计算机工程安全维护策略

赵志元
连云港市东辛农场医院　江苏连云港　222000

摘　要：随着计算机技术的快速发展，计算机已经渗透到我们生活的方方面面，而在这一过程中，也使得计算机工程安全受到了严重威胁。计算机技术的广泛应用，不仅提高了人们的生活质量，还为社会各行各业提供了技术支持。但是在计算机应用的过程中，安全问题始终是人们关注的重点，特别是计算机网络技术的广泛应用，更是对计算机信息安全提出了新要求。本文主要从计算机工程安全维护问题入手，分析了加强计算机工程安全维护策略。

关键词：计算机工程；安全隐患；维护方案；研究

引言

近年来，随着我国信息化技术的不断发展，使得计算机技术在我国社会各行各业中的应用也越来越广泛，其中以计算机网络技术、电子商务技术为代表的计算机工程应用，对推动我国社会经济发展和提高人们生活水平起到了重要作用。但是从目前我国计算机工程安全维护的情况来看，由于受到多种因素的影响，很容易出现安全隐患问题，造成信息泄露、计算机病毒入侵等情况，从而给用户带来严重损失，甚至是人身安全隐患。因此在计算机工程安全维护过程中，必须加强对存在的安全隐患问题进行全面分析和研究，并采取有效措施予以解决，以确保计算机工程安全稳定运行。

1　计算机工程安全维护的必要性

计算机工程安全维护的必要性在当今数字化时代变得越来越重要。随着计算机和互联网的普及，我们的生活和工作越来越依赖于计算机系统的正常运行。然而，与此同时，计算机系统也面临着越来越多的安全威胁和风险。因此，进行计算机工程安全维护变得至关重要。首先，计算机工程安全维护可以保护个人和组织的数据安全。个人和组织在计算机系统中存储了大量的敏感信息，如个人身份信息、财务数据和商业机密等。如果这些信息被黑客或恶意软件攻击者窃取或破坏，将对个人和组织造成严重的损失。因此，通过进行计算机工程安全维护，可以加强数据的保护，防止未经授权的访问和数据泄露。其次，计算机工程安全维护可以防止计算机系统被恶意软件感染。恶意软件包括病毒、木马、蠕虫等，它们可以在计算机系统中隐藏并进行破坏、窃取信息或控制系统。如果计算机系统被感染，将导致系统崩溃、数据损失和个人隐私泄露等问题。通过定期更新防病毒软件、安装防火墙和加强网络安全措施，可以有效防止恶意软件的感染，保护计算机系统的安全。此外，计算机工程安全维护还可以提高计算机系统的性能和稳定性。在进行安全维护的过程中，可以检查和修复系统中存在的漏洞和错误，优化和升级系统软件和硬件，提高系统的运行效率和可靠性。

2　计算机网络工程安全问题分析

2.1 环境因素影响网络信息传播

网络信息传播受到各种环境因素的影响。首先，物理环境因素包括网络设备的位置、温度、湿度等。如果网络设备暴露在恶劣的环境中，如高温、潮湿或有害物质的环境下，可能会导致设备故障或信息传输错误。其次，网络拓扑结构也会影响信息传播的安全性。不同的网络拓扑结构具有不同的安全特性。例如，星型拓扑结构中，所有的设备都连接到一个中心节点，这样一来，一旦中心节点遭到攻击，整个网络都容易受到影响。而网状拓扑结构中，设备之间相互连接，可以提供更好的冗余和容错性，但也增加了信息传播的复杂性。此外，网络规模也会对信息传播的安全性产生影响。大型网络通常拥有大量的用户和设备，这增加了网络管理的难度。在这样的网络中，很容易出现管理不善、漏洞未及时修补等问题，从而给攻击者提供机会。

2.2 计算机病毒的影响

计算机病毒是指一种恶意软件，它可以通过网络传播并感染计算机系统。计算机病毒会破坏计算机的正常运行，导致系统崩溃、数据丢失以及网络服务中断等问

题。病毒可以通过电子邮件、下载文件、共享网络等途径传播，一旦感染了计算机系统，就会开始破坏和复制自己，继续传播给其他计算机。计算机病毒对网络信息传播的影响是多方面的。首先，计算机病毒会破坏计算机系统的正常运行，导致网络服务中断，使得信息无法正常传输。其次，病毒还会破坏或篡改存储在计算机中的信息，导致数据丢失或者信息被窃取。此外，病毒还可能通过网络传播恶意软件，例如间谍软件、广告软件等，进一步威胁网络安全。

2.3 黑客攻击

黑客攻击是指未经授权的个人或组织利用计算机技术手段侵入他人计算机系统或网络的行为。黑客攻击可能造成严重的网络安全问题，包括信息泄露、数据损坏、系统崩溃等。黑客攻击可以通过各种手段实施，例如密码破解、漏洞利用、拒绝服务攻击等。黑客攻击对网络信息传播的影响也是很大的。首先，黑客可以窃取敏感信息，例如个人身份信息、公司机密等，导致信息泄露和隐私泄露问题。其次，黑客可以篡改或破坏网络中的信息，造成数据损坏和不可信的信息传播。此外，黑客攻击还会导致系统崩溃或网络服务中断，使得信息无法正常传输和接收。为了应对黑客攻击，网络安全工程师需要采取一系列的安全措施，例如加密通信、防火墙设置、入侵监测系统等，以保护网络信息的安全传播。同时，用户也需要增强安全意识，避免点击可疑链接、使用强密码等，以减少黑客攻击的风险。

2.4 计算机信息被窃取

计算机信息被窃取是指未经授权的个人或组织获取计算机系统或网络中的信息的行为。这种行为可能导致用户的隐私泄露、商业机密被窃取以及其他不良后果。信息被窃取的途径有很多，包括黑客攻击、恶意软件、网络钓鱼等。当计算机信息被窃取时，对网络信息传播会产生严重影响。首先，被窃取的信息可能被用于非法目的，比如个人信息可能被用于身份盗窃、欺诈等活动。其次，窃取的信息可能被用于敲诈勒索，例如勒索软件常常通过窃取用户文件后威胁用户支付赎金才能恢复文件。此外，被窃取的信息也可能被泄露给竞争对手或黑市，造成商业机密的流失。最后，如果用户意识到自己的信息被窃取，他们可能会对网络的安全性产生怀疑，降低对网络信息的信任度，从而影响信息的传播和共享。

2.5 软件漏洞

软件漏洞是指在软件设计或实现过程中存在的错误或缺陷，这些错误或缺陷可能被攻击者利用来入侵系统或者执行恶意操作。软件漏洞对网络信息传播的影响是很大的。首先，攻击者可以利用软件漏洞来获取用户的个人信息或者系统的权限，从而导致信息泄露和隐私泄露问题。其次，软件漏洞可能导致系统崩溃或者功能异常，使得网络服务中断或者无法正常使用。此外，软件漏洞也可能被利用来传播恶意软件，例如通过利用浏览器的漏洞来下载并安装恶意软件。

3 计算机工程的安全维护建议

3.1 制定出完善可行的安全监管制度

为了确保计算机系统和数据的安全性，制定一个完善可行的安全监管制度是必要的。首先，为了确保安全监管制度的有效执行，应该明确责任分工。指定专门的安全监管人员或团队负责制定和执行安全策略，并监督系统的安全状况。其次，制定明确的安全策略和规范。安全策略应该包括密码管理、访问控制、数据备份、恶意软件防护等方面的规定。规范应该明确禁止一些风险行为，比如使用未经授权的软件、访问未经授权的网络等。此外，定期进行安全演练和漏洞扫描。通过定期的安全演练，可以测试系统的安全性，并及时发现和解决漏洞。漏洞扫描可以帮助发现系统中的漏洞和风险，及时采取措施加以修复。最后，建立安全事件响应机制。当出现安全事件时，应该有一套完善的响应措施，包括紧急修复措施、数据恢复计划等。同时，应该对事件进行调查和分析，以便改进安全策略和防护措施，避免类似事件的再次发生。

3.2 数据备份和恢复技术

在制定安全策略和规范的同时，应该建立定期的数据备份和恢复机制。首先，确定备份频率和备份存储位置。根据系统的使用频率和重要性，确定数据备份的频率，可以是每天、每周或每月进行备份。同时，选择合适的备份存储位置，可以是本地硬盘、网络存储设备或云存储服务。其次，选择适当的数据备份方式。常见的数据备份方式有完全备份、增量备份和差异备份。完全备份是将整个系统或文件夹的数据全部备份，增量备份是备份系统或文件夹中自上次备份以来发生变化的部分，差异备份是备份自上次完全备份以来发生变化的部分。根据需要和数据的重要性选择合适的备份方式。然后，确保备份的可靠性和安全性。备份数据应该存储在可靠的介质上，如硬盘、磁带或云存储服务商的服务器。同时，备份数据应该进行加密，以防止未经授权的访问和

泄露。

3.3优化系统盘

为了提高计算机系统的安全性和稳定性，可以采取一些措施来优化系统盘。首先，清理系统盘上的无用文件和垃圾文件。这些文件占用了系统盘的空间，并可能导致系统运行缓慢。可以使用磁盘清理工具来删除这些文件，释放系统盘的空间。其次，及时更新和升级系统盘上的软件和驱动程序。软件和驱动程序的更新和升级通常包含了一些安全补丁和修复，可以提高系统的安全性和稳定性。另外，可以考虑对系统盘进行分区和格式化。通过将系统盘分为多个分区，可以将系统文件和用户文件分开存放，提高系统的稳定性和安全性。同时，定期进行系统盘的健康检查和修复。定期检查系统盘的健康状态，并修复可能存在的问题，可以提高系统的稳定性和性能。此外，还可以使用一些优化工具来优化系统盘的读写性能，如清理无效的注册表项，优化文件系统等。通过这些优化措施，可以提高系统盘的稳定性和性能，减少系统故障和安全漏洞的发生。

3.4合理应用防火墙技术、补丁和杀毒软件

合理应用防火墙技术、补丁和杀毒软件是保障计算机系统安全的重要措施。首先，安装和配置防火墙是必要的。防火墙可以监控和控制网络流量，阻止未经授权的访问和恶意攻击。根据实际情况，可以选择硬件防火墙或软件防火墙，并针对内部和外部网络进行适当的配置。其次，及时应用补丁和更新。软件和操作系统的漏洞是黑客攻击的主要目标。及时应用供应商提供的补丁和更新，可以修复已知的漏洞，提高系统的安全性。同时，定期检查和更新杀毒软件也是必要的。杀毒软件可以检测和清除系统中的恶意软件，防止数据泄露和系统崩溃。最后，定期进行系统安全性评估和渗透测试。通过对系统的安全性评估和渗透测试，可以发现系统中存在的安全漏洞和风险，并及时采取措施加以修复。同时，还可以通过模拟黑客攻击的方式，测试系统的安全性和防护能力，找出可能的漏洞和问题。通过合理应用防火墙技术、补丁和杀毒软件，可以提高计算机系统的安全性，保护系统和数据的安全。

3.5构建安全维护平台

为了进一步提高计算机工程的安全性，可以考虑构建一个安全维护平台。这个平台可以包括以下几个方面：首先，建立一个全面的监控系统。这个监控系统可以监测计算机系统中的安全事件，如入侵尝试、病毒感染等。监控系统应该具备实时监测的能力，并能够及时发出警报和采取相应的应对措施。其次，建立一个信息共享平台。在这个平台上，不同的计算机工程师和安全专家可以共享他们的经验和知识，相互学习和交流。这样可以提高整个行业的安全水平，共同应对各种安全威胁。再次，建立一个漏洞管理系统。这个系统可以对计算机系统中的漏洞进行管理和修复。当发现一个新的漏洞时，系统应该能够及时通知系统管理员，并提供相应的修复方案。最后，建立一个跨部门的协作机制。计算机工程的安全维护是一个综合性的工作，需要不同部门和人员的协作。建立一个跨部门的协作机制，可以提高各个部门之间的信息共享和协调配合，从而更好地保护计算机系统的安全。通过构建这样一个安全维护平台，可以整合各种资源和力量，提高计算机工程的安全性，为用户提供更可靠的服务。

结语

综上所述，计算机工程安全维护对于保证计算机网络安全稳定运行具有重要意义，而在实际的计算机工程安全维护过程中，要加强对计算机工程存在的安全隐患问题进行全面分析和研究，并采取有效措施予以解决，从而有效提升计算机工程安全性。

参考文献

[1]张星梅.探讨计算机网络存在的安全隐患及其维护措施[J].电子技术与软件工程，2015（9）：225-225.

[2]吴志毅，茅晓红.探讨计算机网络存在的安全隐患及其维护措施[J].科技传播，2014（5）：223-224.

[3]周振柳，刘宝旭，池亚平，等.计算机BIOS安全风险分析与检测系统研究[J].计算机工程，2017，33（16）：114-116.

[4]甘泉.基于计算机工程的安全维护措施分析.2017