ISSN: 2661-3719(Print); 2661-3727(Online)

大数据时代的计算机网络安全及防范措施

贾银河
中国铁路北京局集团有限公司　北京　100000

摘　要：在大数据时代的背景下，计算机网络系统应用越来越广泛，Internet上的数据量也呈几何级数增长，因此做好网络保护变得越来越重要。基于大数据时代的计算机网络安全问题，文章对如何有效保护网络信息安全进行了分析和研究，重点对网络教学过程中防范计算机网络信息安全的措施进行了探讨，以促进大数据时代网络信息安全技术的优化与发展。

关键词：大数据时代；计算机网络；安全；防范

引言：

在信息时代下，计算机网络技术获得繁荣发展，但计算机网络技术在为社会大众生活、工作提供便捷的同时，亦为社会大众的信息资料造成诸多安全隐患。一直以来，网络都有着较强的开放性与虚拟性特点，网民用户于虚拟空间当中展开沟通与交流，这在较大限度上会提高网络犯罪现象出现的可能性。而大数据技术作为信息时代不断发展的必然产物，大数据环境下的计算机网络安全现已成为社会各界广泛关注的热点话题，如何加强计算机网络信息技术的安全性，已成为当前亟待解决的现实问题。

一、大数据与计算机网络安全相关概述

正确、恰当地应用大数据技术，可有效优化当今社会生产及管理环境，切实提升数据信息收集能力和共享效率，促进数据实现多元化发展。简言之，大数据技术即融合社会生活中的所有数据信息，集聚了大量信息内容。而所谓大数据，实际上便是借助运用特定的高科技设备展开信息收集和管理，并且数据库中囊括了各个领域的信息数据，具有超强的数据处理水平，可以解决数据信息使用和管理过程当中产生的各类问题，可以转变现阶段社会大众的管理模式，以数据库为依托实施一切生产与管理工作，有效提升数据使用及管理的质量和效率。基于现如今国家社会生产的发展现状而言，目前大数据技术发展和应用已融入社会生活的各个角落，且无时无刻不在对社会生产及国民生活造成重大影响。然而，大数据技术作为新兴技术，对于大数据技术的监管无法避免地会出现诸多问题与不足，而这些因素便会对社会大众信息安全带来消极影响。所以，强化信息安全与计算机网络安全的管理具有必要性。

二、大数据时代下计算机网络安全问题

1.由安全意识不足所引发的网络安全问题

在大数据时代背景下，网络平台中的各种信息数据都有着一定的关联性，从而引发出了一系列的网络安全问题。有部分网络用户对于信息安全方面的防范意识较为薄弱，经常会将不同网站的用户密码设置成同一个，并且用户权限开放较高，再加上开放了远程访问等多个权限，让网络黑客有了可乘之机，导致安全隐患问题层出不穷，用户自身的数据信息与个人财产也会受到较大的损失[1]。

2.计算机漏洞

所谓计算机漏洞，指的是计算机存在的内在问题，这一问题对计算机网络安全而言有着十分重要的有影响。众所周知，计算机系统具体由软件设备、相关协议与硬件设备等元素构成，然而不管是软硬件设备，还是相关协议都会出现一定漏洞，而这漏洞便是我们常说的Bug。诚然，计算机系统Bug是普遍存在的问题，往往表现出随机性与不规律性等特点，所以其是否会造成计算机网络安全隐患具有不确定性。但是，如果这些Bug被某些不法分子与黑客等群体发现并进行利用，则会成为破坏计算机网络安全的突破口，从而成为不法分子盗取数据信息乃至控制计算机系统的直接通道。尽管近些年来伴随计算机系统和运行程序的不断更新与完善，诸多Bug通过相应补丁进行了有效修补，但多数Bug仍难以修复，更甚至在修复后会出现其他Bug。

3.用户安全意识较差以及不正确操作

大数据时代下，计算机网络是一个复杂的生态系统，每个个人用户、企业用户或政府用户都是这个庞大的计算机网络生态系统构成元素。并且，这些用户只有更好地参与利用互联网，才能发挥其价值，才能让计算机网络资源更丰富，构建更有利于推动经济发展、社会进步

作者简介：贾银河，1979.9.20，汉，男，山西，中国铁路北京局集团有限公司，科员，高级工程师，本科，网络安全、信息化建设，邮箱：jiayinhe@163.com。

的计算机网络新业态。用户和企业用户由于技术问题，可能会出现不当，造成一系列的计算机网络安全问题，影响个人计算机信息保护企业信息和财产保护，甚至给整个计算机网络带来重大的冲击。个人安全意识较差，没有更强的网络安全管理观念，对个人信息的保护力度不够，对企业财产和重要信息的保护不当，网络安全保护技术等级较低，都会给更多黑客以可乘之机，被植入木马，受到各种网络病毒的感染。一些个人用户没有安装杀毒软件和防火墙，整个电脑都在互联网上裸奔；一些企业虽然安装了杀毒软件和防火墙，不能及时更新病毒库，或防火墙安全等级较低，不能更好地起到防护作用。

另外，用户在使用过程中由于操作不当，会造成网络安全隐患。特别是缺乏必要的风险规避意识，在使用过程中将个人的信息泄露出去，安装来自互联网没有安全保障的娱乐软件，这些软件安装会将信息泄露出去。企业或单位在安全管理方面缺乏更可靠、更完善的管理制度，个人随意进入机房数据中心，并且将个人存储工具带入，会让公司或单位的计算机数据中心系统感染病毒，甚至给一些木马安装提供了路径，造成信息泄露，引发更严重的安全问题[2]。用户在使用互联网过程中浏览一些不安全的网站，下载一些没有安全保障的数据，或者打开不安全邮件，都会让病毒入侵或木马植入，带来重大的安全隐患，甚至间接充当了一些病毒或木马传播者，不仅影响个人的网络安全，也给整个系统带来非常大的隐患和危害。

三、大数据时代下计算机网络安全防范措施

1.加强网络管理，确保网络信息的稳定运行

网络管理作为一种自主防御的方式，能够有效提高网络系统的安全等级。首先利用网络操作系统、应用软件系统等定期更新的方式来确保软件运行环境的安全性，若是不及时更新，系统漏洞则无法得到有效修复，容易引发木马病毒展开一系列的恶性攻击行为。其次可以利用安全防护软件的帮助来提高整个信息系统的安全性，通常会选择安装防火墙、安全管家等防护性软件，对于不被信任的数据、网站和软件做好过滤工作，通过提高网络信息数据之间的互通性，从而避免出现网络内部互相进行恶意攻击的行为。通过网络信息管理能够提高网络系统的安全性，并为其运行发展提供保障。

2.加强计算机网络安全立法工作

大数据时代背景下，科技进步日新月异，大数据的应用给计算机网络和信息技术发挥提供了更好的保障，网络对人类社会经济发展的影响力越来越突出，在社会经济发展中的地位举足轻重，充分保证网络安全刻不容缓，是各国都在强化的重要问题。依法加强计算机网络安全是最为可靠的保障，通过立法来强化网络计算机安全，加大对计算机网络安全危害的惩处力度。注重计算机网络数据安全保护工作，依法对计算机网络信息进行保护，构筑起更加可靠的信息安全保护体系。突出强调法律的权威性，保证法律的执行力，确保个人信息安全、网络稳定，对各种利用计算机网络进行违法活动的人形成强大的威慑力。

同时，进一步加强计算机网络信息安全的监管力度。互联网发展非常迅速，我国计算机和网络建设也在不断加快进度，5G建设全面铺开，在信息化高速公路上的追赶速度越来越快，甚至处于领先地位。要在未来的互联网应用方面进一步保持优势和较强的竞争力，必须做好网络安全保障工作，进一步强化网络监管。对接入互联网的个人和企业等进一步加大管理，强化技术培训和网络道德宣传，注重法制教育和引导，确保所有接入互联网的个人和企业都能够严格遵守国家信息安全法律，保证互联网的信息稳定和安全。并且组织安排关人员定期对网络运行进行监督和检测，发现可疑问题及时进行制止和处理，确保计算机信息网络稳定和网络信息安全，将监管和法律惩处以及网络安保有机统一起来，以此来确保计算机网络安全[3]。

3.加强对平台管理人员的培训

向负责平台的管理人员提供特殊的技术培训。专业的网络安全维护人员属于专业技能型人才，应具备扎实的网络安全知识基础，上岗前应有对应的培训。培训内容应包括数据通信网络安全维护知识，以提高其综合专业素质。此外，应改进注册管理系统。对于某些设备的维护，应进行注册工作以确保系统配置、技术参数、管理和维护以及维护系统的数据性能处于最佳状态。

四、结束语

综上所述，在大数据时代背景下，信息的采集、运用等都发生了较大的转变，且网络安全问题层出不穷，针对这种情况需要对网络安全风险的发生类型、规律等进行详细分析，并制定出相应的防控措施。只有不断提高用户自身的防范意识、软件安全性，构建完善的网络环境监管机制，才能够提高大数据时代背景下计算机网络安全防范水平，从而不断优化网络监管模式。

参考文献：

[1]戴辉.计算机网络信息安全中防火墙技术的应用探究[J].信息与电脑（理论版），2020，32（1）：227-228，231.

[2]杜博杰，钟慧茹，葛运伟.计算机网络信息安全中防火墙技术的有效运用分析[J].中国新通信，2020，22（1）：154-155.

[3]刘永辉.计算机网络安全中的防火墙技术研究[J].科学技术创新，2020（1）：78-79.