大数据背景下计算机网络信息安全问题分析

吴秀娟　荣　曦
济南市气象局　山东　济南　250000

摘　要：随着我国科学技术的飞速发展，大数据技术得到了广泛的应用，成为未来计算机发展的重要方向。然而，在现实生活中，大数据技术在使用过程中，受到诸多因素的制约。本文探讨大数据与网络信息安全，分析大数据背景下网络信息安全风险特征及风险问题，提出大数据背景下计算机网络信息安全防护对策，助力网络信息安全。

关键词：大数据；计算机；网络信息安全；风险；对策

引言

随着计算机网络技术的不断发展，人类社会发生了翻天覆地的变化。大数据时代，计算机网络成为数据传输和共享的主要载体，带动了各行各业的发展。虽然计算机网络的出现为人们的日常生活和工作提供了很多便利，但是安全问题已经成为限制计算机网络发展的主要障碍。因此，在大数据时代，为了计算机网络的健康发展，必须采取积极、科学的防护策略，确保计算机网络信息安全的高水平。

1 大数据背景下计算机网络信息安全防护的重要性

从根本上说，大数据是一种从大数据中快速、准确地提取有价值信息的科学工具，与之密切相关的技术都属于大数据技术范畴。随着大数据时代的到来，计算机网络信息安全的重要性日益凸显，大数据技术为经济社会发展带来了宝贵的收益和创新机遇。在数据时代的背景下，传统的数据分析方法往往依赖于通信层来分析不同的数据内容，如视频、图像等。在分析和处理大数据的过程中使用计算机网络技术可以提高效率。数据传输和数据处理质量，但在实际应用中存在一些不足。由于计算机网络的实际实施，信息安全隐患会更多，导致信息安全问题时有发生，也会影响公民的人身安全。为防止因各种不利因素造成数据泄露、修改和丢失，个人应充分注意保护网络信息安全，营造安全的网络运行环境，进一步增强计算机网络安全防护的效果。

2 大数据特征及网络信息安全

2.1 大数据

大数据技术的一个显着特点是数据框架的层次结构，在经济性和效率上具有很大的优势。大数据主要具有以下特点：（1）容量性。在数据信息的存储、传输和处理方面，大数据不再采用传统的GB、TB存储结构。目前信息处理主要集中在PB和ZB类型。同时，它可以准确地分析和计算各种冗余信息。（2）数据结构的多样性。信息传输一般是借助计算机网络和设备完成的，内部的文本、音频和视频信息在结构上主要具有非线性特征。随着网络平台和网络终端架构的推广实施，数据信息处理方式越来越多样化，只有调整和优化数据信息网络结构才能符合网络运行的内在要求。（3）价值性。大数据技术可以进行数据挖掘，如通过计算机系统挖掘综合数据库信息。与传统的信息和数据架构相比，大数据技术的主要特点是更具层次性，是数据技术的有效延伸[1]。

2.2 网络信息安全

网络信息安全是指保护网络系统内的数据、软硬件信息安全，使其不被攻击、泄露或恶意修改，确保系统安全稳定运行。首先，网络信息安全事件具有突发性特点；其次，运行过程中网络信息环境的主要特点是开放性和交互性，在传输数据时往往为黑客和病毒入侵提供了一定的路径。一旦计算机网络受到攻击，各种数据很可能会立即丢失，网络系统也会瞬间瘫痪。

3 网络信息安全面临的威胁因素

3.1 制度建设不到位

大数据时代背景下，信息管理系统为数据网络信息安全提供了重要基础，明确了大数据时代背景下信息数据安全的方向。因此，在网络数据信息安全的发展中，信息管理系统扮演着重要的角色。但在开发过程中，由于对网络数据信息安全管理系统缺乏重视，系统建设不到位，导致企业及相关机构信息管理系统建设出现问题，如无法确定相关制度职责、保障建设层次模糊不科学的网络和网络保护直接导致统筹规划和方案问题的出现，已成为大数据时代背景下网络数据信息安全的严重威胁[2]。

3.2 病毒与黑客的攻击

如果网络数据存在漏洞，将无法有效防止黑客攻击，也难以抵御木马程序的渗透。也就是说，黑客攻击就是一些网络用户使用一些特殊的技术手段，恶意破坏

他人的网络信息。通过攻击他人的用户信息来达到破坏其目的。在主动攻击下，此类网络攻击不仅对用户数据的信息完整性造成负面影响，还会严重损害用户的操作指令；在被动攻击下，用户信息将被破坏，或者重要信息将被破坏。虽然黑客攻击一般是被动的，不会对用户使用网络的过程造成任何不良影响，但用户会遇到信息窃取、泄露等一系列问题。无论黑客使用何种攻击方式，都会威胁到数据信息的安全。由于计算机网络的开放性，病毒隐匿性较高，所以极有可能会出现一种情况，即病毒被隐藏在硬盘或软盘上，其传播将会严重威胁计算机网络的数据信息安全。

3.3 计算机软件漏洞

在计算机网络应用过程中，用户借助各种计算机软件，可以获得各方面的网络信息服务。随着计算机网络的不断发展，越来越多的计算机软件被开发和使用，从而为用户提供了更多的便利。但是，在软件开发中，由于受到各种内外因素的影响，自身难免会出现一些差距。外界的攻击只能利用这些软件漏洞，从而非法窃取和破坏用户网络信息。此类情况若得不到有效防范，将严重威胁用户信息安全、财产安全乃至人身安全。

3.4 用户网络安全防护意识不足

在计算机网络的特殊应用中，总是存在着来自各个方面的信息安全隐患，也容易遇到各种网络信息安全问题。因此，只有用户有足够的安全保护意识，掌握一定的网络信息安全保护技术和方法，才能有效降低网络信息安全事故发生的概率。但就目前我国的计算机网络用户而言，很多用户网络安全防护意识不足，不能定期排查漏洞，也不能及时修复和维护。在这种情况下，网络信息安全无法得到妥善保障[3]。

3.5 人为操作因素

对计算机网络信息安全的影响用户是计算机网络的主要运营者，是参与计算机网络信息服务的主体之一。但是，由于计算机网络的开放性涉及的领域非常广泛，很多用户没有足够的安全意识和足够的计算机技术水平，因此在实施计算机网络时，往往是由于操作不当或疏忽造成的，对计算机网络的信息安全构成威胁。例如，在设置用户密码时，缺乏安全保护意识，仅使用简单的数字或字母组合作为密码进行加密。在删除文件或注册表时，没有意识到这些文件的重要作用，操作不当造成计算机网络信息安全隐患。此外，计算机网络管理人员对网络信息的管理能力也较差，难以保证计算机网络信息的安全。此外，没有对计算机网络进行日常维护和保养，给计算机网络信息安全带来了严重的隐患。

4 大数据背景下提高我国网络安全的对策

4.1 采取适当的网络安全犯罪预防措施

随着计算机和互联网的发展，网络犯罪也在增加。由于犯罪分子的动机难以改变，防控计算机犯罪需要发挥战略优势。第一，使用密码生物识别设备、指纹或语音识别技术以及视网膜成像技术来增加未经授权访问信息系统的难度；第二，使用拦截和过滤程序进行病毒检测，可以识别和拦截恶意计算机。反间谍软件（Anti Spyware Software）有助于防止犯罪分子控制个人电脑，并在个人电脑受到攻击时帮助清理您；第三，安装原始软件，因为原始软件中包含许多安全措施，而盗版软件不包含原始软件中存在的许多安全功能；第四，设计实时入侵报警系统，有效保护整个网络安全系统；第五，制定相应的法律法规来应对各类计算机犯罪，严惩网络犯罪分子[4]。

4.2 加强防火墙网络技术

防火墙网络技术在信息网络安全中的应用已经处于比较成熟的状态。近年来，越来越多的公私企业将网络防火墙技术应用到其互联网网络安全环境中，对保护数据中心信息安全起到了重要作用。设置防火墙是网络防御的基本措施，是维护网络安全的重要措施，可以有效防止对计算机网络的攻击。防火墙通常用于控制访问规模，拦截无法访问的IP，有效防止来自不安全IP和软件的入侵和攻击。它们根据安全策略阻止某些网络流量，并且一般会自动安装补丁，可以自动修复软件安全漏洞。一般来说，防火墙是保护计算机安全、防止计算机故障的安全屏障，同时也是用户保护计算机所采取的最基本的措施。防火墙可以是硬件、软件，也可以是两台或多台计算机之间的防火墙，它们在保护计算机方面执行多项重要功能。对于瞬息万变、变化莫测的传统计算机网络病毒，有关部门人员应对病毒的性质、特点和影响范围进行详细了解和分析，并以此作为有效震慑盗窃的依据。计算机病毒是根本。一旦发生用户数据信息事件，彻底做好计算机网络病毒安全防范工作。总的来说，在当今大数据时代的背景下，加强网络防火墙技术对我国计算机网络的信息安全具有一定的积极作用。

4.3 加强计算机网络平台账号的安全管理

首先，要从用户登录账户入手，从用户做起，完善用户账户管理和保护措施，用户更加关注账户，尤其是网银账户等与财产相关的账户，提高帐户级别很重要。设置密码时，请务必将密码设置为安全性较高的密码，以降低信息被窃取的风险，提高安全级别。其次，用户也要定期更换密码，不能长期使用同一个密码，因为我

们每天都会收到数以万计的信息，我们无法识别哪些信息含有病毒，所以我们可以看到通过我们的密码。因此，定期更改密码也可以保证账户安全，避免可能的密码泄露，减少网络信息安全事故发生的可能性[5]。

4.4 杀毒软件的应用

用户要想增强网络信息安全，除了在使用电脑时打开防火墙外，还需要使用杀毒软件来防止病毒对电脑的攻击。杀毒软件+防火墙是目前大多数用户保障信息安全的方式。用户在使用电脑时，可以打开杀毒软件对电脑环境和网络进行检查和修复。如果在查杀过程中发现病毒，当软件或某些网站或程序存在漏洞，容易被黑客攻击时，用户应及时点击杀毒软件进行下一步防护。杀毒软件可以保护电脑信息，防止泄露，达到保护电脑的效果。但是需要注意的是，用户在使用杀毒软件的时候一定要与时俱进，使用最新的杀毒软件，因为网络病毒在不断的更新，杀毒软件也在不断的完善旧的杀毒软件可能对一些新的电子病毒没有作用，也检测不到。

4.5 提高信息网络安全技术

黑客的攻击手段不断涌现，而且攻击手段越来越简单，是威胁计算机网络信息安全的重要因素。加强信息网络安全技术建设，加强网络防火墙技术实施。它不仅可以控制对内部网络的访问，还可以有效防止外部用户的入侵，保护计算机网络安全。系统采用防火墙技术自动检查计算机网络上的数据，及时发现并清除计算机病毒。加强计算机网络入侵检测识别技术的实施，防范外部非法入侵。常用的网络检测技术有两种：统计分析和特征分析。统计分析使用统计理论来计算计算机如何运行，以确定在该范围内运行是否安全。特征分析法主要是对计算机薄弱环节的攻击行为进行分析，利用入侵检测技术及时发现计算机系统的非法行为和入侵行为，并采取一系列反制措施防止黑客入侵，有效保护计算机网络信息安全，下一步一代防火墙技术从保护本机数据包转换转变为状态链路保护，后者参考签名分析的收集。

4.6 创设健全的计算机网络管理体制

在大数据环境下，企业和个人用户在正常使用计算机的过程中，必须特别注意保护计算机网络安全。构建安全的计算机网络系统，可以实现计算机硬件运行环境的不断完善，同时可以实现对相关运行设备的严格管理。建立可靠的计算机网络管理体系可以从以下几个方面着手：（1）社会企业和协会应积极建立可靠的计算机网络安全管理体系，建立保护网络信息安全的新方法，建立和设计计算机技术平台，以及不断提高计算机网络系统的稳定性和安全性。（2）加强对计算机操作人员的规范引导。一方面，企业要积极推动计算机操作人员的自主学习，不断提高计算机操作人员的上网技能；另一方面，信息安全教育，提高操作人员的计算机网络安全意识；能够准确把握和合理实施主要信息安全软件市场，进一步加强计算机数据和信息安全。（3）企业应结合实际应用环境实施数据认证技术，科学合理地控制计算机网络访问频率，依托多种形式的数字计算机网络认证，进一步增强内部计算机网络的可靠性和安全性，以及有效防止他人窃取和篡改网上信息[6]。

5 结束语

总之，随着大数据时代的到来，计算机在运行过程中经常会受到网络安全问题的威胁。尽管网络安全技术和产品多种多样，但病毒感染、黑客入侵等问题时有发生。对此，有必要根据实际情况开发更先进的防范技术和系统，全面加强日常防护，确保计算机数据和信息网络足够安全，为用户的日常生活提供各种便利。

参考文献

[1]张令.大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用，2022（04）：69-71.

[2]钟建坤.大数据下计算机网络信息安全及防护[J].数字技术与应用，2022（02）：203-205.

[3]丁卫兵.大数据时代下计算机网络信息安全问题研究[J].中国科技投资，2020（34）：219-221.

[4]李洪敏.基于大数据时代下的计算机网络信息安全问题分析[J].数字技术与应用，2019（10）：199-200.

[5]方巍，郑玉，徐江.大数据：概念、技术及应用研究综述[J].南京信息工程大学学报（自然科学版），2020，6（05）：405-419.

[6]李国杰，程学旗.大数据研究：未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考[J].中国科学院院刊，2020，27（06）：647-657.