大数据背景下计算机网络信息安全及防护策略研究

姚庆来
中国机械设备工程股份有限公司　北京　100073

摘　要：现如今，人们的日常生产及生活都已经离不开大数据的有力支撑，大数据时代已经到来。但是人们在享受到大数据时代的便利的同时，也同样面临着巨大的网络安全隐患。近年来各种网络安全事件频发已经引起了各行业的广泛关注，如何在有效利用大数据时代的优势的同时也对网络安全进行防护已经成为当下相关工作者研究的重点。

关键词：计算机网络；信息安全；防护

1 大数据的概述

大数据是指规模庞大、结构多样、速度快和价值密度低的数据集合。它涵盖了传统数据库管理工具难以处理的数据，包括结构化数据、半结构化数据和非结构化数据。大数据的产生主要源于互联网、社交媒体、物联网和传感器技术的发展，以及各行各业在日常业务中产生的海量数据。大数据具有“4V”特征：Volume（数据量大）、Velocity（数据速度快）、Variety（数据多样性）和Value（价值密度低）。第一，数据量大意味着数据规模庞大，通常以TB、PB甚至EB来衡量。第二，数据速度快意味着数据以极高的速度持续产生和流动，要求实时或近实时地处理和分析。第三，数据多样性意味着数据来源和数据类型多样，包括结构化数据（如数据库中的表格数据）、半结构化数据（如日志文件和报告）和非结构化数据（如文本、图像和音频）。第四，价值密度低意味着大数据中的很多数据可能并不具备即时的商业价值，但精确、及时地分析和挖掘这些数据可以为决策提供有力的支持和见解[1]。大数据的应用涵盖了各个领域，如金融、医疗、零售、制造业、交通、能源等。借助大数据技术，企业可以更深入地了解客户需求，制定更有效的营销策略；医疗机构可以利用大数据来提高诊断准确性和治疗效果；政府可以利用大数据分析来优化城市规划和交通流动等。

2 大数据时代计算机网络信息安全防护的重要性

在大数据时代，计算机网络信息安全的防护显得更为重要。大数据时代，各种形式的数据不断增长，网络通信成为了信息的主要传输媒介。然而，与此同时，网络安全威胁也愈发严峻，如黑客攻击、恶意软件、数据泄露等问题频频出现。因此，加强计算机网络信息安全防护，对于保护用户的个人隐私和企业的商业机密，维护信息的完整性和可用性，具有重要意义。首先，计算机网络信息安全防护保护了用户的个人隐私。在大数据时代，个人信息泄露的风险日益增加，黑客可以通过网络窃取用户的个人信息，用于非法活动。如果没有有效的安全防护，用户的个人信息如身份证号码、手机号码、银行账户等就可能被他人不经授权地使用，给个人造成不可逆的损害。因此，加强计算机网络信息安全防护，对于保护用户的个人隐私至关重要。其次，计算机网络信息安全防护维护了企业的商业机密。在大数据时代，企业的核心竞争力往往来自于其所拥有的客户数据、产品设计、市场策略等商业机密。黑客攻击和企业间谍行为等安全威胁对企业的商业机密构成了巨大威胁。如果企业的商业机密被泄露，将会导致企业的竞争地位受损，严重的还可能导致企业倒闭。因此，加强计算机网络信息安全防护，对于企业的发展和生存具有重要影响[2]。计算机网络信息安全防护保障了信息的完整性和可用性。大数据时代的数据量庞大且多样，数据的完整性和可用性成为了重要问题。恶意攻击者可能通过篡改数据或者破坏数据的可用性等方式来损害信息的完整性和可用性。无论是个人用户还是企业，都需要确保其信息的完整性和可用性，以避免不必要的损失。因此，加强计算机网络信息安全防护，对于确保信息的完整性和可用性至关重要。

3 引发计算机网络安全风险的主要因素

3.1 网络安全防护方式比较落后

第一，安全技术跟不上攻击手段的演变。黑客攻击手段不断发展和改进，包括零日漏洞利用、社交工程学攻击、隐蔽威胁等高级威胁手段。而当前网络安全防护技术尚未充分应对这些新型威胁，导致防护措施相对滞后。第二，网络安全意识薄弱。在许多个人和组织中，对网络安全风险和防护措施的认识仍然不够，缺乏安全意识和自我保护意识。这使得人为因素成为攻击者攻击的主要目标，例如社交工程学攻击中的钓鱼攻击[3]。第三，缺乏综合而全面的安全防护措施。现有的安全防护

方式更多是针对特定威胁或特定层面的防护，而缺乏整体性的综合防护。例如，许多组织重视数据安全，但忽视了物理安全、员工安全意识培训等方面的防护。第四，网络安全防护的人力和资源投入不足。随着网络攻击的复杂性增加，专业人才和先进设备的需求也随之增加。然而，许多个人和企业在网络安全防护方面的投入仍然不足，导致防护能力相对较弱。

3.2 黑客攻击带来的安全风险

黑客利用未经公开披露的软件或系统漏洞，通过网络入侵目标系统。这种攻击方式使得目标系统暴露在攻击者的威胁下，导致数据泄露、系统瘫痪等严重后果。黑客通过各种手段获取用户的个人信息、财务数据或企业的商业机密，从而导致个人和企业面临隐私泄露、经济损失及声誉损害等风险。黑客通过向目标系统发送大量伪造的网络数据流量，使其超负荷运行，从而导致系统崩溃或服务不可用，给目标系统带来严重的经济损失和声誉损害。黑客通过恶意软件感染大量计算机，形成僵尸网络，然后利用这些僵尸计算机进行网络攻击，如发送垃圾邮件、进行网络钓鱼等。这种攻击方式可能导致系统运行缓慢、流量过载等问题，造成业务中断和经济损失[4]。黑客通过虚假身份或欺骗手段获取用户的敏感信息，如用户名、密码、银行账号等。这种攻击可能导致个人财产损失、身份盗窃等严重后果。黑客通过在系统中植入后门程序，使得系统可被远程控制或绕过系统防护，进而进行数据窃取、信息篡改、恶意操作等活动。这种攻击方式对系统的安全性和可信度构成了严重威胁。

3.3 网络安全制度不够健全

在一些组织或机构中，网络安全责任没有明确的划分和分工。缺乏专业人员负责网络安全事务，导致安全措施不够全面和有效。网络安全制度缺乏明确的规范与标准，导致各个组织或机构在网络安全防护方面缺乏统一的要求和标准。这使得网络安全的防护措施不够规范和有效。如果网络安全制度中没有明确的监管和处罚措施，违反网络安全规定的行为可能得不到及时惩处。这可能鼓励了违规行为，提高了网络安全风险。网络安全制度缺乏定期的安全评估和检查机制，难以及时发现和解决安全问题。这导致隐患可能长时间存在，给黑客攻击提供了机会[5]。

4 大数据时代计算机网络信息安全及防护策略

4.1 建立动态化的监测与维护机制

在大数据时代，计算机网络信息安全面临着更为复杂和严峻的挑战。为了有效防范网络安全威胁并保护用户数据隐私，我们需要建立动态化的监测与维护机制。（1）实时监测并及时响应：建立实时监测系统，对网络流量、用户行为、系统日志等进行持续监控。及时发现和分析异常活动，快速做出反应并进行必要的处置，以减少潜在的安全威胁。（2）强化访问控制与身份认证：采用双因素身份验证、访问权限控制等安全机制，确保只有经过授权的用户能够访问敏感数据和系统资源。建立严格的身份验证流程，减少非法入侵和数据泄露的风险。（3）数据加密与隐私保护：对敏感数据进行加密处理，确保数据在传输和存储过程中的安全性。采用隐私保护技术，如数据脱敏、数据匿名化等，最大限度地保护用户隐私和敏感信息[1]。（4）加强安全教育与培训：提高用户和员工的网络安全意识，增强防范网络攻击和社会工程学攻击的能力。定期进行网络安全培训，确保用户能够正确使用和管理网络资源，避免由个人疏忽导致的安全漏洞产生。（5）使用先进的安全技术与工具：采用入侵检测与防御系统、数据库防护工具、行为分析等先进的安全技术，提高对网络威胁的识别和防范能力。确保网络安全设备、软件和系统的及时更新和升级，以修复已知漏洞和弥补安全风险。（6）建立网络安全应急响应机制：制定完善的网络安全应急预案和修复机制，一旦发生网络安全事件，能够迅速、有序地响应和处理，减少损失和影响。

4.2 加强对网络传输数据的加密处理

在大数据时代，网络传输的数据量庞大且复杂，对计算机网络信息安全的保护提出了更高的要求。为了确保数据在传输过程中的机密性和完整性，加强对网络传输数据的加密处理成为一项重要的安全策略。首先，可以采用传输层安全协议（TLS）或安全套接字层（SSL）来加密网络数据。这些协议提供了端到端的加密通信，确保数据在传输过程中不会被窃取或篡改。同时，设立有效的密钥管理机制，确保密钥的安全存储和传输，进一步加强数据的保密性。其次，可以使用虚拟专用网络（VPN）技术来实现加密传输。VPN通过在公共网络上建立加密隧道，将数据传输加密，在保证通信安全的同时，还可以隐藏真实的网络地址，增加了数据的保护层次。另外，对于敏感数据的传输，可以采用对称加密和非对称加密相结合的方式。对称加密速度快，但密钥传输存在风险；非对称加密安全性高，但速度较慢。使用混合加密算法，可将二者的优势结合起来，既保证了安全性，又提高了数据传输的效率。除了加密传输，应加强网络边界和终端节点的安全防护。通过安全防火墙、入侵检测系统（IDS）和入侵防御系统（IPS），对网络边界进行监控和防御，及时发现和阻止

潜在的攻击[2]。同时，加强对终端节点的安全管理，定期更新操作系统和软件的补丁，禁用不必要的服务，加强用户权限管理，有效防止终端安全漏洞的利用。加强对员工和用户的安全教育培训也是关键。提升他们对网络安全的认知和意识，教授正确的网络安全操作方法，警惕网络钓鱼、恶意链接、社交工程等攻击手段，降低内部人员存在的风险。

4.3 使用杀毒软件

在大数据时代，计算机网络信息安全的保护变得尤为重要。为了抵御各种恶意软件和病毒的威胁，使用杀毒软件是一项必要的安全策略。杀毒软件通过实时监测，识别和清除计算机病毒，有效保护计算机网络的安全。杀毒软件能够实时监测计算机系统中的文件和程序。它运行于后台，持续不断地监控系统的各个文件和程序的行为。一旦发现可疑的活动或存在潜在威胁的文件，它会立即采取相应措施进行处理，以阻止恶意软件和病毒的入侵。杀毒软件提供定期全盘扫描功能。通过定期进行全盘扫描，杀毒软件能够检查整个计算机系统中的文件和程序，确保没有任何潜在的威胁存在。这样可以保证计算机网络的整体安全性，减少潜在的病毒传播和数据泄露的风险。杀毒软件的供应商会定期更新病毒数据库，并为用户提供实时的病毒库更新[3]。随着新的病毒不断出现，杀毒软件持续地更新病毒数据库，以及时识别和清除新出现的威胁。这样可以确保杀毒软件具备对新型病毒的识别和清除能力，提高计算机网络的抵御能力。随着网络安全威胁的不断增加，许多恶意网站会诱导用户点击链接或下载文件，以进行网络钓鱼、恶意广告等攻击。使用杀毒软件可以拦截用户访问这些恶意网站，并给予警告和阻止，从而保护用户免受恶意攻击。

4.4 加强软硬件系统安全防护

在大数据时代，计算机网络的信息安全和防护至关重要，而加强软硬件系统的安全防护是保护计算机网络信息安全的核心策略之一。在加强软硬件系统的安全防护方面，可以采取以下措施：首先，对硬件设备进行安全保护。保证服务器、路由器和交换机等关键设备的安全，比如加密通信内容、配置安全访问密码和开启硬件防护功能等，以阻止非授权的访问和攻击。此外，设置物理安全措施，如控制机房的进入权限、安装监控摄像头等，以确保硬件设备的物理安全。其次，对软件系统进行安全加固。定期更新操作系统、数据库和相关应用程序的安全补丁，以修复已知漏洞和提升系统的安全性。加强对软件系统的访问控制，限制敏感权限的使用，并定期审计和监测系统中的异常行为，从而提前发现和阻止潜在的攻击[4]。

结束语

总的来说，在计算机技术的全面普及和应用之下，计算机已经成为了大众生活和工作中的关键内容，在这一背景下就形成了海量数据信息，这些信息的出现将会给用户个人利益带来重大影响。为了最大程度上提升计算机网络信息安全，就要重视起安全防护，加大防护力度，树立防护意识，通过相应防护技术和措施促进网络信息安全，促进计算机事业的良好发展。

参考文献

[1]龙振华.大数据时代计算机网络信息安全及防护策略[J].中国管理信息化，2019，22（06）：161-162.

[2]郭皓迪.大数据时代计算机网络信息安全及防护策略[J].电子技术与软件工程，2019，（24）：195-196.

[3]彭博.网络环境下计算机信息安全与合理维护分析[J].中国管理信息化，2020，23（24）：206-207.

[4]王魏,赵奕芳.大数据时代计算机网络信息安全及防护策略[J].中阿科技论坛(中英文),2022(01):72-75.

[5]张璐明.大数据时代计算机网络信息安全及防护策略分析[J].网络安全技术与应用,2021(03):153-155.