计算机网络安全存在的问题及对策

周 铀
中国民用航空东北地区空中交通管理局黑龙江分局 黑龙江 哈尔滨 150000

摘 要：在信息更新、流动非常快的今天，互联网技术、网络已经深入人们的生活中。本文深入分析了当前网络安全存在的主要问题，并提出了针对性的对策，旨在加强安全防护，保障信息安全，维护网络空间稳定。通过技术防护、用户教育、安全监测等多方面的措施，为构建安全的网络环境提供有力支持。

关键词：计算机网络安全；问题；对策

引言：随着信息技术的日新月异，网络安全问题愈发凸显其紧迫性。网络钓鱼、欺诈行为和恶意软件的肆虐，不仅对个人隐私构成严重威胁，更对企业和社会的安全稳定构成重大挑战。基于此，深入剖析这些网络安全问题，并制定和实施针对性的应对策略，显得尤为迫切和重要。这不仅是保护信息安全的关键，更是维护网络空间和谐稳定、促进信息化健康发展的必要举措。

1 计算机网络安全的重要性

计算机网络安全的重要性在当今信息化社会中显得尤为突出。随着互联网的普及和技术的飞速发展，计算机网络已经深入到人们生活的方方面面，无论是个人、企业还是政府，都离不开计算机网络的支持。然而，网络安全问题也随之而来，给人们的生产生活带来了极大的威胁。第一，计算机网络安全直接关系到个人隐私和财产的安全。在网络时代，个人信息的泄露和滥用已经成为一个严重的问题。黑客通过入侵个人计算机系统，可以窃取用户的个人信息、银行账户密码等敏感数据，进而进行非法活动，给用户带来经济损失和安全隐患。第二，计算机网络安全对于企业的运营和发展具有重要意义。企业通过网络开展业务、存储数据、进行交易等活动，网络安全问题直接关系到企业的商业机密、客户信息和财产安全。一旦企业的网络系统遭受攻击，可能导致数据泄露、系统瘫痪等严重后果，给企业带来巨大的经济损失和声誉损害。第三，计算机网络安全还关系到国家安全和社会稳定[1]。政府机构和要害部门依赖计算机网络进行信息传输、决策支持等关键任务，网络安全问题可能导致国家机密泄露、系统瘫痪等严重后果，对国家安全构成威胁，还可能引发社会恐慌、破坏社会稳定。因此，保障计算机网络安全是维护国家安全和社会稳定的必然要求。

2 计算机网络安全存在的主要问题

2.1 外部威胁与攻击

计算机网络安全面临的外部威胁与攻击是多样且复杂的，这些威胁和攻击不仅给个人和企业带来了极大的安全风险，也对整个社会的稳定和发展构成了潜在威胁。（1）恶意软件与病毒是计算机网络面临的最常见的外部威胁之一。这些软件通过电子邮件附件、下载的未知文件或受感染的网站等途径，悄无声息地潜入用户的计算机系统。一旦成功入侵，它们便能够窃取用户信息、破坏数据、甚至控制整个系统，导致数据丢失、系统崩溃或个人信息泄露。恶意软件和病毒的传播速度极快，且变种繁多，使得防范和清除变得异常困难。（2）网络钓鱼是另一种常见的外部攻击手段。攻击者通过伪造电子邮件、虚假网站等方式，诱骗用户点击带有恶意链接或附件的邮件，进而窃取用户的个人信息、银行账户密码等敏感数据。网络钓鱼的手法日益高超，攻击者往往能够精心伪造出与真实网站几乎无异的虚假页面，让用户难以分辨真伪。（3）分布式拒绝服务（DDoS）攻击也是近年来网络安全领域的一大难题。这种攻击方式通过向目标服务器发送大量无效请求，使其过载并无法处理正常请求，从而导致服务中断。DDoS攻击具有极高的隐蔽性和破坏性，攻击者可以通过控制大量“僵尸网络”来发动攻击，使得防御变得异常困难。（4）高级持续性威胁（APT）也是计算机网络面临的一种严重外部威胁。APT攻击通常针对特定的目标，如政府机构、大型企业等，通过长期潜伏在目标网络中，窃取敏感信息、破坏关键设施等。APT攻击的手法复杂多样，攻击者往往具备高超的技术水平和丰富的经验，使得防范和应对变得异常困难。

2.2 内部安全漏洞

在计算机网络安全中，内部安全漏洞同样是一个不容忽视的问题。这些漏洞可能源于系统的设计缺陷、配置错误、人为疏忽等多种因素，对组织的敏感信息和资产构成严重威胁。一方面，软件漏洞是内部安全漏洞的

重要组成部分。操作系统、应用程序、数据库等软件系统中可能存在各种已知的或未知的漏洞，这些漏洞可能被攻击者利用，以获取对系统的非法访问权限，进而窃取数据、破坏系统或执行其他恶意操作。软件漏洞的存在往往是由于编程错误、设计缺陷或安全更新不及时等原因造成的。另一方面，配置错误也是内部安全漏洞的一个常见来源。在部署和使用计算机系统的过程中，如果网络管理员或系统管理员对系统进行了错误的配置，就可能导致系统存在安全隐患。例如，未启用必要的安全功能、未设置合适的访问权限、未安装必要的安全补丁等，都可能使系统暴露在攻击者的视线之下。除此之外，人为疏忽也是内部安全漏洞的一个重要因素。员工在使用计算机系统的过程中，可能会因为缺乏安全意识或操作不当而泄露敏感信息或引入恶意软件。例如，点击带有恶意链接的邮件、下载不明来源的文件、使用弱密码等，都可能使系统面临安全风险。最后，内部安全漏洞还可能与组织的文化和制度有关。如果组织缺乏安全文化，员工可能不会对网络安全问题给予足够的重视，也不会主动采取安全措施来保护自己和组织的利益。

2.3 网络钓鱼与欺诈

网络钓鱼与欺诈，作为计算机网络安全领域的重大问题，已经成为现代网络环境中的一大威胁。这些欺诈手段通过伪装成合法机构或个人，诱骗用户泄露个人信息、银行账户密码等敏感数据，给个人和组织带来了巨大的经济损失和隐私泄露风险。首先，网络钓鱼攻击是欺诈者通过伪造电子邮件、虚假网站或社交媒体消息等手段，诱骗用户点击恶意链接或下载带有病毒的附件。这些欺诈邮件或消息通常会模仿银行、政府机构、电子商务网站等可信机构的外观和口吻，以获取用户的信任。一旦用户点击了恶意链接或下载了病毒文件，攻击者就能够窃取用户的个人信息、银行账户密码等敏感数据，进而进行非法活动。另外，网络钓鱼与欺诈的隐蔽性极高。欺诈者通常会精心伪造虚假网站或邮件的外观和内容，使其看起来与真实机构几乎无异。他们还会利用社交工程学技巧，通过了解用户的个人信息和兴趣爱好，制作更具针对性的欺诈邮件或消息，以增加欺诈成功的概率[2]。这种隐蔽性使得用户很难分辨真伪，容易上当受骗。再者，网络钓鱼与欺诈的危害性极大。一旦用户的个人信息被窃取，攻击者就能够利用这些信息进行非法活动，如盗取银行账户资金、申请信用卡、进行网络购物等。这不仅会给用户带来经济损失，还可能导致用户的信用记录受损，影响其日常生活和工作。

3 加强计算机网络安全的有效对策

3.1 完善安全策略与制度

在加强计算机网络安全的过程中，完善安全策略与制度是一项至关重要的措施。一个健全的安全策略与制度能够为组织提供一个明确的安全框架，指导各项安全工作的开展，确保网络安全防护的全面性和系统性。（1）制定全面的安全策略：安全策略应该明确网络安全的目标、原则、方法和措施，确保网络安全的各项工作能够有序进行。在制定安全策略时，需要充分考虑组织的实际情况和需求，结合当前网络安全形势和威胁特点，制定出既符合实际需求又具有前瞻性的安全策略。（2）建立健全的安全制度：安全制度应该包括安全管理制度、应急响应制度、安全审计制度等多个方面。安全管理制度要明确各级安全责任人的职责和权限，确保安全工作的顺利开展；应急响应制度要规定在发生网络安全事件时的处理流程和应对措施，提高组织应对安全威胁的能力；安全审计制度则要对网络安全工作进行定期检查和评估，及时发现并纠正安全问题。

3.2 强化技术防护措施

在应对计算机网络安全威胁时，强化技术防护措施是确保网络安全的关键一环。通过采用先进的安全技术和工具，可以有效地降低网络攻击的风险，保护组织的敏感信息和资产。首先，部署防火墙和安全网关是强化技术防护措施的基础。防火墙能够监控和控制进出网络的流量，根据设定的安全规则对数据包进行过滤和隔离，阻止未经授权的访问和恶意攻击。安全网关则能够提供更高级别的安全保护，如VPN（虚拟私人网络）网关、入侵检测与防御系统（IDS/IPS）等，进一步加强对网络流量的监控和防护。其次，使用加密技术保护数据传输是确保网络安全的重要手段。通过采用SSL/TLS、VPN等加密技术，可以对传输中的数据进行加密处理，确保数据在传输过程中的安全性和保密性。这样，即使数据在传输过程中被截获，攻击者也无法轻易获取到原始数据的内容。另外，定期进行安全漏洞扫描和风险评估也是强化技术防护措施的必要步骤。通过使用专业的安全扫描工具，可以及时发现和修复系统中存在的安全漏洞和隐患，降低被攻击的风险，可以了解组织面临的安全威胁和潜在风险，为制定针对性的安全策略提供依据。最后，建立入侵检测与响应机制也是强化技术防护措施的关键环节。入侵检测系统（IDS）能够实时监控网络流量和系统日志，发现异常行为和潜在威胁，并及时发出警报。

3.3 加强用户安全教育与培训

在维护计算机网络安全的过程中，用户作为网络系统的直接使用者，其安全意识和操作习惯对网络安全具有至关重要的作用。因而加强用户安全教育与培训是确保网络安全的重要措施之一。一是用户安全教育与培训需要涵盖广泛的内容，包括但不限于网络安全基础知识、常见网络威胁的识别与防范、安全密码的设置与管理、个人信息保护的重要性等。通过向用户普及这些基础知识，可以让他们了解网络安全的重要性，掌握防范网络威胁的基本技能。二是针对不同用户群体，需要制定个性化的安全教育与培训计划。例如，对于企业员工，可以定期组织网络安全培训，让他们了解公司的安全政策和操作流程，掌握使用公司设备和系统时的安全注意事项。对于普通用户，可以通过社交媒体、网络论坛等渠道，发布网络安全知识和案例，提高他们的安全意识。三是还可以采用多种形式的安全教育与培训方式，如线上课程、讲座、研讨会等。这些方式可以根据用户的兴趣和需求进行选择，提高用户的参与度和学习效果，还可以结合实际操作演示和模拟攻击演练，让用户亲身体验网络威胁的严重性，从而更加重视网络安全。在加强用户安全教育与培训的过程中，还需要注意，持续性：网络安全是一个持续的过程，用户的安全教育和培训也需要持续进行。组织应定期评估用户的安全意识和技能水平，并根据评估结果制定相应的培训计划。互动性：在培训过程中，应鼓励用户积极参与讨论和提问，增强培训的互动性[3]。这样不仅可以提高用户的学习兴趣，还可以帮助他们更好地理解和应用所学知识。反馈机制：建立有效的反馈机制，及时收集用户对安全教育与培训的意见和建议。根据用户反馈，不断完善和优化培训内容和方式，提高培训的质量和效果。

3.4 建立安全监测与应急响应机制

在加强计算机网络安全的过程中，建立一个完善的安全监测与应急响应机制是至关重要的。这样的机制能够及时发现网络中的安全威胁，并迅速采取应对措施，从而最大限度地减少潜在损失。通过建立全面的安全监测系统，可以实时监控网络流量、系统日志、用户行为等关键信息，及时发现异常情况和潜在的安全威胁。这些监测系统可以采用各种技术手段，如入侵检测系统（IDS）、安全信息和事件管理（SIEM）工具等，以实现对网络安全的全方位监控。再者，一个完善的应急响应机制应该包括明确的响应流程、责任分工、资源调度等要素。一旦监测系统发出警报，应急响应团队应立即启动响应流程，对安全事件进行快速定位、分析和处置。为了建立有效的安全监测与应急响应机制，还需要注意，跨部门协作：网络安全不仅仅是技术部门的事情，还需要其他部门的支持和协作。因此，在建立安全监测与应急响应机制时，需要与其他部门进行充分的沟通和协调，确保各部门能够共同应对网络安全威胁。持续更新：随着网络技术和安全威胁的不断变化，安全监测与应急响应机制也需要不断更新和完善。组织应定期评估机制的有效性和适用性，并根据评估结果进行相应的调整和改进。实战演练：通过定期进行实战演练，可以检验安全监测与应急响应机制的有效性，并发现存在的问题和不足。

结语

总之，计算机网络安全是一个持续演进且不容忽视的领域。面对日益复杂的网络威胁，我们需要保持高度警惕，持续更新安全策略，强化技术防护，加强用户教育，并不断完善应急响应机制。只有这样，我们才能有效应对网络安全挑战，保护个人和组织免受网络攻击的侵害，确保网络空间的安全与稳定。

参考文献

[1]蔡海珍.计算机网络安全性维护研究思路构建[J].网络安全技术与应用,2020(11):5-6.

[2]赵任飞.计算机网络信息安全威胁及数据加密技术探究[J].网络安全技术与应用,2020(11):40-41.

[3]蒋回生.大数据时代计算机网络安全及防范措施研究[J].网络安全技术与应用,2020(11):71-72.