信息系统管理及网络通信安全

李雪莲
西吉县人民医院　宁夏　固原　756299

摘　要：网络通信安全中存在的问题是多方面的，既有技术层面的漏洞与缺陷，也有人为因素和管理漏洞的影响，还有网络攻击和病毒威胁的挑战以及法律法规与监管的缺失。我们需要从多个方面入手，采取综合措施来加强网络通信安全的保障，确保网络通信的安全、稳定和可靠。只有这样，我们才能更好地利用网络通信技术，为人们的生活和工作带来更多的便利和效益。

关键词：信息系统；管理；网络通信安全

引言：随着信息技术的迅猛发展，网络通信已成为现代社会不可或缺的一部分。它极大地便利了人们的生活和工作，使得信息传输更加迅速、高效。然而，网络通信安全问题也日益凸显，给人们的隐私、财产乃至国家安全带来了严重威胁。论文将对网络通信安全中存在的主要问题进行分析和探讨。

1 信息系统管理的核心作用

信息系统管理在当今快速发展的数字化时代中，扮演着举足轻重的角色。它不仅关乎企业的日常运营，更影响着企业的长远发展和市场竞争力。以下是对信息系统管理核心作用的详细阐述。

首先，业务流程优化是信息系统管理的一大核心作用。随着信息技术的飞速发展，企业可以通过信息系统管理来整合和优化业务流程，从而显著提高企业的运作效率。例如，通过引入自动化工具和智能系统，可以大幅减少人为操作，降低出错率，同时加快业务处理速度[1]。此外，信息系统管理还能帮助企业实现跨部门、跨地域的协同工作，进一步提升工作效率。这种优化不仅有助于降低企业成本，还能提升服务质量，增强客户满意度，从而为企业赢得更多市场份额。

其次，决策支持是信息系统管理的又一重要作用。在信息爆炸的时代，如何获取准确、及时的数据和信息，成为企业决策者面临的一大挑战。信息系统管理通过数据整合、分析和挖掘，为管理者提供了一套科学、客观的决策依据。通过深入了解市场需求、客户行为、竞争对手动态等信息，管理者可以更加精准地制定市场策略、产品规划和运营计划。另外，信息系统管理还能帮助管理者预测未来趋势，提前布局，从而确保企业在激烈的市场竞争中立于不败之地。

再者，风险管理和控制也是信息系统管理不可或缺的一环。随着信息技术的广泛应用，网络安全、数据泄露、系统故障等风险也日益凸显。良好的信息系统管理能够识别这些潜在风险，并采取相应的预防措施，确保企业信息系统的安全稳定运行。例如，通过建立完善的网络安全防护体系，可以有效抵御黑客攻击和病毒入侵；通过制定严格的数据管理制度，可以防止数据泄露和滥用；通过定期维护和升级系统，可以确保系统的稳定性和可靠性。这些措施不仅有助于保护企业的核心资产，还能避免因信息系统故障而导致的业务中断和损失。

最后，促进创新和变革也是信息系统管理的重要使命。在当今快速变化的市场环境中，企业要想保持竞争力，就必须不断创新和变革。信息系统管理通过探索新技术的应用潜力，为企业提供了源源不断的创新动力。例如：第一，利用云计算、大数据、人工智能等先进技术，企业可以开发出更具创新性的产品和服务，满足客户的多样化需求；第二，通过数字化转型，企业可以重塑业务流程和组织结构，提升整体运营效率；第三，通过跨界合作和生态共建，企业可以拓展新的业务领域和市场空间。这些创新举措不仅有助于提升企业的核心竞争力，还能推动整个行业的进步和发展。

2 网络通信安全中存在的主要问题

2.1 技术漏洞与缺陷

网络通信安全的首要问题来自于技术层面的漏洞与缺陷。这些漏洞可能存在于网络通信协议、加密技术、操作系统、应用软件等多个方面。黑客或恶意攻击者可以利用这些漏洞，对网络通信进行非法侵入、篡改或窃取信息。例如，一些旧版的网络通信协议可能存在安全隐患，若未能及时更新升级，就容易被攻击者利用。此外，加密技术的强度和安全性也是网络通信安全的关键因素。若加密算法被破解或密钥被泄露，那么网络通信中的信息就可能被轻易获取。

2.2 人为因素与管理漏洞

除了技术层面的问题外，人为因素和管理漏洞也是网络通信安全的重要隐患。人为因素包括用户安全意识薄弱、操作不当等。许多用户在使用网络通信时，往往忽视对隐私信息的保护，随意泄露个人信息或密码，给攻击者提供了可乘之机[2]。此外，一些用户还可能在不安全的网络环境下进行敏感信息的传输，增加了信息泄露的风险。管理漏洞则主要体现在企业或组织对网络通信安全的管理不到位。例如，一些企业未能建立健全的安全管理制度，对员工的网络行为缺乏有效的监管和约束；或者对安全事件的应急响应能力不足，无法在第一时间发现并处理安全威胁。

2.3 网络攻击与病毒威胁

网络通信安全还面临着来自网络攻击和病毒威胁的挑战。网络攻击者可能利用各种手段，如钓鱼网站、恶意软件、拒绝服务攻击等，对目标进行攻击和破坏。这些攻击不仅可能导致信息的泄露和篡改，还可能造成网络服务的瘫痪和数据的损失。病毒威胁则是指通过网络传播的恶意程序，它们可能潜伏在用户的计算机或网络设备中，窃取信息、破坏数据或破坏系统的正常运行。

2.4 法律法规与监管缺失

网络通信安全的另一个问题是法律法规与监管的缺失。目前，我国在网络通信安全方面的法律法规还不够完善，对违法行为的打击力度也有限。这导致一些不法分子在网络通信领域肆意妄为，进行各种违法犯罪活动。同时，监管部门的监管力度和有效性也有待提高。一些监管部门对网络通信安全的重视程度不够，对违法行为的查处不够及时和严格，使得网络通信安全形势更加严峻。

3 网络通信安全措施

网络通信安全，作为信息技术领域的核心议题，对于保障数据安全、维护用户隐私以及促进信息社会的健康发展具有举足轻重的地位。随着网络技术的迅猛发展和广泛应用，网络通信安全问题日益凸显，成为亟待解决的重要课题。

3.1 针对技术漏洞与缺陷的措施

网络通信安全的首要任务是应对技术层面的漏洞与缺陷。在这个信息化快速发展的时代，技术更新迭代迅速，网络通信协议和软件系统必须保持与时俱进。为此，我们必须及时更新网络通信协议和软件系统，确保使用的是最新版本。这不仅可以减少已知漏洞被利用的风险，还能提升系统的整体性能和稳定性。与此与此同时，加密技术是网络通信安全的基石，其强度和可靠性直接关系到信息传输的安全性。所以，我们必须加强加密算法的研发和应用，采用更加先进、高效的加密算法，提高加密技术的安全性和可靠性[3]。除此之外，定期进行风险评估也是不可或缺的一环。通过对网络通信系统的全面评估，我们可以深入了解系统的安全状况，识别可能存在的安全风险，从而制定相应的安全策略和防护措施。这样不仅可以降低安全风险的发生概率，还能在网络安全事件发生时，迅速做出响应，减少损失。

3.2 应对人为因素与管理漏洞的策略

人为因素和管理漏洞是网络通信安全的另一大隐患。许多网络安全事件往往是由于用户安全意识薄弱或操作不当引起的。因此，提升用户的安全意识至关重要。通过举办网络安全培训和教育活动，我们可以向用户普及网络安全知识，使他们更加了解网络通信安全的重要性，避免随意泄露个人信息和密码。并且，我们还应引导用户养成良好的网络使用习惯，如不在不安全的网络环境下传输敏感信息，不点击来历不明的链接等。这些良好的网络使用习惯能够有效降低用户遭受网络攻击的风险。除此之外，企业和组织也应建立完善的安全管理制度，明确员工的网络行为规范，加强对网络通信的监管和约束。通过制定严格的网络安全规定和奖惩机制，我们可以确保员工遵守网络安全规定，减少因人为因素导致的安全事故。

3.3 应对网络攻击与病毒威胁的方案

在数字化时代，网络攻击与病毒威胁日益猖獗，对网络通信安全构成了严重威胁。为了有效应对这些挑战，我们必须采取一系列切实有效的措施来保障网络通信的安全与稳定。第一，安装可靠的防火墙和杀毒软件是应对网络攻击与病毒威胁的基础措施。防火墙作为网络安全的第一道防线，能够监控和控制进出网络的数据包，有效阻挡外部攻击者的非法访问和入侵。它通过对网络流量的过滤和检查，能够识别并阻止潜在的恶意行为，保护内部网络免受攻击。而杀毒软件则是保障系统安全的重要工具，能够及时发现并清除计算机中的病毒和恶意程序。通过定期更新病毒库和进行全盘扫描，杀毒软件能够确保系统的正常运行，防止病毒对数据的破坏和窃取。第二，仅仅依赖防火墙和杀毒软件是远远不够的。我们需要定期对系统进行全面的安全检查和病毒扫描，以发现和修复潜在的安全隐患。这包括对系统漏洞的扫描和修复，以防止攻击者利用漏洞进行入侵；对恶意软件的检测和清除，以确保系统的纯净与安全；以及对网络流量的监控和分析，以发现异常行为和潜在威胁。通过这些检查，我们能够及时发现并应对潜在的安全风险，确保网络环境的清洁和安全。

3.4 加强法律法规与监管的措施

法律法规是保障网络通信安全的重要手段。（1）为了应对日益复杂的网络安全问题，我们必须不断完善网络通信安全相关的法律法规。这些法律法规应明确各方责任和义务，为网络通信安全提供有力的法律保障。（2）我们还需要加大对违法行为的打击力度，提高违法成本，让不法分子望而却步。这包括加强对网络犯罪的打击力度、对违法行为的处罚力度以及对违法者的追责机制等。（3）加强监管部门的监管力度和有效性也是必不可少的。监管部门应定期对网络通信服务提供商进行安全检查和评估，确保其符合相关法律法规的要求。这包括对服务提供商的网络安全管理制度、技术防护措施以及应急响应机制等进行全面检查。对于存在安全隐患或违法行为的服务提供商，监管部门应依法进行处罚并督促其整改。

3.5 加强技术研发与创新

在当前数字化时代，网络通信安全技术的研发与创新显得尤为重要。为了应对日益复杂的网络安全威胁，我们必须投入更多资源进行技术研发和创新，以开发出更加先进、高效的网络通信安全技术。这包括：（1）开发新型的安全防护系统，能够自动识别并阻挡恶意攻击和病毒的入侵，为网络通信提供全方位的保护。（2）我们还应鼓励企业、研究机构和高校加强合作，共同推动网络通信安全技术的发展和进步。通过产学研合作，我们可以汇聚各方优势资源，形成合力，共同攻克网络通信安全领域的技术难题。

3.6 建立完善的安全审计和监控机制

建立完善的安全审计和监控机制，无疑是保障网络通信安全的重中之重。在数字化、信息化的时代背景下，网络通信已渗透到社会生活的方方面面，无论是个人信息的传输，还是企业商业机密的交互，都离不开一个安全、稳定的网络环境[4]。因而，我们急需一套全面、高效的安全审计和监控机制来保驾护航。首先，安全审计，作为预防安全风险的重要一环，它如同网络的“体检医生”。定期对网络通信系统进行安全审计，就如同对身体进行定期检查，能够及时发现并处理潜在的安全隐患，防止“疾病”的恶化。这包括对系统漏洞的深入扫描和及时修复，对安全管理制度和操作流程的细致审查和改进。只有通过这样的“体检”，我们才能确保网络通信系统的“身体健康”，为数据传输提供坚实的保障。其次，安全监控，则是网络通信安全的“守护神”。通过实时监控网络通信系统的运行状态和安全事件，我们能够像拥有了一双“千里眼”和“顺风耳”，随时掌握网络的安全动态。对网络流量的监控，能够及时发现异常流量和攻击行为，对系统日志的分析，能够揭示潜在的安全威胁和入侵痕迹。而对安全事件的应急响应，则能在最短时间内采取有效措施，将损失降到最低。最后，建立完善的安全审计和监控机制，不仅是为了应对已经发生的安全事件，更是为了预防潜在的安全风险。它需要我们综合运用先进的技术手段和管理理念，不断提升安全防护能力，确保网络通信系统的稳定运行和安全可靠。只有这样，我们才能为用户提供更加安全、可靠的网络通信服务，让信息传输更加畅通无阻，为社会的繁荣发展贡献力量。

结语：总之，在今天的信息社会里，信息的传播速度也是突飞猛进，让人们的工作、生活、学习都更加方便，个人的品质和影响力也成倍增加。随着工业的迅速发展，技术的进步和社会的发展，对企业的安全和经济效益都产生了很大的影响。强有力的网络审查能够支撑行业的发展，为企业的发展提供强有力的动力，从而产生巨大的经济效益和社会效益。为使通信技术的应用和应用得到充分的验证，其背后的安全性问题也是不容忽视的。

参考文献

[1]黄武涛.网络通信安全与信息系统管理的安全探讨[J].农家参谋,2019(5):215.

[2]李娟娟,王宏仂.企业的信息系统管理与网络通信安全维护研究[J].中国管理信息化,2018,21(11):53-55.

[3]李洁,张维峰.信息系统管理及网络通信安全分析[J].科技创新导报,2019,16(22):178-179.

[4]王东洋.浅淡网络通信与信息系统的安全管理[J].通讯世界,2019,26(7):102-103.