大数据时代下的计算机网络安全技术

李俊元

DOI:10.12238/acair.v1i1.5872

[摘要] 随着大数据的发展和应用,数据信息已渗透在社会领域的方方面面,并且人们在日常生活和生产工作中均离不开信息技术的应用。但是如果人们生活、生产中的网络数据信息出现泄漏隐私、丢失重要数据的情况可能会造成严重的安全事故,为此,需借助有关的信息安全技术并将其有效落实,从而保护这些数据信息的安全私密性。因此为了保证计算机网络安全,本文概述了大数据与计算机网络安全,阐述了大数据时代下的计算机网络安全维护意义,对大数据时代下的计算机网络安全技术进行了探讨分析。

[关键词] 大数据; 计算机网络安全; 影响因素; 维护; 意义; 技术
中图分类号: G633.67 **文献标识码:** A

Computer Network Security Technology in the Era of Big Data

Junyuan Li

[Abstract] With the development and application of big data, data information has penetrated into all aspects of society, and people cannot do without the application of information technology in their daily life and production work. However, if there is a leakage of privacy or loss of important data in people's daily life and production, it may cause serious security accidents. Therefore, relevant information security technologies need to be utilized and effectively implemented to protect the security and privacy of these data information. Therefore, in order to ensure computer network security, this article provides an overview of big data and computer network security, elaborates on the significance of computer network security maintenance in the era of big data, and explores and analyzes computer network security technologies in the era of big data.

[Key words] big data; computer network security; influencing factors; maintain; significance; technology

互联网信息技术的快速发展,使得大数据技术已经被广泛应用于人们生产生活中,其可以高效收集和分析大量数据,有效提高了信息管理工作效率。基于此,以下就大数据时代下的计算机网络安全技术进行了探讨分析。

1 大数据与计算机网络安全概述

大数据技术的发展使各类网络信息和数据在实际当中得到有效的应用,而且随着网络数据的发展和进步,和人们的生活生产有着密切的联系。大数据一般是指以海量数据为依托的全新数据处理态度和方法,其主要是运用新技术对数据进行全新的观察和处理,并将结果运用于社会生产生活各部门,从而实现社会价值和经济效益。大数据具有海量性、多样性、高速性、易变等特点。其中海量性指全球的数据量异常庞大,保持逐年增长之势;多样性指多媒体、网络日志等新型数据大量涌现,呈现多结构之势;高速性指数据分析与处理的速度不断提高,流程不断简化;易变性指大数据具有多层级的结构,具有不规则和模糊的特性,会造成分析结果的不确定性。

计算机网络信息安全其实上就是在网络环境各种,利用科

学安全技术保护策略及管理制度,对计算机用户信息安全可靠性进行保证,避免网络信息在传输及存储过程中收到不法分子盗取。基于大数据时代背景中,计算机市场网络具有多样化特点,用户利用多种渠道实现信息的传输及分享,使网络信息安全保护工作难度得到了提高。目前,对计算机网络信息安全影响的主要因素包括人为操作因素、网络系统漏洞和自然因素等。在现代计算机网络中最明显的特点是开放性,在应用中计算机网络系统会受到黑客攻击,对计算机网络安全环境造成了严重的威胁。

2 计算机网络安全的主要影响因素分析

2.1 系统漏洞因素

计算机系统有硬件、软件两个主要组成,硬件上的主要组成有显示器、CPU和硬盘等硬件设备,软件上的主要组成成为操作系统和一些应用软件。虽然长时间以来电脑操作系统都在不断的更新、完善,但其实无论是何种系统,都潜存一定的漏洞,而且基于电脑操作系统功能的越来越强大,所涉及范围越广,随之系统漏洞出现的也就越多,由此给黑客发生攻击行为提供了便利条

件,电脑也易于受到病毒侵袭。

2.2网络黑客攻击

黑客非法入侵是互联网的飞速发展的产物,在信息技术飞速发展发展的今天,黑客已经开发出了更多的入侵模式,在一定程度上造成的伤害是不容忽视的。黑客无孔不入的入侵手段,对信息和网络安全造成了多种不同程度的损害,方法包括但不限于IP地址欺骗,发送电子邮件攻击,网络信息服务攻击,口令攻击,病毒和破坏性攻击,在一定意义上,黑客造成的网络安全问题甚至大于网络病毒攻击所引发的问题。

2.3网络病毒因素

网络病毒就是针对电脑系统予以恶意破坏的程序,其包含木马、脚本、间谍等不同表现形式。当中出现频率最高的莫过于脚本病毒,其具体凭借网络脚本形式介入到用户的电脑系统当中,进一步从中盗取重要信息;而木马病毒则习惯于借助诱惑方式来令用户自行下载,随后在不自觉中盗取用户的重要信息;至于间谍病毒则存在较小的破坏力,经常会在用户连接主页过程中强制性地增加某些网页访问数量。

2.4计算机木马病毒因素

木马病毒使计算机被严重侵害,一部分图谋不轨的“小偷”为了自己的利益,将计算机的相关法律法规于不顾,通过对各种技术的应用,来大范围传播木马病毒,致使我们的计算机随时面临木马病毒侵害的危险,还会引发计算机网络安全问题,对人们的生活与生产工作都是百害无一利的。

2.5网络安全维护意识因素

随着社会经济高速发展,使得计算机网络信息技术被广泛利用,但是通过调查可知,目前计算机网络信息技术的专业技术人员稀缺,充分掌握先进技术水平的高素质人才非常少。这就导致在使用计算机网络时,一大部分人没有按照安全操作习惯和网络安全维护意识。通过调查可知,大部分人应用计算机都是按照自己的习惯去网上冲浪或者娱乐,几乎不会考虑自己电脑上的信息有没有被盗窃,久而久之就会逐渐养成错误的操作习惯。

3 大数据时代下的计算机网络安全维护意义

3.1可以全面提升数据准确性

大数据时代下的计算机网络安全维护能够全面提升数据准确性。基于大数据时代数据信息的收集和整理体现出了广泛性、数据处理方式多样性,而且数据存储空间更大,在这种情况下数据信息的总量更加庞大,面对海量信息要想保证数据库的有效构建,就必须要进一步提升数据信息的准确性。

3.2增强大数据平台服务质量

合理开展计算机网络安全维护能够实现大数据平台服务质量的进一步强化。完整的大数据平台构建需要经历复杂的过程,大数据平台从本质上讲与一个巨型存储器类似,用户可以在平台上自由的搜索和选择所需的数据信息,这也充分体现出了大数据平台的服务性。在当今社会发展过程中,人们通过数据平台来获取信息的频率越来越高,在此情况下对数据

平台存储和计算的功能要求越来越高,如果数据平台不能够为用户提供基本的计算机网络安全,必然会对其服务性能产生极大影响。

3.3整合大数据资源

在大数据时代下,通过对计算机网络安全信息有效维护能够实现数据资源的有效整合。随着大数据时代下的来临,人们在利用和共享数据资源的过程中会产生大量新的数据资源,而这些数据资源信息的获取和获取都是通过计算机网络来实现的,在数据资源交互过程中需要充分依赖于计算机网络安全防护系统来提供基本安全保障。只有在保证数据安全的基础上才能够充分体现出信息数据的有效性,而通过对计算机网络安全进行有效维护能够进一步推动数据信息资源的整合效率提升。

4 大数据时代下的计算机网络安全技术分析

4.1防火墙技术

大数据时代下的计算机网络安全要充分注重对防火墙技术科学的应用,这是保障计算机网络安全必不可少的应用技术。技术应用中主要是发挥着将内网和外网进行隔离的效果,从而就能对内网的运行操作安全得到有效的保护,外网进行入侵的时候就能在防火墙的防护下提高内网的运行安全性能。防火墙是在计算机一级连接的网络间的软件,计算机流入流出的网络通信需要在这一防火墙下进行,所以这对流经网络通信的数据信息的安全就能起到很好的保护作用,能有效将一些攻击进行过滤。防火墙技术的应用中,能关闭使用端口,禁止特定端口流出通讯等,有效的封锁特洛伊木马,以及能够禁止来自特殊站点访问,在防火墙技术的应用下,对保障计算机网络安全起到了积极作用。

4.2扫描技术

大数据时代下的网络安全扫描技术应用是为保证系统管理员对网络中的不足之处及时发现,并且能够依据实际制定对应措施,确保计算机网络系统安全。扫描技术的应用,对于站点、主机操作系统与局域网等漏洞扫描有明显作用,系统管理员可以对系统中影响稳定运行的因素及时排除,而且对主机是否被监听进行有效检查,同时还可以对防火墙的配置安全进行观察。

4.3加密技术

在大数据背景下一些有价值的数据类型正朝着多样性的方向不断发展,这些数据类型同时也是行业发展重要基础,所以在实际工作中需要融入数据加密技术,防止出现信息丢失的现象,在实际工作中需要解决系统边界模糊和消失的问题,通过集体性的防御来提高实际的处理效果。例如可以在系统外部加入防弹护甲,保证安全领域中信息的私密性以及完整性。在新时期下,随着计算机处理能力的不断提高,传统的数据加密技术已经无法满足相关的标准了,所以在实际工作中需要加强对新技术的合理性研究,例如可以融入新型的群组密码技术,支持全系统用户的密码方案,并且为每个用户发送唯一的身份认证信息,根据用户的条件来进行数据解密,提升数据安全管理的效果。在后续

工作中还可以采取访问模型,从而根据加密技术完成角色的加密。近几年随着我国量子技术的不断发展,为了防止在密码应用方面的一些问题,数据加密还融入了抗量子密码,根据网格化的加密方式来提高加密效果,最大程度上保证了数据本身的安全性。

4.4 访问控制技术

访问控制技术属于保障信息安全的主要核心,也是维持系统运行的重要基础,和传统访问控制技术相比,这一技术不仅仅适用于用户身份权限的识别,更能根据用户的请求和需求,从海量数据中提取有效的信息完成信息的权限匹配,做到在保证信息私密性的同时还能够满足相关的标准。在数据访问的过程中,要转变以往传统以人工方式为主的自主性访问控制模式,通过更加大规模的数据库满足实际管理,就需要通过强制性的访问来具备较高的形式化推理和验证能力。理论上而言,需要以大数据访问控制技术作为主要基础,实现主体角色的有效控制,为后续使用和管理提供诸多的便捷。但值得注意的是,在这一技术实际实施的过程中还存在着安全机制灵活度不足的问题,无法实现动态化的授权,因此在新时期下发展这一技术,就需要进行不断的改进以及创新。例如可以设置新的属性访问控制,根据动态化的工作要求来完成整个访问控制模式,满足多样化和动态化的授权标准。特别是对于数据来说需要进行资产价值的有效管理,具备良好的适用空间,从而实现提高安全防护的效果。

4.5 计算机病毒查杀技术

计算机病毒对计算机网络系统的危害不可忽视,其具有严重破坏性,被病毒入侵的计算机网络系统,数据信息和文件信息的安全性能将无法保障,大部分不法分子均是利用病毒来实现对计算机网络系统的控制,篡改数据信息,达成获利的目的。计算机病毒长期潜伏在网络中,用户在浏览网页时,经常会出现弹窗,一旦错误操作点携带病毒的弹窗,病毒将入侵计算机,此时,需要依靠相关安全软件进行全盘查杀(比如360安全卫士或者金山毒霸等),当病毒存在于系统盘时,则需要通过重新安装系统

来消灭病毒,当病毒在硬盘中,可以备份硬盘信息之后,进行格式化操作,同样可以起到消灭病毒的作用。由于病毒的具有较强的潜伏性,在日常使用计算机时需要注重对潜在病毒的预防,尽量避免点开未知链接和网页,保证计算机系统的正常运行。

4.6 入侵检测技术的应用分析

大数据时代下的入侵检验技术能将网络数据资料和相关的使用程序信息的采集工作执行到位,并对计算机中的入侵行为进行分析,高效控制病毒的入侵行为。因此,入侵检验技术是一种极为安全的防范技能,能将计算机系统中不安全的信息实施有效监控。入侵前,检验技术主要有主机系统、历史审核数据等,这种技术的扫描准确性极高,可以对其存在的缺漏进行有效的检验。入侵检验技术分为两种,一种是误用检验,另一种是异常检验。误用检验是将入侵方法作为检验方法,此法速度相对较快,误差也较低,但相对来说检验工作所需时间较长。异常检验是对计算机本身存在的资源量、系统中的非正常行为、非正常现象进行检验,使用过程中一般会耗费较多的时间。

5 结束语

综上所述,互联网技术的普及应用给人们生活以及工作提供了诸多便利,而应用计算机网络技术过程中,也要从多方面加强重视,尤其是安全防护的工作要加强力度。只有保障计算机网络的应用安全,才能真正发挥计算机网络技术的应用价值。大数据时代下的计算机网络安全显得比较重要,但在计算机网络技术应用当中,还存在诸多安全问题。因此为了保障网络安全,必须加强对大数据时代下的计算机网络安全技术进行分析。

[参考文献]

- [1]张维大.浅谈大数据时代背景下的计算机网络安全技术[J].数字技术与应用,2018,36(12):170-171,173.
- [2]刘雨初.大数据时代下加密技术在计算机网络安全中的应用[J].数码世界,2019,(1):183.
- [3]张皓钧.计算机网络安全技术的应用策略[J].电声技术,2022,46(2):59-61.