计算机网络信息通信的安全防范

杨 杨
中邮通建设咨询有限公司，江苏 南京 210000

[摘要]随着现代社会信息化进程的不断推进，计算机网络已经深入到人们生活的各个领域。然而，随之而来的网络安全问题日益突出，严重威胁到了个人、企业和国家的信息安全。文章主要分析了计算机网络信息通信中存在的安全隐患，并提出了相应的防范措施，以提高网络安全水平，保障信息时代的社会稳定和发展。
[关键词]计算机网络；信息安全；防范措施；网络安全
DOI：10.33142/sca.v7i8.13069 中图分类号：TP3 文献标识码：A

Security Precautions for Computer Network Information Communication

YANG Yang
China UTCC Construction Consulting Co., Ltd., Nanjing, Jiangsu, 210000, China

Abstract: With the continuous advancement of modern society's informatization process, computer networks have penetrated into various fields of people's lives. However, the accompanying network security issues have become increasingly prominent, seriously threatening the information security of individuals, enterprises, and countries. This article mainly analyzes the security risks in computer network information communication and proposes corresponding preventive measures to improve the level of network security and ensure social stability and development in the information age.
Keywords: computer network; information security; preventive measures; network security

引言

计算机网络技术的发展和普及，极大地推动了社会生产力的发展，提高了人们的生活质量。然而，网络攻击、信息泄露等安全问题也日益严重，给个人、企业和国家带来了巨大的损失。为了保障计算机网络信息通信的安全，有必要分析其中存在的安全隐患，并采取有效的防范措施。

1 网络通信安全防范的重要性

计算机网络通信的安全防范对于保护个人隐私至关重要。在网络通信过程中，个人信息、聊天记录、银行密码等容易暴露，给不法分子可乘之机。一旦个人信息被泄露，可能导致财产损失、名誉受损等问题。因此，加强网络安全防范，能有效保护个人隐私，维护个人信息安全。

网络安全防范对企业来说也具有重要意义。随着企业信息化建设的深入，越来越多的企业依赖网络进行办公、数据传输和业务运营。一旦网络安全出现问题，可能导致企业重要数据泄露、业务中断，给企业带来严重的经济损失。因此，加强网络安全防范，有助于保障企业信息安全，维护企业正常运营。在全球化的背景下，国家间的网络安全斗争愈发激烈。如果国家的网络安全防护不到位，可能导致国家重要信息泄露，影响国家安全。因此，加强网络安全防范，对维护国家信息安全、保障国家安全具有重要意义[1]。

在实际应用中，计算机网络通信安全防范需要从多方面入手。一方面，要加强对网络设备的保护，例如使用防火墙、入侵检测系统等安全设备，防止外部攻击。另一方面，要注重内部安全管理，加强对员工的网络安全意识培训，制定严格的网络安全规章制度，确保网络通信安全。

2 计算机网络信息通信的安全隐患

2.1 软件漏洞

软件漏洞问题由于编程错误、设计缺陷或者更新不及时等原因造成的。一旦黑客发现了这些漏洞，他们就可以利用这些漏洞进行攻击，获取系统的敏感信息。例如，网络钓鱼攻击就是一种利用软件漏洞进行的攻击方式。黑客通过伪造官方网站或者邮件，诱骗用户点击链接或者下载附件，一旦用户执行了这些操作，黑客就可以通过软件漏洞获取用户的敏感信息，如用户名、密码。另一种常见的网络安全隐患是网络攻击。网络攻击是指黑客通过各种手段，对计算机网络进行攻击，以达到破坏网络、获取网络资源或者窃取网络信息的目的。网络攻击的方式有很多种，如 DDoS 攻击、网络嗅探、恶意代码攻击等。DDoS 攻击是指黑客通过控制大量的计算机，对目标计算机网络发送大量的请求，使得目标网络瘫痪。网络嗅探是指黑客通过监听网络数据包，获取网络中的敏感信息。恶意代码攻击是指黑客通过在目标计算机上植入恶意代码，窃取计算机中的敏感信息或者破坏计算机的系统。

网络间谍是指黑客通过各种手段，窃取国家机密、企业机密或者个人隐私的行为。网络间谍的行为可能涉及到窃取国家机密、企业机密或者个人隐私的行为，这些行为

Copyright © 2024 by authors and Viser Technology Pte. Ltd.

都可能对国家安全、企业利益或者个人权益造成严重的损害。信息通信安全是计算机网络中非常重要的一部分，而软件漏洞、网络攻击和网络间谍是其中最常见的隐患。我们应该加强网络安全意识，定期更新软件，避免点击不明链接或者下载不明附件，以保护自己的网络安全[2]。同时，政府和企业也应该采取措施，加强网络安全防护，防止网络攻击和网络间谍的行为，以保护国家安全和企业利益。

2.2 病毒入侵

计算机网络信息安全面临着各种隐患和威胁。其中，病毒入侵是计算机网络信息安全中最为常见和危险的一种威胁。病毒是一种恶意程序，能够在未授权的情况下自我复制并传播，对计算机系统的正常运行造成破坏，窃取用户的信息，甚至导致整个系统的瘫痪。

病毒入侵的途径多种多样，其中最常见的方式是通过下载恶意软件。用户在下载软件时，如果不小心下载了含有病毒的软件，那么病毒就会随着软件的安装而侵入系统。此外，用户在使用互联网时，如果点击了恶意链接，也可能导致病毒入侵。这些恶意链接可能会隐藏着病毒程序，用户一旦点击，病毒就会侵入系统。还有一种途径是使用非法拷贝的软件。使用非法拷贝的软件，不仅违法，而且包含病毒，一旦使用，就会对系统造成威胁。

2.3 黑客攻击

密码破解是黑客攻击的手段之一。黑客通过破解用户的密码，获取系统的访问权限，进而实施进一步的攻击。黑客通常会使用暴力破解、字典攻击等方法来破解密码。暴力破解就是尝试大量的密码组合，直到找到正确的密码。字典攻击则是利用预先收集的用户密码字典，逐个尝试其中的密码。此外，黑客还可能利用系统漏洞，通过特定的代码来绕过密码验证，实现无需密码登录。

钓鱼攻击通过伪造邮件、网站等，诱骗用户泄露自己的账号密码等敏感信息。黑客会发送看似正规的邮件，诱导用户点击其中的链接，进而进入伪造的网站。这些伪造的网站与真实网站几乎一模一样，用户很难分辨出真假。当用户在伪造网站上输入自己的账号密码时，黑客就能轻松获取这些敏感信息。

拒绝服务攻击（DoS 攻击）是黑客用来破坏系统正常运行的一种攻击手段。黑客通过发送大量的请求，使得目标系统的资源被耗尽，导致合法用户无法访问服务。这种攻击会导致系统瘫痪，给企业或个人带来严重的损失。拒绝服务攻击的类型有很多，如 SYN Flood 攻击、UDP Flood 攻击等。

3 计算机网络信息通信的防范措施

3.1 加强网络安全意识

在现今数字化时代，网络已经成为人们日常生活和工作的重要组成部分。然而网络安全问题也日益严峻，网络攻击和黑客行为屡见不鲜。因此，提高用户对网络安全的认识，加强网络安全意识是防范网络安全风险的基础。

用户应该定期修改自己的密码，以保证账户安全。如果密码过于简单或者长期不更改，就很容易被黑客破解。此外用户还应该避免在公共场合使用不安全的网络连接，以免个人信息被窃取。用户还应该避免点击未知链接。这些链接可能会引导用户访问恶意网站，从而导致计算机感染病毒或者个人信息被盗取。用户还应该对电子邮件和社交媒体等平台保持警惕。这些平台是黑客常用的攻击手段，用户应该避免打开来路不明的邮件和消息，以免遭受网络攻击。

3.2 采用先进的加密技术

计算机网络信息通信的防范措施，采用先进的加密技术是保障信息安全的关键。加密技术是保护数据在传输过程中的安全性的重要手段，它可以防止数据在传输过程中被窃取或篡改。数据加密的基本原理是将数据转换成一种难以理解的形式，只有掌握了相应的密钥才能将其转换回原始数据。采用先进的加密算法，如对称加密、非对称加密和混合加密等，可以有效提高计算机网络信息通信的安全性。对称加密是最常见的加密方式，它使用同一个密钥对数据进行加密和解密。对称加密算法的优点是加密和解密速度快，但密钥的传输和管理存在安全隐患。非对称加密则使用一对密钥，即公钥和私钥，公钥用于加密数据，私钥用于解密。非对称加密的优点是解决了密钥传输的安全问题，但加密和解密速度较慢。混合加密则是将对称加密和非对称加密相结合，既保证了数据的安全性，又提高了加密和解密的效率[3]。除了加密技术，其他防范措施还包括防火墙、入侵检测系统、安全协议等。防火墙可以防止非法访问和攻击，入侵检测系统可以实时监控网络流量，发现并响应安全事件，安全协议则是在数据传输过程中提供加密和认证的机制。

总之，计算机网络信息通信的防范措施，采用先进的加密技术是保障信息安全的关键。通过采用对称加密、非对称加密和混合加密等先进的加密算法，可以有效提高计算机网络信息通信的安全性。同时，结合防火墙、入侵检测系统和安全协议等其他防范措施，构建更为安全可靠的计算机网络信息通信环境。

3.3 建立完善的网络安全防护体系

建立完善的网络安全防护体系是保障计算机网络信息通信安全的关键。为此，需要从多个方面入手，综合运用各种防范措施，以构建一个坚固的网络安全防线。

首先，防火墙是网络安全的第一道防线。通过设置防火墙，我们可以对进出网络的流量进行监控和控制，从而防止未经授权的访问和非法的数据传输。防火墙可以基于 IP 地址、端口号和协议类型等条件进行过滤，以确保网络的安全性和稳定性。其次，入侵检测和防御系统（IDS/IPS）是网络安全的重要组成部分，入侵检测系统可以实时监控网络流量，发现并报警异常行为和潜在的攻击活动[4]。入侵防

Copyright © 2024 by authors and Viser Technology Pte. Ltd.

御系统则可以根据预设的安全策略，自动采取措施对抗恶意流量和攻击行为，从而减轻或阻止攻击对网络的影响。

此外，安全审计也是构建网络安全防护体系的关键环节。通过对网络设备和系统的日志进行审计，可以及时发现和追踪安全事件，分析攻击手段和漏洞，从而提高网络的安全防护能力。安全审计可以帮助我们了解网络运行状况，发现潜在的安全隐患，并为网络安全的改进提供依据。

除了上述措施外，还应加强网络安全意识和培训。网络安全的实质是人的安全，只有提高员工的网络安全意识，才能有效预防内部安全风险。通过定期的网络安全培训，可以让员工了解最新的网络安全知识，掌握防范技巧，降低网络安全风险。总之，建立完善的网络安全防护体系需要综合运用多种防范措施。防火墙、入侵检测和防御系统、安全审计等技术的运用，可以有效防止网络攻击和病毒入侵。同时，加强网络安全意识和培训，提高员工的安全素养，也是保障网络安全的重要手段。只有全方位、多层次地加强网络安全防护，才能确保计算机网络信息通信的安全。

3.4 定期更新软件和系统

首先，要重视软件和操作系统的更新。定期更新软件和操作系统，修复已知的安全漏洞，可以降低系统被攻击的风险。许多安全漏洞都是由于软件或操作系统存在缺陷而导致的，一旦黑客发现了这些漏洞，就会对系统发起攻击。因此，及时更新软件和操作系统，是对网络安全的首要保障。其次，要加强系统安全性能的检查。定期对系统进行安全性能检查，可以发现并解决潜在的安全问题。这包括对系统设置进行检查，确保没有不合理的安全配置；对系统账户进行检查，确保没有滥用权限的情况；以及对系统日志进行检查，及时发现异常行为。通过这些措施，可以有效提高系统的安全性。最后，还需要加强网络安全意识。网络安全意识是防范网络攻击的重要环节。我们要时刻提醒自己，不要轻信陌生的电子邮件、短信或电话，避免点击不明链接或下载未知来源的文件。同时，要定期对重要数据进行备份，以防数据丢失或被篡改。此外，还要加强对密码的管理，使用复杂的密码，并定期更换密码，以防止密码被破解。

3.5 做好病毒防范工作

主机防范主要是通过实时监控信息以及文件传输、交换的过程来进行的。在这个过程中，系统会查找其中的可疑数据流及病毒文件等，并对其进行科学验证。如果发现数据或是文件确实已经被病毒感染，那么就要立即采取行动，将文件删除或是隔离，以防病毒文件侵害计算机系统。这种防范方式可以有效地保护计算机的安全，避免病毒对系统造成的损害。

与主机防范不同，网关防范是在网络层面对病毒进行防范。网关是计算机网络中的关键节点，所有的数据流都必须通过网关才能进入或离开网络。因此，通过在网关处设置病毒防范措施，可以有效地阻止病毒进入网络，保护整个网络的安全。网关防范的方式包括对进出网络的数据进行扫描和过滤，以及对网络流量进行监控，及时发现并阻止病毒的传播。总的来说，主机防范和网关防范是两种重要的病毒防范方式。主机防范侧重于对计算机本身的安全进行保护，通过对文件和数据的实时监控和验证，有效地防止病毒对计算机系统的侵害。而网关防范则侧重于对整个网络的安全进行保护，通过对数据流的扫描和过滤，阻止病毒进入网络，保护网络中所有计算机的安全[5]。这两种防范方式各有侧重，但又相辅相成，共同构成了计算机病毒防范的坚实防线。

4 结语

计算机通信已经全面地深入到人们的日常生活中，只有确保计算机通信的安全性和稳定性，才能让网络和计算机在日常生活中发挥更大的作用，才能体现科技带给人们的幸福感和先进性，促进社会的全面发展。计算机网络信息通信的安全防范是保障信息安全、维护社会稳定的重要措施。通过分析计算机网络信息通信的安全隐患，采取有效的防范措施，可以提高网络安全水平，为信息时代的社会发展提供保障。

[参考文献]

[1]李强,苗敬峰.计算机网络信息通信安全防范措施研究——评《计算机网络安全原理》[J].现代雷达,2021,43(4):107.
[2]李鹏.计算机网络信息通信的安全防范[J].集成电路应用,2020,37(10):36-37.
[3]张勤贵.计算机网络信息通信的安全防范措施探讨[J].现代信息科技,2020,4(6):156-157.
[4]王舵.初探计算机网络信息通信的安全防范措施[J].信息通信,2020(3):288-289.
[5]李红海,马锦绣.计算机网络通信中的安全问题与防范策略[J].河南科技,2020(34):8-10.

作者简介：杨杨（1993.2—），男，单位名称：中邮通建设咨询有限公司，毕业学校和专业：无锡太湖学院-土木工程。

Copyright © 2024 by authors and Viser Technology Pte. Ltd.