

大数据背景下计算机网络安全问题与防范措施研究

陈晓霞

宁夏理工学院 宁夏 石嘴山 753000

摘要:在互联网时代,通信技术发展速度较快,计算机网络系统全面普及。计算机网络系统不仅自身运行效率高,而且具有较好的可扩展性和共享性。在大数据时代背景下,数据信息高度共享,这也对计算机网络系统的安全性带来了较大的挑战。因此,需要加强对计算机网络安全重视,进一步加强对计算机网络系统安全的有效管控。本文分析了大数据背景下计算机网络安全存在的问题,并进一步针对加强计算机网络安全防范提出了有效措施。

关键词:大数据;计算机网络;安全;防护措施

引言:大数据背景下,计算机网络安全防范的重要性得到进一步的凸显。然而从实际情况来看,网络技术发展日新月异,受多因素的影响,我国计算机网络安全防范工作仍存在诸多问题,从而一定程度上对公众的日常生活、企业的经营发展以及国家的持续建设产生不利影响^[1]。因此,本文在全面分析大数据时代背景下我国计算机网络安全防范现状及问题的基础上,深入探究具体的安全防范实施策略,具有重要的实践意义。

1 大数据的概念及特点分析

随着时代的飞速发展,各类信息与数据以指数级别迅猛增长,对各种数据与信息进行有效收集、分析和挖掘成为当前产业融合发展的重要部分。大数据时代背景下,大数据、云计算、物联网等技术已经应用到人们生活的各个方面,帮助企业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,无限制地获取相应的信息与数据,从而了解到对自身有用的各种讯息^[2]。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,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果。

2 大数据时代计算机网络安全存在的问题

2.1 病毒入侵问题

病毒入侵的方式很多,它往往会隐藏在邮件、二维码、链接甚至图片中,不仅普通人难以防范,甚至一些专业技术人员有时也会防不胜防。病毒的破坏形式是多

种多样的,比如:病毒入侵计算机系统,并在内部传染其他计算机。病毒可能会破坏系统文件,不断复制和派生新的形式,最终可使网络瘫痪。虽然随着计算机病毒防范软件不断升级,病毒入侵的危害相比过去所造成的危害正在逐渐降低,但也绝不能掉以轻心。

2.2 垃圾邮件威胁

垃圾邮件的存在也是威胁大数据时代计算机网络安全的信息安全的因素之一,尤其是最初的爆炸性电子邮件,对计算机网络安全构成了更大的威胁。与病毒感染相比,垃圾邮件不具有传播的特征,与网络黑客相比,垃圾邮件不具有高延迟的特征。但垃圾邮件可以利用电子邮件本身的开放性来渗透并被发送到电子计算机。一般来说,垃圾邮件的总数非常大,并且不断被推送,驱使计算机用户接收垃圾邮件。当打开这种电子邮箱时,计算机网络系统软件将遇到威胁。一旦计算机网络系统软件被禁止,将危及到电子计算机的正常操作,从而导致个人数据的泄露以及对个人信息和安全的威胁。

2.3 网络安全防护工具更新速度慢

大数据环境下,计算机网络系统一旦出现漏洞,信息发生泄露的可能性会增加。当前随着计算机技术和网络技术的发展,病毒类型也更具多样性,病毒危害性增强,传播速度较快,一旦防范不到位,则会出现大量数据和资料被盗取的情况,导致用户资料丢失,严重时还会造成无法估量的经济损失。但当前网络安全防护工具更新速度较慢,而且防护工具的更新存在一定的被动性,往往是病毒蔓延或是大面积用户受到感染的情况下,才会对防护工具进行更新。在防护工具滞后于网络病毒感染速度的情况下,用户的信息安全和经济安全受到严重的威胁。

2.4 计算机自身存在的安全漏洞

虽然我国科学技术在飞速发展,但人们在使用计算

机时不可避免会遇到一些系统的漏洞,或者部分软件的安全隐患也给系统带来的危害。因人们所下载的软件不同以及使用计算机的方式不同,或多或少地会在使用计算机时遇到一些 Bug,就是人们所指的漏洞。计算机系统可以自动修复相应的 Bug,但是在当前科技飞速发展的背景下,许多不法分子会抓住相应的时机,根据计算机系统漏洞,非法侵入用户的计算机,从而窃取相应的信息与数据,同样会给人们的计算机网络安全带来一定的隐患。

3 基于大数据背景的计算机网络安全防范措施分析

3.1 提升用户的计算机安全防范意识

基于大数据时代背景,为了有效地提高计算机网络安全防范效率,就应该注重提升用户对自身对计算机安全防范的意识,国家与相关部门应该积极地宣传,有效地引导人们树立计算机安全防范意识,能够在使用计算机时提高警惕,做好专业性防范。尽可能地减少计算机网络安全对人类经济与生活所带来的威胁。尤其是在网络金钱交易过程中,更应该提高警惕,应该反复确认交易的对象以及交易的渠道,随时保持较高的安全防范意识,避免不必要的经济损失。同时,负责大数据时代背景下计算机网络安全防范的相关组织也应该积极地净化网络环境,严重打击网络上一些非法分子的不正当行为。同时,还应该对大数据背景下网络安全给予高度的关注,及时有效地对计算机网络安全隐患进行处理与控制,积极地优化网络环境,为人们提供一个安全绿色的网络生活环境^[3]。另外,相关部门也应该通过各种方式积极地对计算机网络安全防范的知识进行普及与宣传,引导更多的人掌握相关的安全防范知识以及与计算机网络安全相关的法律知识,积极通过相应的案例引导人们树立较高的防范意识也能够极大的维护人们自身的财产与人身安全,为人们提供一个更加绿色、舒适的网络生活空间,有效地提升大数据时代背景下计算机网络安全防范的效率。

3.2 健全计算机网络安全防范机制

完善健全的防范机制是高效开展网络安全防范工作的重要保证,对网络安全防范效果具有积极的影响。因此,大数据时代背景下,必须要积极健全和完善网络安全防范机制,以此为网络安全防范工作的开展提供有力保障。具体实施过程中应包含以下内容:(1)完善网络使用管理机制。例如:加强对非法网站、异常网站或存有安全风险网站的打击力度;制定详细具体的安全用网条例;加强对移动存储设备安全性的检查;做好重要数据信息备份工作等。(2)完善安全防护责任机制。对于企业或单位而言,针对不同部门、岗位的工作内容和数

据信息重要性,制定针对性的网络安全及数据信息安全防范制度和责任制度,一方面,帮助员工树立网络安全防范意识,提升数据信息安全保护能力;另一方面将具体的网络安全防范责任落实到个人,以此提高安全防范工作的执行力和实效性。

3.3 加快网络安全防护工具更新速度

当前由于在网络信息安全技术引进、研发和推广等方面都存在速度缓慢的问题,导致网络运行过程中受病毒侵袭现象十分严重,这对网络环境的稳定性造成了较大的影响。因此在实际工作中,需要积极更新网络安全防护工具,重视先进防护工具的同时,加大投入力度,提高研发水平,特别是要重视现有病毒防护技术的更新,确保病毒感染和传播被及时发现,从源头上遏制黑客和病毒的入侵。同时,还要打造专业化技术团队,重视病毒预警技术和截取工具的相关研究,这样在网络病毒入侵时,截取工具能够对病毒传播速度和感染范围起到减缓的作用,预警系统也能够及时将病毒情况和传播信息向技术管理部门传输,管理部门要及时启动预定方案,做好网络安全防护工作。

3.4 运用网络加密技术

大数据时代下,互联网数据加密设计方案是密码学在计算机技术行业的运用。密码学作为计算机技术与数学课的边缘学科,伴随着互联网的普及化和运用,愈来愈遭受大家的高度重视。在欧美一些国家,此项技术早已变成电子计算机安全领域的一个关键课题研究。在应用层面,客户能够依据自身的需求挑选不一样的加密方法,完成对数据网络和互联网传输的合理维护^[4]。现阶段,加密方法各种各样,依据密钥的一致性,能够将密码分成基本密码和公钥密码。在信息网络传输全过程中,信息内容传输彼此应用的密钥是同样的,即其数据加密或破译方式是同样的。这类加密方法安全性强,但对密钥的安全性传输有高的规定。比较之下,公钥密码是相关应用不一样的密钥。这类加密方法适用对外开放的网络空间,具备优良的密钥管理方法优点,但与传统式数据加密对比,其数据加密速率较低。从运用的视角看来,将来伴随着密码学技术性的持续发展趋势,它将有更宽阔的发展前途,愈来愈多的互联网客户趋向于将这两种加密方法融合起来,进而尽快完成信息网络的安全性。

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，提高自身的安全防范能力。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。

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

全及防范对策探讨[J].电脑知识与技术,2021,17(30):68-69.

[2]于伟波.大数据时代计算机网络安全问题及防范策略[J].网络安全技术与应用,2021(10):177-179.

[3]黄茂成.大数据时代下计算机网络安全及防护措施[J].电子技术与软件工程,2021(20):258-260.

[4]张国雄,何恩南.大数据时代下计算机网络信息安全问题的探讨与防范[J].珠江水运,2021(17):38-39.