浅析网络信息安全

张　强
中国航空工业集团公司西安航空计算技术研究所　陕西　西安　710065

摘　要：随着信息技术的飞速发展，网络信息安全问题日益凸显，对个人隐私、企业运营乃至国家安全构成严重威胁。本文旨在浅析网络信息安全的重要性，探讨当前面临的主要威胁和挑战，并简要介绍一些有效的信息安全防护措施。通过对网络信息安全的概述和策略分析，本文旨在提高公众对网络信息安全的认识，为相关从业者提供有益的参考和启示。

关键词：网络信息；安全；措施

引言：网络信息安全的重要性不容忽视。我们每个人都应该提高网络安全意识，采取必要的防范措施；企业应加强网络安全管理，保障企业信息资产的安全；相关部门应加强对网络安全的监管和防范，维护网络安全和利益。只有这样，我们才能共同构建一个安全、和谐、有序的数字世界。

1 网络信息安全的重要性

网络信息安全的重要性，如同坚固的堡垒，守护着数字时代的安宁与秩序。在信息化、数字化高度发展的今天，无论是个人、企业，都愈发依赖于网络环境进行信息的传输、存储和处理。然而，网络安全威胁也如影随形，不断侵袭着我们的数字世界。对个人而言，网络信息安全是保护个人隐私和财产安全的重要保障。随着社交媒体的普及和电子商务的蓬勃发展，我们的个人信息越来越多地暴露在网络空间。一旦这些信息被不法分子获取，就可能导致身份盗用、财产损失等严重后果。加强个人网络信息安全意识，采取必要的防范措施，如设置复杂密码、定期更换密码、不轻信陌生链接等，显得尤为重要。对企业而言，网络信息安全更是关系到企业的生死存亡。企业的商业秘密、客户数据等都是其核心竞争力的重要组成部分，一旦泄露或被篡改，可能给企业带来无法估量的损失。企业需要建立完善的网络安全防护体系，包括防火墙、入侵检测系统、数据加密等措施，以确保企业信息资产的安全[1]。此外，网络信息安全还关系到社会的和谐稳定。随着网络媒体的兴起，网络舆论的影响力越来越大。一些不实信息、恶意言论等在网络上的传播，可能引发社会恐慌和混乱。因此，加强网络信息安全监管，打击网络犯罪，维护网络空间的清朗，对于维护社会稳定具有重要意义。

2 网络信息安全技术

2.1 防火墙技术

防火墙是网络信息安全的第一道防线，其主要功能是在内部网络和外部网络之间建立一个安全屏障，以控制进出网络的数据流。防火墙通过检查数据包的来源、目的地、端口等信息，并根据预设的安全规则来决定是否允许数据包通过。根据工作原理的不同，防火墙可分为包过滤型、代理服务型以及状态监测型等。包过滤型防火墙主要基于网络层的信息，如IP地址和端口号，进行安全控制。它速度快、效率高，但对应用层的攻击防护能力较弱。代理服务型防火墙则作为内外网之间的中介，对数据包进行完全解析和代理，从而提供更高级别的安全保护。然而，其性能开销较大，可能影响网络速度。状态监测型防火墙则结合了前两者的优点，能够动态地监测网络状态并做出相应的安全决策。尽管防火墙技术不断发展，但仍存在一些挑战。例如，随着云计算和物联网等技术的普及，网络边界变得模糊，传统防火墙的防护能力受到挑战。新型攻击手段如零日漏洞攻击、APT攻击等也对防火墙提出了更高的要求。

2.2 入侵检测技术

入侵检测技术是网络安全的重要组成部分，它通过对网络系统的行为进行实时监控和分析，以发现潜在的入侵行为。入侵检测系统（IDS）能够检测来自内部和外部的恶意活动，包括未经授权的访问、数据篡改、拒绝服务攻击等。根据检测方式的不同，入侵检测技术可分为基于签名的检测和基于行为的检测。基于签名的检测主要依赖于已知的攻击模式和特征，通过匹配来识别攻击。而基于行为的检测则通过分析网络流量的统计特征、系统调用的异常模式等来发现潜在的攻击行为。入侵检测技术在提高网络安全方面发挥了重要作用，但也存在一些局限性。因此，如何提高入侵检测的准确性和效率是当前研究的热点。

2.3 数据加密技术

数据加密技术是保护数据在传输和存储过程中不被非法获取或篡改的重要手段。通过数据加密，可以将明文数据转换为密文形式，只有持有相应密钥的用户才能解密并获取原始数据。数据加密技术包括对称加密和非对称加密两种类型。对称加密使用相同的密钥进行加密和解密，速度快但密钥管理复杂。常见的对称加密算法有AES、DES等。非对称加密则使用一对公钥和私钥，公钥用于加密数据，私钥用于解密数据。这种加密方式安全性更高，但计算复杂度也更大[2]。常见的非对称加密算法有RSA、ECC等。随着云计算和大数据技术的发展，数据加密技术的应用场景也在不断扩展。如何在保证数据安全性的同时提高加密和解密的效率，以及如何在分布式环境中实现密钥的安全管理和分发，是当前数据加密技术面临的挑战。

2.4 身份认证与访问控制

身份认证与访问控制是确保网络系统中用户身份合法性和访问权限的重要手段。身份认证通过对用户提供的身份信息进行验证，确认其是否具备访问系统的资格。而访问控制则根据用户的身份和权限，对其在网络系统中的行为进行限制和管理。常见的身份认证方式包括用户名/密码认证、生物特征认证（如指纹、面部识别等）、数字证书认证等。每种认证方式都有其优缺点，需要根据实际应用场景进行选择和组合。访问控制则可以通过设置访问策略、权限管理等方式来实现。随着网络环境的复杂化和攻击手段的多样化，身份认证与访问控制也面临着新的挑战。例如，如何防范钓鱼攻击和社交工程攻击等新型攻击手段，如何确保认证信息的安全性和隐私性，以及如何适应动态变化的网络环境等都是当前需要解决的问题。

3 网络信息安全管理体系

3.1 安全策略与规范

安全策略与规范是网络信息安全管理体系的基石，它为组织提供了明确的指导方针和操作规范。（1）安全策略的制定。需要综合考虑组织的业务需求、技术能力和安全风险，策略内容应涵盖信息资产保护、访问控制、数据加密、安全事件响应等方面，确保各项安全措施能够有针对性地应对潜在威胁。策略应具有前瞻性和灵活性，能够随着业务发展和技术变化进行调整和优化。（2）规范是安全策略的具体化。它规定了组织在网络安全方面的操作标准和行为准则，规范应包括但不限于网络设备的配置标准、操作系统的安全要求、应用程序的安全开发规范等。通过制定和执行这些规范，可以确保网络环境中的每个元素都符合安全要求，降低安全风险[3]。（3）安全策略与规范的执行。需要得到组织内部各部门的支持和配合，需要建立相应的考核机制，对各部门的安全工作进行定期检查和评估，确保安全策略与规范得到有效执行。

3.2 安全组织架构与职责

一个高效的网络信息安全管理体系离不开合理的安全组织架构和明确的职责划分。第一，组织应设立专门的信息安全管理部门，负责统筹协调网络安全工作。该部门应具备专业的技术能力和管理经验，能够全面评估组织的网络安全状况，制定并实施有效的安全措施。信息安全管理部门还应与其他部门保持密切沟通，共同应对网络安全事件。第二，组织应明确各部门在网络安全方面的职责和权限。各部门应负责各自业务范围内的网络安全工作，包括制定并执行安全策略、配置和管理网络设备、监控和应对安全事件等。各部门之间应建立协作机制，共同应对跨部门的网络安全问题。第三，组织还应建立网络安全责任制，将网络安全责任落实到具体岗位和个人，通过明确责任划分和考核机制，可以确保每个员工都能够认真对待网络安全工作，共同维护组织的网络安全。

3.3 安全培训与意识提升

安全培训与意识提升是网络信息安全管理体系中的重要环节，它对于提高员工的安全意识和技能水平具有重要意义。第一，组织应定期开展网络安全培训活动，针对不同岗位和职责的员工提供有针对性的培训内容。培训内容应包括但不限于网络安全基础知识、安全操作规范、安全事件应对等方面。通过培训，可以使员工了解网络安全的重要性和紧迫性，掌握基本的安全技能和操作方法。第二，组织还应通过多种形式提升员工的安全意识。例如，可以定期发布安全公告和警示信息，提醒员工注意网络安全问题；可以开展安全知识竞赛和宣传活动，增强员工对网络安全的认识和兴趣；还可以建立安全文化，将安全意识融入组织的日常管理和工作中。第三，组织还应建立安全培训考核机制，对员工的培训效果进行定期评估和反馈。通过考核，可以发现员工在安全意识和技能方面存在的问题和不足，进而制定针对性的改进措施和提升计划。

4 网络信息安全措施

4.1 加强技术防范

技术防范是网络信息安全的第一道防线，它依赖于先进的安全技术和设备来抵御各种网络攻击和威胁。第一，建立完善的防火墙系统是保障网络安全的基础。防火墙能够监控和控制进出网络的数据流，有效隔离内外

部网络，防止未经授权的访问和攻击，通过合理配置防火墙的安全规则，可以限制非法访问和恶意攻击，保护内部网络的安全稳定。第二，部署入侵检测系统（IDS）和入侵防御系统（IPS）是及时发现和应对网络攻击的重要手段。IDS能够实时监控网络流量，检测异常行为和潜在威胁，并及时发出警报。IPS则能够主动防御，对检测到的恶意流量进行拦截和阻断，防止攻击者进一步破坏系统。第三，数据加密技术是保护信息传输和存储安全的关键措施。通过对数据进行加密处理，可以确保数据在传输过程中不被窃取或篡改，即使数据被截获，攻击者也无法解密获取原始信息。对于敏感数据，还应采用强密码和密钥管理，确保数据的机密性和完整性。第四，定期更新和升级安全设备和软件也是必不可少的[4]。随着技术的不断发展和网络攻击手段的不断演变，安全设备和软件也需要不断更新以适应新的安全威胁和漏洞。

4.2 完善安全管理制度

除了技术防范外，完善的安全管理制度也是保障网络信息安全的重要基础。第一，制定明确的安全策略和规范是确保网络安全工作的有序进行的前提。这些策略和规范应涵盖网络安全的各个方面，包括访问控制、数据保护、安全审计等，并明确各级人员的职责和权限。第二，建立健全的安全组织架构是形成有效安全管理体系的关键。企业应设立专门的安全管理部门或岗位，负责网络安全的整体规划、监控和管理。还应建立跨部门的安全协作机制，确保各部门之间的信息共享和协同配合。第三，加强安全培训和意识提升工作也是至关重要的。通过定期的安全培训和教育活动，可以提高全体员工对网络信息安全的认识和重视程度，使其掌握基本的网络安全知识和技能。还可以通过举办安全知识竞赛、发布安全警示等方式，增强员工的安全意识和防范能力。

4.3 建立应急响应机制

网络安全事件往往具有突发性和不可预测性，因此建立应急响应机制对于及时应对和处置网络安全事件具有重要意义。（1）制定详细的应急预案和处置流程是建立应急响应机制的基础。这些预案和流程应涵盖网络安全事件的识别、报告、处置和恢复等各个环节，并明确各级人员的职责和处置措施。（2）定期组织应急演练和测试是提高应急响应能力的有效手段。通过模拟真实的网络安全事件场景，检验应急预案的可行性和有效性，发现存在的问题和不足，并及时进行改进和完善。（3）建立网络安全事件报告和共享机制也是必要的。通过及时报告和共享网络安全事件信息，可以加强与其他组织和机构的合作与协同，共同应对网络安全威胁。

4.4 提高用户自我保护意识

用户是网络信息安全的第一责任人，提高用户自我保护意识是保障网络信息安全的重要措施。第一，用户应增强对网络安全风险的认识，了解常见的网络攻击手段和防范方法。在使用网络服务时，应保持警惕，注意保护个人隐私和信息安全，避免泄露个人敏感信息。第一，学习并掌握基本的网络安全知识和技能是必要的。例如，学会设置复杂且不易被猜测的密码、定期更换密码、不轻易点击可疑链接等。还应了解并使用安全软件和工具，如杀毒软件、防火墙等，以增强系统的安全防护能力。第三，对于企业和组织而言，加强员工网络安全意识教育也是至关重要的。通过定期开展网络安全培训和宣传活动，提高员工对网络信息安全的认识和重视程度，使其自觉遵守网络安全规范和要求。

结语

综上所述，加强技术防范、完善安全管理制度、建立应急响应机制和提高用户自我保护意识是保障网络信息安全的重要措施。通过综合运用这些措施，可以有效提升网络安全的防护能力，降低网络安全事件的发生概率和损失程度。然而，网络安全是一个不断发展和变化的领域，我们需要持续关注新技术和新威胁的出现，不断完善和更新我们的安全策略和措施，以应对日益复杂多变的网络安全挑战。

参考文献

[1]李庆红.浅析网络信息安全技术管理的计算机应用[J].中外交流,2021,28(6):903.

[2]林俊辉.电子信息工程与网络安全浅析[J].电脑爱好者(普及版)(电子刊),2021(7):1368-1369.

[3]赵奕霖,沈涛,宋齐军,等.企业网络信息安全自动化防护方案浅析[J].邮电设计技术,2022(9):71-76.

[4]马聿北.网络信息安全问题浅析[J].中国信息化,2022(8):81-82.