性扩展和灵活部署能力，提升网络安全的应对速度和效率；利用大数据分析和挖掘技术，发现潜在的安全威胁和攻击模式；通过物联网设备的智能感知和监控，增强对物理环境的安全防护。

4.4 合作与信息共享机制

在企业信息化建设的进程中，构建合作与信息共享机制是提升网络安全防护能力的重要途径。面对日益严

峻的网络安全挑战，企业不能仅仅依靠自身的力量来应对，而需要积极与合作伙伴、行业协会、科研院校、安全机构等外部实体建立紧密的合作关系，共同分享安全信息、资源和经验，以形成合力对抗网络安全威胁。企业应与供应商、客户和其他业务伙伴建立明确的网络安全合作框架，共同制定安全标准和要求，确保在数据交换、业务合作和系统对接过程中遵循统一的安全准则。积极参与行业协会和安全机构的合作与交流活动能够为企业带来宝贵的安全信息和资源。通过参加行业协会组织的安全论坛、研讨会等活动，企业可以了解行业最新的安全动态和趋势，与同行分享安全实践经验，共同研究应对网络安全威胁的策略和方法。建立信息共享机制也是提升网络安全防护能力的关键，企业应建立与合作伙伴之间的安全信息共享平台，及时分享安全漏洞、威胁情报、事件处置经验等信息，以便快速响应和协同应对网络安全事件。同时，为了确保合作与信息共享机制的有效运行，企业还应建立完善的信任机制和保密协议。通过明确的信任关系和保密约定，确保合作伙伴在共享安全信息时能够相互信任、遵守保密义务，防止敏感信息泄露和滥用。通过建立合作伙伴间的网络安全合作机制、积极参与行业协会和安全机构的合作与交流活动、建立信息共享机制以及完善信任机制和保密协议，企业可以汇聚外部力量、共享安全资源、提升整体安全防护能力，共同构建更加安全、稳定的网络环境。

5 企业网络安全建设的未来展望

随着信息技术的飞速发展和数字化转型的深入推进，企业网络安全建设的未来展望充满了挑战与机遇。在未来，企业网络安全将更加注重智能化、协同化、自适应和持续创新，以应对不断演变的网络威胁和攻击手段。（1）智能化将成为企业网络安全建设的核心趋势。通过引入人工智能、机器学习等先进技术，企业可以实现对网络威胁的自动化检测、分析和应对，大幅提升安全防御的效率和准确性。智能安全系统将能够实时学习、自我优化，并为企业提供前瞻性的安全预警和应对策略。（2）协同化将成为企业网络安全建设的重要方向。未来的企业网络安全将更加注重内部部门之间、企业与合作伙伴之间以及企业与安全机构之间的协同合作。通过打破信息孤岛、加强沟通与协作，企业可以构建更加紧密的安全防护体系，共同应对网络安全挑战[5]。（3）自适应安全将成为企业网络安全建设的关键要素。面对不断变化的网络威胁和攻击手段，企业需要构建具备自适应能力的安全系统。这些系统能够根据网络环境和威胁情况的变化，自动调整安全策略、优化防护措施，确保企业信息系统的持续安全。（4）持续创新将是企业网络安全建设的永恒主题。随着新技术的不断涌现和网络安全威胁的不断演变，企业需要保持持续的创新精神和投入，不断探索新的安全理念、技术和解决方案。通过持续创新，企业可以不断提升自身的网络安全防护能力，确保在数字化转型的道路上稳健前行。

结束语

随着信息技术的快速发展，信息技术已被公认为当代最核心的高技术之一[6]，企业信息化建设已成为提升企业竞争力的关键。然而，网络安全问题始终是企业信息化建设过程中不可忽视的一环。通过对企业信息化建设中网络安全问题的深入探析，可以看到，网络安全不仅仅是技术问题，更是涉及到企业管理、人员意识等多个层面。

参考文献

[1]郭俊,郭煜.医院信息化建设中的网络安全分析[J].实用医技杂志,2021,28(11):1358-1359.

[2]刘小宇,李璐.医院信息化建设中网络安全及防护的探析[J].网络安全技术与应用,2021(10):131-132.

[3]刘生堂.试论企业信息化建设中的信息安全问题[J].中国新通信,2020,17(22):17-18.

[4]谢志宏.企业信息化建设中的信息安全问题研究[J].企业导报,2019(06):132-134.

[5]吴捷.企业信息化建设中信息安全问题的研究[J].通讯世界,2020(1):247-248.

[6]侯炳辉.我国信息系统发展道路与模式的探讨[J].信息化历程上的脚印,2011(3):10.