大数据时代计算机网络安全管理策略探究

鄢梦思
水利部海河水利委员会引滦工程管理局　河北　唐山　064309

摘　要：大数据时代计算机网络安全管理策略是确保信息安全的关键手段。本文深入探讨了大数据时代网络安全管理的特殊性，包括数据规模庞大、数据类型多样和数据流动频繁等方面。针对这些特点，本文提出了建立完善的网络安全应急响应机制、采用先进的网络安全技术和工具等策略，旨在有效地保障大数据时代计算机网络安全。这些措施将有助于提高网络安全水平，确保单位和个人的信息安全。

关键词：大数据；计算机网络；安全管理

引言：在大数据时代，计算机网络安全管理策略的研究和实施至关重要。单位和个人都依赖于网络来存储、传输和处理数据，而这些数据往往包含着重要的隐私和商业机密。随着数据规模的不断扩大，网络攻击者有更多的机会窃取或篡改数据，给单位和个人带来巨大的风险。同时，数据类型的多样化也给网络安全管理带来了新的挑战，因为不同类型的数据需要不同的保护措施和安全策略。因此，探究大数据时代计算机网络安全管理策略，对于提高网络安全水平，保障数据安全具有重要意义。

1 大数据时代的网络安全问题

1.1 数据泄露风险

在大数据时代，数据的价值已经远远超过了传统的认识。它不再仅仅是一个简单的记录或统计，而是成为了一种可以揭示规律、预测未来、指导决策的重要资源。数据的关联性和预测性使得我们能够从海量的数据中挖掘出有价值的信息，从而更好地理解世界、把握市场、提升效率。然而，随着数据量的不断增加，数据泄露的风险也随之提高。一旦数据泄露，可能会被不法分子利用，造成严重的后果[1]。例如，个人信息泄露可能导致身份盗窃、金融欺诈等问题，给个人带来财产和精神的损失。

1.2 恶意软件和网络攻击

大数据中心，作为现代社会的信息枢纽，汇集了众多单位的核心信息和个人的隐私数据。这样的价值密度使得数据中心成为网络攻击的主要目标。从外部来看，恶意软件，如我们所知的勒索软件、病毒、木马等，都可能成为攻击者的工具，对数据中心进行渗透和破坏。一旦这些恶意软件侵入数据中心，它们可能会锁定数据，要求赎金以解锁，造成数据泄露或系统完全崩溃，给单位和个人带来巨大的损失。另外，我们还需要关注到一种更为复杂和隐蔽的攻击方式，那就是高级持续性威胁（APT）。这种攻击通常来自高度专业的黑客组织，他们对目标进行长期、持续的网络入侵活动。他们的目的可能是为了窃取商业机密、个人隐私，或者更为严重的，为了瘫痪某个关键基础设施。由于APT攻击的复杂性和长期性，它们往往比普通的网络攻击更难被察觉和防御。

1.3 网络安全法规和合规性问题

随着科技的快速发展和数字化进程的不断推进，网络安全问题已经上升为一个全球性的议题，不仅涉及到技术的安全，更与国家安全、社会稳定和公共利益息息相关。面对这一严峻的挑战，我们事业单位深知加强网络安全制定和执行工作的重要性与紧迫性。作为事业单位，我们肩负着保障网络安全、维护数据安全的重任。我们深知，遵守网络安全法规不仅是我们的义务，更是我们对社会的承诺。任何违反规定的行为，不仅可能受到法律的制裁，还会对我们的声誉和公信力造成严重的损害。

1.4 社交工程攻击

社交工程攻击，又称为SocialEngineeringAttack，是一种利用人类心理和社会行为的弱点，诱导或误导个体进行非授权的行为，从而窃取、篡改或破坏目标的攻击方式。在大数据时代，这种攻击方式变得更加常见和复杂。大数据技术的快速发展，使得攻击者可以轻易地获取并分析目标的数据，从而更加精准地掌握目标的心理和行为模式。攻击者可以利用这些信息，制定出更加具有针对性的攻击策略，使得社交工程攻击更加难以防范。例如，钓鱼邮件是一种常见的社交工程攻击手段。攻击者会伪装成信任的第三方，发送带有恶意链接或附件的邮件给目标。一旦目标点击这些链接或附件，攻击者就可以窃取目标的个人信息或账户密码。虚假网站也是一种常见的社交工程攻击手段。攻击者会建立一个与

真实网站非常相似的虚假网站，诱导目标输入个人信息或进行交易。一旦目标输入了个人信息或进行了交易，攻击者就可以窃取目标的个人信息或财产。

2 计算机网络安全管理策略

2.1 强化网络安全意识

为了确保网络环境的稳定与安全，计算机网络安全管理策略是不可或缺的重要环节。而在这其中，强化网络安全意识尤为关键。我们必须深刻认识到网络安全对于单位工作的正常运行和国家利益的重要性。随着互联网的广泛普及和数字化进程的加速，网络安全问题愈发凸显，恶意攻击、数据泄露、身份盗用等事件屡见不鲜，给国家安全和社会稳定带来了严重威胁。因此，我们事业单位必须时刻保持高度警惕，不断增强对网络安全的认知。提高全体职工的网络安全意识，我们应加强网络安全教育。事业单位应定期组织网络安全培训，向职工普及网络安全知识，传授防范技能，提高他们的安全防范意识和应对能力。同时，我们还应制定完善的网络安全策略和流程，明确各岗位的责任分工，确保网络安全工作的有序开展。

此外，加强对网络设备和系统的安全监控也是至关重要的。我们应建立健全的安全监控体系，实时监测网络设备和系统的运行状况，及时发现并处置潜在的安全风险，确保网络环境的稳定与安全。

2.2 定期进行安全培训和演练

计算机网络安全管理策略中，定期进行安全培训和演练是不可或缺的一部分。通过安全培训，职工可以深入了解网络安全的重要性，掌握防范网络攻击的基本技能，提高对网络安全的认知。同时，定期进行安全演练可以模拟真实场景，让职工在实践中学习和掌握应对网络安全事件的方法，提高应对能力和反应速度。这种培训和演练相结合的方式，能够有效地提高职工的安全意识和应对能力，为事业单位的网络安全提供有力保障。因此，定期进行安全培训和演练是计算机网络安全管理策略中的重要一环，值得我们持续关注和投入。

2.3 制定并执行严格的网络安全规章制度

计算机网络安全管理策略中，制定并执行严格的网络安全规章制度是至关重要的。规章制度是保障网络安全的基础，它明确了网络安全的标准和规范，为网络安全工作提供了明确的指导。规章制度的制定需要充分考虑单位的实际情况和需求，确保其具有针对性和可操作性。同时，规章制度应明确责任分工，确保各项安全措施得到有效执行。规章制度的执行是关键[2]。同时，应建立监督机制，对规章制度的执行情况进行定期检查和评估，及时发现问题并进行整改。制定并执行严格的网络安全规章制度是计算机网络安全管理策略的核心环节。通过规章制度的制定和执行，可以确保网络安全工作的有序开展，提高单位的网络安全水平。

2.4 采用先进的网络安全技术和工具

计算机网络安全管理策略中，采用先进的网络安全技术和工具是确保网络安全的重要手段。随着技术的发展，网络安全领域涌现出许多先进的技术和工具，如防火墙、入侵检测系统、加密技术等，这些技术和工具能够有效地提高网络的安全性。单位应了解并掌握当前最新的网络安全技术和工具，根据自身需求进行选择和应用。这些技术和工具能够实时监测网络流量，发现潜在的安全威胁，及时进行阻断和处置。注重技术的更新和升级。网络安全领域的技术发展迅速，事业单位应保持对新技术和新工具的关注，及时进行更新和升级，确保网络安全防护的时效性和有效性。采用先进的网络安全技术和工具是计算机网络安全管理策略中的重要环节。通过合理选择和应用这些技术和工具，能够提高网络的安全性，减少安全风险，为事业单位的发展提供有力保障。

2.5 建立完善的网络安全应急响应机制

随着信息技术的迅猛发展，计算机网络安全管理策略的建立和完善对于保障事业单位和个人的信息安全具有至关重要的意义。为了应对网络安全风险，事业单位应建立完善的网络安全应急响应机制，确保在发生网络安全事件时能够迅速、有效地应对，保障信息系统的安全稳定运行。事业单位应明确应急响应机制的目标和原则。目标应包括快速响应和处理网络安全事件，最大程度地减少损失和影响，尽快恢复网络正常运行等。原则应包括预防为主、快速响应、协调配合、及时总结等，以确保应急响应工作的有效开展。事业单位应完善组织架构和流程。组织架构应明确领导机构、技术小组、协调小组等各部门的职责和分工，确保各部门之间的协调和沟通。同时，应建立健全的流程，包括事件报告、分析、处置、恢复等环节，确保每个环节都有明确的责任人和时间要求，以提高应急响应的效率和准确性。事业单位应加强技术保障和人员培训。技术保障方面，应采用先进的安全技术手段，如防火墙、入侵检测系统、数据备份等，确保网络的安全性和稳定性。人员培训方面，应定期开展安全意识培训、技能培训、应急演练等，提高人员的安全意识和技能水平，增强他们应对网络安全事件的能力。

3 大数据时代网络安全管理的特殊性

3.1 数据规模庞大

大数据时代网络安全管理的特殊性主要表现在数据规模庞大这一方面。随着互联网和信息技术的飞速发展，大数据已经成为了各行各业不可或缺的重要资源。然而，随着数据规模的不断扩大，网络安全问题也日益突出。大数据时代的数据规模庞大，使得网络安全管理面临着前所未有的挑战。传统的网络安全管理方法往往难以应对如此大规模的数据量，需要借助新的技术和手段来提高管理效率。大数据时代的网络安全管理需要更加注重数据的保密性和完整性。由于大数据中包含了大量的敏感信息和重要数据，一旦泄露或被篡改，将对个人隐私和单位利益造成重大损失。因此，网络安全管理需要更加注重数据的保密性和完整性，采取更加严格的措施来保护数据的安全。大数据时代的网络安全管理需要更加注重数据的可用性和可扩展性。由于大数据中包含了大量的非结构化和半结构化数据，需要进行数据清洗、整合和分析才能得到有价值的信息。为了应对这一挑战，需要采取更加先进的技术和手段来提高管理效率，同时注重数据的保密性、完整性和可用性、可扩展性等方面的保护。只有这样，才能确保大数据时代的网络安全得到有效保障。

3.2 数据类型多样

随着各行各业对大数据的依赖程度不断增加，数据类型也变得越来越复杂和多样化。这使得网络安全管理变得更加困难和挑战性。数据类型的多样性使得网络安全管理需要更加全面的技术手段和更加细致的安全策略。不同的数据类型可能存在不同的安全风险和漏洞，需要针对不同的数据类型采取不同的安全措施和防护手段。不同类型的数据也可能存在不同的隐私和保密要求，需要采取更加严格的安全措施来保护用户隐私和单位商业机密。数据类型的多样性也使得网络安全管理需要更加注重数据的安全性和可靠性。在大数据时代，数据的来源和种类繁多，有些数据可能存在不准确、不完整或是虚假的情况。这就需要对数据进行有效的清洗、整合和分析，确保数据的真实性和可靠性。同时，也需要采取更加严格的措施来防止恶意攻击和数据泄露等安全事件的发生。数据类型的多样性也使得网络安全管理需要更加注重数据的安全存储和备份。由于大数据中包含了大量的敏感信息和重要数据，需要进行安全存储和备份以防止数据丢失或被篡改。同时，也需要采取更加先进的技术手段来提高数据存储和备份的可靠性和安全性。

3.3 数据流动频繁

随着信息技术的快速发展和网络攻击的不断升级，数据流动的频率和范围也在不断扩大。这使得网络安全管理需要更加注重数据的流动性和安全性。数据流动的频繁性使得网络安全管理需要更加注重数据的保密性和完整性。在大数据时代，数据流动频繁，保密性和完整性面临威胁。需采取严格的安全措施，如数据加密、访问控制、身份认证，确保数据传输和存储的安全性。数据流动的频繁性也使得网络安全管理需要更加注重数据的可用性和可扩展性[3]。在大数据时代，数据的流动和共享变得越来越普遍，数据的可用性和可扩展性也变得越来越重要。为了确保数据的可用性和可扩展性，需要采取更加先进的技术手段，如数据清洗、整合、分析等，对数据进行有效的处理和管理，确保数据的质量和可靠性。数据流动的频繁性也使得网络安全管理需要更加注重数据的安全存储和备份。由于数据的流动性和多样性，需要进行安全存储和备份以防止数据丢失或被篡改。

结语

随着技术的不断进步和威胁的不断变化，计算机网络安全管理策略也需要不断地更新和完善。只有紧跟时代的步伐，不断学习和掌握新的技术手段，才能更好地应对新的挑战和风险，确保单位和个人的信息安全。因此，我们需要保持敏锐的洞察力和创新精神，不断探索和实践新的网络安全管理策略，为大数据时代的信息安全保驾护航。

参考文献

[1]张全盛.计算机网络数据库的安全管理技术研究[J].网络安全技术与应用,2021(10):59-61.

[2]周萍.数据加密技术在计算机网络安全中的应用价值[J].软件,2021,42(10):168-170.

[3]戴冬生.计算机网络数据库的安全管理研究[J].信息与电脑(理论版),2021,33(19):226-228.