大数据时代下计算机网络信息安全问题探讨

田 秋
（贵州健康职业学院　铜仁　554300）

摘　要：随着信息技术的不断发展，大数据时代给社会带来了前所未有的机遇和挑战。在数字化、信息化时代，计算机网络已经成为数据信息传输通讯、存储和处理应用的核心基础设施。然而，与之相随的网络信息安全问题也愈发突出。数据信息在应用传播过程中，也促使了网络病毒的攻击手段和方式不断翻新，对网络安全的威胁日益严、峻复杂，给网络安全防护提出了更高、更新的要求。文章通过分析大数据时代的特征，分析了计算机网络信息安全现状及面临的问题，并就此提出了相应解决策略和方案，希望给计算机网络信息安全保障提供参考。

关键词：大数据时代；计算机网络；信息安全；应对策略
中图分类号：TP393.083　　**文献标识码**：B　　**文章编号**：231128-10861

Exploration & Discussion on the Information Security Issues of Computer Network in the Era of Big Data

Tian Qiu
（Guizhou College of Health Professions, Tongren 554300, China）

Abstract: With the continuous development of information technology, the era of big data has brought the unprecedented opportunities and challenges to society. In the era of digitalization and informatization, the computer networks have become the core infrastructure for data transmission, communication, storage, and processing applications. However, the accompanying network information security issues have become increasingly prominent. In the process of application dissemination, data information has also prompted the continuous renovation of network virus attack methods and techniques, posing increasingly the severe and complex threats to network security, and putting forward higher and updated requirements for network security protection. The article analyzes the characteristics of the big data era, analyzes the current situation and problems faced on computer network information security, and proposes corresponding solutions and strategies, hoping to provide reference for ensuring computer network information security.

Keywords: era of big data; computer network; information security; response strategies

0 引言

大数据是指规模庞大、类型多样、处理速度快的数据集合，它对各个领域的发展都产生了深远影响。然而，大数据时代也带来了一系列计算机网络信息安全问题，不仅威胁到个人隐私和财产安全，还可能对国家安全和社会稳定造成严重影响。因此，探讨大数据时代下计算机网络信息安全问题具有重要现实意义。

1 大数据时代的特点

大数据的快速发展给各行各业带来便捷的同时也给计算机网络信息管理带来了新的挑战。大数据时代下，计算机网络信息也呈现出了全新的特点，主要体现在一种规模大到在获取、存储、管理、分析方面大大超出了传统数据库软件工具能力范围的数据集合。大数据时代主要有数据体量大、处理速度快、种类多样和价值密度低这四个特征。首先，大数据时代的数据体量巨大，起始计量单位是P（1000 个 T）、E（100 万个 T）或 Z（10 亿个 T），很多企业的数据总量已经达到百 PB 以上；其次，大数据的处理速度快且时效性高，能够高效地处理海量的数据，并给予用户及时甚至实时的反馈信息；此外，大数据的类型繁多，包括网络日志、音频、视频、图片、地理位置信息等多种类型；最后，大数据的价值密度相对较低，即数据中真正有价值的信息可能只占一小部分。在这个基础上，大数据技术也得到了快速的发展，包括大数据采集和预处理、大数据存储与管理、大数据分析和挖掘、以及大数据展现和应用等关键技术。这些技术的发展使得我们能够更好地理解和掌握数据分析能力，成为符合时代要

求的人才。除了上述四个方面的特点，大数据时代还具有以下特点：

1.1 数据来源广泛

大数据的来源不仅包括企业内部的业务数据，还包括社交媒体、传感器、智能设备等外部数据源。这些数据来源的多样性使得数据分析更加复杂和有挑战性；

1.2 数据质量不稳定

由于数据来源的多样性和数据采集方式的不同，大数据的质量往往不够稳定。例如，有些数据可能存在缺失、错误或重复等问题，需要进行数据清洗和预处理；

1.3 数据分析方法多样

大数据分析需要使用多种分析方法和算法，包括机器学习、深度学习、自然语言处理等。这些方法的选择和应用需要根据具体的业务场景和数据特点进行灵活调整；

1.4 数据价值实现难度大

虽然大数据中蕴藏着巨大的价值，但是如何将这些价值转化为实际的商业收益是一个难题。因此，企业需要通过深入的数据分析和挖掘，找到数据中的商业机会和创新点，才能实现数据价值的最大化。

2 大数据时代下计算机网络信息安全的重要性

2.1 个人隐私的保护

随着大数据时代的到来，个人信息的收集、存储和利用变得更加普遍。无论是社交媒体、在线购物还是移动应用等各种互联网服务，都在不断收集用户的大量数据，包括个人身份信息、行为习惯、地理位置等。这些数据被用于用户画像、个性化推荐等方面，为用户提供了更好的服务体验。然而，如果这些信息被不法分子窃取或滥用，个人隐私将受到极大的侵犯。因此，计算机网络信息安全的重要性在于保护用户的隐私权，防止其个人信息被非法获取、传播或利用。为了实现这一目标，需要加强数据加密技术的应用，建立完善的个人信息保护法律、法规体系，提高用户的安全意识和防范能力；

2.2 商业机密和知识产权的保护

在大数据时代，企业对数据的依赖程度不断加深，商业机密和知识产权成为企业最重要的资产之一。网络攻击者可能试图入侵企业网络，窃取商业计划、研发成果、客户信息等敏感数据，给企业带来巨大的经济损失。因此，计算机网络信息安全的重要性在于保护企业的商业机密和知识产权，维护其竞争优势和可持续发展。为了实现这一目标，需要加强网络安全技术的研发和应用，建立健全的数据安全管理机制，提高员工的安全意识和保密意识。同时还要加强国际合作，共同打击跨国网络犯罪活动，维护全球信息安全秩序；

2.3 国家安全的维护

在大数据时代，国家的政治、经济、军事等重要信息大多通过计算机网络传输和存储。这些信息包括国家机密、战略计划、军事部署等，如果被不法分子窃取或滥用，将会对国家的安全构成威胁。例如，黑客攻击可能导致政府机关的网络瘫痪，影响政府的行政能力和公信力；敌对势力可能通过网络渗透获取国家机密，对国家的战略安全造成严重威胁。因此，保障计算机网络信息安全对于维护国家的整体安全至关重要。为了实现这一目标，需要加强网络安全技术的研发和应用，建立健全的数据安全管理机制，提高国家的网络安全意识和防范能力；

2.4 社会稳定和信任的维护

计算机网络信息安全的威胁不仅可能导致个人、企业和国家的损失，还可能对社会稳定和信任产生负面影响。如果用户对在线交易、电子支付、社交网络等不再信任，整个社会的信息化进程将受到阻碍。例如，如果用户对电子支付的安全性有疑虑，他们可能会选择不使用这种支付方式，这将对电子商务的发展造成影响；如果用户对社交网络的隐私保护措施不满意，他们可能会减少使用社交网络的频率，这将对社交媒体的发展造成影响。因此，计算机网络信息安全的重要性在于维护社会的稳定和信任，推动数字经济和社会发展。

3 大数据时代下计算机网络信息安全存在的隐患

3.1 网络攻击的多样性

网络攻击的多样性在大数据时代显得尤为突出。传统网络攻击手段如病毒、蠕虫、木马仍然存在，新型的网络攻击手段也不断涌现，包括网络钓鱼、勒索软件以及无文件攻击等。这些攻击手段危害网络系统的正常运行，直接威胁到用户的隐私和信息安全。大数据背景下，计算机网络系统自身的漏洞也是导致信息安全问题的主要原因，在安装计算机系统的过程中，可能因为系统自身问题或者环境方面的影响，计算机系统会存在一定的漏洞和问题；

3.2 安全漏洞的普遍存在

大数据时代下，计算机网络系统由于其规模庞大、软、硬件环境复杂的特点，安全漏洞的存在变得非常普遍。这些安全漏洞可能由于设计缺陷、编程错误、配置不当等各种原因引起。黑客利用这些安全漏洞，可以通过恶意攻击或入侵的方式，获取系统的权限并控制整个网络。这不仅导致数据

泄露和财产损失,还会破坏系统的正常运行,如何有效地发现和修复系统中的安全漏洞,成为亟待解决的问题;

3.3 数据泄露与隐私保护

在互联网时代,个人的敏感信息如姓名、地址、电话号码、银行账户等很容易被泄露。一旦这些信息落入不法分子手中,就可能导致身份盗窃、诈骗等问题;此外,个人在互联网上的行为轨迹也会被记录下来,包括搜索历史、购物记录、社交媒体活动等。这些数据不仅暴露了个人的兴趣爱好和消费习惯,还可能被用于精准广告和个人定向推送;其次,企业的商业机密也面临着风险。企业在运营过程中会产生大量的商业数据,包括客户信息、销售数据、研发成果等。如果这些数据泄露给竞争对手或恶意人士,将对企业造成巨大的经济损失和声誉损害;另外,一些敏感行业如金融、医疗等对数据的保护要求更高,一旦数据泄露将引发更严重后果。

4 大数据时代下计算机网络信息安全应对策略

4.1 重视部署 IPv6 网络

部署 IPv6 网络,首先需要确定 IPv6 的部署计划和时间表,考虑现有网络设备的支持情况、IPv6 过渡方案及培训和测试的时间安排等因素;其次,要升级网络设备以支持 IPv6 协议,包括路由器、交换机、防火墙等设备。在 IPv6 网络中,每个设备都需要唯一的 IPv6 地址,要为每个设备分配 IPv6 地址,确保地址的唯一性。IPv6 网络中的路由协议与 IPv4 不同,需要重新配置路由协议以确保网络的连通性和稳定性,由于 IPv6 网络的安全性比 IPv4 更高,但仍存在一些安全威胁或隐患,要实施更加严格的安全措施,如访问控制、加密通信等,确保网络安全;最后,在部署 IPv6 网络之前,也要对用户开展测试和培训,使他们更加安全地使用 IPv6 网络,确保网络使用的稳定、安全;

4.2 使用 WAF 防火墙和入侵检测系统联动

使用 WAF 防火墙和入侵检测系统联动。首先,要部署 WAF 防火墙,这是一种基于 Web 应用的安全防火墙,可以阻止 SQL 注入、XSS 攻击、CSRF 攻击等常见的 Web 攻击。通过部署 WAF 防火墙,可以有效防止黑客利用 Web 漏洞对网站进行攻击;其次,需要实时监控网络流量,入侵检测系统可以实时监控网络流量,检测并阻止潜在的入侵行为。通过实时监控网络流量,可以及时发现并处理异常行为,从而保护网络安全;同时,将 WAF 防火墙和入侵检测系统联动,可以实现更加完善的安全防御机制。当入侵检测系统发现异常行为时,可以通过 WAF 防火墙自动阻断访问请求,避免网络受到攻击。安全设备的更新和升级可以修复已知的漏洞和弱点,提高设备的防御能力。因此,要定期更新和升级 WAF 防火墙和入侵检测系统等安全设备,建立安全事件响应机制也非常重要。当发生安全事件时,要及时响应并采取措施进行处理,可以在发生安全事件时快速响应、迅速处置,降低损失。

综上所述,使用 WAF 防火墙和入侵检测系统联动是提高网络安全性的有效措施之一;

4.3 安装防病毒软件系统

安装防病毒软件系统是保障计算机网络安全的重要措施之一。在大数据环境下,由于数据量的增加,病毒的感染率也会相应提高。要采取以下实施策略。首先,企业需要选择适合自身的防病毒软件。市场上有多种防病毒软件可供选择,企业需要根据自身需求和实际情况选择适合的软件。其次,定期更新病毒库也是必要的。防病毒软件的病毒库需要定期更新,以识别新出现的病毒并及时防范,实时监控计算机病毒也非常重要。防病毒软件可以实时监控计算机病毒,及时发现并处理异常行为;此外,建立安全事件响应机制也必不可少。当发生安全事件时,要及时响应并采取措施进行处理,可以在发生安全事件时快速响应、迅速处置,降低损失;最后,加强员工安全意识培训也是关键。员工是企业网络安全的第一道防线,加强员工安全意识培训可以提高员工的安全意识和防范能力,减少发生安全事故;

4.4 加强培养网络安全的意识

在当前网络攻击日益猖獗的情况下,仅仅依靠技术手段并不能完全保障网络安全。要采取以下实施策略。首先,企业应该定期组织网络安全教育和培训活动,向员工传授网络安全知识和技能,提高员工的安全意识和防范能力;其次,企业应该制定完善的网络安全管理制度和规范,明确各项安全措施的具体要求和操作流程,确保员工能够按照规范执行;同时,企业还应该强化密码管理,要求员工使用强密码并定期更换密码,避免长时间使用相同密码或弱密码;此外,企业还要加强社交工程防范,加强员工的防范意识,不轻易泄露个人信息和公司机密;另外,建立安全事件响应机制也必不可少,它可以在发生安全事件时快速响应、迅速处置,从而降低损失;最后,企业可以与其它企业或机构开展合作与交流,分享经验和技术,共同应对网络安全的威胁。

综上所述,加强培养网络安全的意识也是保障计算机网络安全的重要策略之一。

(下转第 8 页)

下，匆忙启动信息化战略。以致在后续的战略实施过程中，引发了一系列的安全性、性能以及时间延迟、成本超支等问题，最后，导致了数字化转型的虎头蛇尾，得不偿失。因此，企业数字化转型是一个长期过程，做好数字化转型，首先应做好充分的信息化规划。可以考虑从如下几个方面着手：

第一，做好充分调研，分析当前企业信息化短板及现状；第二，做好长期规划与短期规划相结合，长期规划结合企业战略远景，短期规划侧重解决当前实际问题；第三，构建信息化建设管理机制，保证信息建设真正落到实处；第四，组建信息化专业团队，培养既懂业务又懂技术的复合型人才。

同时，企业信息化过程中还应警惕“一买到位”的误区。调查显示，IT 系统占企业信息化成功的因素不足 40%[4]，脱离信息化规划直接买软件易导致如下问题：

第一，价格昂贵但并不适用。很多购买的大型系统依据“别人”的模式创建，未必适合企业实际的场景需要；

第二，定制化开发工作量巨大，有时修改和二次开发的时间消耗可能已经超过全新开发的工作量。

5.5 应坚持业务驱动，而非技术驱动

对于大多数科技公司，由于拥有良好工程师文化、代码文化，其核心竞争力往往是领先的技术或知识产权，工程师往往有较强的技术情结和对技术的狂热追求，技术人员福利待遇好、所在企业话语权高，这样很易让员工以为公司以技术为驱动并引以自豪。然而公司的本质是商业组织，无论是技术、产品、设计、财务、市场等，一定都是为了业务服务而存在，只是在业务驱动的后面，哪方面发挥的力量更大一些。只有业务需要才能倒逼技术向前推动，技术往往不是源头，业务需求才是根本，舍弃业务需要而一味追求技术反而是舍本逐末。因此一切技术问题，都要服从业务需要、产品交付和市场反馈为出发点。

企业 IT 架构的选择应以匹配业务目标为根本，选择一个最合适的架构方案。不能为了“学技术”而“用技术”，不能为了“微服务”而“微服务”。企业的 IT 架构方案应该是以业务支撑性、系统可用性、系统扩展性、成本投入、可持续运维等多方面作为评判依据，进行综合选择。如果为了学习微服务架构，而选择一个完美的微服务框架，也许方法论很科学，模型、文档、验证报告也很完善，里面可能还附加了很多业界标杆和最佳实践，但企业如果按照这个去做，未必能收到很好的效果。原因是当前数字技术的高速发展，没有任何平台或架构能保证自身在三到五年后还很适用，永远不会被淘汰；同时，如果一旦掌握这些技术的核心人员离职，企业将面临高额的招聘费用，短期内系统可能会陷入无人维护的瘫痪局面。

6 结语

企业 IT 技术架构在不断演进，没有万能的银弹式架构，很多互联网企业的技术架构，也是从最初的单体架构模式，逐步演进到基于分布式的微服务架构，适合业务发展的技术架构才是好的技术架构。

微服务架构并不一定是最好的企业开发架构，是否采用微服务架构需要综合评估利弊后再进行方案选定。微服务一般是不得已而为之，主要用在系统迭代快、变化多的需求场景中，比较适合互联网公司。如果通信企业系统已经成熟、稳定，架构设计良好，没必要进行微服务拆分。即便是单体应用，通过分布式的部署，一样可以解决高可用性和高负载问题，切忌为了微服务而微服务。

参考文献

[1] 李延明.基于“松耦合”的职业院校智能化校园建设模式——以兰州石化职业技术学院信息化建设为例[J].世界教育信息，2019，23：12.
[2] 胡 越.微服务架构下公安情报协作平台构建研究[D].北京：中国人民公安大学，2018.
[3] W.Brian Arthur.技术的本质[M].浙江：浙江人民出版社，2018：45.
[4] 沈鹰尔.信息化投资不是买软件[J].企业管理，2019，12：103-105.

作者简介

龚 平（1986-），男，硕士，中级工程师，研究方向：智能信息系统、企业信息化。

（上接第 38 页）

5 结语

综上所述，大数据时代下，要认识到计算机网络已经成为信息传输、存储和处理的核心基础设施，其中的计算机网络信息安全的重要性日益突出。大数据的广泛应用和传播，使得网络攻击手段不断翻新，威胁日益复杂，对网络安全提出了更高的要求。因此，必须关注大数据时代的特点，分析大数据时代下计算机网络信息安全问题并提出相应防护策略和措施，更好地保护个人隐私和财产安全，推动数字经济的安全、稳定发展。

参考文献

[1] 刘占凤.大数据时代如何加强计算机网络信息安全管理[J].网络安全技术与应用，2023，（7）：162-164.
[2] 倪 瑞，梁嫘良，马雯阳.大数据时代背景下的网络信息安全管理分析[J].数字通信世界，2023，（6）：188-190.
[3] 梁超强.大数据时代计算机网络信息安全与防护研究[J].大众科技，2022，24（12）：1-3.
[4] 金 秋，裴 斐.大数据时代背景下计算机网络信息安全教学的创新研究[J].中国新通信，2022，24（23）：107-109.
[5] 曾德胜，何 健，宁建飞等.大数据时代计算机网络信息安全防护策略分析[J].软件，2022，43（9）：64-66.
[6] 张 冰.基于大数据时代下计算机网络安全问题及应对方法探讨[J].中国新通信，2021，23（24）：52-53.

作者简介

田 秋（1993.02-），女，汉族，贵州余庆人，本科学历，助教，研究方向：医学信息工程。