# 网络信息安全与防范

杨明强
玉林市市场监督信息服务中心　广西　玉林　537000

**摘　要：**在信息化浪潮的推动下，网络信息安全愈发成为不容忽视的焦点；随着黑客技术的日益精湛，内部人员泄露敏感信息的风险加剧，以及恶意软件层出不穷，网络空间的安全防线正面临前所未有的挑战。为应对这些威胁，必须采取一系列综合性措施，如加强安全教育培训，构建多层次的防火墙防御体系，广泛应用先进的数据加密技术，实施定期的数据备份策略，以及积极采用安全软件和服务，这些举措将共同织就一张严密的网络安全防护网。

**关键词：**网络信息；安全；防范

## 引言

随着信息技术的迅猛进步，全球数字化浪潮愈演愈烈，网络信息安全问题亦随之凸显。黑客技术日新月异，攻击手段愈发狡猾多变；内部人员因疏忽或恶意行为泄露敏感信息的情况屡见不鲜；恶意软件如病毒、木马等更是层出不穷，严重威胁着网络环境的稳定与安全。面对这些日益严峻的挑战，构建一个坚实可靠的网络信息安全防护体系刻不容缓。

## 1 网络信息安全概述

网络信息安全，作为现代信息科技领域的核心议题，主要涉及保护网络系统中的硬件、软件及其数据，确保它们不受偶然或恶意因素的破坏、更改或泄露。其核心目标在于确保网络系统的连续可靠运行，以及网络服务的无中断供给；从技术层面看，网络信息安全涵盖了计算机科学、网络技术、通信技术、密码学、信息安全技术等多学科的知识。它要求信息在存储、传输和交换过程中保持其保密性、完整性、可用性和真实性；保密性意味着信息仅供授权用户访问，完整性确保信息不被未经授权的修改，可用性保证网络服务和系统资源的持续可用性，而真实性则确保信息在传输过程中不被篡改或伪造。网络信息安全不仅关注技术层面的防御，还涉及到管理和策略的制定。这包括建立有效的安全管理制度，如强制密码策略、定期安全审计、恶意行为检测等，以及制定适当的安全策略，如数据加密、数据备份、防火墙设置等；这些措施共同构建了一个多层次的防御体系，以应对来自内部和外部的各种安全威胁[1]。

## 2 网络信息安全面临的主要威胁

### 2.1 黑客攻击

网络信息安全领域面临着诸多威胁，其中黑客攻击尤为突出；黑客攻击即未经授权的个人或团体通过技术手段对网络系统进行非法访问、破坏或窃取信息的行为，对网络信息安全的威胁是多维度且深重的。（1）黑客攻击的主要危害在于数据的泄露和丢失，黑客通过精湛的渗透技术，能够突破系统防线，窃取敏感信息如用户数据、商业机密等。这些信息一旦落入不法分子之手，就可能被用于非法目的，如身份盗窃、敲诈勒索等，对个人和企业造成不可估量的损失。于是，黑客还可能通过删除或篡改数据，造成数据的永久丢失或损坏，对业务运营造成严重影响。（2）黑客攻击对网络系统的正常运行构成严重威胁，黑客利用恶意代码或系统漏洞，对系统进行攻击，可能导致系统崩溃、服务中断等严重后果；这不仅会影响用户的正常使用，还可能对依赖该系统的业务运营造成致命打击，导致业务中断、经济损失等。（3）黑客攻击还可能引发更广泛的安全风险，一旦黑客成功渗透系统，他们可能利用该系统对其他系统进行攻击，形成连锁反应，导致更大范围的安全事件；黑客还可能利用系统漏洞进行大规模的网络钓鱼、恶意软件传播等活动，进一步扩大其影响范围，对整个网络环境构成严重威胁；黑客攻击对网络信息安全的威胁不容忽视。

### 2.2 内部人员泄密

在网络信息安全与防范的领域中，内部人员泄密是一个不容忽视的威胁。第一，内部人员通常拥有对系统、数据和应用程序的深入了解和访问权限，这使得他们有能力在不被察觉的情况下泄露敏感信息，这种泄密可能源于员工对数据的无意识误操作，比如将机密文件发送至错误的收件人，或者是在公共网络上进行不安全的数据传输。第二，内部人员也可能出于个人动机，如个人利益、职业竞争或报复心理，故意泄露公司的商业机密、客户数据或其他敏感信息。这种有意识的泄密行为对组织的声誉、业务运营和客户关系都可能造成严重影响。第三，内部人员的身份和权限使得他们更难以被

外部安全系统所识别和防范，传统的安全策略往往侧重于防止外部攻击者的入侵，而对于内部人员的行为监控和审计则相对薄弱，组织需要采取更为细致和全面的措施来防范内部人员泄密[2]。

2.3 恶意软件

黑客攻击作为网络信息安全的主要威胁，其危害深远且多面。（1）黑客攻击严重威胁数据的完整性和保密性，黑客利用先进的渗透技术，能够轻易获取敏感信息，如用户数据、商业机密等。这些信息一旦落入不法之手，可能会被用于身份盗窃、敲诈勒索等非法活动，给个人和企业带来巨大损失；于是黑客还可能通过恶意篡改或删除数据，导致数据永久丢失或损坏，对业务运营造成不可估量的影响。（2）黑客攻击会破坏网络系统的正常运行，黑客利用恶意代码或系统漏洞，对目标系统进行攻击，可能导致系统崩溃、服务中断等严重后果；这不仅影响用户的正常使用体验，还可能对依赖该系统的业务运营造成严重影响，甚至导致业务瘫痪。（3）黑客攻击还可能引发连锁反应，扩大安全风险；一旦黑客成功渗透系统，他们可能会利用该系统对其他系统进行攻击，形成安全风险的连锁反应。黑客还可能利用系统漏洞进行大规模的网络钓鱼、恶意软件传播等活动，进一步扩大其影响范围，对整个网络环境构成严重威胁；黑客攻击对网络信息安全的威胁是多方面且严重的，必须引起的高度重视[3]。

## 3 网络信息安全的防范措施

3.1 提高网络安全意识

在保障网络信息安全的过程中提高网络安全意识无疑是一项至关重要的任务；这不仅关乎个人的信息安全，也直接关联到整个组织或企业的数据安全。（1）提高网络安全意识意味着每个用户都应认识到网络空间并非完全安全，用户需要时刻保持警惕，警惕各种潜在的网络威胁；不轻易相信不明来源的信息，不随意点击可疑链接或下载未知来源的文件，是防止恶意软件攻击的基本步骤；这种警觉性有助于用户在复杂的网络环境中做出明智的决策，避免不必要的风险。（2）用户需要掌握基本的网络安全知识和技能，这包括但不限于设置强密码，以保护账户免受暴力破解；保护个人隐私信息，避免在公共网络上泄露敏感数据。识别网络钓鱼等常见网络攻击手段，防止被欺骗；通过不断学习和实践，用户可以提升自己的网络安全防护能力，减少成为攻击目标的风险。（3）提高网络安全意识还需要组织或企业的共同参与，组织或企业可以通过定期开展网络安全培训和演练活动，增强员工的网络安全意识；这些活动不仅能让员工了解最新的网络威胁和攻击手段，还能提高他们应对网络攻击的能力；组织或企业还需要建立完善的网络安全管理制度，规范员工的网络行为，确保网络系统的安全稳定运行；这包括限制访问权限、监控网络活动、及时修复安全漏洞等；提高网络安全意识是保障网络信息安全的重要一环，只有每个人都意识到网络空间的潜在威胁，并采取相应的防护措施，才能确保个人和组织的数据安全。

3.2 建立强大的防火墙

在网络信息安全与防范的实践中，建立强大的防火墙是至关重要的防范措施。第一，防火墙作为网络安全的第一道防线，其核心功能是监控和控制进出网络的流量。它能够根据预设的安全规则，对数据包进行过滤和检查，从而阻止潜在的安全威胁进入内部网络；这种过滤机制可以基于IP地址、端口号、协议类型等多种条件，有效拦截未经授权的访问和恶意流量。第二，防火墙还能够提供网络地址转换（NAT）功能，隐藏内部网络的真实IP地址，降低被外部攻击者直接探测和攻击的风险。通过NAT，防火墙可以将内部网络的私有IP地址转换为公共IP地址，使得外部网络只能看到转换后的公共IP地址，而无法直接访问内部网络的真实地址。第三，防火墙还具备日志记录和报警功能，可以记录网络流量、会话和事件信息，并在发现异常或可疑行为时及时发出警报。这些日志和警报信息对于安全管理员来说至关重要，可以帮助他们及时发现潜在的安全威胁，并采取相应的应对措施；为了建立强大的防火墙，组织需要选择可靠的防火墙设备和软件，并进行合理的配置和管理[4]。

3.3 数据加密技术

在网络信息安全与防范的领域中，数据加密技术无疑是一项至关重要的技术手段；该技术通过对信息进行编码，将明文转换为无法直接读取的密文，为数据的机密性和完整性提供了坚实的保护。（1）数据加密技术能够有效保证数据的机密性，在数据传输和存储过程中，加密技术构筑了一道坚不可摧的防线，防止未授权的个人或组织通过非法手段访问和窃取数据；即使数据在传输过程中被截获，由于已被转换为密文形式，未拥有相应解密密钥的攻击者也无法获取数据的真实内容，从而确保了数据的机密性。（2）数据加密技术对于维护数据的完整性同样具有关键作用；在数据传输过程中，数据可能会面临被篡改或破坏的风险，然而，通过使用数据加密技术，可以确保数据在传输过程中保持完整；任何对数据的非法修改都会在解密过程中被检测出来，从而防止了数据被篡改或破坏的情况发生，保证了数据的完

整性和准确性。（3）数据加密技术的应用范围十分广泛，无论是在个人用户层面，还是在企业和组织层面，数据加密技术都能够发挥重要作用。在个人用户层面，数据加密技术可以帮助保护个人隐私和敏感信息，如银行账户密码、社交媒体账号等；在企业和组织层面，数据加密技术则能够保护企业的商业机密、客户数据等重要资产，防止数据泄露和损失；在电子商务交易中，通过加密技术可以保护消费者的支付信息不被泄露；在云计算环境中，加密技术可以确保存储在云端的数据安全可靠，防止数据被非法访问和窃取。

3.4 定期数据备份

在网络信息安全与防范的实践中，定期数据备份扮演着举足轻重的角色。第一，数据备份是组织应对意外情况的关键手段，当硬件故障、自然灾害或人为错误导致数据丢失时，定期备份能够确保组织迅速恢复数据，从而避免业务中断和潜在损失；这种能力保障了数据的完整性和可用性，是任何组织在信息安全策略中不可或缺的一环。第二，定期数据备份有助于组织应对潜在的安全威胁，在遭受网络攻击或恶意软件入侵时，攻击者可能会尝试删除、加密或篡改数据，如果没有定期备份，组织可能面临数据永久丢失的风险，对业务造成严重影响；而定期备份则提供了数据恢复的可能性，将潜在损失降至最低。第三，为了实施有效的数据备份策略，组织需要采取一系列措施；选择可靠的备份解决方案是关键，以确保备份数据的完整性和可用性，确保备份数据的存储位置安全且易于访问，以防止数据丢失和非法访问；组织还需要制定明确的备份计划和时间表，确保备份的及时性和完整性[5]。

3.5 使用安全软件和服务

在网络信息安全与防范的实践中，使用安全软件和服务是一项至关重要的措施；这些安全软件和服务能够为用户提供多层次的安全防护，有效抵御各种网络威胁。（1）使用安全软件可以防范恶意软件的攻击；安全软件，如防病毒软件、反间谍软件等，能够实时监测和识别系统中的恶意软件，并通过隔离、删除等手段将其清除，保护用户的系统免受病毒、木马等恶意软件的侵害。（2）使用安全服务可以提升系统的整体安全性，这些服务通常包括安全咨询、风险评估、漏洞扫描、应急响应等，能够为用户提供全面的安全保障。安全咨询服务可以帮助用户制定适合其业务需求的安全策略；风险评估可以帮助用户识别潜在的安全威胁和漏洞，漏洞扫描可以检测系统中的安全漏洞并提供修复建议；应急响应可以在系统遭受攻击时提供及时的技术支持。（3）使用安全软件和服务还可以提高用户的安全意识和操作规范，以定期的安全培训和演练，用户可以了解最新的安全威胁和攻击手段，并掌握正确的安全防护方法；安全软件和服务通常会提供详细的安全日志和报告，帮助用户了解系统的安全状况，及时发现和解决问题。

**结束语**

网络信息安全，是当代社会不可忽视的基石，随着数字技术的发展，网络安全威胁层出不穷。必须以高度的责任感和专业的眼光，面对这些挑战；从培养个人的网络安全素养做起，每个人都应当成为守护网络安全的卫士。构建坚固的防火墙，运用前沿的数据加密技术，确保信息的传输安全无虞。定期备份重要数据，利用可靠的安全软件和服务，为网络空间打造一道坚不可摧的防线；让共同守护这片数字净土，确保信息安全，促进数字世界的繁荣与发展。

**参考文献**

[1]李明.人工智能在网络信息安全防范中的应用分析[J].网络安全技术与应用,2021(5):56-58.

[2]王锋.基于大数据时代计算机网络安全防范的措施刍议[J].网络安全技术与应用,2021(9):71-72.

[3]陈丹.大数据时代下计算机网络信息安全问题探讨[J].网络安全技术与应用,2020(12):66-67.

[4]金立群.大数据背景下的网络信息安全[J].金立群.电子世界,2020(24):11-12.

[5]周奇慧.企业网络安全建设中的关键因素分析[J].网络安全技术与应用,2021,(04):96-97.