浅谈计算机信息网络安全防护策略

吴晓莹　侯晓林
中电伟恒（北京）科技发展有限公司天津分公司　天津　300000

摘　要：计算机信息网络的安全防护是一项长期而艰巨的任务，需要不断地更新和完善防护策略，以适应不断变化的网络安全环境。基于此，本文分析了计算机信息网络安全风险的种类，包括技术风险、管理风险以及人为风险，接着针对网络安全防护策略提出了几点有效措施，以期为计算机信息网络的安全防护提供理论支持。

关键词：计算机；信息网络安全；防护

引言

在信息化时代，计算机信息网络已经成为社会发展的重要基石，它承载着大量的信息传输和交换任务。然而，随着网络的普及和应用领域的不断拓展，网络安全问题也日益严重。黑客攻击、病毒传播、数据泄露等网络安全事件频发，给企业和个人带来了巨大的经济损失和信息安全风险。因此，如何有效防护计算机信息网络的安全，已成为当前亟待解决的问题。

1 计算机信息网络安全风险的种类

1.1 技术风险

随着网络技术的日新月异，黑客攻击手段也日趋狡猾和复杂。在这个高度信息化的时代，网络安全问题已成为全球关注的焦点。网络病毒、木马、钓鱼网站等恶意程序层出不穷，给个人、企业和国家的网络安全带来了严重威胁。首先，网络病毒是一种通过网络传播的恶意程序，具有极高的传播速度和破坏力。它们能够悄无声息地侵入计算机系统，窃取敏感信息、破坏数据、甚至导致系统崩溃。木马则是一种隐藏在正常程序中的恶意代码，它会在用户不知情的情况下，远程控制用户的计算机，窃取信息或进行其他非法操作。而钓鱼网站则通过伪装成合法网站，诱骗用户输入个人信息，如银行账号、密码等，以达到盗取财产的目的。其次，网络系统的漏洞和配置不当也为黑客提供了可乘之机。网络系统的漏洞可能是由于系统设计缺陷、编程错误或软件更新不及时等原因造成的。这些漏洞一旦被黑客发现并利用，就会导致严重的安全问题。此外，网络配置不当也可能导致安全漏洞，如防火墙设置不合理、访问控制策略不严格等。最后，技术风险的主要成因在于网络安全技术的滞后和网络安全意识的不足。随着网络技术的不断发展，黑客攻击手段也在不断演变和升级。然而，网络安全技术的更新速度往往滞后于黑客攻击手段的发展，这使得网络安全面临着巨大的挑战。同时，许多用户和企业对网络安全的认识不足，缺乏必要的防范意识和措施，这也加剧了技术风险的发生。

1.2 管理风险

在网络安全领域，管理风险是一个不容忽视的问题。企业和组织在网络安全管理方面的疏忽，不仅可能引发重大的安全事件，还可能对企业的声誉、财务和运营产生深远影响。一方面，管理风险的形成往往源于企业组织内部管理制度的不完善。许多企业在网络安全管理方面存在制度空白或执行不力的情况。例如，密码管理不善，员工可能使用过于简单的密码，或者密码定期更换的规定没有得到执行，导致密码长期不变，增加了被破解的风险。此外，权限设置不合理也是一个常见问题[1]。在某些企业中，员工可能拥有过多的权限，这意味着他们可以访问和操作更多的数据和信息，从而增加了数据泄露或被滥用的风险。另一方面，安全培训不到位也是管理风险的重要来源。许多员工对网络安全的认识不足，缺乏基本的安全意识和技能。他们可能随意点击来路不明的链接，下载未经验证的附件，或在公共场合使用不安全的网络，这些行为都可能导致恶意软件的感染或敏感信息的泄露。因此，加强员工的安全培训，提高他们的安全意识和技能，是降低管理风险的关键措施之一。除了以上两点，安全文化的缺失也是导致管理风险的重要原因。安全文化是指企业内部对安全问题的重视程度和对待方式。在一个缺乏安全文化的企业中，员工可能缺乏对安全问题的关注和重视，甚至将安全问题视为次要任务。这种文化氛围可能导致安全管理制度的执行不力，安全培训的效果不佳，以及员工对安全问题的忽视和敷衍。

1.3 人为风险

网络安全事件并不仅仅是由技术漏洞或外部攻击所引发，人为因素同样在其中扮演着重要的角色。员工的不当行为、误操作以及社会工程学攻击等人为风险，已

经成为许多组织在网络安全领域面临的重要挑战。这些风险不仅可能导致敏感信息的泄露，还可能引发一系列连锁反应，给组织带来不可估量的损失。首先，员工的不当行为是人为风险中最为常见的一种。由于员工安全意识淡薄，他们可能会在不经意间泄露敏感信息，如将密码、账户信息或机密文件随意分享给他人[2]。此外，员工还可能在未经授权的情况下访问、修改或删除重要数据，给组织带来严重的数据安全风险。这种不当行为可能源于员工对安全规定的忽视，或者是因为他们缺乏足够的安全意识和培训。其次，误操作也是导致网络安全事件的重要原因之一。在日常工作中，员工可能会因为疏忽或操作不当而导致数据丢失、系统崩溃等问题。例如，错误地删除重要文件、错误地配置网络设备等都可能给组织带来重大的损失。这些误操作往往是由于员工缺乏必要的技能或经验，以及对工作流程的不熟悉所导致的。此外，社会工程学攻击也是人为风险中不可忽视的一部分。社会工程学攻击通常利用人们的心理弱点、信任关系或社会习俗来实施攻击。例如，通过发送伪造的电子邮件或消息来诱导员工点击恶意链接，或者利用人们的信任关系来窃取敏感信息。这些攻击方式往往具有较高的隐蔽性和欺骗性，使得员工在不知不觉中成为攻击者的帮凶。

2 应对计算机信息网络安全风险的策略

2.1 加强技术层面的防范措施

在应对计算机信息网络安全风险的众多策略中，加强技术层面的防范措施无疑是基础且至关重要的一环。随着网络技术的飞速发展，网络安全威胁日益增多，黑客攻击、病毒传播、数据泄露等事件频发，给企业、个人乃至整个国家带来了极大的损失。因此，企业必须建立完善的网络安全防护体系，以抵御这些日益复杂的网络攻击。首先，防火墙是网络安全防护体系中的重要组成部分。它如同一道屏障，能够监控和控制进出网络的数据包，有效阻止非法访问和恶意攻击。防火墙能够过滤掉潜在的危险信息，只允许经过授权的合法用户访问网络资源，从而大大降低了网络安全风险。同时，防火墙还能记录网络活动的日志，为后续的网络安全审计和溯源提供了重要依据。其次，入侵检测系统则是网络安全防护体系中的另一大利器。它能够实时监测网络流量和系统行为，发现异常模式和潜在威胁。通过收集和分析网络数据，入侵检测系统能够及时发现并报告未经授权的访问、恶意软件的传播等异常活动。这为企业提供了及时的预警机制，使其能够在威胁扩散之前采取相应的应对措施。最后，数据加密技术则是保护数据机密性和完整性的关键手段。在数据传输和存储过程中，采用加密技术可以确保数据即使被非法获取也无法被轻易解密。这大大降低了数据泄露的风险，保护了企业的核心利益[3]。同时，数据加密技术还能防止数据在传输过程中被篡改，确保数据的完整性和真实性。

2.2 加强网络安全意识教育

在应对计算机信息网络安全风险的众多措施中，加强网络安全意识教育显得尤为关键。网络安全不仅仅是一个技术问题，更是一个涉及到每个人的社会问题。因此，提高用户的安全防范意识，成为保障网络安全的重要一环。第一，企业和组织应高度重视员工的网络安全培训。员工是企业信息安全的第一道防线，他们的行为举止直接关系到企业网络安全的稳定。因此，企业需要定期开展网络安全培训课程，让员工了解网络安全的基本知识和防范技能。这些课程应涵盖常见的网络安全威胁、攻击手段以及应对策略，帮助员工识别并防范网络钓鱼、恶意软件等风险。同时，企业还可以通过模拟攻击、应急演练等方式，提高员工的应急响应能力，确保在发生网络安全事件时能够迅速应对。第二，除了企业内部培训，政府和社会各界也应加强网络安全宣传教育。通过媒体、网络等渠道，广泛传播网络安全知识，提高公众对网络安全的认识和重视程度。可以举办网络安全知识竞赛、网络安全宣传周等活动，吸引更多人关注和参与网络安全事业。此外，还可以开展网络安全进校园、进社区等活动，让网络安全知识深入人心，形成全社会共同关注网络安全的良好氛围。第三，加强网络安全意识教育的同时，我们还应建立健全的网络安全法律法规体系。法律法规是保障网络安全的重要基石，它为网络安全提供了有力的法律保障。政府应加强对网络安全的监管和立法工作，制定严格的网络安全法规和标准，明确各方在网络安全中的责任和义务。这些法规应涵盖网络基础设施安全、个人信息保护、网络安全事件应急处置等方面，为网络安全提供全方位的保障。第四，我们还应注重网络安全意识教育的长期性和持续性。网络安全是一个不断发展的领域，新的威胁和挑战不断出现。因此，网络安全意识教育应贯穿于每个人的日常生活和工作中，成为一种常态化的行为。企业和组织应定期更新培训内容，关注最新的网络安全动态和技术发展，确保员工的网络安全知识和技能始终保持在较高水平。

2.3 关注新技术

随着科技的飞速发展，新技术不断涌现，为网络安全领域带来了前所未有的机遇和挑战。特别是人工智

能、大数据和云计算等技术的广泛应用，不仅推动了网络安全防护手段的升级，也为我们提供了全新的视角和思考方式。首先，人工智能技术在网络安全领域的应用日益广泛。智能安全防护系统通过深度学习和机器学习等技术，能够自动识别和应对各种网络威胁。这些系统能够实时分析网络流量、用户行为等数据，快速发现异常模式和潜在风险，并及时采取相应措施进行防范。相比传统的人工分析和处理，智能安全防护系统具有更高的效率和准确性，大大提升了网络安全的防护能力。其次，大数据技术也为网络安全提供了强大的支持。通过对海量数据的收集、分析和挖掘，我们能够更深入地了解网络威胁的来源、传播途径和攻击方式。大数据分析技术能够实时监测网络流量和用户行为，发现异常模式和潜在风险，为安全决策提供有力支持[4]。同时，大数据还可以用于构建网络安全威胁情报库，帮助企业和组织更好地了解网络安全态势，制定更有效的安全策略。此外，云计算技术也为网络安全提供了新的解决方案。云计算具有弹性、可扩展的计算资源，能够为网络安全提供强大的后盾。通过云计算平台，我们可以实现安全资源的共享和协同，提高安全防护的效率和灵活性。同时，云计算还可以为网络安全提供高效的数据存储和备份服务，确保数据的安全性和可用性。

2.4 建立备份与恢复机制

随着信息技术的迅猛发展，网络安全事件愈发频繁，给企业和个人带来了巨大的损失。在这样的背景下，建立有效的数据备份和恢复机制成为了确保业务连续性和信息安全的重要一环。备份与恢复机制是网络安全事件的最后防线，能够在关键时刻帮助企业迅速恢复业务运行，减少损失。（1）数据备份是建立备份与恢复机制的基础。企业应定期备份重要数据，包括数据库、文件系统、配置文件等，以确保数据的完整性和可用性。备份数据的存储位置应远离主数据中心，以防万一主数据中心受到攻击或自然灾害影响。同时，备份数据的加密和访问控制也至关重要，以防止未经授权的访问和数据泄露。（2）备份数据的可恢复性是确保备份机制有效的关键。企业应定期测试备份数据的完整性和可恢复性，以确保在发生网络安全事件时能够顺利恢复数据。测试过程应包括数据恢复演练和应急响应流程的模拟，以检验恢复机制的可行性和效率。此外，企业还应关注备份技术的更新和升级，以适应不断变化的网络安全威胁。（3）除了数据备份和恢复，制定详细的恢复计划也是建立备份与恢复机制的重要一环。恢复计划应涵盖应急响应流程、资源调配、人员协作等多个方面。在应急响应流程中，企业应明确安全事件的发现、报告、处置和恢复的各个环节，确保在发生安全事件时能够迅速响应并有序应对。资源调配方面，企业应提前规划好恢复所需的硬件、软件和网络资源，确保在需要时能够及时调用。人员协作方面，企业应建立跨部门、跨团队的协同机制，确保在发生安全事件时能够形成合力，共同应对。

结语

综上所述，通过实施本文提出的安全防护策略，企业和个人可以显著提高信息网络的安全防护能力，降低网络安全风险。然而，网络安全防护并非一蹴而就，而是需要持续的投入和努力。未来，我们还应进一步加强网络安全技术的研究和创新，提升网络安全防护的智能化和自动化水平，为构建安全、稳定、高效的计算机信息网络提供有力保障。

参考文献

[1]李帷笳.计算机网络信息技术安全与防护策略研究[J].无线互联科技,2020,17(11):13-14.

[2]夏梁.计算机网络信息安全及防护措施研究[J].计算机产品与流通,2020,(06):55.

[3]蒋志刚.计算机信息网络安全技术及发展方向的探讨[J].电子元器件与信息技术,2020,4(6):2.

[4]姚申,董静.计算机网络安全技术的影响因素与防范措施[J].网络安全技术与应用,2021,(01):154-155.