计算机网络安全管理与维护

赵德非
张家口市实验中学　河北　张家口　075100

摘　要：计算机网络安全管理与维护涉及多个重要方面。网络安全管理包括制定和实施网络安全策略、访问控制和数据加密等措施，以保护计算机网络系统免受未经授权的入侵、破坏、篡改或窃取数据等行为。网络安全维护则包括防病毒、防火墙、安全扫描和备份与恢复等措施，以应对网络安全威胁和故障。

关键词：计算机；网络安全；管理与维护

引言：随着信息技术的快速发展，计算机网络已成为生活和工作中不可或缺的一部分。然而，随之而来的是网络安全问题。计算机网络安全是指通过一系列技术和管理措施，保护计算机网络系统免受未经授权的入侵、破坏、篡改或窃取数据等行为。网络安全不仅是信息技术问题，也是管理问题。因此，本文将重点探讨计算机网络安全管理与维护的问题。

1 网络安全管理

1.1 安全策略

（1）制定网络安全策略。这需要对网络环境进行全面的评估，包括硬件、软件、网络结构、数据安全等方面。在评估的基础上，制定出适合企业的网络安全策略，包括访问控制策略、密码策略、备份策略、恢复策略等。同时，还需要定期对网络安全策略进行审查和更新，以应对网络环境的变化和新的威胁。（2）实施网络安全策略。这需要通过各种手段，如技术手段、管理手段等，将网络安全策略落实到实处。例如，可以通过设置防火墙、安装杀毒软件、使用加密技术等方式，来防止网络攻击和数据泄露。同时，还需要定期对网络安全策略的执行情况进行检查和评估，以确保其有效性。（3）提升网络安全意识。这需要通过网络安全教育和培训，提高员工的网络安全意识，使他们了解网络安全的重要性，掌握基本的网络安全知识和技能。同时，还需要通过各种活动，如网络安全知识竞赛、网络安全宣传周等，来进一步提高员工的网络安全意识[1]。（4）发现和修复安全漏洞。这需要通过定期的安全检查和漏洞扫描，发现网络中的潜在安全漏洞。一旦发现安全漏洞，就需要立即进行修复，以防止被黑客利用。同时，还需要对修复过程进行记录和分析，以便找出漏洞的根源，防止类似问题的再次出现。

1.2 访问控制

访问控制的基本过程包括身份认证和授权两个阶段。身份认证是确认用户的身份，而授权则是确定用户可以访问哪些资源以及可以执行哪些操作。这两个阶段相互关联，共同构成了访问控制的完整过程。（1）在传统的访问控制模型中，通常采用用户名和密码的方式进行身份认证。然而，这种方式存在一些明显的缺陷。例如，用户的密码可能被窃取，或者用户可能会忘记密码。此外，如果用户的密码过于简单，也容易被破解。因此，为了提高访问控制的安全性，现在越来越多的系统开始采用动态口令、指纹识别等更复杂、更安全的身份认证方法。（2）动态口令是一种基于时间的一次性密码，它的特点是每次生成的密码都是随机的，且与之前的密码没有任何关系。这样即使用户的密码被窃取，攻击者也无法使用这个密码来登录用户的账户。指纹识别则是一种生物特征识别技术，它通过分析用户指纹的独特性来确认用户的身份。由于每个人的指纹都是独一无二的，因此指纹识别具有很高的安全性。（3）除了身份认证之外，访问控制还包括授权管理。授权管理主要是确定用户可以访问哪些资源以及可以执行哪些操作。在传统的访问控制模型中，通常采用基于角色的访问控制（RBAC）方式。在这种模式下，用户被分配到不同的角色，每个角色都有一组特定的权限。用户只能访问其角色允许的资源，并只能执行其角色允许的操作。（4）随着网络技术的发展，单一的基于角色的访问控制已经无法满足所有的安全需求。因此，现在越来越多的系统开始采用基于属性的访问控制（ABAC）方式。在这种方式下，不仅考虑用户的角色，还考虑用户的属性（如年龄、性别、地理位置等）。这样可以根据用户的实际属性来确定其是否具有访问某个资源的权限。

1.3 数据加密

在当今信息化社会，数据已经成为了各种信息和知识的核心载体，而数据的安全性对于个人和企业都具有重要意义。通过加密技术，即使数据被窃取，也无法被

未经授权的用户读取。因此，数据加密在网络安全、电子商务、金融等领域得到了广泛应用。对称加密和非对称加密是两种常用的加密方法。对称加密是指加密和解密使用相同的密钥，常见的对称加密算法有DES、AES等。非对称加密则是使用一对密钥，即公钥和私钥，公钥用于加密数据，私钥用于解密数据。非对称加密算法有RSA、ECC等。这两种加密方法各有优缺点，适用于不同的场景。（1）对称加密的优点是加密和解密速度快，适合大数据量的场景。然而，由于对称加密需要对每个数据进行单独的加密和解密操作，因此在处理大量数据时效率较低。此外，对称加密算法的密钥管理也是一个挑战，因为密钥需要在通信双方之间安全地传递。（2）非对称加密的优点是计算复杂度较低，适合处理大量数据的应用场景。同时，非对称加密不需要对每个数据进行单独的加密和解密操作，因此在处理大数据量时效率较高。然而，非对称加密的缺点是加密和解密速度较慢，且密钥管理较为复杂[2]。（3）为了提高数据安全性，通常采用混合加密的方法。在这种方案中，对称加密和非对称加密相互补充，共同保证数据的安全。例如，可以使用非对称加密来传输对称密钥，然后使用对称加密对实际数据进行加密。这样既可以利用非对称加密的优势，又可以避免其缺点。

2 网络安全维护

2.1 防病毒

它们可以对个人和企业的计算机系统造成严重的损害，包括数据丢失、系统崩溃、隐私泄露等。因此，采取有效的防病毒措施至关重要。防病毒软件是一种专门设计用于检测和清除计算机病毒的软件工具，它可以帮助保护计算机免受病毒的侵害。（1）定期更新防病毒软件。这是因为病毒开发者会不断开发新的病毒和恶意程序来攻击计算机系统。防病毒软件需要及时更新，以便能够识别和清除这些新出现的病毒威胁。此外，防病毒软件还会根据最新的病毒库进行升级，以提高对已知病毒的检测和清除能力。因此，定期更新防病毒软件是确保计算机安全的重要步骤。（2）定期更新操作系统。操作系统是计算机系统的核心组件，它提供了许多底层功能和服务。然而，操作系统也可能存在安全漏洞，这些漏洞可能被病毒利用。因此，定期更新操作系统可以修复这些漏洞，提高系统的安全性。同时，操作系统的更新还可能包含一些安全增强功能和性能优化，进一步提高计算机的整体安全性和稳定性。（3）采取其他措施来保护计算机免受病毒的威胁。例如，可以安装防火墙来监控网络流量，阻止未经授权的访问；可以使用强密码来保护用户账户和敏感数据；可以限制用户权限，确保只有授权用户可以访问系统资源；可以教育用户正确使用计算机和互联网的方法，避免点击可疑链接或下载未知文件等。

2.2 防火墙

（1）软件防火墙是指安装在计算机上的防火墙程序，它通过监控网络流量、分析数据包内容和执行过滤规则来实现对网络的访问控制。软件防火墙通常具有较低的成本和较高的灵活性，可以根据用户的需求进行定制和配置。然而，软件防火墙的性能受到计算机资源的限制，可能无法应对大量的网络流量和复杂的攻击行为。（2）硬件防火墙是指专门设计用于保护计算机网络的硬件设备，它通常具有高性能的处理能力和较大的内存空间，可以有效地应对大规模的网络流量和复杂的攻击行为。硬件防火墙具有独立的操作系统和处理器，不受计算机其他任务的影响，因此具有较高的稳定性和可靠性。然而，硬件防火墙的成本较高，安装和维护也相对复杂[3]。（3）在选择防火墙时，应根据网络规模、安全需求和预算等因素综合考虑。对于小型企业或家庭用户来说，软件防火墙可能是一个经济实惠且易于管理的选择；而对于大型企业或政府部门来说，硬件防火墙可能更能满足其对网络安全的高要求。此外，为了提高整体网络安全水平，还可以采用多层防御策略，结合使用不同类型的防火墙技术。

2.3 安全扫描

（1）明确什么是安全扫描。简单来说，安全扫描就是对计算机网络系统进行的一种全面检查，以发现可能存在的安全问题。这种检查可以是对系统的硬件、软件、网络连接等方面进行的，目的是找出可能被黑客利用的弱点，以便及时进行修复。（2）安全扫描的重要性。在当今这个信息化的时代，网络安全问题日益严重，任何一个环节的疏忽都可能导致整个系统的安全受到威胁。因此，定期进行安全扫描，及时发现并修复系统中的安全隐患，是保障网络安全的重要措施。（3）安全扫描的方法，常见的有黑盒测试、白盒测试、灰盒测试等。其中，黑盒测试是最直接、最有效的一种方法。它不需要了解系统的内部结构和工作原理，只需要通过模拟黑客的攻击行为，就可以发现系统中的安全漏洞。而白盒测试和灰盒测试则需要对系统的内部结构有一定的了解，但它们可以更深入地发现系统中的潜在问题。

2.4 备份与恢复

（1）理解数据备份的重要性。在当今的数字化世界中，数据是最重要的资产之一。企业和个人都依赖数据

来进行决策、运营和创新。然而，数据也可能因为各种原因而丢失或损坏，如硬件故障、软件错误、病毒攻击、人为错误等。因此，定期备份数据是非常重要的，可以保护免受这些风险的影响。（2）数据备份有多种方式。最常见的方法是使用外部存储设备，如硬盘驱动器、USB闪存驱动器、CD或DVD等。这些设备可以提供额外的冗余存储空间，以防止原始数据丢失。此外，许多操作系统也提供了内置的数据备份功能。例如，Windows用户可以使用“文件历史记录”功能来自动备份重要的文件和文件夹。（3）数据恢复是数据备份的另一重要方面。当系统出现故障时，如果没有备份，可能会导致重大损失。通过定期备份数据，可以在需要时快速恢复系统，减少停机时间，并尽快恢复正常运营。此外，数据恢复也可以帮助在数据丢失或损坏后找回重要信息。（4）注意一些潜在的风险。例如，如果备份数据没有正确存储或加密，它可能会被黑客攻击或泄露。因此，需要使用安全的备份解决方案，如加密的云存储服务、物理安全存储设备等。同时，也需要定期测试和更新的备份策略，以确保它们能够有效地应对新的威胁和挑战。

3 云安全技术

随着云计算技术的不断发展，越来越多的企业和个人开始将其业务迁移到云端，以降低成本、提高效率和灵活性。然而，随着云计算的普及，网络安全问题也日益凸显。云安全技术作为一种新兴的安全技术，正逐渐成为保护云计算环境免受网络攻击的关键手段。云安全技术是一种基于云计算环境的安全防护技术，通过对大量网络客户端的监控，实时检测和分析网络中软件行为的异常，从而及时发现并阻止恶意程序的传播。这种技术利用了云计算的分布式处理能力，具有高效、快速、低成本的特点，为企业和个人提供了一种全新的安全防护解决方案。云安全技术主要包括以下几个方面：（1）威胁情报共享。云安全技术的一个重要特点是其威胁情报共享功能。通过与全球各大安全厂商合作，云安全平台可以实时获取最新的威胁情报，包括病毒、木马、钓鱼网站等恶意程序的最新信息。这些信息可以帮助云安全系统快速识别并阻止潜在的网络攻击[4]。（2）自动化分析和处理。云安全技术的另一个重要特点是其自动化分析和处理能力。通过对网络中软件行为的实时监控，云安全系统可以自动识别出异常行为，并将其分发给Server端进行进一步的分析。Server端可以利用先进的机器学习和人工智能技术，对恶意程序进行深入分析，从而找到病毒和木马的解决方案。最后，这些解决方案会分发给每个客户端，确保整个云计算环境的安全。（3）多层次的安全防护体系。云安全技术采用了多层次的安全防护体系，包括数据层、网络层和应用层。在数据层，云安全系统会对用户的数据进行加密存储，以防止数据泄露。在网络层，云安全系统会对网络流量进行实时监控，阻止恶意程序的传播。在应用层，云安全系统会对用户的应用程序进行安全检查，确保其没有被恶意程序感染。（4）弹性扩展和高可用性。云安全技术具有很强的弹性扩展和高可用性。随着云计算环境中用户数量的增加，云安全系统可以自动扩展其资源以满足需求。同时，云安全系统采用了高可用性的架构设计，确保在任何情况下都能正常运行，为用户提供持续的安全保护。

结语：总之，计算机网络安全是一个系统性、复杂性的问题，需要在多个层面上进行管理和维护。除了技术手段外，还应注重网络安全管理策略的制定和执行，如访问控制、数据加密等。同时，为了应对新的网络安全威胁，需要不断学习和掌握新的安全技术，如云安全技术等。

参考文献

[1]唐高阳.计算机网络安全管理与维护[J].数字通信世界,2023(8):194-196.

[2]吴暇.试论计算机网络安全与维护[J].中国新通信,2020,22(3):140-141.

[3]陈小兵.企业计算机网络安全管理与维护研究[J].网络安全技术与应用,2020(3):59-60.

[4]周琳.探析计算机网络安全维护与管理[J].中国新通信,2020,22(1):43-44.