

# 基于大数据时代的计算机网络安全防范措施研究

周 博

河北省水利水电勘测设计研究院集团有限公司 天津市 300000

**摘要:**虽然大数据为社会大众予以诸多便利,但随之也带来诸多影响与危害,很可能在使用过程中威胁到个人财产与信息安全,因此,社会大众在大数据时代应当做好计算机网络安全防范,从根本上对个人信息与财产予以相应保障。基于此,本文以大数据时代为基础,在对大数据时代的基础概念进行介绍后,分析大数据时代计算机网络安全风险隐患,继而指明计算机网络安全防范措施。

**关键词:**大数据时代;计算机网络安全;防范措施

## 引言

随着经济的发展和技术的进步,人们的生活越来越离不开计算机技术。计算机在改变行业发展规律的时候也改变了人们的生活习惯,由此社会进入了大数据时代。在大数据时代,人们很容易就能查到来自世界各地的信息,只要想知道就会有途径。这种对于信息搜集发现的能力导致了人们对于信息的获取变得容易。在大家进行信息搜集和相互交流的时候,每个人都会在大数据中形成自己的痕迹,这就有可能发生隐私暴露。在人们还没有反应过来的时候,不法分子已经盯住了大数据时代这一特点,将信息技术应用到盗取他人信息的方面,将人们的信息非法提取并从事对用户不利的行为。面对信息技术带来的便捷与风险,每个人都要树立一定的风险防范意识,从而保护自身的隐私和财产安全。

## 1 大数据的概念及特点分析

随着时代的飞速发展,各类信息与数据的数量也在飞速增长,为了有效地提高人们生活与工作的节奏,对各种数据与信息进行有效收集分析成为当前极为重要的组成部分。大数据时代背景下,大数据以及云计算可以有效地应用到人们生活的各个方面,帮助人们更快地收集分析相关的数据信息,更好地提高信息的利用效率。大数据在人们生活中的运用可以极大地提升信息的共享性与开放性,人们都能够改变传统的生活观念,可以无限制地获取相应的信息与数据,从而学习到对自身有用的各种内容。同时,大数据还能将各种信息与数据进行有效分类与收集,人们可以更加快速地查找各个类别的信息与数据。大数据虽然为人们生活与学习提供了各种便利,但仍然会被一些心术不正的人所利用,为计算机网络安全带来一定的隐患。所以基于大数据时代背景下,有效地提升计算机网络安全防范意识是当前需要解决的重要问题之一,人们要正视大数据为人类带来的利与弊,客观地对待大数据时代的优势与

弊端。唯有如此,才能够有效地提升大数据时代背景下计算机网络安全与防护的效率<sup>[1]</sup>。

## 2 大数据时代计算机网络安全问题

### 2.1 计算机病毒与黑客攻击

病毒与黑客攻击作为当前计算机网络安全问题的重要因素,大数据时代下,数据信息的大容量传输,加大基层软件运行压力,且整个高效率、智能化的运行环境,对计算机脆弱性的环节产生严重影响,诱发出计算机的各类漏洞问题,且伴随着不同网络攻击手段造成的影响,加大整体防护难度。(1)在计算机病毒方面。从现有的网络病毒入侵形式而言,多种多样的病毒造成的影响面较广,受到病毒可移植性、隐匿性以及拓展性的问题,造成计算机单体以及整个区域内计算机网络的瘫痪问题,令内部程序以及文件产生丢失或损毁。(2)在黑客攻击方面。黑客攻击主要是寻找网络漏洞,完成对计算机系统内部信息的定向化攻击,现有计算机网络多元结构的完善下,黑客攻击形式也在逐步发生改变,逐渐向隐蔽化、破坏化的方向发展,对大体量信息以及数据关联信息进行攻击,增加计算机网络安全防护的识别压力,产生安全威胁问题<sup>[2]</sup>。

### 2.2 缺乏安全意识

当前,部分企业用户在模拟实际计算机网络应用过程中,未能充分重视网络安全的整体重要性,导致其未能对当前计算机应用进行合理的安全防护管理,尤其是在个人应用中,由于当前个人信息网络存在较强的信息开放性,导致应用信息的安全真假性难以及时确认,增加了应用数据自身的安全风险性,如果此时用户的网络安全意识不高,将会导致当前的个人信息网络完整性安全遭到严重破坏,甚至可能发生个人信息的安全泄露,为用户带来严重的影响,甚至造成经济损失与侵权情况。

### 2.3 网络系统自身安全问题

计算机网络系统具有较大的特性,自身就存在着一

定安全隐患,例如Windows、Linux等系统自身就存在着一定缺陷,而这些安全风险是没办法进行完全规避,并且计算机系统还容易遭遇硬件危险,例如用户在进行软件下载和安装时就会很容易导致其安全性受到威胁,增大计算机网络安全隐患出现的概率。从理论上而言,自身缺陷所带来安全隐患问题较为容易解决,但如果由于用户应用计算机网络技术进行软件下载和安装时出现安全隐患问题,并且在出现安全问题时遭受到外来入侵,如病毒,黑客,就会导致其数据安全性和保密性大幅度下降,导致用户信息出现泄露。

### 3 大数据时代计算机网络安全防范措施

#### 3.1 构建网络安全防火墙

在大数据时代,人们接收信息的来源多种多样,信息泄露的风险也越来越高。面对这样的信息使用环境,建立良好的网络安全防火墙能够在一定程度上增加信息的安全性。在如今的网络世界中,个人可识别的身份信息就是在网络中能够通过识别和匹配形成的个人信息内容。随着信息技术的发展,有一群精通信息技术但是心思不正的非法分子,在进行信息挖掘的时候就会专门盗取别人的身份信息,从而对个人进行威胁和锁定。面对这样的邪恶势力,建立安全防火墙就是一种非常有效的方式。网络安全防火墙是一种能够为网络提供屏障的安全保护系统。网络安全防火墙对于每个系统是不一样的,在不同的系统中可以有不同的防火墙,这就提升了防火墙的防范能力<sup>[3]</sup>。防火墙的主要功能就是提供了一种网络数据流动的合理性空间。在防火墙运行的时候,一旦发现外来非法数据进入就会启动防火墙功能,管理其他人员的访问权限,避免计算机内的资料被盗取。对于非法入侵的用户,防火墙会及时通知本机的用户,限制非法分子的使用,并拦截弹出的窗口,为用户提供安全的上网环境。因此,在使用计算机的时候,构建网络安全防火墙能够提高计算机的安全等级,是为计算机的使用提供保障的措施之一。

#### 3.2 建立并完善相应工作管理制度

在大数据的背景下,计算机网络的影响范围逐渐变大,对大众学习、生活以及工作产生了巨大的影响,因此相关工作人员可以根据自身发展需求建立并完善相应安全管理制度,通过科学合理的制度对计算机使用人员以及管理人员行为进行相应的约束,从而在根源上提高网络安全整体水平,相关工作人员在制定网络安全管理制度时需要先做好相应的调研工作,根据该区域的计算机使用情况进行相应管理,从而提高安全检查工作有效性、科学性,除此以外,相关领导人员还需要将其责任与义务进行明确,将运行维护安全管理的责任明确到每

一位工作人员身上,让安全管理工作人员能够以积极认真的态度进行日常工作,将自身责任与义务进行全面落实,从而保证其管理工作整体质量与效率,提高计算机网络安全防范工作整体进度。

#### 3.3 持续强化安全意识

针对目前的实际应用情况,应不断加强我国计算机网络用户的安全防范意识,特别是现阶段我国计算机网络用户覆盖率逐渐提高,老年人使用网络的人数比例明显提高,老年人网络防范安全意识较弱,甚至连最基本的网络保护安全意识也不具备,直接增加了当前计算机网络的各种风险。因此,需要不断加强对手机用户安全意识的教育和推广,合理优化系统,积极宣传,从根本上提高手机用户的安全意识,满足当前需求。例如要求用户自身的密码安全意识提高,在设置密码的过程中提高优化意识,避免过于简单的密码,应保证密码本身具有较强的密码组合性和密码复杂度,在优化密码的过程中,总体上需要确保当密码被破解时难度增加<sup>[4]</sup>。

同时,积极探索培养国际先进网络人才,充分发挥优秀网络人才的综合优势,加强国际网络安全体系建设,从根本上为国际网站用户创造良好的网络环境,该安全人才充分利用网络服务商的技术服务优势,为国际网络的环境安全提供强大的技术支持,优化整个网站网络效果,降低用户计算机网络安全隐患的概率。

结束语:总之,大数据时代背景下,人们的生活方式得到了极大的改变,信息开放与共享也极大地便利了人们的生活。当然网络信息的飞速发展也极大地增加了计算机网络安全隐患对人类带来的威胁与挑战。所以,新时代背景下,人们应该积极地提高自身的计算机网络安全防范意识,相关的部门也应该采取相应的举措,有效地净化网络环境,打击网络非法行为,争取为人们提供一个绿色、干净的网络生活空间。同时,相关的部门也应该积极的宣传,呼吁人们携起手来,共同提高自身的安全防范意识。

#### 参考文献:

- [1]魏忠,李光明,郭盛刚,等.大数据时代下的计算机网络安全及防范对策探讨[J].电脑知识与技术,2021,17(30):68-69.
- [2]李冰枫.大数据时代的计算机网络安全防范措施研究[J].电子技术与软件工程,2021(07):259-260.
- [3]孟华.基于大数据时代的计算机网络安全防范措施研究[J].网络安全技术与应用,2021(01):157-158.
- [4]王国清.大数据时代计算机网络安全防范探讨[J].网络安全技术与应用,2021(4):164-165.