大数据下的计算机网络信息安全措施

徐 喆
中通服咨询设计研究院有限公司 江苏 南京 210019

摘 要：随着互联网的普及和信息技术的不断发展，大数据时代已经来临，网络信息安全防护面临着前所未有的挑战。在这个背景下，加强计算机网络信息安全防护显得尤为重要。本文将探讨在大数据时代下如何加强计算机网络信息安全防护的措施。

关键词：大数据下；计算机网络；信息安全；措施

引言

随着互联网的广泛普及和信息技术的持续发展，我们已迈入大数据时代。在这个时代，计算机网络信息安全防护显得尤为重要，因为数据的价值不仅在于其数量，更在于其质量和安全性。然而，网络攻击和恶意软件的肆虐，给企业和个人的信息安全带来了严重威胁。因此，加强计算机网络信息安全防护措施是至关重要的。

1 大数据和网络信息安全概述

1.1 大数据概述

在信息爆炸的时代，大数据已经成为了一个家喻户晓的词汇。它代表了海量、复杂、快速变化的数据集，对于各行各业来说，大数据都发挥着越来越重要的作用。大数据，又称巨量数据，是指数据量巨大、复杂度高、处理速度快的数据集合。这个数据集合可以是结构化数据、半结构化数据，也可以是非结构化数据。大数据的产生速度非常快，每天都会产生大量的数据，而且这些数据的来源和格式各不相同[1]。同时，大数据的应用非常广泛，几乎渗透到了各个领域。在商业领域，企业可以利用大数据进行市场分析、用户行为分析等，从而制定更加精准的商业策略。在金融领域，金融机构可以利用大数据进行风险管理、投资分析等，提高金融业务的效率和准确性。在医疗领域，医疗机构可以利用大数据进行疾病预测、治疗方案优化等，提高医疗质量和效率。此外，大数据还可以应用于城市规划、环境保护、交通管理等领域。

1.2 网络信息安全概述

随着信息技术的飞速发展和互联网的广泛应用，信息安全问题日益凸显。网络信息安全旨在保护网络系统免受未经授权的入侵和破坏，确保网络数据的机密性、完整性和可用性。这不仅关系到企业的商业机密和客户的个人隐私，还对国家安全和社会稳定具有重大意义。首先，商业机密和客户隐私是企业最重要的资产之一，一旦泄露将会给企业带来无法估量的损失。网络信息安全可以有效地保护商业机密和客户隐私，防止泄露事件的发生。通过采取严格的安全措施，如数据加密、访问控制、安全审计等，可以确保商业机密和客户隐私不被未经授权的人员获取和利用。其次，网络系统是企业和客户进行业务交流和信息共享的重要平台。网络信息安全可以有效地保护网络系统的稳定和安全，防止网络攻击和破坏事件的发生。通过采取防火墙、入侵检测系统、安全审计等安全措施，可以及时发现并阻止恶意攻击行为，确保网络系统的正常运行。最后，网络信息安全是国家安全和社会稳定的重要保障。随着互联网的普及和信息技术的广泛应用，网络犯罪和网络恐怖主义行为逐渐增多，给国家安全和社会稳定带来了极大的威胁。网络信息安全可以有效地防止网络犯罪和网络恐怖主义行为的发生，保障国家安全和社会稳定。

2 计算机网络安全存在的问题

2.1 网络钓鱼

网络钓鱼是一种针对个人用户和企业的重要网络安全威胁。这种攻击方式常常利用虚假的电子邮件、链接或网站来获取用户的敏感信息，如用户名、密码、信用卡号等，这些信息可以用于进行进一步的恶意活动，如身份盗用、诈骗、财务损失等。并且，网络钓鱼攻击通常采用伪装成合法网站或服务的方式，诱骗用户点击恶意链接或下载恶意附件。这些链接可能会将用户重定向到含有恶意软件的网站，或者通过社交工程手段获取用户的个人信息。社交工程是一种利用人类心理和社会行为的弱点，如信任、好奇心、欲望等，来获取敏感信息的攻击方式。此外，网络钓鱼攻击的危害性非常大。一旦攻击者成功获取了用户的个人信息，他们就可以利用这些信息进行各种恶意活动。例如，攻击者可以使用这些信息登录到用户的银行账户、在线购物账户等，进行欺诈活动；攻击者还可以使用这些信息进行身份盗用，

给用户带来长期的困扰和损失。

2.2 恶意软件

恶意软件是一种计算机程序，旨在破坏、窃取或传播数据，并且通常以隐蔽的方式进行这些活动。这些软件可以通过各种途径传播，如网络、电子邮件、社交媒体等，给计算机系统和数据带来重大威胁。恶意软件有多种类型，包括病毒、蠕虫、特洛伊木马等，这些不同类型的恶意软件具有不同的特点和攻击方式。其中，病毒是一种自我复制的恶意软件，它可以通过感染其他文件或程序来传播。病毒通常隐藏在其他程序中，当用户运行这些程序时，病毒就会感染用户的计算机系统。病毒可以导致系统崩溃、数据损坏或窃取等严重后果。而蠕虫是一种利用网络进行传播的恶意软件，它可以通过扫描网络中的计算机，寻找漏洞并利用这些漏洞来传播自身[2]。蠕虫可以导致网络性能下降、数据泄露等严重后果。特洛伊木马则是一种伪装成合法程序的恶意软件，它通常隐藏在其他程序中，当用户运行这些程序时，特洛伊木马就会在后台运行，并窃取用户的个人信息或进行其他恶意活动。特洛伊木马可以导致用户信息泄露、财务损失等严重后果。

2.3 拒绝服务攻击

拒绝服务攻击（Denial of Service Attack，简称DoS攻击）是一种常见的网络攻击方式，其目的是通过发送大量的无效请求或垃圾数据，耗尽服务器的资源，使其无法响应正常请求，从而导致网站或应用程序无法访问。这种攻击方式在互联网上广泛存在，对网站和网络服务提供商造成了严重的威胁和损失。一方面，拒绝服务攻击的主要方式包括洪水攻击、同步攻击、畸形报文攻击等。其中，洪水攻击是最常见的一种，它通过发送大量的无效请求或垃圾数据，使得服务器无法处理正常的请求。同步攻击则利用了TCP协议的缺陷，通过发送大量的虚假连接请求，使得服务器资源被耗尽。畸形报文攻击则是利用了某些协议的漏洞，使得服务器无法处理正常的请求。另一方面，拒绝服务攻击的危害性非常大。一旦攻击者成功实施了拒绝服务攻击，受害者的网站或应用程序将无法正常访问，给用户带来极大的不便和损失。同时，拒绝服务攻击还会导致服务器的资源被耗尽，使得服务器的维护和管理变得更加困难和昂贵。此外，拒绝服务攻击还会影响服务提供商的网络服务质量，给其他用户带来不必要的困扰和损失。

3 大数据时代下加强计算机网络信息安全防护的措施

3.1 提高计算机网络管理人员的专业素质

网络管理人员是维护网络正常运行和信息安全的关键力量，他们的专业素质直接关系到网络的安全与稳定。因此，加强计算机网络管理人员的专业培训和技术提升，对于防范网络攻击、保护数据安全具有至关重要的作用。第一，为了提高计算机网络管理人员的专业素质，首先要加强专业培训和教育。企业和机构应该定期组织网络安全培训课程，让管理人员学习最新的网络安全知识和技术，了解网络安全形势和应对策略。培训内容可以包括入侵检测、漏洞修复、应急响应等，以提高管理人员的安全意识和应对能力。第二，知识交流和分享是提高计算机网络管理人员专业素质的重要途径。企业和机构可以定期组织技术研讨会和经验交流会，让管理人员分享网络安全方面的经验和心得。同时，可以邀请业内专家和学者进行授课和分享，让管理人员了解最新的网络安全动态和技术趋势。第三，实践经验和技能提升是提高计算机网络管理人员专业素质的关键环节。企业和机构应该提供实践机会，让管理人员在实际操作中掌握网络安全技术和应对策略[3]。例如，可以组织模拟网络攻击的演练活动，让管理人员体验真实场景下的应急响应和处理能力。同时，可以鼓励管理人员参与技术认证和考试，提高他们的技能水平和实践能力。第四，除了专业知识和技能外，培养综合能力和跨界思维同样重要。计算机网络管理人员需要具备多学科知识，包括计算机科学、网络安全、数据分析等领域。此外，他们还需要具备跨界思维和创新能力，能够从不同角度分析问题，提出创新的解决方案。企业和机构可以通过跨学科培训、案例分析等方式，培养管理人员的综合能力和跨界思维。

3.2 健全计算机网络信息安全防护机制

在大数据时代下，计算机网络信息安全防护面临着前所未有的挑战。随着信息技术的飞速发展，各种数据泄露、网络攻击事件屡见不鲜，给企业和个人带来了巨大的经济损失和隐私威胁。因此，加强计算机网络信息安全防护措施势在必行。（1）企业和组织应建立完善的安全管理制度，包括网络安全管理政策、安全审计制度、应急响应机制等。同时，应明确各级人员的安全职责和权限，确保安全制度的贯彻和执行。（2）针对网络安全威胁，应加强技术防护措施，如建立防火墙、实施访问控制策略、定期进行安全漏洞扫描和修复等。此外，应加强对重要数据的加密存储和传输，确保数据的机密性和完整性。（3）用户是网络安全的基石，应通过加强安全教育和培训，提升用户的网络安全意识。企业和组织应定期开展网络安全知识普及活动，帮助用户识别网络攻击和诈骗行为，提高防范能力。（4）政府应加

强网络安全的法律监管力度，完善相关法律法规，加大对黑客和网络犯罪的惩处力度。同时，应建立完善的网络安全举报机制，鼓励用户和企业积极举报网络犯罪行为。

3.3 积极应用病毒查杀软件

病毒查杀软件是专门用于检测和清除计算机病毒的工具，能够有效地防范和清除各种类型的病毒。通过使用病毒查杀软件，可以保护计算机免受病毒的攻击和感染，维护系统的正常运行和数据安全。首先，要选择可靠的病毒查杀软件是积极应用病毒查杀软件的基础。企业和机构应该选择经过权威机构认证、具有良好口碑和广泛用户基础的病毒查杀软件。这些软件通常具有强大的病毒库和实时监测功能，能够有效地检测和清除各种类型的病毒。其次，定期更新病毒库是保证病毒查杀软件有效性的关键。病毒库是包含已知病毒特征信息的数据库，用于比对和识别病毒。企业和机构应该定期更新病毒库，以便及时检测和清除新出现的病毒。同时，实时监测和定期扫描是防范和清除计算机病毒的重要手段。实时监测可以及时发现并阻止正在进行的病毒攻击，而定期扫描可以检测并清除潜在的病毒。企业和机构应该设置实时监测和定期扫描的计划，确保计算机始终处于安全状态[4]。最后，强化软件安全设置可以进一步提高病毒查杀软件的有效性。例如，开启自动更新功能、禁用不必要的网络共享、限制未知文件的执行等措施，都可以减少计算机感染病毒的风险。

3.4 建立完善的应急响应计划

在当今高度互联的世界中，网络安全事件随时都可能发生。为了应对这些突发的网络安全事件，建立完善的应急响应计划显得尤为重要。而在应急响应计划中，识别攻击是第一步。为了及时发现并识别网络攻击，需要建立有效的监控和检测机制。这包括对异常流量、异常行为以及各种已知的攻击手段进行监测和识别。企业和组织可以通过安装入侵检测系统（IDS）、网络监控软件和安全日志分析工具等来监控网络流量和用户行为，以便及时发现攻击迹象。第二，一旦识别出攻击，应立即采取措施隔离攻击源，以减小攻击的影响范围。这可能涉及到网络隔离、服务器隔离、数据隔离等措施。例如，可以通过防火墙、路由器等设备切断攻击者与目标之间的网络连接，或者关闭受攻击的服务器或服务，防止攻击扩散。此外，对于数据隔离，可以通过加密、访问控制等手段保护敏感数据不被非法访问或篡改。第三，及时向上级领导或相关部门报告攻击事件，以便组织内各部门协同应对攻击。同时，向相关机构报告攻击事件，如CERT（计算机应急响应小组）等。报告攻击事件不仅有助于内部协调和决策，还可以获得外部机构的支持和帮助。及时报告可以加快应急响应的速度，减少损失。第四，根据攻击类型和影响范围，采取适当的修复措施。这可能包括修复漏洞、更新软件、恢复数据等。修复攻击是应急响应计划中的关键步骤之一。企业和组织应建立快速响应机制，及时修复漏洞和更新软件，以防止攻击者利用漏洞进行进一步攻击。同时，对于被篡改或丢失的数据，应尽可能恢复到正常状态或进行备份恢复。第五，对攻击事件进行详细记录，并进行深入分析。这有助于了解攻击者的手段、动机和来源，以便改进安全策略和加强安全管理。

结语

综上所述，在大数据时代下，计算机网络信息安全防护是一项至关重要的任务。企业和机构应该采取有效的措施来防范和清除病毒，同时提高计算机网络管理人员的专业素质。通过这些措施，企业可以提高网络安全性和稳定性，保护企业资产和声誉，为大数据时代的发展提供有力保障。

参考文献

[1]叶维裕,陈景.大数据背景下计算机网络信息安全问题分析[J].电脑知识与技术,2020,16(32):69-70,75.

[2]段英杰.大数据时代计算机网络信息安全及防护探讨[J].信息记录材料,2020,21(11):222-223.

[3]陶冶,李汝峰.大数据背景下的计算机网络信息安全及防护措施[J].信息与电脑(理论版),2020,32(18):202-204.

[4]周迪民.大数据背景下的计算机网络信息安全及防护措施初探[J].办公自动化,2020,25(14):29-31.