计算机网络安全防范在大数据时代的探索

李　聃

（中国大唐集团科学技术研究总院有限公司西北电力试验研究院，陕西　西安　710000）

摘要：大数据时代计算机网络安全不仅是支撑数字经济发展的基础，更是计算机网络安全防范战略基石。计算机网络的最大特点是信息通信、信息共享、负载均衡和分布式计算。在这些过程中产生的大量数据需要一个安全的网络来保护，以避免出现信息泄露和黑客入侵等问题。基于大数据技术建立更加全面系统的计算机网络安全防范体系，通过各种安全防护技术的应用，有效满足计算机网络安全防范的需求，在此基础上要引导更多用户树立较强的安全防范意识，从而有效提升计算机网络安全防范水平。

关键词：大数据；计算机；网络安全

中图分类号：U656.135　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2024.02.015

计算机网络安全是计算机行业发展的重要基础，自计算机网络诞生之始，其安全防范就成了各方关注的焦点。大数据技术是利用计算机网络系统对海量、多样的数据信息进行整合和处理，并根据特定需求获得科学结果的一种新型分析技术。与传统技术手段相比，大数据技术具有更快的信息处理速度和更高的准确性，可以在短时间内根据设定的条件对数据资源进行整合和分析。计算机网络安全防范需要充分应用各类大数据技术的优势，从而保障提升计算机网络安全防范水平。

1 大数据时代计算机网络安全防范的重要性

大数据技术的本质是从历史数据中发现规律，进行预测、分类、决策。现代数据挖掘技术不是采样和分析数据，而是基于所有数据的数据挖掘。通过数据挖掘，可以发现由网络流量数据和日志数据构成的历史数据，发现合法数据和信息的模式，从而发现相应的入侵数据和入侵模式。在此基础上，可以建立数据识别和预防模型，及时发现和处理入侵和非法访问，并在计算机网络入侵之前进行拦截。与传统的网络安全技术相比，大数据技术更具有精准、及时、可靠等特点。数据是网络安全平台的基础，可以引入公开可用的网络安全数据和网络使用过程中产生的历史数据，并进行有效的将历史数据进行整合[1]。

大数据技术、云计算方法和互联网平台实现了技术融合和功能互补，在计算机网络安全防范方面得到了广泛应用，取得了良好的效果。然而，大数据技术在为人们的工作和生活提供便利的同时，也带来了一定的网络安全风险。因此，要重视计算机网络的安全防范与管理[2]。

2 计算机网络安全风险分析

2.1 计算机网络病毒入侵

计算机病毒本质上是一个可执行的代码程序。一旦病毒被植入计算机系统，它将不能正常工作，在严重的情况下，它会导致系统瘫痪和数据信息丢失。目前，网络环境更加开放，这也为病毒入侵计算机网络系统提供了机会。计算机网络运行过程中存在的网络病毒可以分为特洛伊木马和蠕虫病毒两类。因此，在应用计算机系统时，要做好病毒的检测和拦截工作，及时扫描和拦截潜在的病毒危害，防止病毒程序的入侵。

2.2 计算机网络系统漏洞

大数据时代计算机网络系统本身并不完善，在开发过程中也存在着系统漏洞的问题。大数据时代，计算机网络应用要求也向着多元化方向发展。同时，受大数据时代的影响，网络环境日趋复杂。因此，需要采取科学合理的安全措施来保证计算机网络的安全。计算机随时容易受到病毒和网络攻击，造成数据丢失等现象，甚至可能影响经济利益。由此可见，更有必要加强计算机网络安全防范工作，为计算机网络安全以及用户的隐私和利益安全提供保障[3]。

3 大数据时代计算机网络安全防范技术

3.1 智能防火墙技术

防火墙作为计算机网络最基本的保护基础之一，被广泛使用，主要是通过在内部和外部网络之间建立一个人为的屏障来保护用户信息。在大数据时代，人工智能技术可以提高防火墙的自动识别性能。在增强防火墙防御能力的同时，也赋予了防火墙自学习能力。当不断面临病毒的新攻击时，实际上会增强防火墙的防护能力，因为智能防火墙的自学习能力可以帮助防

火墙掌握最新的攻击方式。因此，与普通防火墙相比，智能防火墙具有更高的效率和更好的防护性能，并且在大数据技术的支持下，还可以为防火墙提供更准确的判断和决策。例如：2021 年推出的新一代智能防护墙，配备 SSL 硬件解密引擎，大大提高了流量处理能力，有效降低了成本 [4]。

3.2 漏洞侦破技术

所谓漏洞检测技术，是指在计算机初始化阶段对其进行静态检测。该技术主要针对计算机表面进行检测，经过广泛的实践，在技术上取得了重大进步，并逐渐向静态和程序化方向发展。静态检测是利用计算机源代码扫描发现漏洞，分析其语法和语义，根据自身特点发现系统缺陷。它主要观察计算机的运行状态，一旦发现运行异常，就可以判断系统是否可以安全运行。静态检测技术通过对计算机内部的全面检测，可以更好地识别系统与缺陷之间的关系。计算机网络中的安全漏洞种类繁多，但共性相对较少。具体来说，安全漏洞可以分为两类：硬盘安全漏洞和内存安全漏洞。目前的技术还不够成熟，只能检测到某些特定的缺陷，限制了该技术的广泛应用。

3.3 数据加密技术

数据加密技术是保证隐私和机密信息不泄露的有效手段，也是完善计算机网络安全体系的关键环节。所谓数据加密技术，是指对关键数据或重要信息进行专门的、隐蔽的处理，使其他用户无法直接了解信息的真实含义。其中，公钥加密和私钥加密是数据加密技术的两种基本形式。虽然公钥加密技术发展相对较晚，但它比私钥更安全，而且私钥加密分为加密和解密两个过程，两个过程相互对应。值得注意的是，私钥加密没有用户限制，任何用户都可以使用，而且解密速度更快，在日常生活中更容易实现。当然，如果将公钥和私钥结合使用，数据加密效果会更好，从而确保计算机网络中的数据不会被窃取。

3.4 入侵检测技术

入侵检测技术主要分为两种方法：签名分析法和统计分析法。这两种方法基于完全不同的原理。其中，签名分析法是基于目前已知的系统漏洞，主要利用匹配等方法发现签名中存在的攻击类型；统计分析方法的基础是统计原理，它对系统的正常运行进行分析，判断系统是否正常或异常。大数据背景下入侵检测技术的基础是大数据技术的挖掘和存储技术。当计算机网络系统发生数据丢失时，需要及时建立有针对性的入侵检测程序。记录各种攻击方式下数据渗透行为产生的数据信息，汇总相应的攻击模式，并存储在数据库中。通过总结，形成了一系列参数指标，作为网络攻击的参考标准，从而有效地保证了计算机网络安全。

3.5 网络加密技术

计算机网络安全的保密技术一般从网络结构、网络协议、安全设备部署等方面进行设计。最主要的代表是安全隔离网关技术，它是一种基于网关的内部和外部网络之间的物理隔离技术。然而，在隔离的同时，该技术也可以实现各种形式的内外信息和数据交换。网关技术还具有各种控制功能的固态开关。但对于物质固态存储的命令，只有两类：读和写。其次，防火墙技术包括包过滤技术、应用网关技术、代理服务器技术、NAT 技术和 Internet 网关技术。这类技术主要涉及对数据包的选择性控制，对一般用户是透明的。当合法数据进出网络时，保密技术不会产生直接反馈；当增加来自危险区域的通信时，应用层网关可以关闭或隐藏有价值的数据，并记录通信过程。该技术最大的优点是可以在一定程度上弥补信息系统自身的漏洞，从而有效地防范计算机网络安全 [5]。

3.6 大数据神经网络技术

大数据神经网络可以模拟人脑的正常运行，与其他应用系统相比，大数据网络具有良好的可接受性和容错性。通过大数据神经网络，结合各种检测系统，准确识别带有噪声和失真的输入模式，可以提高计算机网络检测的效率。将大数据神经网络应用于海量数据信息的主要优势在于对低值密度数据进行分析，主要包括噪声输入和失真输入两种模式。研究人员利用信号检测方法来保证计算机网络管理的安全性，利用大数据神经网络可以在大数据背景下分析海量数据信息。此外，利用大数据神经网络还可以处理复杂多变的数据信息，以及识别语言、音频、图像等信息。在实际应用中，大数据神经网络具有高容错性、智能化、自学习等优势，解决了传统大数据在直观处理方面的不足，如处理非结构化信息、语音模式识别等，使其成功应用于神经专家系统、组合优化、智能控制、预测、模式识别等领域。此外，在计算机计算能力快速增长的过程中，大数据神经网络也在不断变化。大数据神经网络技术响应速度比 CPU 快，提高了大数据神经网络的处理精度、深度和速度。大数据神经网络优化算法可以实现人脑的自动匹配。虽然在应用过程中存在问题，但大数据神经网络算法技术的改进已经得到发展，可以有效地处理计算机网络风险问题 [6]。

3.7 专家数据库的搭建技术

大数据应用于计算机网络技术，还可以建立专家数据库，更好地吸收和借鉴专家的实践经验，总结经验教训，促进计算机网络结构、系统内容等方面的不断完善。大数据可以促进计算机专家系统的工作，在分析专家系统数据的基础上，编写有针对性的指令。当检测到“外敌”入侵时，通过实例可以判断

专家系统的可靠性，识别威胁因素。这样可以显著提高计算机网络安全数据的检测精度。

4 大数据时代计算机网络安全防范策略

4.1 加强计算机网络数据安全监控

随着技术水平的不断提高，计算机网络中的攻击方式变得更加隐蔽，并将不断升级，从而避免传统安全防护软件构建的防御系统通过各种攻击方式。因此，有必要积极引入新技术来实现对网络信息的安全管理。用户可以利用大数据技术中强大的算法和架构技术，在保证原始信息完整性的同时，简化数据信息。在不破坏原始数据的情况下，可以提高数据的传输效率，并利用相关技术实现数据关联。一旦数据的某一部分出现异常，就可以第一时间发现并处理，实现对数据信息的安全监控。在数据信息的存储过程中，为了提高安全性，可以采取以下措施：首先，建立云存储空间，将数据信息同步到云存储空间，实现数据信息的备份，防止数据丢失。其次，对重要的数据信息进行加密，通过技术手段对数据进行加密后，将加密后的信息与关键数据分开保管。最后，要建立重要数据的多重备份处理机制，严格按照相应的程序进行数据传输。在数据传输过程中，需要进行安全监控，需要建立数据信息处理分析平台，实现对所有数据的统一管理，从而减少人为失误对数据的破坏。在访问数据信息方面，可以设置密钥，明确访问者的权限级别，并根据级别获得相应的信息访问权限。最后，要严格执行接入用户的身份认证，有效降低被黑客非法入侵的风险[7]。

4.2 加强防火墙和安全检测系统的应用

大数据时代计算机网络安全防范过程中相关人员必须建立相应的管理制度，从源头上提高计算机网络安全管理水平。在大数据环境下，越来越多的恶意软件和新型病毒对计算机网络安全构成威胁。因此，相关人员需要采用适当的安全检测技术和网络防火墙，阻断日常计算机应用程序中的恶意信息，防止恶意信息在计算机网络中的传播。网络防火墙技术主要是利用拓扑结构来屏蔽恶意信息，更好地保证计算机网络的安全。网络防火墙技术广泛应用于大中型公共网络和企业网络中。大规模信息传输的安全管理。一般来说，员工分为内部架构管理和外部架构管理，内部架构管理相对安全。因此，在发布和存储信息时，如果运行在外部系统上，防火墙可以检测内部和外部系统，消除安全风险和计算机本身的安全级别。通过防止病毒对数据和信息的攻击，可以有效避免计算机网络安全问题[8]。

4.3 加强用户网络安全意识

计算机用户的综合素质在计算机网络中起着至关重要的作用。因此，为了保证计算机网络安全的整体效率，相关人员必须提高计算机用户的综合素质，使用户能够按照相应的标准进行操作。相关人员可以利用新媒体技术对公众开展计算机网络安全宣传教育。公众的计算机网络安全观念也可以在日常操作中受到安全标准的约束，进一步提高计算机网络安全防范水平。同时，加强对管理员进行网络安全宣传和思想指导，使其意识到自己工作的必要性，学习新的网络安全知识和技能，并将其应用到计算机网络安全防范过程中。计算机网络安全防范的整体质量和效率，使用户能够安全、规范地实施计算机网络的使用。

5 结语

综上所述，在大数据发展的过程中，计算机网络面临的威胁日益多样化，计算机网络安全是大数据技术的基础保障，因此，计算机网络运行过程中需要相关人员采取相应的防范措施，提高计算机网络的整体安全性和可靠性。大数据技术的应用也为计算机网络信息安全的维护和网络环境的建设提供了相应的保障，进一步推动计算机网络信息安全朝着智能化、多元化的方向发展，从而充分发挥大数据技术的优势，实现计算机网络信息安全的管理，从而进一步提升计算机网络安全防范的效果。

参考文献：

[1]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，2020，14(24)：40-41.

[2]汤东.大数据时代计算机网络信息安全及防护策略研究[J].中文科技期刊数据库(全文版)社会科学，2017,(07)：277-278.

[3]王芳.大数据时代计算机网络信息安全及防护策略研究[J].电脑迷，2021，26(05)：66.

[4]蔡琴.关于大数据时代计算机网络安全防范的途径分析[J].现代工业经济和信息化，2023，13(04)：69-71.

[5]刘强，陈益全.大数据时代下计算机网络安全防范分析[J].网络安全技术与应用，2023,(02)：165-166.

[6]孙辉中.大数据时代下计算机网络安全的防范研究[J].无线互联科技，2022，19(13)：24-26.

[7]敬甫盛.大数据时代下计算机网络安全及防范措施探究[J].网络安全技术与应用，2022,(03)：66-67.

[8]张孝若，段莉华.大数据时代下计算机网络安全防范的研究[J].网络安全技术与应用，2022,(03)：179-180.

作者简介：李聃(1992-)，女，陕西西安人，硕士研究生，工程师，主要从事网络安全与信息化研究。