Engineering Technology and Development, 工程技术与发展 (12)2020,2
ISSN:2661-3506 (Online) 2661-3492(Print)

大数据时代计算机网络安全防范研究

党拴杰
北京鲁电国际电力工程有限公司 北京 100029

摘 要：现阶段，科学技术快速发展，互联网、信息技术、计算机等在人们生活中的应用不断增多，普及率不断提升，信息安全问题也越来越突出，网络安全问题也受到越来越多的关注。文章介绍了大数据时代计算机网络应用的主要安全威胁因素，并探索了大数据时代计算机网络安全技术的有效运营策略。

关键词：大数据；计算机；网络安全技术；运用

一、引言

大数据技术主要指的是通过构建数据平台来针对海量信息数据进行获取，同时经过加工后构建起数据库，在此基础上，用户通过计算机终端就能够从自身需求角度出发来进行数据信息的搜索和选择。大数据平台的出现颠覆了传统的信息获取方式，在大数据技术的支撑下，计算机相关技术迎来了巨大发展机遇，通过大数据的共享性、广泛性能够进一步提升计算机网络的利用效率。

二、大数据时代计算机网络安全维护重要意义

（一）可以全面提升数据准确性

大数据时代下通过对计算机网络安全进行有效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。因此，在数据库构建过程中不仅需要依赖于大数据平台的强大计算能力，而且还需要对计算机网络安全的维护给予高度重视，从根本上实现数据信息处理难度的进一步控制[1]。

（二）强化大数据平台服务质量

通过不断加强计算机网络安全问题能够实现大数据平台服务质量的进一步强化与提升。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[2]。

（三）进一步推动大数据资源整合

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。随着大数据时代的来临，人们在利用和共享数据资源的过程中间会产生大量新的数据资源，而这些数据资源信息的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。

三、计算机网络安全在大数据时代面临的问题

（一）用户网络安全意识有待提高

目前，已有一部分网络用户意识到网络安全的重要性，他们在日常生活和工作中，使用计算机网络时会有意识提高警惕，避免下载一些没有来历的软件，打开来源不明的网页等严重的安全隐患行为；同时用户也会下载各类杀毒软件，借助这些杀毒软件对病毒定期进行排查，进而保证安全网络管理工作能顺利开展，并取得较高的安全防范效果。故此需加强网络用户的安全意识，使网络技术的操作进一步得到规范，让用户的数据信息不致出现泄密的问题。

（二）不可避免的操作系统安全漏洞需进一步完善

计算机操作系统是由水平较高、专业技术较强的程序员有效开发的系统软件，并且计算机操作系统会在计算机开发软件人员的努力下不断完善。但从目前来看，计算机操作系统中仍然不可避免地存在一定的系统漏洞，需工作人员对其进行检测并不断完善和修正。这些操作系统中存在的系统漏洞如果得不到及时的解决和修正，会让整个计算机网络的安全受到严重的威胁。黑客对电脑进行攻击或病毒入侵电脑，都通过对系统漏洞进行捕捉和利用来实现。想要提高操作系统的安全性让其得到有效的保证，还需减少系统漏洞让其得到修正并难以让黑客发现。

（三）计算机网络本身的风险

计算机网络是一个开放的系统，在这其中，计算机网络运行也呈现阶段性特征。在计算机网络系统中，系统稳定性不够，有些部分还是比较脆弱的。此外，在互联网快速发展和应用中，互联网协议安全风险也被暴露出来，这对网络基础设施安全也会造成严重的威胁。在计算机网络系统运行中，可能会出现网络系统运行中数据信息功能问题，导致计算机网络安全问题突出。

（四）计算机病毒威胁

在计算机网络系统建设中，也存在一定的病毒攻击。在计算机网络运行中，计算机病毒是重要的威胁因素，这类病毒一般是一种比较特殊的程序，能够借助相关网络、光盘、移动储存设备等来实现复制和传播，遭受病毒入侵的计算机系统和硬件、软件等都可能被破坏。

目前最早的计算机病毒在 20 世纪 80 年代就出现了，随着相关病毒技术的进一步发展，计算机病毒和计算机网络始终保持着此消彼长的发展态势，不能得到根本性去除。目前，计算机网络建设中出现的各类病毒已经多达成千上万种，且相关的发展速度也在不断增加，随着相关网络化程度发展深入，相关计算机病毒还在进一步加速扩散中，导致病毒的破坏范围和程度都在不断发展。

四、大数据下网络信息安全的防范措施

（一）数据存储方面的防范措施

在大数据量大的环境下，数据的存储安全问题十分重要。现在的存储数据的方式主要是通过本地的存储和现在新出来的云服务的存储，像阿里云就是云服务中的佼佼者。

对于本地的存储，要做的就是预防存储被攻击或者是被窃取，首先说下假设存储的数据被攻击的时候，这个时候数据肯定是不能够再使用的，就算能够使用里面可能也是藏着很多病毒，所以可以选择直接放弃这些数据，那么有人会说那原来的数据怎么办，对于这个早有准备，每天定时去制定一个工作计划，每天凌晨的时候做个自动备份。另一方面，数据可能会被窃取，我们需要在系统上安装杀毒软件，并且我们需要设立防火墙，关闭远程 80 的端口。

对于云服务一般都是第三方的应用，因此要时刻都要做好被泄露的风险。时时刻刻的备份不能少，加上对于云储存的软件需要实时更新，一定要保持最新的版本，每个版本都会有漏洞，但是新的版本一定是最安全的[3]。云服务的管理者也一定要注意加强保护措施，不能外露管理员的密码，管理员的密码一定要时时刻刻进行更新，保证密码的安全性。

（二）发展量子加密技术

为了保障大数据时代下计算机网络的安全性，创新网络安全加密技术是最行之有效的办法。在当今的信息技术领域中，量子加密技术已经被公认是计算机网络安全领域最有效的安全加密技术，量子加密技术目前仍然没有实现实践应用，但人们需要充分认识到在计算机网络安全防护的发展过程中量子加密技术的重要价值，并不断加大对量子加密技术的研究。

（三）强化计算机网络层级保护

强化计算机网络层级保护是当前计算机网络安全最主要的防护措施，但是在大数据时代下，数据资源的共享性日益突出，为了充分保障计算机网络安全，在进一步强化防火墙技术的过程中，也要对计算机网络层级保护进行不断强化。计算机网络之间会存在一定的等级差别，因此可以按照功能、用途的不同来实现计算机网络的有效区分，在此基础上根据计算机网络区域用途的不同来有针对性设置防火墙，实现对计算机网络的网格化管理，这样在全面提升计算机网络安全水平的同时，也能够针对信息数据资源进行有效分流，数据信息的利用率也能得到全面提升。

（四）对用户强化网络安全教育

计算机网络设计的内容较为复杂，在专业岗位从事计算机工作的操作人员实际开展工作前，首先要对其进行专业操作方面的培训，而对普通的网络用户而言，需通过多个渠道向他们强调网络安全防范的重要性，让用户在使用过程中真正认识到计算机网络出现安全问题时，可能对他们造成的损害。如此，才能有效提高网络用户在使用网络计算机过程中的安全意识，使各类安全问题的出现概率得到有效降低。

五、结束语

大数据背景下，计算机网络应用的普及是必然的，这对于促进社会发展进步是大有裨益的。但是，在实际的计算机网络应用中，安全威胁是必然存在的，相关用户要提升计算机网络安全防护意识，做好计算机网络安全技术应用，有效应对风险因素，构建完善的安全防护框架，有效解决计算机网络安全问题。

参考文献：

[1] 刘先荣 . 大数据时代背景下人工智能在计算机网络技术中的应用 [J]. 电子技术与软件工程 , 2018(24):248-249.

[2] 宋鹏 . 试谈大数据时代人工智能在计算机网络技术中的应用 [J]. 电脑编程技巧与维护 , 2018(12):154-155,172.

[3] 梁丰 . 基于大数据时代计算机网络安全防范探讨 [J]. 网络安全技术与应用 , 2020(06):85-87.

通讯作者：党拴杰，1971 年 5 月，陕西渭南人，男，汉族，就职于北京鲁电国际电力工程有限公司，本科。研究方向：计算机及其应用。