网络工程中的信息安全与对策分析

冷　俊[1]　李亚菲[2]
1. 卡斯柯信号（北京）有限公司　北京　100070
2. 大秦铁路股份有限公司太原电务段　山西　太原　030000

摘　要：通过探讨网络工程中的信息安全问题及其对策，概述了信息安全的定义和在网络工程中的需求，详细分析了网络工程面临的主要信息安全威胁，包括黑客攻击、恶意软件、数据泄露与隐私保护、网络钓鱼与社交工程等。针对这些威胁，文章提出了加强网络安全意识教育、采用先进的安全技术、完善信息安全管理制度、构建联合防御体系以及制定数据备份与灾难恢复计划等对策措施。最后，文章展望了网络工程信息安全未来的发展趋势，强调人工智能、量子计算等技术将对网络安全产生深远影响。

关键词：网络工程；信息安全；威胁分析；对策措施

1 网络工程信息安全概述

1.1 信息安全的定义

信息安全是指为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。从广义角度来看，信息安全涵盖了信息的保密性、完整性、可用性、可控性和不可否认性五个核心要素。保密性要求信息仅被授权者访问，防止信息泄露给未授权的个人或实体，例如军事机密、商业秘密等敏感信息的保护；完整性确保信息在存储、传输过程中不被篡改，保持其原始状态和准确性，如电子合同、财务数据的完整性保障；可用性保证信息及信息系统能够在授权用户需要时正常使用，避免因攻击、故障等原因导致服务中断，像银行在线交易系统的持续可用；可控性指对信息的内容、传播、使用等进行控制，确保信息使用符合法律法规和组织规定；不可否认性则通过技术手段防止信息的发送方或接收方否认已发生的信息传输或操作行为，常用于电子签名等场景。在网络工程领域，信息安全是保障网络稳定运行、数据可靠传输和用户隐私保护的关键，贯穿于网络规划、建设、运营的全过程。

1.2 网络工程中的信息安全需求

网络工程具有网络架构复杂、数据流量庞大、用户终端多样等特点，这些特点决定了其独特的信息安全需求。在网络架构层面，随着网络规模不断扩大，从传统的局域网到广域网、云计算网络等复杂架构，网络节点众多，连接关系复杂，每个节点都可能成为安全风险的入口，需要保障网络架构的安全性，防止非法入侵和攻击。例如，企业内部网络与外部互联网连接时，需要防范外部黑客通过网络边界渗透到内部网络。在数据传输方面，网络工程中大量的数据在不同设备、系统之间传输，包括用户个人信息、商业数据、重要文件等，这些数据在传输过程中面临被窃取、篡改的风险，因此需要确保数据传输的保密性和完整性。例如，金融机构的网上交易数据传输，必须采用加密技术防止数据泄露和篡改[1]。另外，网络工程涉及众多用户终端，如个人电脑、智能手机、物联网设备等，这些终端的安全性参差不齐，容易成为恶意软件攻击的目标，进而威胁整个网络安全，所以需要对用户终端进行安全管控。

2 网络工程中的信息安全威胁分析

2.1 黑客攻击

黑客攻击是网络工程面临的主要威胁之一，其手段多样，对网络安全造成严重危害。常见的黑客攻击方式包括口令破解，黑客通过暴力破解、字典攻击、社会工程学等手段获取用户账号和密码，进而非法访问系统和获取信息。例如，利用弱密码漏洞，通过自动化工具尝试大量密码组合，破解用户账号。漏洞利用也是黑客常用手段，黑客利用操作系统、应用软件、网络设备等存在的安全漏洞，植入恶意程序、获取系统控制权或窃取数据。如针对Windows系统的永恒之蓝漏洞，黑客利用该漏洞传播勒索病毒，导致全球大量计算机系统遭受攻击，数据被加密勒索。此外，网络监听攻击通过在网络中部署监听设备或利用网络协议漏洞，获取网络中传输的敏感信息，如用户登录密码、信用卡信息等。黑客攻击严重威胁网络工程的安全性和稳定性，可能导致数据泄露、系统瘫痪等严重后果。

2.2 恶意软件

恶意软件是指在未经授权的情况下，在用户设备上安装并执行恶意行为的软件，包括病毒、木马、蠕虫、

勒索软件等。计算机病毒具有传染性、潜伏性、破坏性等特点，能够自我复制并感染其他文件和系统，破坏计算机中的数据，导致系统崩溃。例如，CIH病毒能够破坏计算机主板BIOS，使计算机无法启动。木马程序通常伪装成正常软件，诱使用户安装，然后在后台运行，窃取用户的敏感信息，如银行卡号、密码等，并将数据发送给攻击者。如灰鸽子木马，曾被广泛用于远程控制用户计算机，窃取个人信息。蠕虫病毒则通过网络自动传播，占用大量网络资源，导致网络瘫痪。勒索软件是近年来兴起的一种恶意软件，它通过加密用户数据，然后向用户勒索赎金以换取解密密钥。例如，WannaCry勒索软件在全球范围内爆发，感染了大量计算机，给企业和个人造成了巨大的经济损失。恶意软件的传播和危害严重影响网络工程的正常运行和用户信息安全。

2.3 数据泄露与隐私保护

数据泄露是指敏感信息因各种原因被未授权访问、披露或窃取，对个人隐私和企业利益造成严重损害。在网络工程中，数据泄露的原因多种多样，包括内部人员违规操作、系统安全漏洞被利用、网络攻击等。内部人员由于工作需要能够接触到大量敏感数据，若缺乏有效的管理和监督，可能会出现有意或无意的数据泄露行为。例如，某公司员工为谋取私利，将客户信息出售给竞争对手。系统安全漏洞也是导致数据泄露的重要原因，黑客通过攻击系统漏洞，获取数据库访问权限，窃取其中的数据[2]。随着大数据和云计算技术的发展，数据集中存储和处理，一旦发生数据泄露事件，影响范围更广，后果更为严重。数据泄露不仅侵犯了用户的隐私，还可能导致企业面临法律诉讼、声誉受损和经济损失。因此，加强数据泄露防范和隐私保护在网络工程中至关重要。

2.4 网络钓鱼与社交工程

网络钓鱼是一种通过伪装成可信实体，如银行、政府机构等，诱使用户提供敏感信息（如账号、密码、信用卡号等）的攻击手段。攻击者通常通过发送钓鱼邮件、创建虚假网站等方式实施攻击。钓鱼邮件中包含虚假链接或附件，用户点击链接或下载附件后，可能会被引导至虚假网站输入敏感信息，或者在设备上安装恶意软件。例如，用户收到一封伪装成银行的邮件，提示账户存在异常，要求点击链接进行验证，用户点击后进入虚假银行网站，输入的账号密码被攻击者获取。社交工程是指攻击者通过与目标对象进行交流，利用心理操纵和欺骗手段获取敏感信息或诱导目标对象做出有利于攻击的行为。攻击者可能通过电话、短信、社交媒体等方式与目标对象建立信任关系，然后获取相关信息。例如，攻击者冒充技术支持人员，通过电话联系用户，以系统故障需要修复为由，诱使用户提供账号密码。网络钓鱼和社交工程利用用户的心理弱点，具有很强的欺骗性，给网络工程信息安全带来很大威胁。

3 网络工程信息安全对策分析

3.1 加强网络安全意识教育

加强网络安全意识教育是提高网络工程信息安全水平的基础，首先，针对企业和组织的员工，应开展定期的网络安全培训，内容包括网络安全法律法规、常见的网络攻击手段、个人信息保护、安全操作规范等。通过培训，提高员工的网络安全意识和防范能力，使其能够识别网络钓鱼邮件、避免点击可疑链接、妥善保管个人账号密码等。例如，企业可以通过模拟网络钓鱼攻击场景，让员工在实践中学习如何识别和应对攻击。对于普通用户，应通过多种渠道进行网络安全知识普及，如社交媒体、网络平台、公益广告等。宣传内容可以包括如何保护个人隐私、设置强密码、避免使用公共Wi-Fi进行敏感操作等。提高公众的网络安全意识，能够从源头上减少因用户疏忽导致的信息安全问题。

3.2 采用先进的安全技术

在网络防护方面，防火墙技术作为网络安全的第一道防线，能够对网络流量进行过滤和控制，阻止非法访问和攻击。新一代防火墙除了具备传统的包过滤功能外，还集成了应用层检测、入侵防御、病毒防护等功能，能够更有效地抵御各种攻击。入侵检测与防御系统（IDS/IPS）可以实时监测网络中的异常行为和攻击活动，并及时采取阻断、报警等措施。例如，当检测到黑客的扫描行为或恶意攻击流量时，IPS能够自动阻断相关连接，保护网络安全。在数据安全方面，加密技术是保护数据保密性和完整性的重要手段。对称加密和非对称加密算法广泛应用于数据传输和存储过程中，确保数据在传输和存储过程中不被窃取和篡改。此外，虚拟专用网络（VPN）技术通过加密和隧道技术，在公共网络上建立安全的专用网络连接，保障远程访问的安全性。同时，人工智能和机器学习技术也逐渐应用于网络安全领域，通过对大量网络数据的分析和学习，能够更准确地识别攻击行为，提高网络安全防护的智能化水平[3]。

3.3 完善信息安全管理制度

企业和组织应建立健全信息安全管理制度体系，包括安全策略制定、人员管理、设备管理、数据管理等方面。在安全策略制定方面，明确信息安全的目标、原则和措施，为信息安全管理提供指导。人员管理方面，

建立严格的用户账号管理和权限分配制度，对员工的访问权限进行分级管理，确保只有授权人员能够访问敏感信息。加强对员工的背景审查和安全意识考核，防止内部人员的违规行为。设备管理方面，定期对网络设备、服务器、终端设备等进行维护和更新，及时修复安全漏洞，保障设备的安全运行。数据管理方面，制定数据分类分级标准，对不同敏感程度的数据采取不同的保护措施。建立数据备份和恢复机制，定期对重要数据进行备份，确保在数据丢失或损坏时能够及时恢复，还应建立信息安全事件报告和处理制度，明确事件处理流程和责任分工，确保在发生安全事件时能够及时响应和处理。

3.4 构建联合防御体系

在企业内部，不同部门之间应加强协作，实现信息共享和协同防御。例如，网络运维部门、安全部门和业务部门之间建立沟通机制，及时共享网络安全事件信息和业务需求，共同制定安全防护策略。在企业外部，加强与其他企业、行业组织、安全厂商的合作，建立信息共享平台和应急响应联盟。通过共享网络安全情报和威胁信息，企业可以及时了解最新的攻击手段和威胁趋势，提前采取防范措施。安全厂商可以为企业提供专业的安全技术支持和服务，帮助企业提升安全防护能力，通过构建联合防御体系，形成全社会共同参与、协同防御的网络安全格局。

3.5 数据备份与灾难恢复计划

企业和组织应制定详细的数据备份策略，确定备份的数据范围、备份频率、备份方式和存储位置。对于重要的数据，如业务数据、用户信息等，应采用定期全量备份和增量备份相结合的方式，确保数据的完整性和可恢复性。备份数据应存储在安全可靠的位置，如异地数据中心或云存储平台，以防止因本地灾难（如火灾、地震等）导致数据丢失。同时，制定灾难恢复计划，明确在发生数据丢失、系统故障等灾难事件时的恢复流程和责任分工。定期进行灾难恢复演练，检验备份数据的可用性和恢复计划的可行性，确保在灾难发生时能够快速恢复业务运行。例如，某企业定期进行数据备份和灾难恢复演练，在一次服务器故障导致数据丢失的事件中，通过备份数据快速恢复了业务，将损失降到了最低。

4 网络工程信息安全未来发展趋势

随着网络技术的不断发展，网络工程信息安全将呈现出以下发展趋势。在技术层面，人工智能和机器学习技术将更加深入地应用于网络安全领域。通过对海量网络数据的学习和分析，人工智能能够更准确地识别新型攻击手段和威胁，实现自动化的安全防护和响应。例如，利用深度学习算法构建的入侵检测模型，能够自动识别未知的攻击模式。量子计算技术的发展也将对密码学产生深远影响，传统的加密算法可能面临被破解的风险，促使新的量子加密技术的研究和应用。物联网、5G、云计算等新技术的广泛应用，将带来新的安全挑战，同时也推动网络安全技术的创新和发展[4]。在管理层面，网络安全管理将更加注重风险管理和合规性。企业和组织将建立完善的风险评估体系，对网络安全风险进行全面、动态的评估，并采取相应的风险应对措施。随着网络安全法律法规的不断完善，企业将更加重视合规性管理，确保网络工程符合相关法律法规和行业标准。在产业层面，网络安全产业将迎来快速发展，市场规模不断扩大，技术创新不断涌现，网络安全服务将更加专业化和个性化。

结束语

随着技术的不断发展，网络工程面临的信息安全威胁也在不断变化和升级。因此，必须不断更新安全防护技术和管理制度，提高网络工程的信息安全水平。同时，加强国际合作，共同应对全球性的网络安全威胁，也是未来网络工程信息安全发展的重要方向。只有不断提高信息安全意识和防护能力，才能确保网络工程的安全稳定运行。

参考文献

[1]李玉凡.网络工程中的安全防护技术探讨[J].中国新通信,2023,25(16):126-128+137.

[2]曹超,秦朝.计算机网络工程中的安全问题及其对策探析[J].电脑知识与技术,2023,19(15):77-79.

[3]汲方君.网络工程中的信息安全与对策分析[J].集成电路应用,2024,41(03):380-381.

[4]胡楚然,李传卫.网络工程信息安全管理技术优化研究[J].信息与电脑(理论版),2023,35(17):199-201.