大数据背景下计算机网络信息安全问题分析

钟 琳
电子科技大学成都学院 四川 成都 611731

摘 要：计算机网络安全对于当前的各行各业发展而言有着关键性的作用，在计算机网络技术普遍应用的今天，大部分行业都已经离不开计算机技术的合理应用，为了进一步保障各个行业的信息安全，创建出完整的网络监管机制，让更多人的工作与生活更加便利，降低整体的生产成本，应当将网络安全技术充分融入到工作与生活当中。如果计算机网络中存在着明显的问题，导致很多信息发生丢失，那么会对部分行业造成严重的经济损失。为了能够确保更多行业的工作安全，让更多技术得到合理的应用，让计算机网络技术能够更加全面的发展，让更多信息资料得到安全的储存与交流，应当做好新时代的网络信息安全防护工作。在大数据时代下，发展网络安全技术已经成为了非常重要的一项工作。由此可见，本文基于大数据时代背景，对计算机网络安全应用策略进行探讨是非常有必要的。

关键词：大数据；计算机网络；信息安全问题；安全防范措施

引言：进入大数据时代以后，计算机网络信息系统的应用逐渐广泛，网络上的数据狂开始呈现出集合级增长，这种情况下，加强网络保护至关重要。疫情期间，网络为在线教育的实现提供了便利，为广大师生提供了方便、快捷的服务，然而，短时间内互联网用户激增，也为网络平台增加了安全风险，安全问题成为线上教育工作中极易被忽视的一个重大问题。在大数据时代背景下，安全问题没有暴露出来时，往往表现得风平浪静，毫无波澜，可是一旦有安全事件发生，势必会造成巨大的损失。为此，必须针对网络信息安全问题进行深入分析，探索出计算机网络信息安全的有效防范措施，这样才能更好的推动当前时代背景下网络信息安全技术的深入发展[1]。

1 大数据相关概述

1.1 大数据含义

大数据也叫做巨量数据或者是巨量资料，它是指涉及的资料量规模巨大、主流软件工具不能在合理的时间之内完成其提取、处理、管理等操作的资讯。大数据的主要特征是信息数据庞大、信息种类多、交替更换周期短等。就技术层面来看，大数据和云计算之间具有密不可分的关系，大数据不能通过单个的计算机来完成处理，一定要对分布式架构加以应用，其主要技术特征是分布式的海量数据挖掘，而这一特征一定要借助于云计算技术来实现。但是在这一背景条件下，计算机网络信息在安全方面所面临的问题开始日益明显，此类问题的解决也成为了相关行业、研究者与工作人员的重点研究对象[2]。

1.2 大数据的存在价值

随着信息化技术的快速发展，在大数据背景下更多的信息技术将得到快速发展，如物联网、数字家庭等，大数据将作为汇合点，把海量数据进行处理与优化，然后反应到这些信息数据之上，对它们而言，大数据对它们的各个方面都有着极高的价值。也正是因为这些价值，所以大数据已经慢慢成为了 IT 技术发展的助力，越来越多的用户对大数据开始深入了解、运用以及认可，随着大数据的运用变多，大数据的技术将会越来越成熟，并不断地突破创新。

2 大数据背景下的计算机网络信息主要安全问题

2.1 自身系统存在问题

计算机网络运行中经常会因为外界环境或人为因素而造成网络不稳定情况，埋下安全隐患。随着计算机网络的逐渐普及，安全风险因素会随着使用者数量的增加而成比例增长。从计算机角度来看，现阶段大部分系统都支持数据共享模式，交流途径扩大，加大信息泄露风险，甚至会被黑客所利用，比较常见风险如下所列。第一，TCP/IP 存在脆弱性。这一问题具体可以归纳为协议中的缺陷，针对计算机网络安全的关注度较低，在 TCP/IP 协议中归于强调网络的开放性，这一特点会被黑客利用，并寻找运行漏洞，造成安全隐患。第二，网络结构问题，运行过程中不稳定。由于网络的形成主要依靠局域网，一旦发生通信行为，攻击者只需一台主机便可实现信息窃取。除此之外，系统更新阶段也是风险发生率较高的时期。第三，信息被窃取风险。造成这一问题的主要原因在于保密程序设置不当。第四，工作人员安全意识薄弱。用户在进行操作时由于意识的缺乏造成严重隐患问题，例如认为防火墙影响电脑流畅性便卸载或关闭，并在未获得代理认证时连接网

络，防火墙形同虚设。

2.2 计算机病毒入侵

在计算机网络的应用中，木马病毒十分常见。这些病毒通常会在系统或操作软件中潜伏，在用户操作中实现相应的信息获取，并造成相应的破坏。在计算机网络安全防护技术的发展中，木马病毒的更新也呈现出了惊人的速度，且具有了越来越强大的隐蔽性和攻击性。如果用户的计算机被木马病毒入侵，其中存储的信息便会受到严重破坏，严重的情况下甚至会导致用户的计算机系统瘫痪，对其正常使用和信息安全造成严重威胁。

2.3 垃圾信息与信息剽窃

通常来说，由于网络信息安全面临的威胁因素中包含垃圾信息，而这些垃圾信息主要通过邮件、新闻等途径传播，一些不良分子会通过这些垃圾信息的传播，强制性地在邮件、信息等渠道对竞争对手的商业信息、经济政策等相关内容进行剽窃，很明显，这是一种网络盗窃行为。从网络信息角度来讲，窃取信息是从间谍软件中生成的，如此一来，用户的数据信息将会处于危险之中。

2.4 黑客攻击

黑客是精通计算机技术的人群，是威胁网络信息安全的主要因素之一，黑客对网络信息的攻击可以分为主动恶意攻击以及故意窃取信息两种方式。（1）主动恶意攻击指的是黑客在进攻之前，就已经有了攻击目标范围，并且在寻找到目标之后，通过获取目标的漏洞来进行连续攻击，黑客这种操作不考虑其行动被他人识破，目标性很强，往往会造成目标计算机破坏严重，甚至出现系统瘫痪的情况。（2）故意窃取信息和前者不同的是，其攻击操作是隐秘的，黑客追求的不是对计算机进行简单粗暴的直接攻击，而是因为某种目的来盗取信息，只要能够窃取到信息即可。但对计算机系统而言，不管是被动还是主动，都会有严重影响，造成系统瘫痪、用户信息被窃取等网络信息安全问题，有些攻击甚至会使计算机不能再使用[3]。

3 大数据时代计算机网络安全的应用策略

3.1 注重账号安全防护

网络信息泄露的主要来源集中在账号密码泄露。大部分人在注册各种账号时都有着信息泄露的风险，而随着网络科技的不断发展，人们所需要注册账号的 APP 越来越多，这便要求很多人在网络中不断填写自己的账号与自己的个人信息，这些填写的信息一旦泄露会造成严重的信息安全问题，而且很多人的账号信息与自己的财产是呈现绑定的状态，如果这些信息泄露态度很容易被他人恶意盗取资金。为了进一步保障人们的信息安全，应当积极宣传账户安全防范的各类意识，让更多人的安全防护意识得到提升。比如在注册账号时尽量选择一些比较复杂的密码，通常在填写密码时，网易会提醒密码的安全等级，等级越高的密码防范的效果越好，也越不容易被人盗取。如果等级过低的密码，很容易被他人恶意破解，造成一定程度的损失，所以应当将密码的难度设置得更高。除此之外，也不应当在多个软件上设置相同的账号密码，这种问题的发生，很容易在某一个软件信息泄露的同时让自己其他的账号也被人盗去，很可能直接造成严重的经济损失，所以应当在不同的软件上设置不同的账号与密码，保障自己个人信息的安全性。除此之外，还应当定期更换密码，因为长时间利用同一种密码很容易被一些软件恶意盗取信息，所以应当及时更换自己的密码，将自己的安全信息加密，保证自己的网络账号安全，尽全力做好安全防护工作，保障自身的权益。

3.2 及时修补系统漏洞

系统漏洞属于计算机网络中始终存在的问题，每一次的升级都会修复一部分漏洞，避免遭受黑客入侵影响系统的正常运行。其基本原理在于优化底层程序逻辑，完善程序编写方式。系统应用之前，相关漏洞无法预先解决，只能在运行过程中逐步暴露出来。因此，需要采取针对性的漏洞同步修护策略降低负面影响，及时更新系统解决程序问题，避免受到攻击。大部分网络信息攻击风险所应用的供给渠道均为系统的潜在漏洞，从而帮助去获得更高的控制权限，再利用其权限对指令进行破坏。在实际保护过程中需要建立相关条例进行系统更新，避免其被不法分子利用而形成信息传递体系的损害。

3.3 防火墙技术的合理应用

在进行网络信息安全防护的过程中，防火墙是一种典型且常用的技术形式。就目前来看，防火墙技术的主要类型包括以下几种：第一是数据包过滤防火墙，此类防火墙技术主要是借助于各种类型网络数据、网络地址以及网络端口的打包处理来实现数据的筛选与处理。将被检查数据流中各个数据包的目的地址、源地址、TCP 端口号以及 TCP 链路状态等作为依据，将其和预定义好的规则进行比对，如果数据包与规则相符，防火墙便允许其进入到内部网络中，如果不相符，防火墙便会将相应的数据包删除。第二是代理服务器防火墙，它在两个网络之间运行，可起到服务器以及客户机的双重作用。当用户请求被此类防火墙接收到之后，它会对请求到站点进行检测，如果站点与公司要求相符，也就是公司允许用户对该站点进行访问，防火墙便会从站点中将用户所需的信息取回，然后将其转发给用户。如果站

点和公司要求不符，防火墙不会进行上述操作，同时会将不符合要求的提示发送给用户。第三是应用级网关防火墙，此类防火墙主要是将应用层作为基础来进行协议过滤以及转发功能的建立。它可以将指定的过滤编辑应用到特定的网络协议中，在过滤时进行数据包的必要统计、分析与登记，并形成相应的报告。它和过滤防火墙的特点类似，也是通过特定逻辑来进行数据包安全性判断，如果检测到数据包中有特定的风险逻辑，防火墙便会立即与用户的计算机之间建立起紧密联系。在这样的情况下，用户便可及时发现防火墙的运行状态，并明确安全问题所在。第四是复合型防火墙，此类防火墙的主要应用方案有两种，第一是屏蔽主机，将防火墙连接到 Internet 中，并在网络部安装一个堡垒机，在防火墙中进行相应的过滤规则设置，让堡垒机在 Internet 中成为其他所有节点所能到达的唯一一个节点，这样便可防止未经授权的外部用户对计算机网络的非法攻击。第二是屏蔽子网，在一个子网中进行堡垒机安装，从而形成一个非军事化区域，在该子网两端分别进行过滤路由器设置，将子网和 Internet 以及其他部分的网络分离，以此来实现子网信息安全的良好保障。

3.4 使用加密技术

网络信息存储、流通都有一定规定，对其安全性实施保护是网络安全保护举措中一项重要规定。在数据存储过程中加密技术的应用很有必要，通过使用文件加密技术，可显著提升网络信息系统的保密性，避免网络信息被窃取、损害。外杀毒软件也应该实施加密处理，提前做好检查，一旦有问题发生及时实施处理。近年来，电商活动越来越多，为了确保网络信息安全，电商平台也应该做好加密处理工作，比如数字签名等。

3.5 加强杀毒软件的应用

用户想要提高网络信息安全，除了在使用计算机时打开防火墙之外，还需要用杀毒软件来阻止病毒侵入计算机。杀毒软件 + 防火墙是目前绝大多数用户用来保证信息安全的手段，在使用计算机的时候，用户可以打开杀毒软件，对计算机环境、网络进行检查以及修补，如果在查杀过程中有发现携带病毒的软件或者网站或者某些程序存在漏洞容易被黑客攻击的时候，用户要及时点击杀毒软件进行下一步的防护动作。杀毒软件可以保护计算机信息，防止泄露，达到保护计算机的效果。不过需要注意的是，用户在使用杀毒软件的时候需要与时俱进，使用最新的杀毒软件，因为网络病毒是在不断更新的，杀毒软件也在不断升级，我们用旧的杀毒软件可能会对一些新型电子病毒没有作用，检测不出来。

3.6 进行网络监控

为了进一步做好信息安全防护工作，应当定时进行网络监控。相比于各类杀毒软件，网络监控能够起到的功能更加全面，能够第一时间发现不良网站所传播出的各类病毒以及安装在电脑中的恶意插件。网络监控是新时代网络技术的全新安全手段，能够针对运行系统中的各个环节进行分析计算，及时寻找到系统的漏洞，为各类信息的应用提供了安全的保障，进一步保证了更多人的网络安全。这种方法应当进一步普及开来，这样才能让更多的信息泄露问题得到解决，让更多人拥有更强的网络安全意识，利用智能化的监控系统实现对网络系统的全面监管。

结束语：综上所述，在当今的大数据时代中，计算机网络信息安全问题十分显著。为实现此类问题的有效防治，我们需要对网络信息安全方面的主要问题做到充分了解，然后以此为依据，通过合理的技术措施来做好安全防护工作。这样才可以让计算机网络信息得到良好的安全防护，在满足用户实际应用需求的同时实现其信息安全的有效保障，从而进一步促进计算机网络技术在大数据时代中的良好应用与发展。

参考文献

[1]张令.大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用，2022（04）：69-71.

[2]钟建坤.大数据下计算机网络信息安全及防护[J].数字技术与应用，2022（02）：203.

[3]徐晶.探讨大数据时代计算机网络信息安全防护策略[J].数字技术与应用，2022（02）：240-242.