大数据视角下的计算机网络信息安全防护

宗满贵[1],霍跃虎[2]
(1.中电科网络安全科技股份有限公司,北京 100043;2.北方自动控制技术研究所,山西 太原 030006)

摘 要:为提升计算机网络信息安全防护的有效性,主要针对大数据视角下的计算机网络信息安全防护进行深入的分析,根据实施计算机网络信息安全防护工作的重要意义,阐述了影响大数据背景下计算机网络信息安全的因素,然后又提出了切实可行的防护措施,以期为相关人员提供参考。

关键词:大数据视角下;计算机网络;信息安全;防护
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1004-7344(2023)42-0142-03

0 引言

由于计算机网络信息环境缺少重要的保障，很容易出现安全问题,导致信息发生泄漏。所以,在大属于时代背景下，单位和工作人员应重点的去解决计算机网络信息安全问题，做好计算机网络信息安全防护这项工作。

1 大数据时代计算机网络信息安全防护的重要意义

在大量的数据信息中，通过大数据技术能找到具有价值意义的信息，而大数据技术属于是先进的技术媒介。而大数据还具有非常多的特征,一方面,大数据具有非常丰富的信息数据。在社会经济水平不断提高和科学技术发展下，社会和商业的发展离不开数据和信息。为提高所有数据和信息准确性,确保更加可靠,应具备选择信息和数据能力。另一方面,丰富的信息数据。这主要在通信模式中应用,其这种方法区别于现有的技术。如果涉及非常多的数据,运用大数据技术在对信息选择的过程中,有时会遇到问题。所以,在大数据视角下，提升计算机网络信息安全性已经成为主要的一项任务。而不管是在处理信息,还是应用数据时,利用计算机技术不仅能实现数据处理，还能提升处理的水平。但不管是在工作中,还是在生活中,计算机信息很有可能出现安全问题,导致信息被盗取,致使给公司的运营造成影响。

2 影响大数据背景下计算机网络信息安全的因素

2.1 自然因素

往往由多个电子器件共同组合而成计算机，对外部环境非常的敏感,所以,在利用计算机网络系统的期间很有可能受各种因素的影响，尤其是温度和湿度等自然因素。若是自然因素成为影响计算机网络的最主要一个因素,当降温防湿处理的力度不够,那么这很有可能出现计算机网络信息安全问题。

2.2 人为因素

在应用计算机网络这一期间，如果受人为因素的影响发生操作失误的现象，那么很容易出现计算机网络安全问题,导致发生安全隐患。一般提及的人为因素涉及两个方面,一方面是主动影响方面,另一方面是被动影响方面。其中,主动影响就是对网络系统,不同的影响方法所采取的攻击措施，而被动影响就是利用各种影响方式来攻击网络系统的安全。被动因素就是在不给网络系统安全性造成影响的同时来攻击其中一个数据库,但无论那种方法很有可能发生信息泄漏。

2.3 操作错误

往往应在用户正确操作下，实现计算机网络各种功能,而在具体操作时,有的用户受主观意识的影响容易发生网络安全问题,存在安全隐患。但不管是利用的操作技术,还是安全防护理念,由于用户之间所应用的不同,所以,导致网络操作和密码设定存在差异,这种情况,可能会发生操作错误的现象。

2.4 恶意攻击

恶意攻击就是不法分子主动的去攻击，或者是被动的攻击。主动攻击就是不法分子主动的攻击某一个对象。被动攻击就是不法分子在计算机网络运行期间对网络采取攻击的行为,以得到自己需要的信息。这些进攻的方法会出现计算机网络信息安全问题，还会给企业造成影响。

通过分析计算机网络信息防护存在问题得知,由于一些计算机所利用的协议以 TCP/IP 协议为主，其安全性不高,所以,很有可能受黑客的攻击。一般在这个

视角上看到由于大数据服务器集中的存储数据，导致信息数据多，也很有可能受黑客的攻击，导致个人信息被篡改。在这种情况下，如果计算机网络信息发生丢失，或者是遭到泄漏，那么不仅会出现计算机网络安全问题，也会影响到各个领域的发展。

2.5 病毒侵入

计算机病毒不仅具有一定的隐蔽性，还有很强的传播性，所以，会在媒体中附着以实现传播，导致影响到整个网络系统的运行。其中不管是光盘，还是硬盘，作为病毒的主要载体，会附着在流动数据中，进一步的扩散整个网络系统运行。一般病毒所扩散产生危害非常的严重，会导致系统不能够运行，致使损坏到各类系统的数据信息，数据发生丢失的现象。

3 大数据视角下的计算机网络信息安全防护措施

3.1 合理利用身份证认证技术

随着大数据技术不断的发展，用户信息在网络环境中存在主要是利用一种特定的数据形式，这样若是计算机在对操作者身份进行识别的过程中，可通过特定的数据向用户授权。应用身份认证技术，通过相关的指令，一定程度上，能初步的认定操作者合法性，以实现对网络信息安全防护第一线的构建。尤其是指纹识别技术和面部识别技术等身份认证技术[1]。而对于静态密码和动态口令身份认证技术而言主要以信息秘密方法为主。一般在身份认证识别的这一期间，计算机网络系统能校队操作人员所提交的信息，而这主要根据的是密钥程序，再赋予操作者一系列的权限，尤其是登录访问和文件查看等，以对用户的行为进行监管，并实时的记录，进而提升计算机网络信息安全性。

3.2 注重对防火墙技术

为做好计算机网络信息安全防护工作，提升信息安全性，有必要建立防火墙，因为这非常的重要。其中，网络数据信息最大的一个特点就是多样性，而在利用计算机期间，有的用户由于对网络信息安全防范意识不高，也没有了解到下载软件时很有能存在潜在病毒，导致增加计算机网络信息安全问题发生概率。特别是在进一步的扩大无线网范围下，不管是在那个领域中有非常多的传输数据，所以，为提升用户信息安全性，为其提供重要的保障，工作人员应注重对防火墙技术的应用，以加强计算机信息管理，这样如果计算机网络系统内存在隐藏的安全隐患，防火墙能够及时的发现[2]。基于此，为有效的落实计算机网络信息安全防护工作，提高这项工作实施的有效性，工作人员应从现有的计算机网络信息安全防护体系入手，并不断的优化，再对防火墙技术充分的应用，引入安全检测技术作为重要的辅助，进而就能甄别出恶意的信息。

就当前的情况来看，有时会发生木马侵入电脑对其他人员信息盗取的现象，所以，在对防火墙进行构建的过程中，应尽快的处理病毒，并且在计算机网络安全防护系统中，还应以定期的方式为主进行防火墙升级，在结合当前的状况，为实现网络信息安全防护合理的制订计划，以便日后提升计算机网络信息安全性[3]。与此同时，在运用防火墙的过程中，可引入网络检测技术，其中在检测计算机软件和硬件时，可对检测软件直接的点击，检测是否有文件垃圾，这样在计算机网络信息系统运行时，如果遭到黑客的入侵，能够及时的发现。此外，可把漏洞修复程序合理的应用在计算机网络系统中，实现对修复网络系统的构建，以保障计算机网络信息的安全。

3.3 建立健全的信息安全管理制度

在大数据视角下，为做好计算机网络信息安全防护工作，提高这项工作的有效性，除了要加强信息安全管理外，还应合理的制定信息安全管理制度。详细的来讲，应做好以下方面。首先，在应用计算机系统时，工作人员应高度的重视计算机网络信息安全防护工作，并对计算机网络信息安全防护知识给予充分的了解，熟练的去掌握，而在具体操作的过程中，不仅要结合实际情况，还应严格的按照执行的标准。其次，应存储好计算机网络信息数据，利用安全检测软件和杀毒软件，合理的去筛选处理各类传输数据信息，而且在筛选的过程中，如果发现有的数据信息安全隐患大，应及时的删除，在保存好关键而重要的信息，进而实现计算机网络安全防护，使其取得良好的防护效果；最后，应用动态监测系统，实现对计算机网络信息系统实时监控，把计算机信息系统方式合理的在智能化的信息平台中去展示，减少人为因素给计算机网络信息安全性造成的影响，确保计算机网络信息系统能正常的使用，处于良好的运行状态。

3.4 设置安全权限和做好加密处理

随着大数据不断的发展，经过对网络信息安全权限合理的设置，再加上对加密处理技术的应用，不仅能促使计算机网络信息安全防护工作顺利的实施，还能提升其有效性。一般在利用计算机时，用户应设置好安全权限。特别是非常重要的信息必须要采取有效的措施做好加密处理，避免不法分子在计算机系统中的侵入，导致个人信息被盗取[4]。通常可应用 ID 认证技术对

安全权限合理的进行设置，让这项技术所起到的作用得到最大发挥，促使用户只能对一个 ID 设置，以提升计算机网络数据管理水平。

一般让计算机用户把账号密码合理设置好。因为有时用户由于忘记账号密码发生丢失账号的现象。其中，在进行账号防护期间，应根据不同的账号对各种密码进行设置，并设置出稍微有点难度密码，避免账号被盗，提升账号密码安全性，避免密码发生泄漏的现象，以提高计算机网络信息防护有效性。与此同时，应以不定期的方式为主去更换密码，因为这样不仅能保护好账号，还能确保网络信息安全。基于此，在大数据视角下，为能有效的落实计算机网络防护措施，提高这项工作的有效性，应设置好账号密码，因为这是最主要的方式。例如，随着企业不断发展，在设置 ID 的过程中，员工的 ID 和管理人员的 ID 会导致存在差异，这在对 ID 地址输入时，员工不能得到企业发展中重要的机密信息，促使计算机网络信息系统安全的运行。与此同时，把数字加密处理工作落实到实处，提高关键数据信息准确性。尤其是重要的文件信息，更应进行数字加密处理，这样在对数字输入的过程中，能得到一些文件信息。所以，在大数据视角下，对数据传输权限设置，在进行加密处理工作，采取数字加密的方法，实现数据实时传输，达到计算机网络信息安全防护目的。

3.5 及时进行病毒查杀

随着大数据技术不断的发展，呈现出具有较高的信息融合度这一特点，所以，这向计算机网络信息安全性提出了相应的要求。而对计算机网络系统，运用安全杀毒软件功能不定期的去杀毒，有助于提升计算机网络信息安全性。特别是在科学技术取得进步下，在对数据信息传输这一期间，计算机信息系统很有可能出现

病毒会影响计算机信息系统的运行。在大数据视角上，为提升计算机安全防护的有效性，防止网络遭受到病毒的入侵，计算机网络用户对计算机网络系统，运用杀毒软件定期的去杀毒[5]。其中，在运用杀毒软件的过程中，应去扫描各个网络系统中的软件和硬件，这样一旦有病毒文件，能做到发现及时。这时网络用户在根据杀毒软件中的一些步骤进行杀毒处理，把这项工作落实到实处，进而不仅能把病毒消除掉，还能达到对网络系统内的漏洞修复目的，提高病毒的防御能力。除此之外，应在线去升级现有的一些杀毒软件，并定期的对病毒库进行更新，把计算机网络信息保护好，确保计算机网络系统安全的运行，处于良好的运行状态。

例如，应用 360 安全卫士杀毒软件，借助云安全技术平台，连接用户的客户端，再对计算机信息系统进行检测，检测该系统的安全程度。在运用杀毒软件对计算机系统进行清理，能发现计算机系统内是否有病毒，并对杀毒，避免遭受到不法分子的侵入。

3.6 实现实时监控

就当前计算机信息网络系统运行的情况来看，有时还有给安全造成威胁的因素，而这些因素也会导致出现计算机网络信息安全问题。特别是当前的计算机网路应用范围已经变得更加广泛下，呈现出计算机入侵问题。基于此，在大数据视角下，为提升计算机网络信息系统安全性，有必要去实时监控计算机网络信息系统的运行，并引进入侵技术，通过其应用对计算机网络信息系统内存在潜在安全问题做出相应分析。一般入侵检测技术有两种，一种是统计分析法，另一种是代表分析法。统计分析法就是预判计算机网络信息安全的运动模式，代表分析法就是在系统运行期间，根据了解的数据信息把存在问题找到，在实现实时监控，以提升计算机网络信息安全防护水平。

4 结语

总而言之，在大数据时代背景下，网络信息安全防护是最主要问题。为有效的落实计算机网络信息安全防护工作，提升防护工作的水平，除了要实现网络信息安全数据分析外，还应进行风险评估，把这项工作落实到实处，在引进防范技术，实现对安全防范系统的建立，确保大数据平台更加安全，提升计算机网络信息安全性。

参考文献

[1] 郑秀毅.大数据背景下的计算机网络信息安全问题及防护措施[J].网络安全技术与应用，2022(8)：161-162.

[2] 韩艳.大数据视角下计算机网络信息安全防护路径[J].网络安全技术与应用，2022(1)：55-56.

[3] 杨佳兰.基于大数据环境下的计算机网络信息安全与防护策略研究[J].南方农机，2021，52(23)：132-134.

[4] 杨玉娣.大数据背景下的计算机网络信息安全及防护[J].信息记录材料，2021，22(8)：80-82.

[5] 董毅，汪安祺.大数据环境下的计算机网络信息安全防护对策[J].信息记录材料，2021，22(6)：22-23.

作者简介：宗满贵(1981—)，男，汉族，河北张家口人，本科，工程师，研究方向为计算机科学与技术。

霍跃虎(1979—)，男，汉族，山西晋中人，本科，高级工程师，研究方向为计算机科学与技术。