

大数据时代计算机网络安全与防范措施

井 轩 瞿 源

汉江水利水电(集团)有限责任公司网络信息中心 湖北武汉 430040

摘要: 现代计算机网络信息技术的大面积普及和应用,对各领域发展都产生了十分深远的影响,虽然在一定程度上提升了企业运行的效率,但在实际应用中还是有很多需要解决的问题。而这些问题的存在为后期计算机网络信息安全埋下了不小的隐患,不仅会致使用户隐私被泄露,同时还会被不法分子钻空子。现代计算机网络信息技术使用中,经常会出现用户信息泄露以及私人财产被盗取或是转移,还有企业的机密信息泄露等状况,为社会健康稳定发展带来了极大的负面影响,所以进一步提升计算机网络信息的安全性,成为当下我国首先要解决的问题。

关键词: 大数据时代; 网络安全; 解决策略

Computer network security and preventive measures in the era of big data

Xuan Jing, Yuan Qu

Hanjiang Water Resources and Hydropower (Group) Co., Ltd. Network Information Center Wuhan, Hubei 430040

Abstract: The widespread popularity and application of modern computer network information technology has had a profound impact on the development of various fields. Although it has improved the efficiency of enterprise operations to some extent, there are still many problems that need to be solved in practical applications. The existence of these problems has laid hidden dangers for later computer network information security, which can not only lead to the leakage of user privacy, but also be exploited by criminals. In the use of modern computer network information technology, there are often situations such as user information leakage and theft or transfer of personal property, as well as leakage of confidential information of enterprises, which have brought great negative impact on the healthy and stable development of society. Therefore, further improving the security of computer network information has become the first problem that needs to be solved in China at present.

Key words: big data era; Network security; Resolution strategy

计算机网络信息安全存在的隐患主要体现在信息安全方面,大数据技术十分依赖网络,而互联网中存在的漏洞同时也会成为黑客与病毒攻击的重点,致使信息遭受影响,甚至会导致重要信息被恶意删除或是被篡改以及乱码等。遭受破坏的信息有可能会关系到用户隐私以及个人利益,乃至影响到公司企业以及其他方面机密信息,进而形成更大安全隐患。相关工作者一定要及时采取相应计算机网络信息安全防范技术,进而提升计算机网络信息安全。本文则是主要针对在大数据视域下计算机网络信息安全开展论述,并提出有效措施。

一、大数据和计算机网络信息安全概况

(一) 大数据主要内容

所谓大数据其实就是一种海量特征的数据,其中包含极大信息量,同时这些信息内容较为多元化,信息更新速度也非常快,有显著的非结构化特征。另外大数据不仅有着十分庞大的数据体量,类型也比较多,其处理速度也很快。受现代社会飞速发展影响,相关的大数据

研究日渐增多,更是逐渐成为现代企业发展以及人需分析等方面内容进行战略部署的重要参考依据。不过伴随大数据利用不断深化,信息安全问题体现愈加明显,为社会发展与社会大众生活带来很大负面影响,对于现代计算机网络信息安全性造成极大威胁^[1]。

(二) 大数据背景下计算机网络信息安全主要内涵

在大数据发展视域下,现代计算机网络信息安全方面问题越来越受社会大众关注。而在探讨计算机网络信息安全保护之前,则是需要清楚明确以及全面的分析现代计算机网络信息安全。计算机网络信息安全可以从物理安全,还有信息内容安全两个角度开展分析。若想确保计算机网络信息安全的物理安全,则是需要在实际网络工程中,切实针对网络开展设计与规划,同时对计算机网络信息安全中所应用的硬件以及软件设施进行充分考虑。除此之外,在对相应信息安全内容开展综合分析的时候,要注意保护信息安全,防止信息泄露或是出现被非法截取的现象,以此保证用户信息安全^[2]。

二、大数据视域下计算机网络信息安全关键影响因素

(一) 计算机使用不够规范

在现代人们生活以及工作中,计算机已经成为不可替代的重要工具,但在实际使用中,还是存在一定的使用不规范现象,并且很多用户因为自身网络安全意识不足,在实际使用中经常会无意识或是被诱导输入一些十分隐私的信息,像是个人身份证号码,手机的验证码,还有银行卡的密码以及卡号等,通过这种无意识隐私信息暴露,网络上有心之人便会趁虚而入,这些人利用网络技术对用户信息进行窃取,致使用户遭受损失。另外还有些用户因为使用计算机不当,进而致使电脑出现死机情况,导致之前所做的工作全白费了,并且数据丢失之前十分难以恢复^[3]。

(二) 病毒侵袭

在使用计算机的时候,病毒是对计算机网络信息安全造成威胁的重要因素之一。其实病毒也是一种程序,有时会被不法分子利用,从而损害用户利益,对计算机网络信息安全造成不良影响。病毒是一种对计算机网络信息安全具有极大危害的程序,尤其是“特洛伊木马病毒”这类,能够轻松盗取用户各种隐私信息,利用不法措施入侵计算机,进而导致企业受到极大损失。所以,用户在使用计算机的时候,一定要注意规避与防范病毒造成的危害,有效保证计算机网络信息安全^[4]。

(三) 计算机黑客入侵

计算机网络系统设计十分复杂,难免会有一些漏洞,这些隐藏的BUG就会成为黑客进行入侵的关键突破口。黑客也算是现代互联网出现之后应运而生的一种职业,很多黑客会利用网络漏洞盗取用户隐私信息或是企业商业机密。黑客利用在给计算机植入木马程序的方式,获取使用者重要信息,以此达到获利的目的。尤其是针对性盗取机密信息时,会给使用者造成极大的损失。可以说计算机网络信息安全中,黑客的攻击一般都比病毒侵袭更有杀伤力,会极大威胁计算机网络信息安全,致使计算机应用程序以及整体操作系统都出现非常严重安全隐患^[5]。

(四) 计算机数据管理系统存在安全隐患

伴随现代计算机技术高速发展,计算机系统中包含的数据管理系统在实际运行中也逐渐显现出各种问题,并且因为这些问题致使整体数据系统和分级管理理念出现脱离。用户在使用计算机时,因为信息不仅会自动保存到相应数据管理系统里,同时也会自动储存原本就存在的部分重要信息,而这些保存的信息一旦出现泄露,就会致使使用者受到极大的损失。伴随现代信息技术环境与相应计算机网络发展环境两者的飞速更新,用户对于计算机数据管理系统也提出了新的要求与标准,但当先计算机网络信息安全防护措施还不够完善,并不能有效满足用户的实际使用要求^[6]。

(五) 钓鱼网站大量增加

大数据时代发展不仅为社会大众生活工作提供了便利,同时也为不法分子提供了新的犯罪途径,有效不法分子会重点搜集网络用户兴趣爱好以及需求,进而有针对性的为用户推送一些能满足其需求的不法广告,对使用者安全隐私与经济安全造成极大威胁。

三、大数据时代增强计算机网络信息安全有效措施

(一) 提高网络监管水平

现代网络监管工作通常是由政府相关范围与网络信息系统相关管理人员所负责,其应积极主动对网络系统中出现问题进行解决,更全面的对网络信息系统进行监管,避免黑客利用系统BUG攻击系统。不管是个人企业或是私人用户,都应把网络信息安全维护划为关键内容,保证做好平时的网络系统维护,管理者应确保将大数据基础信息特点与安全防范划分为重点防护内容,持续提高网络安全有效管理,适时对管理手段进行调整,主动积极学习相关网络信息安全防护技能,以此满足现代网络信息时代的发展需求,切实提高自身操作水准,满足现代网络技术安全防范基础准则^[7]。

从宏观角度出发,企业负责网络信息安全维护的工作人员要科学合理配置相应网络安全资源,确保建设安全和有效,充分满足现代企业自身发展特色的计算机网络信息安全漏洞防范机制,利用有效防范措施,构建相应计算机网络信息安全防护系统,进而通过系统对网络安全性能进行充分掌握,保证能及时解决计算机系统出现的漏洞与事故,确保最大限度降低网络安全事故给企业与个人造成的损失。管理者一定要保证自身对网络安全实际重要性有足够了解,认真、仔细做好计算机网络信息安全防护工作,不能有投机取巧的心态。另外,要定期针对企业员工实际情况进行网络安全技术宣传,多方位提高企业甚至是个人计算机网络信息安全的防护水准^[8]。

(二) 规范计算机使用方式,增强对个人账户信息的保护

计算机网络信息安全意识是现代所有计算机用户都应具备的意识,在实际使用中,要确保制定完善健全的计算机网络信息安全防护机制,提升安全防范意识。另外个人账户是用户进行网络行为的基础,分为用户名与密码这两部分,用户一定要保障其安全,若是个人账户被不法分子盗用,就会给个人造成非常大的损失。还有就是在使用计算机的时候,要切实加强对邮箱账户与密码,还有通信软件账号与密码以及网银账号与密码等方面内容的重视与保护。在进行密码设置的时候,要最大限度增加密码复杂性,做到经常更改密码,从而减少计算机应用中的风险。若是发现账号存在异常,一定要给予重视并将密码进行更换,对个人账户予以足够保护。

(三) 利用防火墙进行防护

防火墙是一种针对网络接入做出的防护,相比其他防护措施,防火墙是一种从内进行防护的技术,可以有

效阻隔外部用户利用非法措施入侵用户的计算机网络系统,从而对计算机的内部系统进行保护。较好的网络防火墙技术能够持续提升计算机网络运行的稳定性,还能在保证网络交互基础上对相关数据进行检查,进而设定相关程序允许为或是阻断数据传输。当前防火墙的种类比较多,根据不同技术存在的差异性,能够将其分成检测型与代理型等,可以为计算机网络运行予以充分保障。

(四) 利用网络检测和监控防止病毒入侵

近些年发展中,各种计算机病毒侵入情况频繁出现,引起社会广泛关注。而利用入侵检测技术可以持续提高计算机网络系统真实检测水平,保障在病毒进行入侵的时候及时进行阻碍或是切断传输路径,形成完善预警机制,防止安全因素对用户计算机系统产生不良影响,提高计算机网络信息系统的可靠性与安全性。而入侵检测是现代计算机网络系统安全防护中比较常见的一种技术,能够将其分成两方面内容,也就统计分析法与签名分析法。两种方式中,签名分析法主要是针对现代网络安全防护中入侵系统攻击中存在弱点所设计的内容。统计分析法是通过应用统计学有关原理,对计算机网络系统运行是不是安全和稳定进行深入分析,从外部避免病毒入侵。

(五) 增强计算机网络数据系统的安全管理工作

大数据时代发展下,计算机网络信息数据系统的相应安全管理工作十分重要。因为计算机网络数据信息系统存在虚拟性以及开放性特征,再加上很多用户在实际操作中忽视计算机网络信息安全,非常容易致使部分重要信息被损坏或是丢失。所以为有效提高现代计算机网络信息数据系统的可靠性与安全性,一定要持续完善和优化计算机网络信息安全管理方面机制,构建系统并且完善和可行的相应管理制定,做到定期对系统进行升级与维护,保障其安全性,减少计算机网络信息安全问

题发生的几率。另外,在实际操作中,用户要养成正确规范的使用习惯,尽量不要进入存在安全隐患的连接,提升计算机网络信息安全可靠性与安全性。

四、结束语

虽然现代网络信息技术已经十分成熟,相应网络安全防护体系也在不断完善,但依旧有安全问题存在。在现代社会发展中,人们的个人隐私信息和互联网信息存在非常紧密的联系,许多不法分子便会利用网络盗取企业以及个人兴趣,为其带来巨大损失。因此,落实计算机安全防护工作是必需的,要确保全面保证计算机网络信息的安全。

参考文献:

- [1] 曾德胜,何健,宁建飞,欧国成.大数据时代计算机网络信息安全防护策略分析[J].软件,2022,43(09):64-66.
- [2] 洪宝惜.大数据时代计算机网络信息安全及防护策略[J].电子元器件与信息技术,2022,6(08):220-223.
- [3] 解海燕,朱宁静,马嘉琦.大数据时代计算机网络信息安全及防护策略研究[J].科技经济市场,2022(08):22-24.
- [4] 王哲.探讨如何实现大数据时代的计算机网络信息安全[J].现代工业经济和信息化,2022,12(07):125-126.
- [5] 李飞.大数据时代计算机网络信息安全防护策略分析[J].信息系统工程,2022(07):48-51.
- [6] 石剑霖.大数据时代计算机网络信息安全及防护策略研究[J].电子元器件与信息技术,2022,6(07):151-154.
- [7] 黄斌.大数据时代的计算机网络信息安全与防护措施[J].电子技术与软件工程,2022(14):19-22.
- [8] 姚杰,李浩鹏.大数据时代计算机网络信息安全及防护策略[J].电子测试,2022,36(10):118-120.