大数据下的计算机网络信息安全与防护对策分析

陈达荣

（东莞市闪电狗智能科技有限公司，广东 东莞 523000）

摘 要 随着我国现代科学技术的不断进步，计算机网络技术得到了快速发展，并在人们的日常生产生活中得到了广泛普及。其在给人们带来了诸多方便的同时，也存在着一定的问题，诸如在运用网络技术时会存在信息丢失等问题，降低了人们对于计算机网络使用的信任度。计算机网络信息安全问题得到了人们的广泛关注，要想解决这些问题，相关技术人员就应加强计算机网络信息安全防护力度。基于此，本文首先对大数据内涵进行概述，其次就计算机网络信息安全中遇到的问题进行探讨，并提出相应的防护对策，最后阐述大数据下做好计算机网络信息安全与防护工作的意义，以期为相关技术人员提供借鉴。

关键词 大数据 计算机网络 信息安全

中图分类号：TP393 **文献标识码**：A **文章编号**：1007-0745(2022)07-0025-03

科学技术的发展带动了我国各行各业共同进步，并为我国社会经济建设做出了巨大的贡献。在大数据时代下，计算机网络技术渗透到了社会的方方面面，并且成为人们生活中的重要组成部分。但在其具体应用过程中，仍存在一定安全隐患，例如，在运用计算机网络时容易受到黑客的攻击，出现很多非法授权访问问题，而且有很多用户自身防范意识有所欠缺，导致文件信息泄露，并且网络上还有很多病毒存在，这些问题都影响着人们对计算机网络的正常使用。

1 大数据内涵概述

所谓的大数据，从字面意义上来看，就是指其信息数据规模十分庞大，在现代信息技术的支持下，能够在最短时间内对海量的信息进行筛选、分析、处理等，并帮助企业获得最新的资讯。大数据时代下，其发展与人们的日常生活紧密相连，从最初的大型计算机、摄像采集设备、到后期的电脑、人工智能技术的发展都离不开数据信息的优化升级，而且在不同领域下对于大数据的解释也有所不同。在大数据时代下，由于其自身具备庞大的数据信息，拥有多样化的处理手段，使得其在社会的各个领域都有所渗透，并且成了企业生产的关键性因素。虽然大数据时代的到来提高了人们信息处理速度，但庞大的信息数据也带来了诸多安全隐患问题，例如，个人信息的泄露、数据完整性的破坏等，都是大数据时代下的关键问题[1]。

大数据时代下的核心特征有以下几点：第一，数据量大。大数据时代的核心特征之一就是数据传输量大。以网上交易平台淘宝为例，其商品信息大约有四亿条，注册用户达到两亿以上，每天就有着超过 4000 万人的浏览量[2]。因此，大数据时代，其数据传输量十分大。第二，数据增长速度快。数据增长速度快也是大数据时代的核心特征。随着互联网络信息的快速发展，每天每时每刻都有大量的数据信息产生。诸如淘宝、京东、闲鱼等交易平台，每天都有数以万计的商品信息与交易信息产生。第三，数据的多样性。大数据时代的数据信息产生量大，增长速度快，再加上各种文字、视频、音频等媒体技术的发展，使得各种数据信息模式多种多样，而这也就造就了大数据时代下的数据信息具有多样性。第四，数据的不稳定性。在大数据时代背景下，随着大量数据的出现，使得数据在使用整理，储存过程中其管理模式存在问题，导致数据管理十分混乱，并且由于缺乏专门的法律条文对其进行约束，使得数据在使用与管理过程中，数据发生与管理方式不断发生变化，容易造成数据丢失或错误。因此，大数据时代下，数据存在不稳定性。

2 计算机网络信息安全中容易遇到的问题

2.1 容易受到黑客攻击

容易受到黑客攻击，是计算机网络信息安全中的常见问题之一，黑客通过先进的技术手段侵入他人的计算机内，获取他人信息并用此进行非法交易。在黑客攻击中，将其分为两种类型：一种是破坏性，另一

种是非破坏性，虽然攻击类型分为破坏与非破坏，但其对计算机网络信息安全都造成了较大影响，都会导致个人信息及数据资料的丢失，影响网络安全性[3]。这种黑客攻击属于恶意攻击的一种，并且其也分为主动攻击与被动攻击两种类型。主动攻击是指，具有一定的目的性，对计算机网络进行破坏的行为；而被动攻击则是指，攻击者为了获取计算机中的某些数据，在对计算机网络安全造成影响的基础上，对计算机系统进行攻击的一种行为。但同样的，无论是主动攻击还是被动攻击，都会导致计算机系统内的信息被泄露，影响计算机的正常运行，并对计算机网络信息安全造成严重破坏。

2.2 非法授权访问问题

非法授权访问问题主要是指在未获得相应权限的条件下，就非法入侵他人计算机中，对其信息进行查询与访问，这属于严重的违法行为。通常情况下，非法授权访问主要针对窃取企业内的机密文件或进入其系统数据后，对其数据进行肆意篡改、删除、增加等，从而获取某方面的利益，这种行为会导致企业内部出现混乱，数据信息瘫痪，严重影响了企业的正常运行。

2.3 用户自身安全意识不强

随着大数据时代的到来，信息网络技术已然渗透到了人们生产生活的方方面面，并且在大数据技术的支持下，加快了信息的传播速度，而且其也成了信息传播的重要载体。有部分用户缺乏对个人数据的防护意识，在网络操作过程中，随意点开链接，浏览非法网页或用手机进行扫码，在网络上无意暴露个人信息，从而导致计算机中毒，银行卡被盗刷，各种账号被盗取等安全问题[4]。因此，无论是社会还是个人，都应加强对计算机网络信息安全的重视程度，其不仅会威胁到个人，同时也会威胁到企业乃至国家。

因此，从个人角度来说，要加强自身的安全防范意识。从社会与国家角度来说，应大力加强对计算机网络信息安全的监管力度，不断提高其防护技术，优化网络环境。

2.4 文件储存问题

从目前的文件数据处理以及其运行过程来看，大多采取的都是云计算技术。运用该技术能够实现对文件信息的储存以及筛选，并且在进行数据共享时，还会成为黑客攻击的主要目标。在使用移动 U 盘的过程中，其会携带病毒，若不及时对病毒进行查杀，则容易将病毒带入到电脑中，造成网络中毒，给黑客入侵提供便利[5]。

2.5 共享携带传播

在云计算、互联网技术的支持下，网络中存在很多资源共享平台，用户在这类平台进行信息检索和下载时，极易在网站上留下痕迹，并导致个人信息泄露，很多不法分子通过对个人信息的买卖来获取利益。而且随着互联网络技术的普及，各种网络诈骗案件频频发生。不法分子通过伪造网站或利用电子邮件的进行诱骗，很多受害者由于防范意识不足，在此过程中绑定银行卡或将个人身份信息泄露，从而造成了严重的经济损失。

3 大数据下的计算机网络信息安全与防护对策

3.1 安装防火墙系统，预防黑客攻击

在大数据时代下，要想做好计算机网络信息安全与防护工作，提高信息的安全性，首先要安装防火墙系统。防火墙系统主要是由硬件与软件共同组合而成的，因此，可以将其划分为内部网络与外部网络。该技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术。防火墙技术的功能主要在于及时发现并处理计算机网络运行时可能存在的安全风险、数据传输等问题，其中处理措施包括隔离与保护，同时可对计算机网络安全当中的各项操作实施记录与检测，以确保计算机网络运行的安全性，保障用户资料与信息的完整性，为用户提供更好、更安全的计算机网络使用体验[6]。

3.2 构建网络管理制度，提升人为保护

要想在大数据时代下加强计算机网络信息安全与防护，用户在网络操作过程中，就应对其可能遭受的破坏因素进行明确，树立相关防护意识，做好对信息的保护工作。在其使用互联网络时，加强对各项信息内容的防范，做好信息、密码等方面的保护，以降低被窃取的风险。相关网络信息安全监管部门也要履行自身的职责，加强对网络环境的巡查，一旦发现威胁网络信息安全的因素，及时采取相应防护设施进行防护，以提高信息安全与防护工作的可预见性，并及时对信息进行保护。相关工作人员在工作过程中应严格按照工作规定做好自身的工作内容，加强对网络信息内容的监督与管理。

此外，相关工作人员还需对网络安全的实际问题进行全方位的分析，并制定出符合实际情况、能够切实运行的解决策略，以此来提高网络信息的安全性。同时，网络信息安全监管人员也应不断提高自身的工

作能力，以便于更好地开展信息安全监管工作。

3.3 打造网络信息安全环境，确保数据稳定运行

打造网络信息安全环境也是提高计算机网络信息安全的重要措施。在构建网络信息安全环境时，应运用最先进的网络设施，并采取不同种类的安全防护手段，使其合理地应用于网络环境建设中去，以此来确保数据运行的稳定性，加强各项信息的储存安全，并实现对计算机网络信息安全的全面维护。

3.4 强化大数据技术的应用，提升网络安全

第一，采用杀毒软件定期杀毒。虽然计算机网络系统自身具备一定的防御能力，但这种功能并不强大，若计算机网络系统不小心被病毒入侵，则会导致整个系统崩溃，影响系统的正常运行。而运用杀毒软件定期对计算机网络系统进行杀毒，能够实现对不同类型病毒的查杀。而且将杀毒软件与防火墙相结合，还有利于网络环境的稳定，避免出现网络安全问题。除此之外，要想加强网络信息安全，除了要对网络系统进行定期病毒查杀外，还需对杀毒软件进行优化升级，及时对杀毒软件数据库进行更新，只有这样才能有效保障网络安全性。

第二，合理应用入侵检测技术。入侵检测技术的运用能够有效提高计算机的防护力度，是加强计算机网络信息安全的重要措施之一。通过入侵检测技术的应用能够及时发现人为的侵入行为，并对此展开合理措施，对网络系统进行保护。入侵检测技术在应用过程中能够实时对计算机网络系统进行全方面的检测，保护数据信息，一旦发现违法入侵现象，会对入侵位置进行判断，并发出预警，阻断入侵行为。

3.5 应用安全监控平台，多元化安全监控与管理

在计算机互联网络信息安全建设中加强技术监管，从根本上对用户的计算机版本进行分类，并利用多样化的管理手段进行监控，一旦出现恶意攻击的软件或病毒时，就会根据其监管标准进行对比，若其存在较大的危险性，则会第一时间对用户进行预警提示，并采取正确的应对措施来保障用户信息安全。

4 大数据下做好计算机网络信息安全工作的意义

在大数据时代下，影响计算机网络信息安全的因素有很多，再加上数据更新换代速度较快，很多企业在其发展运营过程中都面临较大的网络威胁。对此，企业内的相关工作人员应做好网络安全防范工作，以避免企业内的机密文件、数据信息等被泄露，从而影响企业的正常运行，为企业发展提供良好保障。

要想在大数据时代下做好计算机网络信息安全工作，对于相关技术工作人员则提出了更高的要求，要求其能够合理运用多种现代化安全网络防护措施进行网络安全环境的构建，这其中不仅包含计算机技术、互联网络技术、通信技术、安全管理技术、信息应用技术，同时也需要相关技术人员加强对计算机网络信息安全管理等方面的理论知识学习。从宏观角度来说，加强计算机网络信息安全，就是对网络上的各种资源数据进行安全管理，也就是人们常说的信息安全。而从个人、企业角度来说，计算机网络安全管理工作就是对个人信息、企业内机密文件的安全管理。计算机网络安全管理工作的主要内容就是提升企业内信息安全管理水平，以保护企业内的机要文件、私密文件等。要想在运用互联网络技术时避免个人信息的泄露，就需加强互联网络技术对数据的传输工作，确保整个数据传输过程中，其数据的安全性、私密性能够得到有效保证。

5 结语

在大数据时代下，要想做好计算机网络信息安全与防护工作，需要经历一个漫长的过程，通过合理的方式对信息安全进行防护，诸如安装防火墙系统预防黑客攻击，构建网络管理制度提升人为保护力度，打造网络信息安全环境确保数据稳定运行，利用数字加密技术提升网络安全，应用安全监控平台，多元化安全监控与管理等，如此才能做好计算机网络信息安全的风险与评估工作，为人们构建一个安全的网络环境。

参考文献：

[1] 杨佳 . 计算机网络信息管理及其安全防护策略 [J]. 贵州农机化 ,2021(04):47-48,51.
[2] 王海澜 . 关于计算机网络信息安全及其防护对策的探析 [J]. 电子元器件与信息技术 ,2021,05(12):249-250.
[3] 梁猛 . 基于大数据的计算机网络与信息安全策略 [J]. 电子技术 ,2021,50(12):136-137.
[4] 汪晓睿 , 张学超 . 一种计算机网络信息安全防护策略 [J]. 电脑知识与技术 ,2021,17(35):30-31.
[5] 刘伊琳 . 计算机网络信息安全及其防护对策探讨 [J]. 冶金管理 ,2021(23):187-188.
[6] 杨佳兰 . 基于大数据环境下的计算机网络信息安全与防护策略研究 [J]. 南方农机 ,2021,52(23):132-134.