基于大数据时代下计算机网络安全思路及对策

孙忠民　赵　刚　范吟雪　郭明建
内蒙古兴安盟大数据中心　内蒙古兴安盟乌兰浩特　137400

摘　要：最近几年，我国信息通信行业发展十分快速，计算机网络安全受到了各行各业的关注。目前，在大数据兴起的背景下，计算机网络安全在面临传统安全问题的同时，也面临着许多新问题，比如数据信息被窃取、遭受网络黑客的攻击、大数据网络安全管理制度欠缺、安全监督力度较差等。基于此，本文就以大数据时代为背景，对计算机网络安全进行深入研究，针对其问题制定相应防范措施。

关键词：大数据时代；计算机；网络安全；防范措施

Ideas and countermeasures of computer network security in the era of big data

Zhongmin Sun　Gang Zhao　Yinxue Fan　Mingjian Guo
Inner Mongolia Xing’an League Big Data Center Inner Mongolia Xing’an League Ulanhot 137400

Abstract: In recent years, the development of the information communication industry is very fast, and computer network security is attracted attention from all walks of life. At present, under the background of the rise of big data, computer network security is facing many new problems as well as traditional security problems. For example, data information is stolen, attacked by network hackers, lack of big data network security management system, poor security supervision, and so on. Based on this, this paper takes the era of big data as the background, conducts an in-depth study of computer network security, and develops corresponding preventive measures for its problems.

Keywords: The era of big data; Computer; Network security; Preventive measures

引言

随着经济的发展和技术的进步，人们的生活越来越离不开计算机技术。计算机在改变行业发展规律的时候也改变了人们的生活习惯，由此社会进入了大数据时代。在大数据时代，人们很容易就能查到来自世界各地的信息，只要想知道就会有途径。这种对于信息搜集发现的能力导致了人们对于信息的获取变得容易。在大家进行信息搜集和相互交流的时候，每个人都会在大数据中形成自己的痕迹，这就有可能发生隐私暴露。在人们还没有反应过来的时候，不法分子已经盯住了大数据时代这一特点，将信息技术应用到盗取他人信息的方面，将人们的信息非法提取并从事对用户不利的行为。面对信息技术带来的便捷与风险，每个人都要树立一定的风险防范意识，从而保护自身的隐私和财产安全。

一、大数据技术与计算机网络安全概述

大数据主要是指在计算机网络中存在着庞大的数据信息资源，这些数据的类型特征也存在较大差异，因此需要计算机拥有强大的数据信息处理能力，为了提高计算机的数据传输与处理效率，云计算、云存储等技术应运而生，并且成了计算机数据传输处理的核心。大数据改变了人们获取资源的方式，以往人们获取资源需要通过有线网络、无线网络等技术设备，而在大数据背景下人们可以通过计算机、无线智能终端等快速获取自己所需的信息资源。大数据具有数量庞大、资源丰富、处理效率高等显著优势，因此成了信息领域的关键技术，在全球范围内广泛应用。但是在实际应用中，由于其需要依托计算机网络来实现强大的数据功能，因此给计算机网络系统带来了一定程度的网络安全风险，尤其是近年来计算机网络信息安全问题频频发生，如何采取有效措施保障计算机网络安全成了社会关注的焦点[1]。

二、大数据时代计算机网络安全的意义

在信息迅速传递的大数据时代，计算机网络安全直接关系到个人利益和社会经济发展以及社会效益。计算机网络资源的开发有利于社会经济发展，能够有效提高计算机应用技术带来的经济效益，同时，为人们的生活带来便利，促进社会的发展与进步。因此，为了保障计算机网络安全技术的发展，相关部门和人员必须深入对计算机信息安全问题的认识，要不断加强对计算机网络的监管，对其中出现的漏洞和问题，及时进行分析和解决。因此，加强大数据时代计算机网络安全保障有利于保障个人利益，促进社会经济发展。

三、大数据时代计算机网络安全存在的问题

3.1. 信息数据泄露

互联网的快速发展使得人们的生活非常方便的同时，也存在较多的风险。大数据背景下，计算机正常、稳定的运行具有很大的发展空间，科技的快速发展，关于互联网的劣质产品也层出不穷，如果计算机软件性能不够优质，用户的信息就会泄露，很大程度上增加了计算机的风险[2]。2019 年，兴安盟突泉县太平乡财政所在网站上发布名为《东升村 2017、2018 年草原生态保护补助奖励项目资金发放公示表》的通告。一次公布了 243 名公民完整的身份证号码，存在公民完整身份证号码泄露问题。

3.2. 网络系统自身安全问题

计算机网络系统具有较大的特性，自身就存在着一定安全隐患，例如 Windows、Linux 等系统自身就存在着一定缺陷，而这些安全风险是没办法进行完全规避，并且计算机系统还容易遭遇硬件危险，例如用户在进行软件下载和安装时就会很容易导致其安全性受到威胁，增大计算机网络安全隐患出现的概率。从理论上而言，自身缺陷所带来安全隐患问题较为容易解决，但如果由于用户应用计算机网络技术进行软件下载和安装时出现安全隐患问题，并且在出现安全问题时遭受到外来入侵，如病毒，黑客，就会导致其数据安全性和保密性大幅度下降，导致用户信息出现泄露。兴安盟电子政务外网信息系统和行署网站信息系统自投入运行以来，两个信息系统近年来多次遭受黑客攻击并存在网上“挖矿”行为。全盟已开展等级备案的 131 个重要信息系统所属部门普遍都存在网络安全意识淡薄、网络安全经费投入不足、安全防护应急处置能力低等问题，据统计，仅 2021 年就发生 16 起网络事故。

3.3. 计算机病毒升级，危害越来越大

随着信息技术的发展和人们技术的提升，越来越多的计算机病毒被制造出来，成为计算机网络安全的隐患。通常，在计算机的使用过程中，虽然适用性非常广泛，但其实存在一些兼容性和缺陷问题，这些问题增加了网络安全风险。同时，虽然计算机网络已经普及到了各家各户，但是操作人员的水平层次不齐，不规范的操作行为也会让计算机在使用过程中产生缺陷，从而破坏计算机的正常运行，这也为一些计算机病毒和不法分子的入侵提供了机会。此外，计算机系统是一种非常严格的编程系统，一旦遭受到来自外界的病毒入侵就会失去操作功能，降低使用的安全性。而病毒也随着计算机系统的升级越来越难清理和察觉。所以，经常会出现一些具有极大破坏性的病毒出现在计算机网络中。这些病毒会让用户的计算机在无形中受到感染、防不胜防。这些病毒最厉害也是最可怕的地方在于，一旦出现病毒感染，就有可能失去计算机中保存的重要信息，甚至破坏原有的计算机系统。这些病毒严重降低了计算机网络安全系数，成为计算机网络安全中重大安全隐患[3]。

四、大数据时代计算机网络安全防范措施

4.1. 建立完善的数据信息安全体系

为了保证数据能够有效执行，保障其安全性能，应构建一个以大数据为背景的数据信息安全体系，以更好地保证数据执行。通过对计算机的数据信息作加密处理，通过对数据信息在传递过程的安全性和高效性进行保障可以提高数据存储过程中出现问题的概率，降低数据的安全隐患，避免不法分子通过对计算机网络的攻击来盗取电脑中的机密文件等，可以将计算机网络的安全性能进行极大地提高，更好地保证网络具备较强的安全性。

4.2. 加强防火墙以及安全检测系统的应用

相关工作人员要想提高计算机安全防护水平，需要建立并完善相应管理体系，从根源上加强计算机网络安全管理工作水平，在大数据背景下，一些恶意软件和新型病毒层出不穷，这对于计算机网络安全造成较大威胁，因此相关人员在日常应用计算机时需要采用相应的安全检测技术以及防火墙对恶意信息进行阻挡，避免恶意信息在计算机网络中通行和传输，其中防火墙技术主要是通过拓扑结构方式对恶意信息进行阻隔，从而提高计算机自身网络防护安全度，在一些大型公共和企业网络环境中防火墙技术应用较为广泛，能够大幅度提高信息传输安全管理工作，通常情况下，工作人员可以将其分为内部管理和外部管理，其中内部管理的安全性较高，因此大众进行信息储存时，要是在内部管理系统中运行，防火墙就能够对内外管理系统进行相应检验，从而将其中安全隐患进行消除，提高计算机自身的防范水平，避免数据信息受到病毒攻击，导致数据信息出现泄露情况。除此以外，由于如今计算机病毒发展较为迅猛，因此相关工作人员要想避免计算机遭受到病毒的攻击，就必须根据各类病毒特点以及原理进行相应防护，提高计算机安全检测技术水平，从根源上对其进行保护。[4]。

4.3. 增强日常检测

随着信息技术的快速发展，信息的泄露变得更加容易和平常。为了预防信息的泄露、保障用户的信息安全，用户可以在使用计算机的时候进行日常的检测，及时了解计算机的状态，为计算机构建良好的运行环境。对于现有的防火墙系统来说，只有在有非法用户入侵的时候才会启动抵御机制。而在计算机的日常使用中，保持良好的检测习惯，能够减少计算机感染病毒的风险和弥补现有计算机的薄弱环节。同时，在日常监测中，计算机往往能够识别过去出现过的风险，并且进行标记。在这些风险点出现的时候，如果防火墙每次都需要启动，就会影响用户的体验，将任何危险标记为特大风险并进行拦截，这对于用户来说很有可能会错过一些重要的事情，于是，在进行日常监测时，就可以让计算机对以往存在的病毒风险进行识别，就像骚扰电话标记一样，只要同样的风险出现，就要进行拦截。如果新出现的风险没有到达这个级别或者危险系数不强就可以不予处理，这样

一来，用户在使用计算机的时候就会顺畅很多，大大提高了用户的体验。这也就相当于为计算机构建了一个病毒风险库，让计算机在运行的过程中与这个库中的风险进行对比，只有符合了某些风险库中的标准才可以判断是非法入侵。

4.4. 积极引入加密技术，保障信息安全

在大数据的时代背景下，为了提高网络信息存储与传输过程中的安全性，应积极引入数据加密等新技术，有效保障网络信息安全。数据加密技术主要是指对需要进行存储和传输的数据信息先进行加密处理，形成密文形式的网络信息，以密文的形式在网络上进行存储和传输，这种技术的优点在于一方面防止网络信息在传输过程中的丢失破坏等安全风险，另一方面，有效防止了网络黑客的恶意攻击或窃取等。通过使用数据加密技术，网络不法分子难以对数据信息进行截取，也无法对这些数据信息进行破译，从而有效保障了网络信息安全。

五、结束语

综上所述，在大数据时代，网络信息资源的获取方式和途径都产生了转变，网络安全问题逐渐增多并趋于复杂化，需要对这些问题提高重视，并对问题产生的原因与影响因素展开深入分析，采取相应的解决措施。在新的发展时期，企业或个人应提高网络安全风险防范意识，加强计算机网络安全管理，引入数据加密等新技术，规范网络行为，保障网络信息安全，从而不断提升计算机网络安全管理水平。

参考文献：

[1] 黄祖健 . 计算机网络安全防御策略及技术研究 [J]. 网络安全技术与应用，2021（10）：173-174.

[2] 周晓晶 . 大数据环境下计算机网络安全研究 [J]. 中国科技信息，2021（19）：46-47.

[3] 戴昀，居巍杰 . 大数据背景下的计算机网络安全研究 [J]. 信息记录材料，2021，22（10）：42-43.

[4] 丁永波 . 大数据人工智能时代下网络安全的实践研究 [J]. 电脑知识与技术，2021，17（26）：30-31.