试谈大数据时代的计算机网络安全及防范措施

陈严杰
中国电信股份有限公司遵义分公司　贵州遵义　563000

摘　要：如今我国计算机技术得到了大幅度提升，越来越多的企业逐渐开始利用大数据技术进行日常管理，但是由于计算机网络特殊性，相关工作人员在进行数据传输管理过程中很容易遭受网络安全威胁，导致数据出现漏丢情况，对于企业运行产生严重的影响，因此相关工作人员必须以大数据时代为背景，针对其特性提高计算机网络整体的安全性、可靠性，做好数据处理工作，从而保障企业正常、可持续发展。

关键词：计算机；大数据；网络安全；防范措施

On computer network security and preventive measures in the era of big data

Yanjie Chen
Zunyi branch of Chinatelecom Co., Ltd. Zunyi City, Guizhou Province 563000

Abstract: Nowadays, computer technology in our country has been greatly improved, and more and more enterprises gradually began to use big data technology to conduct daily management. However, due to the particularity of the computer network, the relevant staff in the process of data transmission management is easy to suffer from network security threats, resulting in data leakage and loss. It has a serious impact on the operation of enterprises. Therefore, the relevant staff must take the era of big data as the background, improve the overall security and reliability of the computer network according to its characteristics, and do well in data processing to ensure the normal and sustainable development of enterprises.

Key words: computer; big data; Network security; Preventive measures

一、概述

1.1 大数据定义

大数据的明显特征是流量较大，并且这些流量数据会存储在电脑中。由于数据的海量及其复杂性，计算机数据处理技术受到人们广泛关注。在大数据背景下，人们对信息的了解途径也逐渐增多。从依靠无线网络或服务器来保护资源，到依靠计算机的隐形终端来保护资源。目前，通过大数据获取的信息被各行各业广泛使用，部分蔑视法律的人，找到计算机技术存在的漏洞，并且大胆妄为的利用计算机开展犯罪行为[1]。

1.2 计算机网络安全概述

计算机网络安全主要是在计算机正常使用的情况下，通过相应的技术手段，保证计算机系统数据信息不受到恶意攻击、系统故障等因素的影响，避免数据信息被篡改、破坏、丢失等情况，能使计算机系统处于稳定、安全的运行状态。计算机网络安全对技术要求很高，涉及信息安全、计算机技术、密码学等方面。在大数据时代，计算机的作用越来越突出，对网络系统的要求也在逐步提高。与此同时，随着大数据时代的到来，计算机网络安全也面临着新的挑战。在实践中，高校企业必须重视计算机网络的安全，采取相应的预防措施。

1.3 大数据与计算机网络之间的关系

计算机在运行过程中会存在海量数据，并且数据所包含的信息较多，在这背景下大数据技术应运而生，大数据技术主要是通过云计算来得以实现，从而提高整体数据处理的质量与效率。大数据计算机网络系统应用较为广泛，主要是因为大数据具有较强特性，如数量多、类型多、价值密度低、处理速度快等。但是由于大数据技术以及计算机网络处于开放状态，因此随着大数据技术深入，所产生的数据种类较多，其数据传播途径发生了巨大改变，更加多元化、多样性，这就会导致计算机所面临的安全隐患问题更加复杂，无疑增加了计算机网络安全维护工作整体难度，因此相关工作人员必须做好相应防范工作，从而提高计算机网络整体安全性，将安全隐患问题扼杀在摇篮之中，为其数据处理工作提供相应良好的运行环境[2]。

二、大数据时代计算机网络安全存在的问题

2.1 信息保护框架不适用于快速更新的网络

计算机技术是当今发展最迅速的技术之一，在短短几年的时间内就变得家喻户晓。而在信息技术发展之初，各地区就建立了一定的信息保护框架。这个保护框架就是为了保障信息安全，但是由于信息技术发展太快，很

快就实现了普及，于是原来建立的保护框架就不再适用于今天的计算机网络了。在保护框架建立之初，是用个人信息的定义作为保护的前提和边界的。这种保护框架的定义是从计算机网络建立的一开始就确定好的。但是随着信息技术的发展，对于个人信息的定义变得狭隘。随着信息的快速发展，很多信息都能被收集并挖掘到[2]。如果仅仅以识别某一个个体的信息作为信息保护的定义，就很有可能在经过某些黑客的深度挖掘后，直接找到某人全部的信息，从而导致隐私的泄露。此外，在信息技术的长期发展中，我国并不是发展最快的，由此导致法律对信息安全的保护也比较晚。在现有的信息安全法律的规定中，都是一些碎片化的规定，并没有形成系统，而且对于信息安全的规定缺乏顶层设计，这就导致信息安全的法律法规如同虚设，在实际应用中无法有效实施。所以，在目前的计算机安全中，安全保护框架保护力度不够，个人信息很容易出现泄露，加上法律的滞后，就导致了有很多不法分子能够通过信息技术得到个人信息，这对于身处大数据时代的人来说是非常危险的。

2.2 计算机漏洞问题

在整个计算机的运行过程中，需要得到计算机各种网络系统的有效支持。为了进一步争取网络安全的稳定，计算机需要有效地支持各种外部运营商。在固定计算机网络的过程中，其主要建设内容由硬件设备和软件设备组成，在具体的网络运行过程中，计算机系统运行，漏洞就会出现，主要原因是整个计算机系统在具体操作过程中的动态发展变形。在计算机发展的过程中，其自身的核心方法和整体运行模式都具有一定的稳定性特点。因此，稳定特征容易产生计算机漏洞，计算机漏洞在具体的操作过程中具有一定的随机性和不规则性，无法得到有效的规范。因此，计算机漏洞对计算机的影响具有一定的不确定性。一般情况下，操作人员需要注意电脑操作过程，尽量不要激活相应的操作漏洞。在整个计算机系统的运行过程中，系统会掌握具体的操作并自动生成修复补丁。因此，就其整体运行而言，影响效果并不严重。但是，如果特定应用中的计算机漏洞被黑客等犯罪分子操纵，则计算机漏洞将成为严重影响计算机网络安全的突破口。他们会利用漏洞攻击整个网络大数据的运行，窃取新的数据，给整个计算机网络安全带来严重的安全风险。在大数据时代，用户的计算机操作水平有了很大提高，但仍存在巨大的层次差异。安全意识不强，数量众多，增加了个人资料及资料外泄的风险。与此同时，一些计算机网络用户没有计算机网络安全意识，容易相信并打开未知的网站链接或观看和下载的软件和视频，甚至因私事使用公共电脑，带来了计算机网络安全威胁。目前的计算机网络操作系统受到技术的限制，存在或多或少的漏洞，无论是由于操作不当引起还是内置的漏洞都是严重的安全威胁。通常，这些漏洞的修复需要通过系统自动下载补丁进行更新来实现，但是这种解决方案有一定的局限性，软件自身的一些问题很难通过系统进行修复，这就成了长期的安全隐患。即使目前针对这些病毒等问题开发了各种防火墙软件或杀毒软件，但从实际应用的角度看，这些软件的开发普遍滞后于计算机网络的发展速度，软件开发者只能修复现有的安全问题，无法预见新病毒的诞生，危机也很难预防。

2.3 信息保护边界模糊

在计算机网络安全中，要想实现信息安全的保护就要分辨出信息的类型和需要保护的级别。在信息技术的发展之初，人们对于信息技术的依赖性不强，用户黏性也不高，信息技术需要保护的信息等级也不高。而随着计算机网络的发展，信息成为推动社会进步的核心力量。随着社会的发展，信息技术被广泛使用，一些依靠信息技术而存活的企业更是将信息技术作为公司的核心。尽管信息技术能够推动社会进步和发展，但是也有一些掌握信息技术的不法分子，利用信息技术的发展将个人和企业的私密文件盗取以换取高额的利益。在这样的背景下，团队和个人对于信息的保护需求变得非常强烈。此时，信息技术的发展和信息技术的安全形成了一定的矛盾。而且信息安全没有了明确的边界和定义。在信息技术的使用中什么样的行为算是触犯了信息安全的底线，是谁规定这个底线，是以用户的角度还是信息服务公司的角度，这些都是真实存在的问题。例如在很多平台上，平台都会要求使用者进行注册。注册的内容大体为姓名、电话、身份证号等。当然，在从平台角度增加了用户信息的可识别度，能够为用户提供个性化的服务，注册信息的使用出发点是好的。但是在实际操作中就变成了如果你不同意这些条款和注册使用个人信息，就没办法使用平台的功能，从而变成了强迫注册。同时，在注册平台之后，很多用户就会收到各种各样的骚扰电话，从而降低了用户体验感。

三、计算机网络安全防范措施

3.1 提高用户安全意识

打击网络违法犯罪，改善网络大环境仅仅依靠国家政府是远远不够的，只有计算机用户提高自身的安全意识，有基本的安全意识操作才能减少网络伤害的概率。所以用户在网络上进行金钱交易时应当更加警惕，避免违规操作或者不正常操作。同时应当掌握生活常识，例如：银行不会自发和用户沟通要求客户提供个人信息和验证码。并且从事网络安全的相关人员应当定期检查网络环境是否安全，将安全隐患及时扼杀。

3.2 增强网络防御措施

第一步，升级计算机防火墙，将智能化技术和防火墙有机结合起来，从而自动筛选出存在安全隐患的信息并拦截成功。同时安全软件在发现异常信息后，应当及时处理，避免有害信息对手机或者计算机造成不良影响。第二步，计算机上均有安装防火墙，要定期检查计算机安全系统是否处于正常状态。第三步，杀毒软件是保护

计算机的可靠方法之一。

3.3 提高管理人员的安全意识

从技术上讲，不仅要做好网络保护，更要从管理上提高网络保护的质量和效果。一方面，要提高安全防护意识。在我们日常使用电脑的过程中，一定要注意个人信息及相关数据的保护，为保证相关数据的安全，可能会针对不同级别的数据设置不同级别的密码。用户还应该根据需要不断升级网络系统，例如经常对计算机网络进行杀毒或升级，以确保计算机的保护系统始终正常工作，并抵御最新病毒，以减少病毒攻击。另一方面，需要重点区域的保护，有的电脑不允许读写

操作，使用 U 盘或硬盘来防止非授权读取数据。此外，相关数据可以存储在本地，且此类数据不得连接到互联网，能够有效防止数据被盗的可能性，有效保护数据安全。

四、结束语

总而言之，在大数据时代背景下，计算机网络所受到威胁更加多元化、复杂性，因此相关工作人员必须做好相应防范措施，从而提高计算机网络整体安全性、可靠性，为我国社会生产以及大众生活质量提供相应保障，提高数据传输、管理、储存过程中安全性、可靠性，将计算机网络作用充分发挥出来。

参考文献：

[1] 颜玲，彭维龙 . 基于大数据时代的计算机网络安全防范措施研究 [J]. 电子元器件与信息技术，2021，5（05）：5-6+8.

[2] 朱军红，周海军，唐明根 . 大数据时代下计算机网络安全及防范措施探究 [J]. 无线互联科技，2021，18（07）：21-22.

[3] 李冰枫 . 大数据时代的计算机网络安全防范措施研究 [J]. 电子技术与软件工程，2021（07）：259-260.