大数据时代的计算机网络安全及防范措施探讨

王婷婷
北部战区海军　山东青岛　266071

摘　要：计算机网络安全主要是在计算机运行过程中，免受未经过用户授权同意的使用、访问、干扰的能力。在网络安全方面，攻击者采取的手段和技术也越来越高级和复杂，因此，为确保计算机能安全稳定运行、保护用户信息安全，应制定科学合理安全防护措施，如强化安全用网意识、优化网络安全监测系统等策略，旨在妥善解决网络安全问题，确保计算机网络更好地为人们服务。

关键词：大数据；计算机网络安全；防范措施

Discussion on computer network security and preventive measures in the era of big data

Tingting Wang
Northern Theater Navy, Qingdao, Shandong, 266071

Abstract: Computer network security mainly focuses on protecting computer systems from unauthorized use, access, and interference during their operation without the user's consent. In the realm of network security, attackers are employing increasingly advanced and sophisticated methods and techniques. Therefore, to ensure the secure and stable operation of computers and protect user information, it is essential to establish scientifically rational security measures. Strategies such as enhancing cybersecurity awareness and optimizing network security monitoring systems should be implemented. The aim is to effectively address network security issues and ensure that computer networks serve people better.

Keywords: Big Data; Computer Network Security; Preventive Measures

引言：

大数据技术是指对大规模数据的处理、分析和管理技术，该技术可以帮助我们从海量数据中挖掘出有价值的信息。计算机网络安全是现代社会的重要组成部分。计算机网络在人们的日常生活中扮演着越来越重要的角色，包括互联网、移动设备、社交媒体和电子商务等。这些应用程序和技术使人们更加依赖网络，但同时也面临着越来越大的安全威胁，如网络病毒、黑客攻击、数据泄露和网络钓鱼等，大数据技术的应用，面临着隐私和安全的问题，因为处理海量数据时可能会涉及到个人隐私和商业机密等敏感信息。因此，在大数据时代下，应深刻意识到计算机网络安全的重要性，并在系统运行过程中，详细分析影响计算机网络安全的主要因素，制定具有较强科学性、合理性以及严谨性的安全防护措施。

一、大数据技术概述

大数据技术的核心是数据挖掘和机器学习，这两个技术通过对数据的分析和建模，可发现有用的信息和规律，从而帮助人们更好地理解数据。而这些信息和规律可以被应用在各个领域，如金融、医疗、物流等。在金融领域，大数据技术可以帮助银行、保险公司等机构更好地了解客户需求，从而提供更加个性化和优质的服务。在医疗领域，大数据技术可以帮助医生更好地诊断、治疗疾病，提高医疗效率和准确度。在物流领域，大数据技术可以帮助企业更好地管理库存、调度运输，提高运输效率和降低成本。

二、大数据时代的计算机网络安全现状分析

1.计算机网络安全

在大数据时代下，人们逐渐意识到计算机网络安全的重要性。在过去的几年中，全球范围内发生一系列严重的网络安全事件，如，2017年的“惊天大盗”事件和2018年的Equifax数据泄露事件。这些事件的发生，都为企业和个人带来不可估量的损失[1]。

（1）应该定期更改密码。无论是企业还是个人电脑，都需要安装防病毒软件和防火墙，以保护设备免受恶意软件和网络攻击。

（2）防火墙可以帮助阻止未经授权的访问。需要注意社交工程攻击，这是一种欺骗性的攻击，攻击者在获取用户信息时使用虚假身份或假冒网站。

（3）用户在使用计算机过程中，需定期备份电脑中的重要数据，以防止数据丢失或遭受勒索软件攻击。除个人保护，企业也需要采取措施来保护自己的网络安全。同时需对网络进行定期检查和漏洞扫描，从而发现和修复可能存在的漏洞。需要备份重要的数据，并建立灾难恢复计划，以便在发生网络安全事故时能够快速恢复[2]。

2.网络安全问题

（1）网络系统漏洞

计算机系统具有多元化特点，因此在系统运行过程中，无论是苹果系统，还是微软系统，都可能存在着不同形式的漏洞。出现漏洞主要原因是计算机出场自带，也有计算机在后续使用中出现的，会严重影响计算机正常使用。一般来说，当计算机系统可能存在漏洞是，在计算机软件后续更新中，会随着软件的升级与完善，修复系统中存在的漏洞，但也可能因为用户在软件下载过程中，出现一系列漏洞问题，未能及时修复漏洞，从而导致用户信息、资料被窃取的情况出现[3]。

（2）信息安全

计算机网络环境具有开放性特性，导致在后续信息收集、分析、存储以及应用过程中，出现被窃取以及丢失的问题。更有部分不法分子利用网络环境不完善特点，恶意窃取信息，给用户带来较大经济损失。

若计算机网络安全技术的发展相对滞后，网络攻击者利用漏洞和弱点进行攻击的手段更加成熟和高效。此外，网络安全技术的更新速度不能满足网络安全形势的快速变化，网络攻击者针对新型的网络安全技术进行破解的速度也比较快。

（3）人为

人为因素是影响计算机网络正常使用的主要因素，主要原因在于，用户在使用计算机时恶意操作或者操作不熟练都会带来较为严重的安全隐患。同时因技术水平影响，部分用户在实际操作电脑过程中会造成数据丢失、系统漏洞等问题，这也给黑客可乘之机，利用漏洞攻击用户计算机系统，造成系统丢失。

三、大数据时代的计算机网络安全防范措施探讨

1.提高对计算机网络安全问题的重视程度

大数据时代下，计算机病毒的种类以及数量都在随着技术发展而增加，严重影响计算机网络安全。基于此，应转变传统观念，提供对计算机网络安全问题的重视程度，有效避免因病毒的出现影响计算机正常使用，做到防患于未然，发挥网络防火墙主要作用，树立科学、合理防范病毒意识。根据相关调查研究发现，大部分用户都缺少安全用网意识，只是在计算机出现网络安全问题之后，才开始安装杀毒软件或者修复漏洞，但这种不良的用网习惯也会在一定程度上引发网络安全问题。因此，需要采取针对有效措施，提高用户网络安全意识，重视网络安全问题的防范工作，确保用户安全用网。

2.优化网络安全监测系统

部分违法犯罪人员会利用计算机防落防护漏洞，入侵企业和个人的电脑，在传播恶性病毒的同时，窃取机密文件，对计算机的使用造成较大影响。目前，杀毒软件、防火墙都能实现对大部分病毒的查杀以及阻隔。因此，病毒查杀软件以及防火墙逐渐成为计算机的“网络医生”，所以不断更新以及升级防火墙与病毒查杀软件，有利于提升计算机抵御病毒的能力。通过实时进行监控以及定期对计算机进行病毒查杀，可确保用户使用计算机安全，保护企业珍贵数据资料。为更好的优化以及完善网络安全检测防控系统，离不开专业人才的支持。因此，应加强专业人才培养力度，为网络安全提供保障。同时也要勇于创新，不断探索，革新技术。计算机网络安全技术是防范网络攻击和入侵的关键。为保护网络安全，需采用各种安全技术，包括网络加密、防火墙、入侵检测系统、数据备份与恢复等。同时需要不断地更新和升级多类型技术，以应对不断变化的网络安全威胁。而网络安全监控是及时发现和解决网络安全问题的关键。需建立科学有效的网络安全监控系统，对网络进行实时监控和分析，发现异常情况及时进行处理。同时，也需要建立网络安全事件响应机制，及时采取应对措施，保障网络安全。

3.完善计算机安全防护系统

在大数据时代背景下，部分不法分子会利用网络防护漏洞，以盗取用户信息或传播恶性病毒，实现不当盈利，而对于系统的保护通常会设置防火墙或者杀毒软件等。因此，强化防火墙与病毒查杀软件的功能以及效用，能够强化计算机对病毒入侵问题的抵抗力，为计算机安全构筑一道安全防线。

4.对杀毒软件进行更新换代

杀毒软件是保护用户计算机安全的重要工具之一，

然后现在市场上杀毒软件数量众多，并且部分杀毒软件自身便带有一定的捆绑软件或者病毒，而一款功能强大的杀毒软件，能够为用户提供健康的计算机使用环境，有效的降低病毒入侵的概率。但是，随着信息技术的迅猛发展，在高额利益的影响下，各种病毒也在不断的进行着升级，因此，一款杀毒软件，无法长效的对用户计算机进行保护，技术人员需要开发出能够及时、准确找到病毒入侵点的杀毒软件功能，以便更好的保护计算机网络。只有跟随着信息技术的发展，不断的对杀毒软件功能进行更新换代，确保用户用网安全

四、结语

综上所述，计算机网络安全是影响计算机安全稳定运行的关键因素，需要针对有效措施，保护个人与企业网络安全。使用强密码、安装防病毒软件和防火墙、注意社交工程攻击、备份重要的数据等方式，都是保护网络安全的关键步骤。企业也需要制定网络安全政策、培训员工、定期检查和漏洞扫描，并备份重要的数据和建立灾难恢复计划，能确保网络安全，并在数字化时代中安心使用计算机和网络。

参考文献：

[1]刘城.大数据时代背景下计算机网络安全防范应用与运行[J].无线互联科技，2023，20（08）：166-168.

[2]高春苹，王静.大数据时代的计算机网络安全及防范措施探讨[J].中国新通信，2023，25（08）：113-115.

[3]郑碧虹.浅谈大数据时代背景下的计算机网络安全防范策略[J].网络安全和信息化，2023（04）：124-127.