网络安全与信息化管理的现状及防范措施

任江红
新疆昆仑工程咨询管理集团有限公司　新疆　乌鲁木齐　832000

摘　要：随着信息技术的迅速发展，网络已经成为人们日常生活和工作中不可或缺的一部分。然而，网络的快速发展也带来了一系列的安全威胁和挑战。信息安全和网络安全问题已经成为各个领域面临的重要挑战，必须采取有效的防范措施来应对这些风险以保护个人、组织和国家的信息资产。

关键词：网络安全；信息化管理；现状；防范措施

引言

随着信息技术的快速发展和广泛应用，网络安全与信息化管理已经成为当今社会中非常重要的议题。在数字化时代，各种互联网攻击和数据泄露事件层出不穷，给个人、企业以及国家的信息资产带来了巨大的威胁。

1 网络安全与信息化管理的现状分析

网络安全与信息化管理在当今社会中扮演着至关重要的角色。然而，在实际应用中，仍然存在一系列问题。首先，黑客、病毒和恶意软件等威胁日益增加，给网络系统的安全性带来了巨大挑战。随着互联网的普及和依赖程度的提高，网络攻击的规模和复杂性也不断增长。黑客利用技术手段入侵系统，窃取个人和企业敏感信息，造成财务损失和声誉风险。病毒和恶意软件可以通过电子邮件、下载文件或访问感染的网站传播，对设备和数据造成破坏和损失。其次，随着物联网的快速发展，使得各种设备能够相互连接和交换数据，但也给网络安全带来了新的挑战。未经充分保护的物联网设备容易受到攻击，可能导致个人隐私泄露、基础设施瘫痪以及对整个社会的影响。第三，随着互联网的发展，个人的身份、偏好和交易记录等大量信息被收集和利用。然而，个人隐私泄露事件时有发生，引发了公众对个人信息安全的担忧。滥用个人信息可能导致身份盗窃、金融诈骗和其他形式的侵犯个人权益的行为。网络犯罪如网络诈骗、网络侵权和网络盗窃等行为给个人和企业带来严重损失。网络诈骗手段不断翻新，通过钓鱼网站、虚假广告和恶意链接等方式欺骗用户获取财务信息。网络侵权行为网络上存在大量盗版文学作品、音乐、电影、软件等内容，侵犯了原作者的版权。很多盗版网站利用技术手段破解和传播盗版作品，给正版创作带来了严重的经济损失。网络侵权行为是指在互联网上侵犯他人合法权益的行为。随着互联网的普及和发展，网络侵权行为也呈现出一些现状：网络提供了一个匿名性强的平台，使得个人或组织可以轻易地散布不实言论、虚假信息或攻击他人名誉。这种网络诽谤行为对被诽谤者的声誉和形象造成了巨大的伤害。网络上存在大量非法色情和淫秽材料的传播，涉及未成年人的情况尤其令人担忧。这种行为违背了社会道德底线，对青少年的身心健康造成了威胁。网络上存在大量侵犯知识产权的行为，包括专利、商标、软件等方面的侵权。这种行为不仅损害了创新者的权益，也阻碍了科学技术的发展和经济的进步。网络上存在大量的个人和机构数据被非法获取、存储、传播的情况。黑客攻击、恶意软件和社交工程等手段使得个人的隐私和信息安全面临风险。随着科技的进步，新的安全威胁和漏洞不断涌现，传统的安全防护措施可能无法应对新形势。随着人工智能、云计算等新技术的发展，给黑客提供了更多的共计手段和路径。因此，持续的研究和创新在网络安全领域变得尤为重要，以保护系统和数据免受威胁。最后，网络安全和信息化管理涉及多个法律领域，包括隐私保护、网络犯罪打击和知识产权保护等。但是，现行法律可能无法完全覆盖新兴技术和威胁所涉及的问题，需要根据实际情况进行修订和完善[1]。

2 网络安全与信息化管理的防范措施

2.1 建立完善的信息安全管理体系

建立明确的信息安全政策，明确规定个人、组织和国家对信息安全的态度和要求。该政策应包括安全目标、责任分配、违规行为处理等内容。制定具体的安全规范和流程，包括密码管理、网络访问控制、备份和恢复等方面的规定。这些规范和流程应当得到广泛传达和执行。定期进行风险评估，识别潜在的信息安全威胁和漏洞。通过评估结果，采取相应的补救措施，降低风险并加强安全控制。利用漏洞扫描工具对系统和应用程序进行扫描，及时发现和修复存在的漏洞。漏洞扫描应当定期进行，并及时更新扫描工具以适应新的威胁。进行

定期的安全审计，检查信息系统和安全控制的有效性和合规性。通过审计结果，及时发现问题并采取纠正措施。信息安全管理体系应定期进行更新和改进，以适应快速变化的威胁环境和技术发展。包括更新安全策略、规范和流程，并及时了解新的安全威胁和防范措施。加强员工和用户的信息安全意识培训，提高他们对信息安全的重要性的认识，并教育他们遵守安全规范和流程。

2.2 使用安全可靠的网络设备和软件

为了确保网络系统的安全性，需要选择具有良好安全记录的网络设备和软件，并及时进行系统补丁更新和安全设置。首先，在选购网络设备时，应该考虑供应商的信誉和产品的安全性能。选择经过认证的品牌和厂家，他们通常会对其产品进行严格的测试和审查，以确保其符合相关的安全标准。对于软件选择，可以借助第三方评估机构的评级和评估结果，选择那些被广泛认可和使用的软件，避免使用存在安全漏洞的软件。其次，随着网络威胁不断演变和增强，软件供应商会发布针对已知漏洞的补丁程序。必须定期检查并安装这些补丁，以修复已知的安全漏洞，防止黑客利用这些漏洞入侵的网络。此外，还需要对网络设备和软件进行适当的安全设置，比如限制访问权限、启用防火墙和入侵检测系统等，以增强系统的安全性。最后，应该建立完善的监控系统，实时追踪网络设备和软件的状态和行为，及时发现异常情况。通过使用网络流量分析工具、日志审计系统等技术手段，可以监测网络流量、检测异常行为，并及时采取相应的措施[2]。此外，还应该定期对网络设备和软件进行安全漏洞扫描，及时修复潜在的安全漏洞，避免被黑客利用。

2.3 强化身份认证和访问控制

通过采用多层次的身份认证机制，包括密码、指纹识别、双因素认证等，可以提高系统的安全性，并确保只有合法的用户能够获取相应的信息资源。首先，用户在登录系统或访问敏感信息时需要输入正确的密码进行验证。为了增加密码的复杂程度，可以要求用户使用包含字母、数字和特殊字符的组合，并定期要求修改密码。此外，还可以采用密码策略，如设置密码长度限制、锁定账户等，以增强密码的安全性。其次，双因素认证结合了两个或多个独立的身份认证要素，如密码和动态口令、指纹和智能卡等。用户需要同时提供多个不同类型的认证信息，以确保身份的真实性。这种方法有效地提高了系统的安全性，因为即使一个认证因素被破解或泄露，攻击者仍然无法通过其他认证因素来获取敏感信息。此外，管理员可以根据用户的职责和需要来分配不同的权限级别，例如只能读取、编辑或删除某些特定信息。细粒度的权限管理可以避免未经授权的用户访问敏感信息，并减少数据泄露和滥用的风险。在实施强化身份认证和访问控制的过程中，还应该加强对身份认证技术的研究和发展，并及时更新系统以抵御新型的安全威胁和漏洞。

2.4 加强数据加密和备份

对重要数据进行加密存储和传输，并定期进行数据备份，以确保数据在传输和存储过程中不被窃取或篡改，同时防止数据丢失或损坏。通过数据加密将原始数据转换为经过特殊算法处理的密文，只有拥有相应解密密钥的人才能够还原成明文，通过加密存储和传输数据，可以有效地防止非授权用户获取敏感信息。对称加密有着速度快，加密强度高，密钥管理简单等特点，但是存在密钥泄露的风险，广泛应用于电子邮件和文件传输协议中；非对称加密有着加密强度高，安全性高，密钥管理简单，但是速度较慢，常应用于数字签名和加密通信中。在实践中，需要根据具体情况及应用场景选择不同的加密方式。通常将两种加密方式结合使用。可以实现更高水平的安全性和效率，确保数据在传输过程中得到保护[3]。除了加密，还需要定期进行数据备份。将重要数据复制到另一个存储介质或位置，以防止数据丢失或被损坏。备份数据可以帮助恢复系统和数据，减少因硬件故障、人为疏忽、病毒攻击等原因导致的数据丢失风险。可以根据实际业务需求及数据重要程度选择全量备份或增量备份。在实施数据加密和备份时，还需要注意以下几点：选择合适的加密算法和密钥长度，确保加密的安全性。定期更新密钥，以防止密钥泄漏导致数据被解密。对备份数据进行存储介质的多样化，可以使用磁带、云存储等方式，并定期测试和验证备份数据的完整性和可用性。制定详细的数据备份策略，包括备份频率、备份目标、备份存储周期等[4]。

2.5 加强网络监控和日志管理

通过建立有效的网络安全监控系统，可以实时监测网络流量、访问行为和异常活动，及时发现并应对潜在的安全威胁。首先，建立网络安全监控系统是保障网络安全的基础。该系统可以收集和分析来自网络设备、服务器、应用程序以及其他相关系统的日志信息，从而全面了解网络环境中的安全状况和风险。通过使用先进的监控工具和技术，可以实时监测网络中的数据流量，检测并预防恶意攻击、未经授权的访问和其他异常行为。其次，定期审查和分析网络日志是及时发现安全威胁的重要手段。网络日志记录了网络中的各种事件和操作，

包括登录记录、文件访问、系统配置变更等。通过对网络日志的审查和分析，可以发现异常行为、漏洞利用或未经授权的访问尝试。这些信息可以帮助安全团队追踪和调查潜在的安全事件，并采取相应的防御措施。另外，网络监控和日志管理也有助于提高网络安全事件的响应能力。当发生安全事件时，网络监控系统可以及时发出警报，并提供详细的信息，帮助安全团队迅速做出反应。通过对网络日志的分析，可以确定攻击者的入侵路径和操作行为，从而更好地应对和阻止类似的攻击。为了有效加强网络监控和日志管理，组织可以部署先进的网络安全监控工具和技术，包括入侵检测系统、入侵防御系统和行为分析工具等，以实现实时监测和防御能力。建立网络日志管理系统，确保所有网络设备、服务器和应用程序的日志都被记录和存储，并定期审查和分析这些日志。培训和培养专业的网络安全人员，使其具备监控和分析网络流量、日志记录和事件响应的能力。与网络服务提供商和其他合作伙伴建立信息共享机制，及时获取有关新型威胁和漏洞的情报，提高应对能力。建立紧急响应和危机处理机制，确保在发生安全事件时能够迅速作出反应、隔离受影响的系统和恢复正常的网络运行[4]。

2.6 加强网络安全教育与培训

在加强网络安全教育与培训方面，可以采取一系列措施来提高用户的网络安全意识，增强用户对网络安全威胁的认知和防范能力。首先，通过各种途径向公众普及网络安全知识，告诉用户网络安全的重要性以及可能存在的风险。这样可以帮助用户认识到自己在网络空间中所面临的潜在威胁，并引起他们的警觉。其次，建立网络安全培训体系，为用户提供全面的网络安全知识和技能培训。可以开设网络安全课程，涵盖网络安全基础知识、密码学、漏洞分析、攻击检测与防御等方面内容。通过培训，用户可以学习到如何制定强密码、如何辨别网络钓鱼等常见网络攻击手段，并掌握相应的防范方法。此外，还可以组织网络安全演练和模拟攻击活动，让用户亲身体验网络攻击的危害和后果。通过实际操作，用户可以更好地理解网络攻击的过程和手段，并针对实际情况进行防范和应对。另外，网络技术日新月异，网络攻击手段也在不断演变。因此，网络安全教育与培训需要及时跟进最新的安全威胁和防御技术，确保培训内容的实用性和有效性。

2.7 推动技术创新和研发

在当前快速发展的信息技术时代，网络安全威胁也不断增加，因此必须持续推动网络安全技术的创新和研发，以提高网络安全产品和解决方案的能力。首先，通过投入更多资源和资金，加强网络安全领域的科学研究，推动新的技术和解决方案的出现，可以提高防范和应对各种网络安全威胁的能力。例如，开发用于检测和防御恶意软件、网络攻击和数据泄露的新型算法和工具，有助于提升网络系统的安全性。其次，随着人工智能、物联网、云计算等新技术的涌现，新的安全风险也随之产生。因此，及早进行风险评估，并主动寻找和挖掘新技术中的漏洞，可以帮助发现和修复潜在的安全隐患，以保障网络系统的安全。在推动技术创新和研发过程中，需要加强与企业、学术机构和政府部门之间的合作与交流。只有通过共同努力，才能更好地理解和应对不断变化的网络安全威胁，并提供更有效的解决方案。同时，建立健全的技术创新和研发体系，鼓励人才培养和创新实践，也是确保网络安全技术持续进步的关键[5]。

结语

网络安全和信息化管理是当今社会面临的重要挑战，需要个人、组织和国家共同努力来应对。通过建立完善的信息安全管理体系、加强网络安全教育与培训、使用安全可靠的设备和软件、强化身份认证和访问控制等多方面的防范措施，可以有效地提升网络安全水平，并保护个人、组织和国家的信息资产。同时，也需要加强合作与信息共享，推动技术创新和研发，加大法律和政策保障力度，以确保网络安全环境的持续改善和进步。

参考文献

[1]王宇,&杨晓慧.(2022).当前网络安全威胁与信息化管理策略[J].科技导报,40(01):48-51.

[2]陈舒.(2021).网络安全问题与信息化管理的关系研究[J].现代市场营销,(03):47-48.

[3]张亮,&王宇.(2020).当前网络安全现状与信息化管理对策研究[J].科技资讯,(05):139-140.

[4]张伟.(2021).信息化管理视角下的网络安全防范策略研究[J].管理科学与工程,15(04):137-142.

[5]赵亚楠,&张莉.(2020).基于信息化管理的网络安全问题研究[J].综合技术,(12):48-51.