

大数据下计算机网络安全技术运用阐述

吴宇琪

武汉东湖学院 湖北武汉 430212

摘要: 伴随着科技的发展以及进步,在计算机技术飞速成为时代背景的关键一环的同时,计算机的网络安全也开始逐渐成为了人们所关心的问题。在大数据时代的影响下,各行各业数据整理方面变得更加快捷以及便利,但是,由于网络的原因也让这些数据信息的安全出现了一些问题。在目前为止,主要影响网络信息安全的有两个方面,一方面是由于社会环境因素所引起的信息安全,另一方面是由于网络运行环境方面的不安全因素。本文针对于大数据时代下如何保证计算机网络安全技术的运用进行阐述。

关键词: 大数据时代; 计算机技术; 网络安全技术

Application of Computer Network Security Technology under Big Data

Wu Yuqi

Wuhan Donghu University, Wuhan, Hubei 430212, China

Abstract: With the development and progress of Science and Technology, computer technology has become a key link in the background of the times, the computer network security has gradually become a concern. Under the influence of the big data age, the data collation in all walks of life becomes more convenient and faster. However, because of the network, the security of these data information also has some problems. At present, there are two main factors that affect the network information security, one is the information security caused by the social environment, the other is the insecurity caused by the network operating environment. This paper expounds how to ensure the application of computer network security technology in the era of big data.

Keywords: Big data era; Computer technology; Network security technology

一、大数据时代下计算机网络安全问题分析

除了社会因素,还有的就是一些不法分子对数据产生安全隐患,比如黑客,黑客作为家喻户晓的名词,是现如今网络技术安全主要面对的问题。我们在进行计算机操作,时常会遇到黑客的入侵,黑客的入侵会影响计算机的正常操作以及运行,更甚者会严重威胁到人们的财产安全以及个人隐私信息。近些年来,由黑客所造成的经济损失比比皆是,其主要攻击手段分为节点软件安装以及主动攻击两种类型,一般黑客会有目的性的进行引导以及主动攻击,往往可能是垃圾短信中的一个网站,或者是朋友给你发的一个软件,都容易是病毒,或者恶意软件,造成计算机系统网络瘫痪以及信息的泄露。在大数据时代下,一定要注意好计算机网络安全,避免自己私人信息以及数据的泄露,一旦被不法分子窃取,造成的后果难以想象。

二、大数据时代下的网络安全技术运用

(一) 防火墙技术运用

现今的防火墙按照技术划分主要包括转换型,包过滤型,代理型。而要想更好的保证算机网络信息的安全,计算机用户在选择防火墙时,就应根据计算机本身的系统运行情况,选择差异性的计算机防火墙技术,合适的计算机防火墙技术,可以避免信息泄露的同时,创造一个更加健康的网络运行环境。而要想提高防火墙的安全性,加强其性能,可以选用拓补的方式来升级防火墙系统,。防火墙系统的广泛应用在各个领域的网络信息安全中起到了十分重要的作用,占据了重要的地位。但是伴随着时代的发展,以及网络安全技术的提升,入侵的病毒也开始变得更加多样性,因此,要想注意网络信息的安全,其管理者也应该充分了解现如今入侵病毒的信息以及类别,对外,要进行资源以及信息的整合提高网络信息安全的程度,对

内，要努力升级防火墙系统的能力，提高其智能化。智能化的防火墙系统在自动开展和分析处理工作的同时，还能够通过自行管理来保障用户个人信息的安全。而除了努力升级防火墙系统外，对于系统的日常维护也很重要，防火墙能够保证网络信息安全，有效的拦截病毒，干扰恶意软件的前提是计算机能够正常运行，且有一个良好的网络环境。所以在日常工作过程中，也要让技术人员对于计算机设备进行定期的年检，包括一些硬件以及软件系统的正常运行，在硬件方面要注重其使用寿命以及运行状态，对于软件要及时的进行修复以及查缺补漏，并利用网络技术对其进行实时的监控。除此之外，数据系统的维护也要同时开展，数据系统的维护以及防火墙系统的升级，可以保证安检的效率以及效果，健全计算机网络安全系统，更好的保证网络信息的安全。

（二）完善网络监管体系以及安全意识

在大数据时代的网络安全工作，作为管理人员，一定要具有高水平的技术能力以及高素质的责任心和耐心。因此在进行相关的管理人员的招聘以及培养的过程中，往往要从源头开始抓起，在开始培养之前，将相关的责任意识深入这些管理人员的内心，在招聘的时候，也要对相应的管理人才进行综合素质以及相关技能的培训和考核，可以通过邀请相关的网络安全技术研究的专家对管理人员进行知识水平的提升，帮助他们更好的适应以及解决网络安全技术的相应问题，以达到更好保障网络信息安全的目的以及要求。除了人为技术方面的网络安全问题，也要对于自然因素所带来的网络安全风险进行及时的防范，要让工作人员定期的对于计算机的线路以及相关电路进行维护，对重要的节点进行故障排查，确保在遇到极端天气时，不会对核心计算机产生损害，造成网络崩溃的情况。保证了管理人员的安全意识以及相关部门的监察权利之外，就是要对于网络安全的重要性要进行积极的宣传，可以通过多种形式以及渠道对个人信息以及数据的泄露所造成的严重后果进行演示和警告，帮助人民群众在使用网络的过程中提升自己的安全意识。

（三）完善数据加密技术以及信息保存和找回功能

数据时代的计算机应用技术以及发展的趋近于成熟，在使用计算机时，信息的保存和流通是计算机技术的最常用的功能，所以在网络安全体系的完善过程中，最需要注意的也是这个方面，信息的盗取以及遗失都是现如今所面对重要的网络安全问题之一。完善数据的加密可以保证文

件的安全指数，无论是在保存还是在流通过程中，都可以避免泄露，而信息的保存以及找回，可以帮助将信息封存在自己的计算机中，可以迅速找到所需文件并且在遗失后找回，更好的保护数据信息。数据的保存以及流通，所采用的加密技术其实也是数字签名技术的体现，帮助数据在流通过程中通过各种加密密钥进行加密，确保对信息的保护。除此之外，还可以通过端对端加密的方式来进行数据的加密，通过第三方软件，在发送文件时对其进行加密，将文件中的数据信息加密成密文，然后在接受方接收到信息后，再使用密钥将加密信息进行解密翻译为明文。这些数据加密的方式都是现如今常用的方式，能够帮助一些企业或者个人之间的重要文件的传输以及数据的保存提供多一层的安全保障，即使截获了信息，但是没有密钥依旧无法获知其中内容，更好的保障了网络信息安全，也是现如今十分重要网络安全技术手段。而数据以及信息的保护，除了加密技术，信息的保存以及找回也同样重要，虽然在现如今的时代，大部分的技术人员已经为了防止这个问题的发生进行了信息的自动备份，但是这样也有着许多的弊端，信息的自动备份在面对大量的信息数据时，自动备份会让计算机的内存占据，造成卡顿、死机等情况，消耗计算机的寿命，而除了备份的方式，也有许多的防御软件也为这个问题专门设置了一键找回的功能，但是，在实际应用的过程中仍旧会由于各种限制的原因产生信息的遗失，所以网络安全的保障中，镜像技术的应用可以让计算机出现故障后，让系统继续正常运行，确保信息的保存。

结束语：综上所述，在大数据的时代下，网络信息的安全问题也随之而来，要想确保网络信息的安全，要提高相应的技术人员的安全意识、加强相关部门的配合、完善网络安全的法案，并伴随时代发展，不断更新防火墙技术，数据加密技术，以及信息的保存和找回技术，确保让网络安全的意识深入到每一个人的心中。

参考文献：

- [1] 马晓燕. 基于大数据时代计算机网络安全技术应用探究[J]. 网络安全技术与应用, 2022, (11): 172-174.
- [2] 解晓丽. 大数据环境下计算机网络安全技术的优化策略[J]. 办公自动化, 2022, 27 (21): 25-27+21.
- [3] 王洋. “大数据”背景下计算机信息技术网络安全的应用[J]. 产品可靠性报告, 2022, (09): 70-72.