计算机通信网络安全与防护策略研究

熊露露[1] 王方士[2]
1. 新疆铁道职业技术学院，新疆 乌鲁木齐 830000
2. 新疆铁道中建三局集团（新疆）有限公司，新疆 乌鲁木齐 830000

[摘要]随着信息技术的飞速发展，在日常生活、商业交易以及社会服务中，网络的广泛应用为人们提供了便利，但同时也带来了诸多安全隐患。网络攻击、数据泄露及信息篡改等安全事件时有发生，给个人、企业甚至国家带来了巨大的经济损失与信誉危机。本篇文章探讨计算机通信网络安全的防护策略，重点分析用户安全意识的提升、网络安全技术的研究与应用以及网络安全管理的强化。

[关键词]计算机通信；网络安全；防护策略；网络攻击；信息安全
DOI：10.33142/aem.v6i10.14397 中图分类号：TP393 文献标识码：A

Research on Computer Communication Network Security and Protection Strategies

XIONG Lulu[1], WANG Fangshi[2]
1. Xinjiang Railway Vocational and Technical College, Hami, Xinjiang, 830000, China
2. Xinjiang Railway China Construction Third Bureau Group (Xinjiang) Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract: With the rapid development of information technology, the widespread application of the internet in daily life, commercial transactions, and social services has provided convenience for people, but at the same time, it has also brought many security risks. Security incidents such as cyber attacks, data breaches, and information tampering occur from time to time, causing huge economic losses and reputational crises to individuals, businesses, and even countries. This article explores the protection strategies for computer communication network security, with a focus on analyzing the improvement of user security awareness, the research and application of network security technology, and the strengthening of network security management.

Keywords: computer communication; network security; protection strategy; network attacks; information safety

引言

近年来，伴随着云计算、大数据及物联网等新兴技术的兴起，网络安全形势愈加严峻。传统的网络安全防护手段已难以应对复杂多变的安全威胁，各类网络攻击不断升级，攻击方式也愈发隐蔽与智能化。在这种情况下，网络安全不仅关乎企业的生存与发展，更是国家安全的重要组成部分。为了应对日益严重的网络安全威胁，各国政府与企业纷纷加大投入，致力于网络安全技术的研发与应用。各种网络安全技术层出不穷，包括但不限于入侵检测、数据加密、访问控制等，力求构建多层次、立体化的安全防护体系。此外，加强网络安全管理，提高全员的安全意识，也是抵御网络攻击的重要手段。

1 维护计算机通信网络安全的重要意义

在当今社会中，计算机通信网络安全的维护显得极为重要，涉及个人、企业及国家层面的安全与稳定。从个人的角度来看，互联网已成为日常生活中不可或缺的一部分，用户的隐私信息，包括身份、财务状况及健康记录，正面临着网络攻击的威胁。若网络安全漏洞被恶意利用，机密数据的泄露可能导致身份盗用等严重后果。保护个人信息不仅是对用户基本权利的尊重，更是维护社会信任的重要举措。

对企业而言，计算机通信网络安全直接影响财务稳定与品牌声誉。关键信息的泄露、客户资料的盗取及财务损失，这些都是网络攻击可能带来的严重后果，而这些损失往往具有毁灭性。统计数据显示，网络安全事件的平均成本逐年上升，企业在遭遇网络攻击后，除了面临直接经济损失外，还需承担由信任度下降引起的长期客户流失。

在国家层面，网络安全则被视为国家安全的关键组成部分。随着信息技术的迅猛发展，计算机通信网络愈加依赖于关键基础设施（如电力、交通与金融系统）。网络攻击可能造成经济损失，甚至引发社会混乱或威胁国家安全。各国政府已意识到网络安全的重要性，通过立法、技术投资及国际合作等方式来加强网络防护。网络安全防护能力的提升不仅是个人与企业的责任，更是国家与社会共同承担的义务。

2 计算机通信网络安全的影响因素分析

2.1 计算机通信网络自身缺陷

在计算机通信网络的设计与实施过程中，潜在的安全隐患影响着网络安全的重要因素。许多传统网络协议在设计时未能充分考虑安全性，导致攻击者能够轻易利用这些

漏洞进行各种攻击，例如中间人攻击（Man-in-the-Middle）及 DNS 欺骗，从而获取敏感信息。许多网络设备（如路由器和交换机）的固件更新不及时或存在编程错误，使得在遭遇攻击时脆弱性显著。由于默认配置常常缺乏安全性，攻击者能够通过扫描网络发现这些设备并实施入侵。更严重的是，某些设备在设计初期未充分考虑安全性，结果成为网络攻击的“软肋”。现代计算机通信网络通常由多个层次的设备与服务组成，信息在不同层次之间传递，每一个环节都可能成为攻击目标。

2.2 人为因素

人为因素在影响网络安全方面的重要性常常被低估。用户的不当操作被认为是导致安全事件频发的常见原因之一。许多用户因缺乏安全意识，选择简单易记的密码，或在多个平台上使用相同密码，使攻击者能够通过密码攻击轻松获得系统访问权限。在收到可疑邮件时，若用户未保持警惕，轻易点击不明链接，恶意软件的入侵随之而来。在系统配置时，若未遵循安全最佳实践，可能导致安全漏洞的产生[1]。缺乏定期的安全审计与风险评估，意味着潜在的安全隐患可能长期存在，直至发生严重安全事件后才被发现。安全意识的缺失不仅存在于普通用户中，部分专业人员在高压工作环境中同样可能忽视安全防护。例如，在维护系统时，网络管理员可能因时间紧迫而选择忽略某些安全配置，或未经充分测试即上线新系统，导致安全漏洞的出现。因此，开展系统的安全培训与意识提升，成为加强网络安全的关键措施之一。

2.3 环境因素

外部环境变化，例如恶劣天气或自然灾害，可能导致网络基础设施的损坏。暴风雨可能使通信线路断裂，影响网络的稳定性与可靠性。在某些情况下，极端天气条件下网络设备可能无法正常工作，进而导致数据丢失或泄露。地缘政治紧张局势可能导致国家间网络攻击频繁发生，企业与组织在这种背景下面临更大的安全威胁。经济状况的波动也可能影响组织在网络安全方面的投资能力，从而削弱防护能力的提升。网络安全政策的制定与执行力度不足，对整体网络安全水平产生负面影响。在某些国家和地区，网络安全法律法规不健全，缺乏明确的安全标准与责任划分，导致网络安全管理存在盲区[2]。总之，计算机通信网络安全受到多种因素的影响，包括网络自身的技术缺陷、人为因素及外部环境的变化。深入分析这些因素能够帮助组织识别潜在风险，进而制定更有效的安全防护策略，提高整体网络安全水平。

3 网络攻击与威胁分析

3.1 不同类型的网络攻击

网络攻击形式多样，涵盖了从简单的恶意软件到复杂的拒绝服务攻击（DDoS）、网络钓鱼及跨站脚本（XSS）等多种手段。其中，恶意软件攻击被认为是最常见的一类。通过病毒、蠕虫、木马等恶意程序，攻击者侵入用户的计算机，意图窃取敏感信息或破坏系统功能。拒绝服务攻击（DDoS）通过大量伪造请求使目标网络或服务超负荷运行，从而导致服务中断。大型网站或在线服务通常是这种攻击的对象，显著的经济损失及声誉受损往往是其后果。网络钓鱼攻击常常伪装成可信的实体，诱使用户提供敏感信息，如用户名、密码及银行账户信息。因其高度隐蔽性与欺骗性，这种手法极具威胁性。跨站脚本（XSS）攻击则利用网页漏洞将恶意脚本注入合法网站，迫使用户在访问时执行这些脚本，进而导致个人信息泄露或账户被劫持[3]。网络攻击不仅涉及技术手段，攻击者往往还运用社交工程技术对用户进行心理操控，以获取信任并实现目的。

3.2 攻击者的动机与目标

攻击者的动机多样，主要包括经济利益、政治目的、意识形态及个人名声等方面。通常，经济利益被视为攻击者的首要驱动力，尤其是在针对金融机构与电子商务平台的攻击中。在这种情况下，攻击者通过恶意软件进行数据窃取，或借助勒索软件对目标实施经济敲诈，从而获取金钱收益。出于政治目的或意识形态，部分攻击者选择针对政府网站与公共机构发起攻击。这类攻击往往具有宣传性质，旨在传播特定的政治理念或抗议现状。例如，某些黑客组织可能针对特定国家或机构实施网络攻击，以破坏其声誉或服务，表达自身立场。个人名声也可能成为攻击者的动机之一。出于对竞争对手的敌意，某些攻击者选择实施破坏性攻击或进行信息泄露，以削弱竞争对手的市场地位。尽管这种攻击方式不如经济利益直接，但其潜在影响同样显著。在选择攻击目标时，攻击者通常综合评估潜在收益与风险。金融机构、政府网站及大型企业因其丰富的数据资源与较高的曝光率，成为主要攻击目标。理解攻击者的动机与目标，帮助组织采取相应的防护措施，从而增强自身安全防护能力。

3.3 网络威胁的趋势与演变

随着技术的迅速发展，攻击者逐渐运用人工智能（AI）等新技术实施高级攻击，基于 AI 的攻击能够迅速适应防御措施，自动生成新型攻击模式，导致传统安全防护措施面临重大挑战。攻击方式日益趋向定向与长期潜伏。通常，攻击者在目标网络中潜伏数月，以进行信息侦查并寻找最佳攻击时机。在此过程中，真实意图的隐藏成为可能，攻击者能够积累足够情报，制定更有效的攻击策略。复杂的攻击工具逐渐取代简单攻击手法，攻击者通过暗网获取专业攻击工具与服务，从而降低实施攻击的门槛。同时，针对特定行业或领域的定制化攻击逐渐增多，网络安全形势愈加严峻。

4 计算机通信网络安全的防护策略探究

4.1 强化用户的计算机网络安全防护意识

在维护网络安全的过程中，虽然技术手段在保障网络

安全方面发挥着重要作用，但安全漏洞往往因用户的不当行为而产生。因此，组织必须实施全面的安全意识培训，通过定期的知识讲座与模拟演练，帮助用户理解网络安全的基本概念及其重要性。这些培训内容应具备针对性，以满足不同层次用户的需求。例如，技术人员需深入掌握复杂的安全知识，而普通用户则应重点关注密码管理与信息识别等基本技能。在日常操作中，用户应保持高度警惕，避免随意点击可疑链接或下载未知文件，通过提升用户对网络钓鱼、社交工程等攻击方式的识别能力，安全事件因人为疏忽引发的可能性显著降低。企业还可引入激励机制，以鼓励员工积极参与安全管理，及时报告潜在的安全隐患[3]。尤其需要强调对敏感数据的保护，以确保信息不会在未经授权的情况下被泄露或滥用。通过实施上述措施，用户的网络安全意识能够得到增强，从而有效降低安全风险，为计算机通信网络的安全防护打下坚实基础。

4.2 加强网络安全技术的研究与应用

随着网络环境的不断演变，攻击手段日益复杂，进一步加强网络安全技术的研究与应用显得尤为重要。技术研发应重点关注防御策略，深入分析网络安全面临的最新挑战，特别是针对网络攻击手法的研究与应对策略。网络安全技术的应用需要构建多层次的防御体系，结合入侵检测、恶意软件防护等多种技术手段，以形成全面的防护网络。同时，组织间的合作与信息共享显得尤为重要，通过借鉴其他机构的安全事件分析与防护经验，整体安全水平可显著提升。新兴技术的深入研究，如人工智能与机器学习在网络安全中的应用，正为实现自动化防护提供新的可能。

4.2.1 安全隔离技术

在网络安全防护中，安全隔离技术的作用不可忽视，其主要目标是通过物理或逻辑手段将不同网络区域分隔，以防止未经授权的访问与潜在攻击。通过实施安全隔离，能够有效保障关键信息资产的独立性，从而降低内部或外部攻击带来的安全风险。在企业网络中，虚拟局域网（VLAN）划分及防火墙流量过滤的应用，能够有效实现不同部门或功能区之间的隔离。在应用安全隔离技术时，需求评估对网络环境至关重要，合理配置网络设备与安全策略显得尤为重要。特别是对于敏感数据存储区，严格的访问控制必须施加，确保仅有授权用户能够访问。此外，安全隔离技术还应与其他安全措施结合使用，如入侵检测系统（IDS）与入侵防御系统（IPS），以提升对潜在攻击的实时监测与响应能力[4]。在云环境中，虚拟网络隔离技术能够在多个客户之间实现安全分隔，以确保每个客户的资源与数据安全。因此，安全隔离技术的持续研究与应用，对于构建安全稳定的网络环境具有深远的影响。

4.2.2 网络加密技术

网络加密技术作为保护数据传输安全的核心手段，有效防止数据在传输过程中被截获或篡改。信息在传输前被转换为不可读的形式，只有持有解密密钥的接收者能够恢复原始内容。通过实施网络加密技术，数据隐私得以保护，同时用户的信任也得以维护。在应用加密技术时，合适的加密协议选择至关重要。例如，安全套接层（SSL）与传输层安全（TLS）协议通常用于保护互联网通信中的数据安全。同时，组织应定期审查与更新加密算法，以确保其能够抵御新型攻击。对于存储在数据库中的敏感信息，必须同样实施数据加密，以保护用户隐私，防止因数据泄露造成的严重后果。在采用网络加密技术时，性能与安全性的平衡应充分考虑。虽然加密提供了强有力的安全保障，但可能导致数据传输的延迟。因此，在部署加密措施时，需评估其对系统性能的影响，并合理配置硬件资源，以确保加密技术的有效性与网络性能的兼容性。

4.3 强化网络安全管理

在确保计算机通信网络安全的过程中，网络安全管理作为关键环节，涉及政策、流程与技术等多个方面。组织必须建立全面的网络安全管理体系，制定明确的安全政策与标准，以指导各项安全措施的实施。通过明确安全职责与分工，员工的安全意识得以提升，确保每个成员在各自岗位上为网络安全贡献力量。在网络安全管理中，通过对网络安全现状的定期检查，潜在的安全隐患能够及时发现，并采取有效措施进行整改。同时，组织间的信息共享也显得尤为重要，借鉴其他机构在安全管理中的成功经验与教训，以提升自身的安全管理水平。针对可能发生的安全事件，组织应制定详细的应急响应计划，以确保在安全事件发生时能够迅速作出反应，降低事件对业务的影响[5]。在此过程中，员工培训的加强也不可忽视，提高其对安全事件的敏感性与响应能力，以确保在危机时刻能够有效处理安全事件。总之，强化网络安全管理不仅需要技术手段的支持，更需全员参与的意识与文化。在安全管理的各个环节中，组织应加强沟通与协作，共同构建安全、稳定的网络环境。

5 结语

网络安全问题已成为全球关注的热点，随着技术的进步与网络环境的变化，安全威胁愈发复杂与多样化。面对如此严峻的形势，提升用户的安全意识、加强安全技术的研究与应用、强化网络安全管理显得尤为重要。通过全面提高网络安全防护能力，组织可以在一定程度上降低安全风险，维护网络环境的安全稳定。在未来的研究中，应继续关注网络安全领域的新兴技术与发展趋势，积极探索多样化的防护措施，以适应不断变化的安全需求。与此同时，借助国际间的合作与经验交流，促进全球范围内的网络安全合作，形成共同防御的强大合力。企业应在安全管理的各个环节中加强沟通与协作，建立完善的安全管理体系，推动全员参与的安全文化建设。

[参考文献]
[1]师远渊,冉新涛,杨东平,等.计算机通信网络安全与防护策略[J].数字技术与应用,2023,41(3):237-239.
[2]王怿超,李执.计算机通信网络安全与防护策略分析[J].数字通信世界,2023(11):97-99.
[3]尹开贤.内网计算机终端安全策略的应用研究[J].信息安全与通信保密,2024(3):103-109.
[4]杨星.计算机通信网络中的安全维护策略分析[J].集成电路应用,2024,41(6):188-189.
[5]冯伯阳.企业局域网安全风险分析与防护策略研究[J].电脑知识与技术,2024,20(22):76-78.

作者简介：熊露露（1988.4—），女，新疆师范大学，计算机应用专业，现就职于新疆铁道职业技术学院，教师，讲师；王方士（1988.1—），男，华南理工大学，能源工程及自动化，现就职于新疆铁道中建三局集团（新疆）有限公司，生产经理，副高级工程师。