Engineering Technology and Development, 工程技术与发展 (17)2022,4
ISSN:2661-3506 (Online) 2661-3492(Print)

大数据时代下计算机网络安全防范的研究

韦焯思
广东培正学院　广东省　广州市　510830

摘　要：随着互联网技术的发展和普及计算机用户越来越多，目前，我国计算计技术的发展速度备受各界关注，尤其是在大数据背景下，给社会各个行业带来了很大的经济效益，促进了社会生产力的发展。与此同时，对于网络数据不能有效地规避，就无法将数据的应用价值发挥到最大化，也将面临着许多新问题，比如数据信息被窃取、遭受网络黑客的攻击也会带来较大的安全问题。基本于此，本文就以数据安全体系、防范木马病毒、网络安全分析了大数据背景下如何最大程度地保障计算机网络安全。

关键词：大数据时代下；计算机网络；安全防范；策略

Research on Computer Network Security in the Era of Big Data

Wei blanching
Guangdong Peizheng College, Guangzhou City, Guangdong Province 510830

Abstract: With the development of Internet technology and the popularization of more and more computer users, at present, the development speed of China's computing technology has attracted attention from all walks of life, especially in the background of big data, to the social industry has brought great economic benefits, promote the development of social productivity. At the same time, if the network data can not be effectively avoided, the application value of the data cannot be maximized, and it will also face many new problems, such as data information theft, network hackers attack will also bring great security problems. This paper analyzed how to maximize computer network security under the background of big data with the data security system, Trojan virus prevention and network security.

Keywords: Big Data Era; Computer Network; Security Precautions

1 大数据概述

大数据指的是计算机中存储的海量数据,具有数据多样化以及查找数据便捷的特点。大数据主要依据云计算,通过对数据的全面感知，保存与共享构建一个数字世界,而使资源的获取方式发生一定程度的改变。大数据时代的到来虽渲染出一片欣欣向荣之感, 但其中不乏存在安全隐患, 网络犯罪现象层出不穷。因此，也不能忽视对于网络安全问题的防范，应采取积极的防范措施,将网络安全问题扼杀在摇篮之中,让网络犯罪无处遁形，从而使人们的切实利益得到保障。

2 大数据时代背景下计算机网络安全存在的问题分析

2.1 计算机使用者安全防范意识薄弱

就目前来看，很多单位、机构和个人还没有深刻认识到大数据对计算机网络安全带来的不良影响，因而在工作、生活、学习的过程中还没有养成良好的计算机网络安全防范意识，直接导致计算机网络安全防范无法取得实实在在的成效。有的单位对计算机网络安全防范工作表面说起来挺重视，但在实际中就和说的不一样了，特别是不注重强化自身数据、信息、资源的有效保护，导致出现了很多问题，甚至造成了重大损失[1]。

2.2 计算机系统中存在的安全问题

计算机网络系统在长期使用下本身即存在着一定的漏洞,计算机操作系统的类型不同，就可能出现不同的故障，进而不能够正常地运行。计算机和操作系统之间存在的兼容性问题可能导致计算机所存储的信息和数据出现丢失或者损坏的情况。对于网络系统而言,没有任何一套系统是完美无瑕的,这是不可避免的。所以网络系统本身也会具有一些漏洞,进而导致安全事故的发生,另外,用户在使用网络程序以及软硬件的过程中,因为人为因素而产生的安全问题也不在少数,甚至一度成为造成网络安全事故发生的重要原因,给不法分子以可乘之机[2]。

2.3 病毒入侵引发的安全问题

病毒入侵的方式很多,它往往会隐藏在邮件、二维码、链接甚至图片中，不仅一般人难以防范，甚至一些专业技术人员有时也会防不胜防。病毒的破坏形式是多种多样的，如：

病毒入侵计算机系统，并在内部传染其他计算机。病毒可会破坏系统文件,不断复制和派生新的形式,最终使网络瘫痪。虽然随着计算机病毒防范软件不断升级，病毒入侵的危害相比过去所造成的危害正在逐渐降低，但也绝不能掉以轻心。

3 大数据时代背景下计算机网络安全防范的策略

3.1 健全计算机网络安全管理法律制度

网络安全问题层出不穷,与制度未落实有着极为密切的关系。对此,我们需要意识到当前网络安全问题的严重性，参考国外先进的立法经验，结合我国的国情，对网络隐私权保护法和互联网安全法等法律法规加以补充和完善，对构成侵权行为和蓄意破坏网络环境稳定的人员严惩不贷，从而维护法律的权威性。立法时需坚持防范为主，从根源上遏制问题的发生，让人们逐步树立起正确的网络安全观，共同维护计算机网络环境安全。

3.2 增强用户的安全防护意识

要想切实做好大数据时代计算机网络安全防范工作，首先要提高计算机网络安全防范意识,只有这样才能在开展计算机网络安全防范的过程中实现更大的突破。当前，很多用户不注重对个人信息的保护，当部分软件需要访问用户信息时，都不仔细阅读协议，直接就选同意，这样就会造成个人相关信息的泄露，黑客就可以利用这些信息进行不法交易，从而造成个人利益损失。因此，首先，一定要建立完善的个人信息保护机制，充分认识网络存在的各种信息安全隐患。其次，不要随意浏览恶意网页等，随意浏览恶意网页会使病毒有机可乘，造成计算机网络信息被破坏和丢失，直接影响用户利益；最后，要加大对计算机网络信息安全的宣传力度，使用户了解更多网络信息安全知识，从而提高他们的网络信息安全意识，严格控制自己的网络言行，从而最大限度降低网络信息安全问题带来的损失。

3.3 提升计算机网络安全防范技术

网络信息技术的发展使得网络安全风险的传播途径、传播形式、危害方式呈现出多元化发展的趋势，导致计算机网络安全防范的难度显著提升，因此，必须要加强安全防范技术的创新力度，确保技术水平的先进性和科学性，这样才能有效应对各类网络安全风险，最大限度地提升安全防范能力，确保网络数据信息及运行环境的安全性与稳定性。大数据时代背景下，要想提升网络安全技术水平可以从以下两个层面入手：第一，加强大数据技术的应用。一方面，利用大数据技术强大的数据采集和分析能力，对当前网络安全风险的类型、特征、传播渠道、危害原理、爆发特点等信息进行全面、深入的分析，并将分析结果上传至网络安全防火墙数据库中，从而大幅度提升防火墙对各类网络安全风险的识别和拦截能力，显著提升网络安全防范效果；另一方面，参考、借鉴大数据技术中先进的计算机算法，如 RSA加密算法、聚类算法等，将其渗透、融合到不同的网络安全防范技术中，以此提高防范技术的科学性、严谨性以及先进性，大幅度增强防范技术对网络安全风险的处理能力， 达到提升网络安全防范能力的目的。第二，注重前沿科技的融合与应用。例如：将人工智能、神经网络系统、专家系统、生物识别等智慧技术与传统的网络安全防范技术进行深度融合，以此全面提升安全防范技术的智能化、智慧化水平，使其具备网络入侵智能检测和防御、网络防火墙自主学习及更新、网络风险智能分类及防御决策制定等先进功能，从而更加高效、全面、准确地防范和处理网络安全风险，切实提升网络安全防范能力[3]。

3.4 合理使用网络安全防护软件

大数据环境下，人们在网络上获取信息的途径日益多样化，但不排除这些渠道可能携带着一些病毒，对计算机网络系统的安全造成极大的威胁。无论是计算机个人用户还是企业，在网络系统运行过程中，一方面要启用防火墙，网络防火墙既可以过滤掉不安全的服务及非法用户，又可以限制且控制用户对特殊站点的访问；另一方面要选用安全可靠性高的杀毒软件，定期对网络系统进行扫描排查，及时发现并清除可疑程序。除此以外，还可以利用网络入侵检测技术实时接收网络数据流，通过与入侵特征数据库作比较，进而判定是否为非法入侵的数据包，一旦确定便启动防火墙系统将其过滤掉。

3.5 加大网络监管力度

政府相关部门和网络信息系统管理人员要加强对网络安全的日常监管工作， 积极排查网络系统中存在的各类漏洞，清除监管死角，防止不法分子利用系统漏洞发起攻击。无论是管理人员还是普通用户，都应当加强重视网络安全问题，做好网络系统的日常维护和管理工作。管理人员应当充分了解大数据的基本特征和安全防范要点，针对性加强网络安全管理，调整管理策略，积极学习相关的安全防范技能，不断更新安全防范手段，紧跟网络信息发展潮流，提升自身技术水平，适应大数据背景下网络安全防范的具体需求。大型企业和机构的网络管理人员还要注意从宏观角度出发，对网络安全资源进行合理配置，建设切实有效，符合企业、单位具体特点的网络安全防范机制，通过强有力的网络安全防范技术措施，建立网络安全信息平台，通过平台实时掌控网络系统中的安全动向，及时发现安全漏洞和安全事故，尽可能减少安全事故对企业、单位造成的损失。管理人员必须充分认识到网络安全防范工作的重要意义认真做好定期安全检查和维护，不可存在侥幸心理[4]。

结束语

总而言之，在现今的网络环境中,人们对于网络环境的安全性越来越重视，如何适应大数据时代，加强和改进计算

机网络安全防范工作，是各个领域和各个层面必须高度重视的重大问题。对此，我们应深刻认识到加强和改进大数据时代计算机网络安全防范工作的极端重要性，运用创新理念和系统思维，破解大数据时代计算机网络安全防范工作存在的突出问题，提高计算机网络安全防范意识、优化计算机网络安全防范技术、推动大数据时代计算机网络安全防范取得更大突破。

参考文献

[1]黄茂成.大数据时代下计算机网络安全及防护措施[J].电子技术与软件工程,2021(20):258-260.

[2]张元喆.大数据时代计算机网络安全及防范的策略分析[J].网络安全技术与应用,2021(9):167-168.

[3]王国清.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,2021(04):164-165.

[4]常振中.大数据时代下的计算机网络安全与防范策略分析[J].科技风,2021(08):100-101.