计算机信息化管理发展与网络安全防范措施

荆俊红
本溪开放大学　辽宁　本溪　117000

摘　要：计算机信息化管理的发展使得人们在工作和生活中极大地依赖于计算机和互联网，同时也使得网络安全问题愈发严重。基于此，本文首先对计算机信息化管理发展现状进行了分析，然后讨论了计算机网络安全技术的影响因素，包括病毒攻击、系统漏洞和网络钓鱼等方面，并提出了一些计算机网络安全防范的有效措施，以期为人们提供更好的网络安全保障。

关键词：计算机；信息化管理；网络安全防范

引言

随着计算机技术普及，计算机信息化管已经成为企业经营和管理的重要手段，但其也给企业和个人的网络安全带来了巨大的威胁。这种威胁带来的风险不仅仅是经济和商业风险，更是涉及到个人隐私、社会稳定等多个方面的问题。因此，有效的网络安全防范措施是保护信息系统和确保信息安全的关键所在。

1 计算机信息化管理发展现状

1.1 集成化

随着计算机技术的迅速发展和普及，各行各业纷纷采用计算机系统来管理和处理大量的数据和信息。集成化是计算机信息化管理发展的一个重要趋势，它旨在将各个不同的信息系统整合在一起，形成一个统一的整体，并能够实现数据共享和协同工作。例如，集成化的发展使得各种信息系统之间的交互变得更加方便快捷。不同部门和岗位之间可以通过共享数据和信息来实现协同工作，提高工作效率。同时，集成化还可以避免数据冗余和重复输入，减少了人为的错误和数据不一致性问题。另外，集成化还能够提供更好的数据分析和决策支持。通过将各个子系统整合在一起，可以获得更全面、准确的数据，从而进行更深入的数据分析和挖掘。这样可以帮助管理者更好地理解企业或组织的运营情况，并做出更明智的决策。最后，集成化的发展也提高了信息系统的可靠性和安全性。通过整合和集中管理，可以更好地进行数据备份和恢复，提高系统的可靠性。同时，集成化也可以实现对用户权限的统一管理，加强信息系统的安全性，保护敏感数据不被未经授权的人员访问。

1.2 智能化

目前，计算机技术在我国已经得到了广泛应用，并成为各行各业进行管理和决策的不可或缺的工具。计算机信息化管理的核心是将信息技术与管理相结合，通过自动化、网络化和数字化手段来提高管理效率和决策水平。并且随着人工智能技术的迅猛发展，计算机系统可以模拟和超越人类智能的能力，实现更加智能化的管理和决策过程。例如，利用机器学习算法对大数据进行分析，可以帮助企业预测市场需求、优化生产流程等。同时，智能化管理也能够提供个性化的服务，满足不同用户的需求，提高用户体验。最后，计算机信息化管理的发展还面临一些挑战。首先是信息安全问题。随着信息化程度的不断提高，信息泄露、网络攻击等安全风险也日益增加。因此，保护信息安全成为计算机信息化管理发展的重要任务。其次是技术更新迭代速度快，新的技术和工具不断涌现，管理者需要不断学习和更新知识，以适应新的发展趋势。

1.3 人本化

现如今，随着计算机信息化管理技术的不断发展和普及，人们逐渐认识到信息化技术与计算机信息化管理之间的紧密联系。信息化技术为计算机信息化管理提供了强有力的支持，使其更加高效、准确地进行各项业务管理。然而，我们也应该意识到信息化技术与计算机信息化管理并非一体化的概念，二者存在着一些区别。信息化技术仅仅是一种工具，只有在计算机信息化管理的指导下才能充分发挥作用。而计算机信息化管理则是一种综合性的管理活动，它需要借助于信息化技术来实现其管理目标。因此，在推进信息化的过程中，我们不能只盲目追求技术的更新和应用，更应该注重人本化的思想。人本化是指在信息化技术与计算机信息化管理相结合的过程中，将人作为核心，关注人的需求、人的行为和人的参与。这意味着我们要在引入信息化技术的同时，注重培养员工的信息素养和能力，提升他们对信息化技术的认知和运用能力。此外，还需要关注员工的工作环境和工作负荷，避免信息化技术给员工带来不必要

的压力。

2 计算机网络安全技术的影响因素

2.1 病毒攻击

随着计算机网络信息技术的不断发展，网络病毒也在不断地更新。计算机系统病毒从本质上来看就是一种计算机应用程序，它们在计算机内部获得自我复制的代码，从而破坏计算机的正常运行，并且对其中的关键性数据信息进行破坏。此外，目前的计算机网络运行过程中，病毒有着多种多样的组成形式，并且还具有隐蔽性的特征。比如，病毒可以通过电子邮件附件、下载软件或者点击恶意链接等方式传播。当计算机的使用者不小心点开了一个链接或下载了一个可疑的文件时，就很可能使得计算机感染病毒。并且网络病毒的危害不容忽视，它们可以导致系统崩溃、数据丢失，甚至可能使整个网络瘫痪。同时，病毒还可以窃取个人敏感信息，如账号密码、银行卡信息等，给用户造成经济损失。此外，病毒还可以利用感染的计算机发送垃圾邮件、攻击其他系统，形成一个恶意的网络攻击链条。

2.2 系统漏洞和网络钓鱼

一方面，计算机系统存在漏洞是一种常见的情况，这种漏洞可以通过系统升级和安全管理人员的管理来不断完善和修复。然而，如果管理不及时或应用了盗版软件等现象，则可能会导致漏洞的增大，从而给违法行为提供了路径。攻击者将利用系统漏洞来攻击计算机网络，进而影响计算机的正常工作，甚至导致计算机崩溃。例如，黑客可以利用漏洞控制系统，攻击网站，从而窃取敏感信息。另一方面，网络钓鱼是一种社会工程学攻击，攻击者常常利用假冒的信任关系进行欺骗。攻击者以欺骗、恐吓、诱惑等方式来诱骗用户点击链接、输入敏感信息等，从而获得用户的账户密码、银行卡信息、个人信息等敏感数据。这些收集来的敏感信息，可以用在其他恶意攻击中，或被出售给其他有意的黑客，以实现非法利益。这两个问题的结合可以产生巨大的威胁，细心的攻击者甚至会利用网络钓鱼来获取敏感信息，通过其中的或者自己开发的漏洞来实现进一步的攻击。

2.3 自然灾害与人为管理问题

自然灾害是一种较为客观的影响因素，对计算机网络安全造成的影响是不可避免的。例如，雷雨可能导致电力中断、设备短路以及数据丢失等问题，地震可能破坏通信基础设施，这些都会对计算机网络的正常运行造成重大威胁[1]。同时，在面对自然灾害时，环境因素也需要被考虑进来。比如，湿度过大可能导致电路系统受潮而损坏，进而引发各种系统问题。因此，在设计和建设计算机设备的场所时，应该考虑到气候和环境因素，采取相应的措施来保护设备免受自然灾害的影响。最后，人为管理在处理自然灾害问题中起着至关重要的作用。尽管我们无法完全阻止自然灾害的发生，但通过科学合理的人为管理措施，可以降低其对计算机网络安全的影响，这包括建立紧急预警系统、制定应急预案、加强设备维护和备份等。同时，定期的检查和演练也是必不可少的，以确保在自然灾害发生时能够迅速、有效地应对。

3 计算机网络安全防范措施的分析

3.1 建立健全网络安全系统

网络安全技术是网络安全系统的基础，只有具备强大的安全技术支持，才能有效防止网络攻击和数据泄露。因此，建立健全网络安全系统的关键是积极完善网络安全技术。为此，应该采取一系列措施来提升网络安全技术水平。首先，构建防火墙系统是保障网络安全的重要一环。防火墙可以监控网络流量，并根据预设规则过滤恶意请求，阻止未经授权的访问。在构建防火墙系统时，需要合理设置规则和策略，确保只有经过验证的用户才能访问敏感信息，从而防止未经授权的访问和攻击。其次，加强数据在传输和存储中的安全也是网络安全系统建设的重点之一。通常情况下，数据在传输过程中容易受到黑客的窃取或篡改，因此必须采取加密和认证等手段来保护数据的安全。对于存储数据，可以使用强大的加密算法将数据进行加密，以防止非法获取和修改[2]。同时，及时做好数据的备份是防止数据丢失的关键步骤。备份数据可以在意外数据删除或硬件故障时恢复数据，减少数据丢失的风险。建议定期制定备份计划，并将数据存储在安全可靠的地方，以确保数据的完整性和可用性。最后，建立健全网络安全系统需要持续的监控和更新。对系统进行实时监控和分析，可以及早发现和应对潜在的安全风险。此外，需要定期更新网络安全设备和软件，以弥补已知漏洞和缺陷，同时保持系统的健壮性。

3.2 应用漏洞扫描技术

在计算机运行过程中，经常会出现各种问题，如安全漏洞、软件缺陷等。而应用漏洞扫描技术能够及时检测这些问题，并提供相关数据信息，帮助工作人员快速解决和排查潜在的风险。一方面，应用漏洞扫描技术对于网络系统的稳定性和安全性非常重要。通过定期进行漏洞扫描，可以发现并修复系统中存在的漏洞，防止黑客入侵和恶意攻击。这项技术不仅可以保护网络系统的正常运行，还可以防止用户数据泄露和财产损失。同时，它还能够提供实时的监控和警报功能，让管理员能

够及时采取措施应对突发事件，保障系统的安全性。另一方面，应用漏洞扫描技术对科研人员的研究工作具有重要意义。在网络环境下，科研人员需要处理大量的数据和信息，而这些数据往往存储在网络系统中。通过应用漏洞扫描技术，科研人员可以及时获取相关数据信息，提高研究工作的效率和准确性。同时，它还可以为科研人员提供实验数据的安全保障，避免数据泄露和篡改。

3.3 进行操作者身份校验的技术

随着计算机网络应用的不断扩大和普及，对计算机系统和数据安全的要求日益提高，身份认证技术已成为重要的基础设施。该技术可以用于确认用户身份，限制用户权限，保护计算机系统和数据不受未经授权的访问和攻击，并对行为进行精确的跟踪和记录，使得计算机系统的安全性和可控性得到提高。第一，基于口令的身份校验技术是最为普遍的一种身份认证技术，其原理是通过密码的比对验证用户的身份。其实现流程通常为：用户输入用户名和密码，系统将密码进行哈希算法加密，然后将加密后的密文与系统中储存的密码比对，如果匹配则验证通过，否则认证失败。这种技术的优点在于简单易用，但缺点在于密码容易被泄露或被猜测，从而被黑客攻击。第二，基于生物特征的身份认证技术是可靠性最高的一种身份认证技术。它是根据人体生理的唯一性特征，如指纹、虹膜、人脸等进行身份认证。该技术精度高，不容易被伪造和模仿，但成本高和适用场景有限是其主要缺点。第三，基于卡片的身份认证技术是通过射频卡或IC卡来进行身份校验的方法[3]。卡片通常包含一些加密信息或证书，用户在使用时需要将卡片插入到读卡器中才能进行认证。该技术常用于银行、金融、政府等领域，具有安全性高、使用方便等优点。

3.4 重视计算机用户的安全教育

由于许多数据丢失或其他安全问题都是由于计算机用户自身的不良操作习惯而引起的，因此，重视培养计算机用户的安全意识是非常必要的。（1）教育用户了解网络安全隐患。通过对计算机用户教育，可以让人们更好地了解网络安全隐患。用户需要知道基本的网络攻击手段，并了解如何防御和避免这些威胁。教育用户如何识别网络钓鱼攻击，防范恶意软件和病毒等，同时也需要告知用户在使用互联网时应当避免随意登录不可靠的网络页面或不安全的公共WIFI等，避免数据泄露和其它问题的发生。只有加强网络安全防范意识，用户才能更好地保护自己和他人的网络安全。（2）规范计算机用户的上网行为，也非常重要。用户应该遵守网络使用相关条例，只在信任的网站或软件中输入个人敏感信息。特别是对于那些涉及到银行、金融或其他商业信息的网站，应在浏览器地址栏上确认网站地址是否准确，避免上钓鱼网站或被黑客攻击。此外，用户还应该定期更新自己的操作系统和重要的应用程序，并安装常用的安全软件和防病毒、防恶意软件软件等保护工具[4]。（3）黑客攻击是互联网上的一个重要问题。用户需要了解黑客攻击的基本知识，防范黑客攻击，并在出现黑客侵入时及时采取必要的防范措施。在具体操作中，用户应该增强电子邮件和即时通讯的防范，不开放过多的个人信息，能主动删除可疑邮件并及时更改密码。如果发现黑客袭击和病毒感染，应及时联系相关的安全机构，防止问题进一步扩大。

结束语

综上所述，随着技术的快速发展和社会的进步，我们必须认识到保护信息系统和防范网络安全威胁的重要性。通过合理的信息化管理和科学的网络安全策略，我们能够有效应对各种安全挑战，并确保信息的机密性、完整性和可用性。同时，政府、企业和个人也应加强对网络安全的重视，积极采取相应的防范措施，共同构建一个安全可靠的信息化环境。

参考文献

[1]彭世春.计算机信息化管理的发展与网络安全的有效防范措施探索[J].现代销(经营版2020(07):102-103.

[2]岑柏滋,刘丽琳.云计算环境中的计算机网络安全分析[J].信息与电脑:理论版,2019(15):220-221.

[3]唐和秀，裘雄伟.信息化建设中计算机网络安全管理与维护[J].科学与信息化,2020(2):174-176.

[4]陈焱.关于计算机网络安全技术的影响因素与防范措施探讨[J].信息记录材料，2019，20（04）：67-68.