大数据背景下的计算机网络信息安全问题及防护措施

杜永聚
洛阳中硅高科技有限公司　河南　洛阳　471000

摘　要：为了有效地确保计算机网络信息技术的安全应用，保障计算机用户网络的信息安全，避免给个人或企业造成严重的经济损失，就必须要结合实际情况，分析现阶段计算机网络技术应用存在的安全隐患，并提出相应的安全防护措施，以保障计算机网络的可持续发展。本文对大数据背景下的计算机网络信息安全问题及防护措施进行探讨。

关键词：大数据时代；计算机；网络信息安全；防护措施

1 大数据背景下的计算机网络信息安全概述

大数据时代背景的到来，对于计算机网络的使用，确实会造成很大影响，除了会为计算机网络提供发展机会外，也会引发一系列的安全风险和隐患，因此当下必须做好防护措施，应对、消除计算机网络信息安全问题，为用户提供更加安全的使用保障。准确来说大数据就是计算机网络运行过程中，所产生的各类信息数据，例如人们在日常生活中，可以随时获取满足工作需求的信息内容，不过在信息分享或传递的过程中，却隐藏大量的安全问题，可能会盗取用户的个人信息以及重要数据，所以需要加强计算机网络信息安全防护工作，以此来避免造成严重的损失。虽然计算机网络的使用，与安全风险问题是并存的，但为了避免不法分子窃取相关信息数据，用户可以通过安全防护措施进行实时保护，这样就能降低安全风险的发生概率，从而确保信息传输与分享的安全性[1]。

2 大数据背景下计算机网络信息防护的要求

2.1 安全性要求

可分两类：计算机系统和硬件的安全性要求，计算机所处网络环境的安全性要求。因此，计算机网络信息相关管理人员，就必须要结合计算机网络信息应用的实际情况，针对以上两个安全性要求进行网络信息的安全防护。可定期排查计算机系统和硬件的性能，定期对计算机网络的安全性进行检测，排除计算机网络使用过程中存在的安全漏洞，确保网络信息应用的安全性。

2.2 完整性要求

确保网络信息的完整性是最基础也是最重要的要求，如果该完整性遭到了破坏，就会导致信息泄露、篡改、丢失等问题，不仅给网络信息安全应用造成了严重威胁，甚至会导致个人或企业产生严重的经济损失。此类完整性破坏主要由于计算机系统硬件问题以及计算机网络信息外部攻击等因素引起的，必须要加强对于计算机网络信息安全防护技术的研究和应用，以促进计算机网络信息防护水平的提升，确保计算机用户网络信息的完整性。

2.3 保密性要求

计算机网络信息资源的共享以及相应计算机网络技术的应用也使得网络信息的保密性有所下降。导致数据保密性问题出现的因素有两个：一是由于计算机用户个人的不合理使用导致网络信息的泄露；二是由于计算机网络信息遭到了黑客的恶意攻击。因此，在计算机网络信息应用的过程中，必须要加强对于计算机网络信息保密性的安全防护[2]。

3 大数据时代计算机网络信息存在的安全问题

3.1 黑客入侵

大数据时代黑客入侵多元化的趋势，几乎成了计算机网络信息防护过程中的共识，一旦相关单位缺乏对黑客入侵的有效防控，那么将会难以通过各类防护手段的有效聚合，满足计算机网络信息安全防护的基本需求。其次，传统情境下计算机网络中的病毒入侵形式，从互联网的数据存储使用至今，已经经历了数十年的变革，相关单位必须重视此领域的网络信息安全防护研究，以便利用更为优秀的安全防护措施，满足大数据背景下各单位对信息安全防护的基本需求。黑客入侵的信息安全防护，首先需要针对黑客入侵的形式布设基本的信息防护屏障，并在防漏信息安全防护屏障的应用中，整合具备信息安全保护价值的技术手段。其次，黑客入侵的基本形式大多以数据窃取、数据破坏的方式进行，是一种基于数据算法的网络攻击形式，只有控制黑客入侵在信息调取过程中的可控范围，才能降低以数据破坏、数据窃取两种主要入侵方式的网络攻击所产生的影响。

3.2 人为操作失误问题

如今，除了黑客入侵会对计算机网络信息安全产生影响外，人为操作问题也会对计算机平台中的数据信息

产生破坏，大数据背景下的计算机网络信息安全隐患问题，其中不少来自于人员操作层面，人为操作失误不仅会对计算机的防护功能产生影响，还会使得计算机平台中存储的数据信息收到不可逆的损害。不仅如此，进入大数据时代，计算机网络下数据信息的应用场景及应用方向都发生了变化，从数据信息的使用功能上看，通过数据信息的统计与估算，可通过数据信息的整合构建相关的预测方向，计算机身为数据信息的存储平台，人为的数据信息录入操作失误，以及人为的数据信息传输失误，都会对计算机网络信息的安全产生复杂影响。可见，人为操作失误对计算机网络信息安全带来的影响大多体现在以下方面：人为的操作失误使得计算机网络数据信息的信息存储模式发生了变化，进而削弱计算机网络信息存储平台的核心防护功能，使其无法通过一级、二级、多级防护手段的构建，成为一种以网络信息数据防护、数据传输为核心功能的数据集成设备[3]。

3.3 计算机网络管理制度问题

计算机网络管理制度的创设，有利于利用标准化的网络防护流程，探索全面化、一体化的网络信息安全防护措施。然而，大数据时代中，相关单位无法基于自身的数据信息使用场景，进行各类数据信息的统筹与保护，这将会增加计算机网络信息安全的应用风险，无法在计算机的现实应用层面、计算机的信息安全管理层面、计算机的信息安全的防护层面进行优化及创新，此种制度问题，给现有的计算机网络信息安全防护手段带来了使用权限上的风险。此外，计算机网络管理制度缺失所造成的信息安全隐患形式，主要为数据流信息，最经典的问题为现有的管理模式，难于适用于大数据时代下的网络安全管理标准，进而当计算机网络信息面临安全风险时，无法按照数据信息流的基本存储方式进行有效的调控。可见，计算机网络管理制度中现存问题的解决，需要通过计算机网络信息数据的基本存储算法，进行计算机信息存储应用的管理革新，并针对相关企业的发展领域进行二次的数据信息防护，做好数据信息的整理任务外，避免黑客入侵、计算机网络管理制度不够规范，所造成的数据信息流失。可见，计算机网络管理制度的缺失，从计算机网络信息的转化角度来说，难于通过精确的数据信息算法，辅助进行计算机网络防护屏障的构建，最终增加相关单位的计算机网络信息防护成本。

4 大数据时代加强计算机网络信息安全防护措施

4.1 合理应用杀毒软件，加强监管工作

大数据时代除了要在监管工作中进行安全防护措施的优化外，还应结合不同应用属性的杀毒软件，推出较为全面的数据信息防护屏障，在以上两项内容的优化与整合中，发力探索网络信息安全防护的具体措施。不过，杀毒软件的信息防护模式与通用的信息数据防护模式略有不同，但两者的应用目的及出发点都是为了满足相关单位，对特定网络信息数据内容的防护需求，这是伴随网络病毒侵害的演变而发展出来的必要防护手段。其次，在应用杀毒软件的初期防护阶段，相关单位应着重探索垂直化的网络信息安全防护措施，以便在大数据时代探索不同网络信息防护措施的基本应用方向，简化传统防护措施的应用标准，并结合杀毒软件的功能支撑，降低计算机网络信息的存储与应用过程中，受到各类病毒侵害的问题发生。此外，大数据时代计算机平台的数据存储率较高，从计算机的数据存储数据来看，用以大数据分析的网络信息使用率现已占据极高的比重，而随着相关单位对计算机平台端的数据信息安全的应用要求提高，相关人员必须通过监管工作的革新，以及杀毒软件的数据安全保护使用，降低病毒侵害与网络安全防护手段之间的差距，构建完整的数据信息存储链条的同时，使相关单位应用的数据加密方法得到保护。

4.2 优化防火墙的应用技术

防火墙技术作为大数据背景下各企业单位进行信息安全防护的一个组成部分，其参数配置是否具备防护弹性，关系着各单位的利益，牵动着单位发展的同时，更会影响各单位的经济收益。因而，相关人员在应用大数据进行数据分析时，还需要关注数据信息的安全度，通过防火墙应用技术的优化，降低网络数据被非法盗取、计算机上存储的数据信息遭受破坏等问题的发生。其次，相关单位还应根据检测型防火墙技术与地质转换型防火墙技术的防护水平差异，实施相关的防护条例，解决计算机网络安全防护制度缺失的问题。同时，一些网络恶意攻击，通常需要借助数据包窃取相关单位计算机网络中的信息数据资源，这不仅影响了相关单位的数据资源利益，还损害了相关单位所存储的数据资源。因而，为了降低此类恶性事件的发生，相关人员应根据检测型防火墙的故障处理依据，进行一系列的访问控制，使检测型防火墙技术能够根据网络节点的变化，构建良性的数据信息防护屏障，降低网络恶意攻击对计算机网络信息安全的扰乱，使计算机网络系统具备体系化的防护措施。

4.3 加大有关人员的教育和培训的力度

负责网络信息安全的人员，其作为促进相关单位计算机网络信息安全发展，以及网络信息安全防护措施落实的关键组成，相关单位应对安全防护人员的素质水平

加以考核，并通过安全培训等一系列的措施，为安全防护人员的技术水平发展提供帮助。同时，相关单位还应在管理措施方面制定具备长期培养意义的方针，以此提高安全防护人员的理论实践水平，使其具备优秀的网络信息安全防护知识，并在安全防护工作中提高安全防护措施落实的规范性、系统性。可见，针对安全防护人员加以必要的教育和培训，在提高计算机网络信息安全层面，具有长期的发展意义，只有在素质培训及技能考核中降低人员素质与企业网络信息安全防护发展的矛盾关系，才能筑牢各单位的网络信息安全防护防线，使企业单位的计算机网络信息安全在集中化的技能培训中得到规范。可见，大数据背景下各企业单位的网络信息安全防护水平的增强，需要以安全防护人员的素质考核及技能培训为主，坚持安全防护理论及实践的培训为原则，使相关人员的技能专业性得到相应的提升[4]。

4.4 构建完善的计算机网络管理制度，提高网络管理安全水平

大数据背景下维护各单位信息数据安全最为重要的要点内容是，强调计算机网络应用与管理的技术标准，坚持可靠性与安全性的数据信息防护原则，以大数据背景下的数据分析及数据整理为方向，使计算机网络管理制度脱离形式化，使其具备一定指导性的同时，采取多样化的网络数据信息安全防护标准，作用于企业单位的良性发展。可见，计算机网络管理制度作为各单位维护数据信息安全的一种管理形式，需要管理制度既要具备一定的安全防护指导意义，不得与网络信息数据安全防护及管理存储的宗旨相互背离，还要使其能够对各单位岗位成员的网络应用意识起到一定的规范作用，使各岗位的人员无论处于何种岗位层级，都能具备一定的安全防护意识。此外，结合数据认证防护措施，各企业单位可在管理制度的完善中，对企业网络系统中的数据访问次数加以限制，并通过数字认证技术的数据包访问约束，可解决企业单位信息数据的泄露、窃取、传输问题的发生。

4.5 做好安全权限设置工作

针对计算机网络的使用安全，可以设置相关权限以此来形成加密效果，这对于企业单位的使用来说，会有较高的安全系数，能够确保在大数据背景下，传输、共享文件的安全性，避免出现数据信息丢失等问题。在实际工作中必须针对重要的数据信息进行加密，这样就能预防陌生人读取、获取信息内容，另外要结合企业与个人的需求，设置相关的安全权限，这样也能预防操作期间出现数据信息丢失问题。目前在计算机网络使用过程中，可以通过ID安全权限进行有效防护，这样就能提高使用过程中的安全管理，并且还能为信息访问、查询等工作提供便利，所以相关企业单位应该重视ID安全权限的应用[5]。

结束语

大数据背景下网络恶意攻击的形式多样，其借助数据包进行网络安全访问的基本攻击形式，使得相关单位的网络信息数据安全难于得到保障，这不仅会对计算机的防护功能产生影响，还会使得计算机平台中存储的数据信息收到不可逆的损害。因而，相关单位需要基于自身的数据信息使用场景，进行各类数据信息的统筹与保护，以便降低计算机网络信息安全的应用风险。此外，大数据时代除了要在监管工作中进行安全防护措施的优化外，还应结合不同应用属性的杀毒软件，推出较为全面的数据信息防护屏障。最后，防火墙技术作为大数据背景下各企业单位进行信息安全防护的一个组成部分，其参数配置是否具备防护弹性，关系着各单位的利益，牵动着单位发展。

参考文献

[1]胡中尧.大数据时代背景下计算机网络信息安全与防护[J].通讯世界,2019,26(01):39-40.

[2]廖兰芳,李耀鹏.大数据时代计算机网络信息安全与防护方法[J].电子测试,2019(09):130-131.

[3]何潇.计算机网络信息安全与防护措施在大数据背景下的实施策略[J].艺术科技,2019,32(07):284-285.

[4]武变霞,王会芳.大数据背景下计算机网络信息安全风险及防护措施[J].漯河职业技术学院学报,2019,18(04):20-22.

[5]焦景云.大数据背景下的计算机网络信息安全及防护措施探索[J].信息通信,2019(11):141-142.