ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.15, No.36, December. 2019
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964
DOI:10.14004/j.cnki.ckt.2019.4268

探究大数据时代下计算机网络信息安全问题

于龙

(中国人民大学信息学院,北京 100872)

摘要:随着社会的进步,各项信息技术在不断的改革和创新,计算机的应用也逐渐普遍,网络用户数量也不断增加。5G和大数据时代的到来,给用户计算机网络信息增加了更多的流量。因此,保护好计算机网络信息安全至关重要。本文就大数据时代背景下,对计算机网络信息安全存在的问题,计算机网络信息安全的特点进行了详细的介绍,并针对现状,提出了改变现状的有效策略。安全带来了安全隐患,此外,网络信息的安全还严重影响着企业和社会的发展。

关键词:大数据时代;计算机;计算机网络;信息安全;策略

中图分类号:TP393 **文献标识码:**A

文章编号:1009-3044(2019)36-0026-03

开放科学(资源服务)标识码(OSID):

现阶段,社会不断发展和进步,加速了计算机网络的普及和应用。随着计算机网络用户的逐渐增加,也增大了网络的覆盖范围,在大数据时代下,计算机网络能够交互用户和企业产生的所有数据信息,这样不仅有效提升了计算机处理信息的能力,解决传统数据处理中存在的问题,还提高了数据信息的作用和价值。

1 概述

(1) 大数据时代

大数据主要是指一种处理数据信息的新模式,能够随时监控、分析和处理数据信息,能够不断提高数据信息处理的流程优化能力和数据决策能力。大数据技术的出现,在社会发展和企业的进步中具有重要的应用价值。在这种广泛应用大数据技术的时代,挖掘出来很多数据信息前所未有的价值。在大数据时代下,信息的数据量非常大的,因此,在大数据时代拥有海量的信息资产,且需要利用大数据技术对这些存在的数据信息进行有效处理。产生的这些海量数据,不仅数量庞大,还有很多种数据类型,主要包括视频、音频以及图片等,由于数据类型繁多,因此,也相应提高了计算机处理数据信息的能力。此外,产生的数据信息的数据价值的密度很低,随着互联网技术的普及和应用,产生了大量的信息,信息基数较大,但是有价值的信息较少。面对如此海量的数据信息,计算机数据处理能力必须要强才能保证信息的时效性,这一特性也是区分传统数据挖掘和大数据之间差异重要依据。

(2) 计算机网络信息安全

在大数据时代下,有效推动了信息时代和计算机网络计算的创新和发展,在各个领域中也发挥着重要的作用,数据和信息对于各行各业的发展至关重要,因此,保护数据和信息的安全也是非常重要的。企业和用户想要安全保护数据和信息,其中的关键是计算机网络安全技术。我院开设课程中,计算机网络信息安全涉及很多理论知识,包括密码学、网络信息安全、网络管理以及网络安全攻防等课程内容,还涉及防火墙技术、病毒防护技术以及网络安全协议等。在大数据背景下,计算机网络信息安全涉及的领域非常广泛,使用技术复杂,只有综合相关技术,才能在一定程度上有效保证计算机网络的信息安全。

2 计算机网络信息安全特点

计算机网络信息安全主要有规模、隐形、跨境三个主要的特点。首先是规模特点,这个特点是由上网人数决定的,由于我国人口较多,网络用户也比较多,网民总量较大。各个网络用户在计算机网络上的所有操作,最终都会被数据化,又因我国网络用户数量本来就很大,产生大量的网络信息,因此,如何安全保护我国这么大规模的网络信息,一直都是各界关注的重要话题。

其次是隐形,因为网络是一个虚拟的空间,因此网络安全问题的发生也是隐形的。生活中常见的就是木马和病毒两种,它们通常都是由一段代码组成,这些代码是隐形的,看不见也摸不着,但是却能严重危害计算机网络,对计算机网络信息安全保护带来威胁。

最后一个是跨境,随着网络技术的广泛应用,增强了用户和用户之间,企业和用户之间以及国家和国家之间的联系,有效推进了实现网络全球化的进程,同时产生了大量的跨国企业和跨境电商。虽然网络技术的应用促进了社会和经济的发展,但是也给计算机网络信息安全带来了安全隐患。在有效促进国家之间的交流的同时,容易导致跨境的网络信息安全事件。

3 计算机网络信息安全存在的问题

(1) 操作不当

用户在计算机上进行主观的操作才能产生相应的数据信息,这些产生的计算机网络信息需要在特定的操作下才能有效完成信息传输。用户在操作计算机时,主观性很强,通过计算机操作来满足用户的上网需求。虽然我国有很多网络用户,但是由于文化水平的不同,用户对于计算机上网的操作能力不同。有部分用户对计算机网络的操作使用和计算机网络信息技术没有一定的了解,此外,由于用户自身网络安全意识比较薄弱,在操作计算机时,容易因为操作不当带来很多安全隐患。

收稿日期:2019-08-20

(2) 网络诈骗

计算机网络是一个开放自由的虚拟空间,近年来,我国经济在不断发展,逐渐提高了人们的经济收入,会有一些不法分子会在利用计算机网络的特点在网络上散播虚假信息,进行诈骗,给用户信息安全造成威胁,导致用户财产损失严重。

(3) 网络病毒

网络病毒是影响计算机网络信息安全的重要因素之一,具有很强破坏性和传染性,传染的方式多种多样,主要有拷贝数据、网络下载以及在计算机中安装非正规的软件。形式多样的传播方式,扩大了网络病毒的范围,同时,也增强了网络病毒的破坏力。一旦入侵计算机网络系统,将会损坏计算机网络数据信息,破坏计算机系统的正常运行,给用户和企业,甚至是国家重要机构带来巨大的经济损失。

(4) 网络系统自身漏洞

在计算机网络中,安装中大量的网络软件,存在许多的网站,是用户上网必须要进行的操作对象。实际上,这些上网的软件和网页自身是存在一定安全漏洞,有些软件研发人员考虑不全面,导致系统漏洞,或者是开发人员自己为了获取便利,自己开发了软件的后门程序。存留的这些程序如果被黑客发现,极有可能导致黑客入侵,泄露用户信息。此外,这些安全漏洞也有可能被网络病毒识别,破坏计算机网络数据信息和计算机系统,造成计算机瘫痪,严重影响了网络信息安全。

(5) 黑客入侵

在大数据背景下,为黑客入侵提供了便利。通常黑客入侵包括主动入侵和无意识入侵两种,前者是有目的有企图的入侵其他的计算机网络系统,后者通常不会影响计算机的正常使用,但是这两种入侵都会影响计算机网络信息安全。黑客是通过网络服务器、电脑的互联网协议地址或则泄露的用户信息等多种信息通道入侵计算机系统,盗取他人的数据资料,会大规模影响计算机网络信息安全。

4 提高计算机网络信息安全的关键技术

(1) 数据加密技术

在大数据时代下,产生了海量的数据信息,面对这些庞大的重要数据,数据加密技术是保证数据能够有效完整的传输的重要前提。数据加密技术利用相关的技术方法把数据信息转换为密文,通过密文的形式将数据进行传输,传输到目的地以后,再利用数据加密技术的还原技术对数据信息进行解密恢复。通常数据加密技术主要包括私钥和公钥加密两种技术。

第一种是私钥加密技术,也是一种对称的密码编码技术,又叫对称加密算法,这种技术是通过使用同一密钥对数据信息进行加密和解密的,使用的密钥既可以用于加密,也可以用于解密。在网络信息安全学中,数据加密标准算法是这种对称加密算法的一个典型代表。使用这种技术能够加速计算机运算速度,简单快捷,但是算法自身具有繁杂的过程和安全隐患,使用时必须要求密钥安全可靠。

使用的第二种技术是公钥加密技术,这种技术具有私有和公开的两个密钥,且两个密钥是一对。倘若数据加密传输采用了私有密钥,则只能使用对应公开的密钥才能解密数据信息,同样,倘若采用了公开的密钥进行数据信息传输,则只能使用对应的私有密钥才能解密数据信息。这种算法由于使用的加密解密密钥不同而被称为非对称的算法,公开密钥的保密性很好,能够消除用户交换密钥,但是这种技术计算机运算速度太慢,加密解密需要时间太久,只适合加密数据量少的数据传输。计算系统可以根据系统实际情况来选择数据加密技术,或者有效结合两种加密技术,来提高数据加密的效率,加速数据传输。

(2) 防火墙技术

防火墙是用于保障网络信息安全的一种重要手段,通常设置在网络边界上,通过不同类型的网络通信来制定的访问规则。目前对于防火墙的选择和设置,需要注意几个方面。首先是网络地址的转换功能,这是防火墙必须具备的,能够满足所有地址的转换。在对防火墙进行设置时,着重考虑重要的子网的边界,不要被整个网络边界局限。其次是需要对安装以后的防火墙,需要根据网络攻击和网络入侵方式及时完善和更新,这是防火墙设置中最为关键的一个环节,能够防止防火墙出现安全隐患。最后,防火墙的设置需要遵循最小授权原则,高度重视对于防火墙的设置规则和顺序,避免后续安装工作混乱。此外防火墙还记录的功能,能够记录日常网络中的异常访问,这样有利于系统随时监控安全隐患,确保系统的正常运行。

(3) 网络地址转换技术

这种技术是用来转换私有地址和合法地址的,没有代理服务器和防火墙的功能,但是这种技术是通过隐藏内部拓扑结构来实现地址转换的,能够避免内部服务器信息泄露,有效防止外网攻击。通常,实现网络地址转换功能可以利用路由器或者防火墙,实现方式主要是静态和动态两种。静态地址转换的能够把内部地址单独转换成外部地址,适用于为外部提供服务的机器,因为其具有私有地址,使用时需要严格控制网络访问和系统安全。动态的地址转换是比较适合普通计算机的,能够同时把多个内部地址转换为对应的动态外部地址。

5 提高计算机网络信息安全的有效策略

(1) 提高用户安全意识

计算机的普及和应用,给用户带来了便利,在生活中具有重要作用。在大数据时代下,用户的个人信息可能会被盗取、贩卖和非法使用,给用户信息安全带来了巨大威胁。因此,为了避免非法分子盗取贩卖用户信息,用户必须要树立一个安全意识,增强信息保护力度,不可轻信他人,点击别人发的网址链接和软件,不要相信不安全的网站和平台,不可随意把自己的个人信息公开上传,提高安全意识,有效避免自己信息泄露给不法分子提供诈骗勒索的机会,同时避免产生的巨大的经济损失。

(2) 规范操作

在实际的上网操作中,用户应当多了解计算机网络的操作使用,可以自主学习安全操作知识,也可让专业的计算机人员来全面评估计算机系统的操作方式。在评估过程中,如果发现操作不合理的地方,或者是不符合使用的地方,应当及时记录下来,并采取措施进行修改。规范用户的计算机操作,能够有效降低了操作难度,保证了操作的方便简洁的同时提高操作的安全性。

(3) 提高技术水平

大数据时代的到来,推进了信息技术的发展,也给数据信息带来了威胁,在计算机网络安全领域,我们应当充分利用好各项先进信息技术,来完善计算机网络信息安全防护措施。因此,应当时刻关注网络安全的技术水平,利用数据加密技术,在传输过程对数据进行加密处理,等到数据信息传输完成以后再利用解密技术,实现信息安全传输。此外,还需要提高防火墙

技术，防火墙是确保计算机网络信息安全的重要保障，传统的防火墙已经不能安全防护网络系统，需要及时更新和完善。

(4) 建立病毒防护体系

计算机病毒是影响计算机网络信息安全的重要因素，破坏力强、传染力大，因此，需要高度重视计算机网络防护病毒的能力，并采取措施来提高计算机防护能力，尽可能建立一个健全的网络病毒防护体系，以有效降低病毒入侵给计算机网络带来惨重的损失。通常，建立病毒防护体系可以在计算机上设置防火墙、杀毒软件，或者有效结合防火墙和杀毒软件来综合管理计算机网络安全。建立病毒防护体系以后，需要定期检查计算机的使用情况，以确保能够及时发现系统存在问题，方便及时解决。

(5) 防范黑客攻击

除了以上提到的有效策略，维护计算机网络信息安全还需要注意防护黑客的攻击。在大数据背景下，容易出现数据漏洞，导致黑客攻击用户电脑的方式多种多样。因此，在实际的黑客防范过程中，技术人员需要增强黑客防范技术，根据黑客的攻击方式来选择相应的应对策略，在保持科学和实用前提下，建立黑客防范机制。在黑客防范机制实际建立过程中，技术人员需要根据实际情况，采取措施有效记录黑客攻击问题，或者开发程序软件来记录黑客攻击数据，这些记录数据还能作为日后计算机信息安全防护工作开展的重要依据。

(6) 建立计算机网络信息安全制度

俗话说，三分靠技术，七分靠管理，对于整个计算机网络，需要建立一个严格的安全制度，只有这样才能够有效管理计算机网络信息的安全问题。建立安全制度通常需要建立关于信息安全的责任制度，然后再把计算机网络信息按领域进行划分，采用保护数据的方式，来进行整个网络信息的保护。此外，国家监管部门应当增强监管意识，制定一个关于计算机网络信息安全的管理标准和规范，并以此来有效推动相关技术的发展，提高我国网络安全的保障标准。

6 结束语

综上所述，计算机网络的普及和应用为用户和企业带来了诸多便利，在大数据时代背景下，保护计算机网络信息安全显得更加重要。为了防止计算机被病毒入侵，破坏系统文件；防止黑客攻击，盗取用户信息，导致严重的后果。因此，必须要从病毒防护、黑客防范以及用户自身等多个方面入手，以确保计算机网络信息的安全。

参考文献：

[1] 时丽平.基于网络信息安全技术管理的计算机应用[J].电子技术与软件工程,2019(17):191-192.
[2] 吴家存.大数据时代计算机网络安全存在的问题及解决对策[J].黑龙江科学,2019,10(16):138-139.
[3] 谭晓明.计算机网络信息安全工作中虚拟专用网络技术的应用[J].中国新通信,2019,21(8):50-51.
[4] 吴红姣.基于人工智能时代下计算机网络信息安全防护对策探究[J].电子元器件与信息技术,2019(4):71-74.
[5] 色登丹巴.基于信息安全的计算机网络应用[J].电子技术与软件工程,2019(05):197.
[6] 曾宏志.虚拟专用网络技术在计算机网络信息安全中的应用[J].电子技术与软件工程,2019(05):201.
[7] 张黎明,刘燕.大数据时代计算机网络信息安全与防护措施[J].电子技术与软件工程,2019(4):190.
[8] 高玲,钱根生.试析“大数据”时代背景下计算机信息安全[J].中国新通信,2019,21(04):150.
[9] 胡家铭.企业计算机网络安全问题分析及应对方案[D].吉林大学,2014.
[10] 衷奇.计算机网络信息安全及应对策略研究[D].南昌大学,2010.

【通联编辑：唐一东】