大数据时代计算机网络信息安全防护策略探讨

王　磊*
天津石化行政事务中心　天津　300270

摘　要：互联网交互技术、大数据及云计算技术快速发展的时代背景下，不同广域网或局域网内的计算机系统会受到黑客、病毒或木马程序的攻击，出现非法用户侵入、数据传输阻断、信息盗用或篡改的问题，这些问题需要通过一系列安全防护技术的应用予以解决。从大数据的相关内容出发，探讨了计算机网络信息安全存在的问题，制定出完善的网络安全处置方案，提升网络信息通信的安全性、可靠性。

关键词：大数据；计算机网络信息安全；防护策略

DOI：https://doi.org/10.37155/2717-5170-0401-7

引言

从现有的计算机网络发展而言，其已经与人们日常工作与生活产生深度融合的现象，通过数据业务的高效率处理，可以真正满足基于互联网视域下的信息共享、信息时效性传输诉求，以此来提高人们工作与生活质量。但互联网在为人们带来便利的同时，其也将产生一定的安全问题，例如大部分人们在使用计算机时，通常将重要信息存储到网络中，而一旦此类信息遭到丢失的风险，将为用户本身造成较大的经济损失[1]。为此，应针对当前计算机网络运行中出现的问题，结合计算机网络运行特征，采用先进技术提高计算机网络的安全性能，保障用户及企业的数据隐私。本文则是针对计算机网络信息安全及防护策略进行探讨，以供参考。

1 大数据相关内容概述

大数据又被称为海量数据，从字面意思理解就是指信息数据的规模及数量方面具有巨大性特点。其主要特征有：数据类型多样化、数据内容更加丰富。相较于传统形式的数据信息，其更具多元化以及立体化特征。大数据本身具有较多类型和数量，随着计算机网络技术的不断发展，很多无用信息也会融入，进而使其没有较为具体形式的结构特点。互联网技术与社会行业的不断融合与渗入，丰富了大数据的信息来源，甚至使其构成了具有相当规模特点的数字化综合体。近年来，很多先进人士和企业重视大数据的深层意义及价值，使得大数据自身所具有的潜在价值不断被运用到各个行业之中。大数据还可看成是众多人群自身行为、习惯、思想等方面信息的集合以及运用数字形式进行的展现，因此加强对大数据信息的分析与价值挖掘，可以使其更好地推动社会进步与行业发展。当前我国的阿里巴巴、腾讯等计算机类型的公司已经在积极地向大数据进军，希望通过开展相应的数据布局，来为其产业发展提供更多帮助与促进[2]。同时，我国相关管理部门也在不断出台相应政策，对大数据的发展提供更多便利与支持。

2 计算机网络信息安全存在的问题

2.1 计算机网络本身的问题

由于互联网经济本质上的劣根性，导致了计算机网络容易出现失真的情况，从而给互联网空间环境的净化带来了前所未有的风险和挑战。这些问题包括日常的信息缺陷，TCP/IP的信息边缘化问题。TCP/IP作为计算机网络普遍适用的条款，但是由于该项条款的共享性和公开性，导致了其对计算机网络空间的影响甚微，所以，很容易受到网络黑客的侵犯，从而极大地危害了网络的空间环境。在这一阶段，众多的本地网络合并形成了互联网。当一个本地网络上的用户开始与另一个本地网络上的用户进行相互通信时，多台主机会同时工作，利用强大的信息流将资源传递出去。黑客会利用计算机网络的缺陷和漏洞，对于主机发起的攻击进行屏蔽，借助其分散的攻击行为，会将所有主机信息一网打尽。计算机网络空间本身就是非封闭性的，这一缺点无形之中增加了其被监听的可能。而且对网络的加密措施也没能够引起足够的重视，当用户选择无偿网络链接的时候，这大大增加了窃听发生的可能性。

***通讯作者：**王磊，1983年12月，汉，男，天津，天津石化，科员，工程师，研究方向：计算机网络科学技术。

2.2 黑客攻击和病毒入侵

黑客攻击及病毒侵袭是计算机安全问题产生的主要因素，且上述两类攻击行为对于用户而言，可能造成信息不可修复的严重问题，降低计算机网络的安全性，令用户面临着严重的经济损失。大数据网络体系下，数据信息的多架构传输模式，加大了数据信息传输的复杂性，对于计算机设备固有的运行模式来讲，大容量、多线程的数据传输，将增加计算机网络安全风险问题的产生概率。黑客攻击属于主动性的攻击行为，其是由黑客人员针对性地入侵到计算机系统中，对用户内部数据进行窃取。与黑客攻击行为相比，病毒则可以看成是一种被动形式，其是依附于数据信息中侵入到计算机设备内，且其具备隐匿性与蔓延性、存储性等，降低计算机设备的运行效率，严重时可能导致整个网络瘫痪，无法运行，对计算机网络造成极大的安全损害[3]。

2.3 数据泄露与隐私侵害

不同计算机网络系统中的海量数据资源交流，往往选取明文加密、密文加密的方式，对数据传输、接收、整合分析与存储的流程，作出规范化管理，以保证多源类别数据流通的系统性、安全性。但面对大数据时代如此庞大、复杂的数据资源，开展不同类别结构化、非结构化数据的筛选与管理，面临着数据信息记录、识别与使用的危机。如部分不法分子可以截留正在传输的计算机数据，通过对明文或密文的破译、代码修改，来达到盗取机密与隐私数据的目的。因而，这一情况下需要增设大数据云空间、网络安全服务系统，进行海量数据信息传输、存储的流程管理，降低信息泄露、个人隐私侵害问题的发生几率。

3 大数据时代计算机网络信息安全防护策略

3.1 利用身份认证技术

大数据时代背景下，网络环境中的用户信息以特定数据方式体现，而与此相对应的即为计算机在对操作者身份加以识别时，以此特定数据为依据，授权并认定的用户。因此，可利用身份认证技术，借助个性化指令、个性化认证密钥的应用，判断当前操作者是否合法，以此推动网络信息安全首道防线的构建。目前生物特征、信任物体、信息秘密为应用身份认证技术的三种执行方式，简而言之，即为你是谁？你拥有什么？你知道什么？以生活中常见的面部识别及指纹识别为例，即为生物特征，而动态口令及静态密码即为信息秘密，门禁卡及IC卡即为信任物体。计算机系统在识别身份认证时，以预设密钥程序为依据，分析、校对操作者所提交信息，为操作者提供相应的数据修改、文件查看及登录访问等权限，记录、监管操作者行为过程[4]。以此为基础，计算机网络信息安全风险存在多样化来源，同时在技术方面也较为成熟，而为对身份认证技术安全等级进一步加强，则可借助多因素身份认证方法的应用，主要即指将至少两种的身份认证执行方法相结合。现阶段，多层静态密码、IC卡+静态密码、静态密码+动态口令等为常用方式，借此方式除可有效提升病毒及黑客等入侵者防护破译难度外，还可保障数据信息安全。

3.2 利用防火墙技术

防火墙是一个由计算机硬件和软件组成的系统，部署于网络边界，是内部网络和外部网络之间的连接桥梁，同时对进出网络边界的数据进行保护，防止恶意入侵、恶意代码的传播等，保障内部网络数据的安全。防火墙技术是建立在网络技术和信息安全技术基础上应用型安全技术，几乎所有的企业内部网络与外部网络（如因特网）相连接的边界设都会放置防火墙，防火墙能够起到安全过滤和安全隔离外网攻击、入侵等有害的网络安全信息和行为。网络内部的安全需要采取一定的措施加以维护。当下，对于内网的管理是维护网络秩序的根本措施，还可以采取加密的方式实现对数据的安全化管理。其最大的优势在于实现了信息的加密处理，提高了加密信息的安全属性。为内网的加密提供了必要的物质准备和支撑。

3.3 加强计算机网络系统的管理与监控

随着现代企业对于计算机网络信息的需求和依赖程度不断加大，加强企业管理工作对于其自身信息安全有着重要作用。因此，相关企业需要加强企业内部计算机网络系统的管理与监控。日常使用较多的计算机系统监控方面的技术主要是入侵检测技术，该技术的应用可以有效降低计算机网络系统在运行过程中被入侵的风险，通过监测数据，可以及时发现网络安全方面的隐患，该项技术主要运用的是统计学技术以及签名分析方法等。该项技术主要是利用统计学方法和相关理论知识对开展计算机网络信息监控过程中所获取的相关数据进行统计与分析，进而判断是否存在安全风险及隐患。

3.4 利用杀毒软件方面的防护

计算机软件在设计时，需要留有一定的操作权限，实现对软件的更新处理，但其将造成软件安全漏洞问题。对此，必须正确利用杀毒软件，及时修复各类程序运行过程中所存在的安全隐患，进一步提高计算机内部的杀毒等级，对大数据环境下产生的各类数据进行病毒识别，同时也可针对计算机内部的隐藏风险进行逐一查证[5]。此外，在实际应用过程中应针对杀毒软件进行定期更新，因为系统本身所具备的属性是针对于当前病毒库而实现逐一查杀的，一旦出现新型病毒的话，极有可能造成因为杀毒软件更新力度不足引发的病毒查杀缺位现象，特别是在大数据运行体系下，多节点的数据爆发将产生更为严重的数据交错问题。为此，通过对杀毒软件定期更新，则可进一步提高数据查杀的安全性，保障计算机网络的安全运行。

结束语：综上所述，计算机在为人们带来便利的同时，也暴露出许多弊端，对用户隐私信息造成严重影响。为确保计算机网络运行的安全性，必须以影响信息安全的因素为切入点，制订立体化防控手段，提高计算机网络的安全性能，为用户构筑出一个安全可靠的网络环境。

参考文献：

[1]冯庆亮.大数据时代计算机网络信息安全与防护策略研究[J].企业科技与发展,2020,(01):94-95,98.

[2]赵培琨.大数据时代计算机网络信息安全及防护策略[J].计算机产品与流通,2020(05):38+54.

[3]汪东芳,鞠杰.大数据时代计算机网络信息安全及防护策略研究[J].无线互联科技,2015(24):40-41.

[4]邹阳.大数据时代下计算机网络信息安全问题研究[J].电脑知识与技术:学术交流,2020(6X):19-20.

[5]卢煜晟.大数据时代计算机网络信息安全及防护策略研究[J].工程技术(全文版),2020(12):293.