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

大数据环境下计算机网络安全研究

张　一
汉中职业技术学院　陕西汉中　723000

摘　要：随着计算机技术与现代化信息技术的高速发展，大数据的时代也随之而来，给人们的生活与工作带来了很大的便利。此外，大数据的概念还渗入了社会的各个领域中，推动着各行各业的进一步发展，促进了我国经济的繁荣发展。虽然计算机网络具有很多突出的优势，但是复杂的网络环境也会引发了很多的网络安全问题，这些问题阻碍了计算机网络的稳定发展。鉴于此，本文就针对大数据环境下计算机网络安全进行了详细的研究，希望能为相关工作者有所帮助。

关键词：大数据环境下；计算机网络；安全

1、大数据背景下计算机网络安全的重要性及意义

第一，计算机网络安全是有效运用计算机网络的基础保障。现阶段，计算机网络的运用和信息存储以及利用具有密切相关性，这些信息涉及到用户的个人机密以及隐私，而这些信息的泄露会直接影响到计算机网络的使用。计算机网络安全的保障，有助于在利用计算机网络信息时更为合理和安全，并使得计算机网络信息价值得以充分发挥；第二，保障计算机网络安全，能够对其网络系统的稳定性进行保证。计算机网络系统非常庞大，具体涉及到诸多内容，这些内容可以结合网络信息得以有效联系，这也是充分运用计算机网络的前提基础。在运行计算机网络系统时，保证计算机网络安全，可以防止不法分子借助于计算机网络来散布计算机病毒，阻止病毒侵害到计算机网络系统，使得计算机网络系统的稳定性得以增强，保证其自身的安全性，进而有效运用计算机网络系统[1]。

2、大数据环境下计算机网络安全存在的问题

2.1 计算机网络本身的缺陷

虽然当前的计算机网络系统随着信息技术的发展在不断的完善，但还是难以避免系统漏洞的出现，从而对计算机网络信息的安全性产生相应的影响与威胁，即使是用户普遍使用的windows系统也存在着漏洞问题，这是无法有效避免。除此之外，用户所安装的软件也有可能存在漏洞，并且计算机在运行不同软件的过程中还有可能导致不同的系统漏洞出现，造成用户的个人信息及隐私泄露，并且现在的许多不法行为都是借助这样的漏洞完成[2]。

2.2 病毒威胁

网络病毒是一种非常常见的网络安全隐患，也经常发生在我们周围，时刻威胁着我们的正常工作和生活。尤其表现在电脑端，当我们在网站进行下载软时，经常会连带下载一些游戏程序，有时还会造成电脑卡顿、瘫痪，影响了我们正常工作。另外，当我们使用U盘时，这种现象会更加明显，不单会对电脑程序造成影响，还会损坏我们的文件。这些都是病毒给我们带来的麻烦，病毒由于其可复制性，非常快速地入侵我们的电脑，影响我们的工作、生活。

2.3 黑客入侵

在目前主要以大数据为中心的社会发展中，网络信息的价值越来越大，因此，这会大大吸引黑客的注意，黑客入侵是影响网络信息安全的主要因素，企业之间发生黑客攻击、盗取信息等现象，大多数都是相同类型的企业之间竞争而产生的后果，当企业计算机被入侵和攻击后，计算机网络会处于瘫痪状态，使得网络不可用，容易被窃取数据。入侵方式有主动性和被动性两种方式，其中，主动性攻击是带有目标和有准备的情况下直接对电脑进行攻击，使其数据和信息丢失和泄露。被动性入侵是在不影响电脑正常使用的情况下，进行电脑数据的窃取和破坏。但是这两种方式有一个共同点就是使得计算机数据和信息丢失和遗漏。

2.4 网络诈骗

在大数据时代，人们对计算机网络很依赖，无论是工作还是生活，都借用互联网的平台进行，这也给一些不怀好意之人有了可乘之机。他们借用计算机网络的普遍性和隐蔽性，开启了一系列诈骗行为。针对一些自我保护意识比较弱或者对网络不了解的人，进行哄骗，利用其同情心，损害大家的利益，甚至会影响人们的性命。网络诈骗与普通诈骗不同，是一种高技术犯罪。它可以进行远距离操作，很难发现作案人，对社会的威胁也是

作者简介：张一，1982.7.15，男，汉族，陕西汉中，汉中职业技术学院，讲师，本科，专业方向：计算机。

不可估量的。

2.5 人为操作不当

对于计算机用户是对于计算机网络信息的直接操作者和观看者，而用户能否按照正确的方式方法操作和查看数据，也是造成网络隐患的一部分原因。比如在日常的生活中，仍会有一部分人员对于计算机的操作不够成熟和不正确，在用户日常使用计算机时对于安全意识的防护不够重视，对计算机的网络信息安全防护意识不够强，有时无意识的操作就会导致个人信息的泄露，给不法分子趁虚而入的机会。

3、大数据环境下计算机网络安全的防范措施

3.1 加强数据加密

为了确保数据信息不产生泄漏，加强数据加密是非常主要的方式，并且也是人们降低数据丢失的方式之一。具体主要就是对于相应的重要信息和数据应用相应的方式将其转化为乱码，并且采用乱码的方式传输到接收人员，这样尽管不法分子获得了相应的数据信息，但是也只是一些毫无意义的乱码，这缺少秘钥解码的状况下，乱码都是以乱码的方式存在，这样就降低了信息数据泄露的安全隐患。在乱码传输到接受者手中当中之后，接收人员只需要输入相应的密码就可以对原始的数据看到。相对于数据信息加密技术来讲，其主要有两方面的内容，第一是私人秘钥，第二是公开秘钥[3]。

3.2 提高用户的黑客攻击防范意识

为了有效地防范黑客的侵入和攻击，应该制定良好的黑客攻击管理体系，计算机的使用者应该加强辨识黑客窃取的行为，因此，升级防火墙的级别、加强区别内外数据等措施能够有效地降低黑客侵入的机率。社会使用大数据的主体主要以学校、企业、政府部门为主，因此，应该积极的推广应用数字认证技术，在完善和优化数字认证技术的过程中，可以通过限制访问次数等方式来加强相关技术，更好地加强网络信息的保护。

3.3 加强防火墙技术的应用

当前，防火墙技术是保障网络信息安全的重要技术之一，主要分为应用级防火墙和包过滤防火墙两大类。应用级防火墙主要是在计算机的源头上对整个系统进行实时检测，这样可以有效地防止病毒的侵入，在渠道上阻断了病毒的传播，从根本上避免了病毒对网络安全的危害，是极为有效的防护措施。包过滤防火墙就好像是在计算机系统的周围设置了一层保护层，是在系统层的方面对整个计算机的安全设置保护措施，通过名字就可以发现其工作的原理，是将进入到系统层的病毒进行检测，分辨并筛选有可能对计算机安全造成威胁的病毒并进行处理，有效防止了病毒的侵入，给计算机的网络安全带来的极大的保障。防火墙技术是在计算机与网络之间进行防护的软件，所有通过网络流入该计算机的网络数据，都要经过防火墙，防火墙会对所经过的数据信息进行扫描处理，从而将一些有攻击性质的恶意软件进行拦阻。防火墙还可以让数据经过特定的端口进行输出，可以有效地封锁特洛伊木马，并且对于一些比较个别的站点访问时，也能够起到良好的封锁作用，从而可以阻止一些不明来意者的通信访问。

3.4 为计算机设备加装网络杀毒软件

为了更好的避免计算机系统遭受计算机病毒的攻击，可以为计算机设备加装网络杀毒软件，来保护计算机系统的安全。随着大数据技术的进一步发展和现代信息技术的进步，一些杀毒软件可以对计算机网络进行监测，监控计算机的实时情况，一旦发现异常情况就及时进行查杀，时刻保护计算机免受病毒软件的危害。此外，网络上的黑客也能给计算机网络安全带来巨大威胁[4]，因此，还要加强防火墙技术的研发与升级，以建立有效的黑客攻击识别模型，可以使用计算机用户的认证识别方式来进行登录，从而有效提升网络安全的强度。

3.5 定期培训员工，熟练操作

针对庞大的数据流，计算机网络技术工作者的操控水平不同，从而保证网络环境的安全可靠性便会有所不同，造成网络的风险差别就会很大，所以计算机网络运营商应该定期培训员工，让每一个员工都不断学习，互相借鉴经验，取长补短，缩小员工之间的水平差异，使得他们熟练操作计算机网络技术，从而保证网络运营的安全性，把风险降到最低。保障计算机网络安全运行的工作人员需要从实际操作过程中积累经验，共同和防火墙技术为信息内容的传输保驾护航。

4、结束语

总之，随着社会经济的快速发展，大数据环境下网络安全对于信息时代的网络通讯、网络办公、网络生活秩序的稳定等有着极为至关重要的作用，而在大力开发和应用网络安全技术措施的同时也要注意对网络垃圾信息的整顿和清理，注意一些不法信息的屏蔽和过滤，从而为净化网络环境提供一份基础支持。

参考文献：

[1]宋雪冬.大数据背景下计算机网络安全研究[J].当代旅游，2018（9）：1.

[2]唐庆谊.大数据时代背景下人工智能在计算机网络技术中的应用研究[J].数字技术与应用，2019，37（10）：72-73.

[3]姚光春.大数据背景下计算机网络安全及防范措施[J].电脑知识与技术，2020，v.16（14）：88-89.

[4]高丽娟.探究大数据时代的计算机网络安全及防范措施[J].才智，2015（23）：360，363.