

计算机工程安全维护策略

李大伟

天津市第一轻工业学校 天津 300131

摘要: 计算机网络技术的发展促进了时代的变迁和进步, 不断增强了全球信息一体化的趋势。本文探讨了计算机工程安全维护的重要性, 分析了当前计算机工程面临的安全隐患及存在问题, 并提出了通过构建病毒防护系统、加强黑客攻击安全防护、优化系统盘程序与硬盘安全保护、强化防火墙技术应用、提升程序设计语言安全性、强化安全防范技术, 以及实施定期检测与安全使用等一系列针对性的安全维护措施。旨在为计算机工程的安全维护提供全面而有效的解决方案, 确保计算机工程系统的稳定运行和数据安全。

关键词: 计算机工程; 安全; 维护; 措施

引言: 随着信息技术的飞速发展, 计算机工程已成为现代社会不可或缺的重要基础设施。然而, 随着计算机应用的广泛深入, 其安全性问题也日益凸显。计算机工程系统面临着来自病毒、黑客攻击、数据泄露等多方面的威胁。因此, 加强计算机工程的安全维护, 确保系统稳定运行和数据安全, 已成为当前亟待解决的重要课题。

1 计算机工程安全维护的重要性

在信息化高速发展的今天, 计算机工程已经成为各行各业不可或缺的一部分, 它不仅推动着科技的进步, 也深刻地影响着人们的日常生活和工作方式。随着计算机技术的广泛应用, 其安全性问题也日益凸显, 计算机工程的安全维护的重要性体现在以下几方面: (1) 保障数据安全。在现代社会中, 数据已成为企业和个人的重要资产, 它记录了我们的工作成果、个人信息以及商业机密等。一旦这些数据被非法获取或篡改, 将会对个人隐私、企业利益乃至国家安全造成不可估量的损失^[1]。通过加强计算机工程的安全维护, 可以有效地防止数据泄露、非法访问和恶意攻击, 确保数据的完整性和保密性。(2) 确保系统稳定运行。计算机工程系统是现代社会的神经系统, 它支撑着各种复杂的应用和服务。如果系统出现安全问题, 如病毒感染、黑客攻击等, 将会导致系统崩溃、服务中断, 严重影响人们的日常生活和工作。通过加强安全维护, 可以及时发现并修复系统漏洞, 防范各种安全威胁, 确保系统的稳定运行。(3) 提升国家竞争力。在全球化背景下, 各国之间的竞争日益激烈, 而信息安全已成为国家竞争力的关键因素之一。通过加强计算机工程的安全维护, 可以提升国家的信息安全保障能力, 保护国家机密和关键信息基础设施不受威胁, 为国家的经济发展和社会稳定提供有力支持。

2 计算机工程安全隐患及存在问题

2.1 病毒侵袭

在计算机网络系统中, 病毒侵袭是长期存在且难以彻底根除的安全隐患。病毒以其隐匿性、触发性及可再生性, 对计算机设备及相关系统构成了巨大威胁。在病毒潜伏期间, 计算机的运行效率可能显著降低, 甚至出现自启动、死机等异常现象。更为严重的是, 病毒会隐藏于数据文件中, 通过文件的传输从一个计算机扩散到另一个计算机, 形成连锁反应。病毒的产生源于编制者在计算机程序中植入的破坏代码, 这些代码能够自我复制, 对系统造成破坏。病毒并非以单一个体形式传播, 而是依附于媒体文件, 如网络病毒、文件病毒、引导型病毒等, 通过数据信息的传输路径实现大范围感染。网络病毒可从执行文件侵入, 而引导型病毒则主动攻击驱动或硬盘系统, 若不及时处理, 将导致计算机无法正常运行或数据丢失, 给用户带来经济损失。

2.2 黑客攻击

黑客通过寻找系统漏洞, 如权限攻击、读取受限文件、拒绝服务等, 对计算机设备进行数字化攻击。在权限攻击方面, 黑客利用系统root身份, 攻击账号管理系统, 获取管理员权限, 从而实现了对计算机的完全控制。这种攻击通常基于缓冲区溢出原理, 对计算机守护进程进行逻辑攻击^[2]。读取受限文件攻击则是黑客利用无权限文件作为切入点, 通过深度分析文件与计算机安全管理特征, 设定文件权限, 进而渗透到用户系统中, 窃取文件或恶意篡改系统指令。黑客攻击手段的多样化, 使得计算机网络系统面临更加复杂的威胁, 用户数据安全和隐私保护面临严峻挑战。

2.3 用户安全意识薄弱

许多计算机用户在使用过程中, 习惯将软件设定为

默认获取信息与安全存储,导致用户隐私信息被同步存储到系统某个区域。用户在浏览网页时往往缺乏辨别能力,难以识别是否存在病毒或攻击行为。当计算机系统出现错误,如垃圾文件过多时,用户往往未能及时处理,导致程序产生漏洞,为病毒或黑客攻击提供了可乘之机。用户安全意识的不足,使得计算机系统暴露在更大的风险之中,不仅可能导致数据丢失或系统崩溃,还可能给用户带来财产损失。

3 计算机工程的安全维护措施

3.1 构建病毒防护系统

为了有效防止病毒入侵,维护计算机系统的安全,需要采取以下一系列严密且高效的措施。(1)应用高安全性的程序。防火墙和杀毒软件作为两大核心工具,发挥着不可替代的作用。防火墙能够精准地阻断恶意网络流量和软件,为系统筑起一道坚实的防线,有效抵御外部恶意攻击。同时通过VLAN系统的划分,将系统和用户进行隔离,进一步增强了系统的安全性。路由的网段划分功能,则使得网络流量更加有序,降低了病毒传播的风险。(2)杀毒技术的应用。选择正规、可靠的杀毒软件,并定期进行病毒库更新和全盘扫描,能够及时发现并清除潜在的病毒威胁。(3)实施身份验证技术。应确保只有合法用户才能访问系统资源,进一步提升了系统的安全性。(4)用户自身的操作规范。用户应养成良好的正规操作习惯,不随意点击未知网址或下载不明文件,以免给病毒提供可乘之机。定期对系统进行安全性排查,及时发现并修复安全漏洞,也是保障计算机安全的重要一环。以上措施共同构成了计算机安全的坚实屏障,为计算机工程的稳定运行提供了有力保障。

3.2 黑客攻击安全防护

黑客往往利用计算机系统已存在的漏洞进行攻击,构建分层次、分级别的检测与修复机制成为关键,应做好以下几方面:(1)以防火墙为基础,对计算机系统的内部程序和硬件设施进行边缘化防护。防火墙能够监控并控制进出网络的数据流,有效阻止未经授权的访问和数据泄露。在此基础上,应设定具有过滤属性的路由器,通过其转发分组功能,对IP地址进行加密处理,增加数据解密的难度,从而有效抵御黑客的IP攻击。(2)实施双速网关机制。该机制利用计算机系统不同应用层或代理层的网关处理形式,对数据信息形成特定服务或请求的响应,将用户与服务器进行关联。这种机制能够将数据信息独立于整个服务体系之上,有效阻隔外部传来的潜在威胁信息^[3]。对于单一信息渠道的数据流,双速网关机制能够实现数据信息在服务代理器之间的合法处

理,确保数据传输的安全性。(3)加强对系统漏洞的检测与修复。通过定期扫描系统,及时发现并修复已知漏洞,防止黑客利用这些漏洞进行攻击。同时建立应急响应机制,一旦发生黑客攻击事件,能够迅速响应并采取措施,将损失降到最低。

3.3 系统盘程序优化与硬盘安全保护

计算机系统盘作为程序安装的核心区域,其状态直接关系到计算机的安全与运行效率。为确保系统高速运行并降低安全风险,用户需采取以下一系列措施来定期优化系统磁盘。(1)避免将所有应用程序一股脑儿地安装在系统盘(通常是C盘)上。系统盘不仅负责存储系统文件,还需处理应用程序的启动与运行。若系统盘空间被大量应用程序占用,将导致计算机启动缓慢,甚至影响系统整体性能。建议用户在安装软件时,选择D盘或其他非系统盘作为安装位置,为系统盘预留足够的运行空间。(2)定期优化系统磁盘内存。用户可借助系统自带的磁盘清理工具或第三方优化软件,定期清理系统中的无用文件、临时文件和垃圾文件,释放磁盘空间。对系统盘进行碎片整理,以提高文件访问速度。(3)硬盘作为存储计算机所有信息的重要载体,其安全性不容忽视。为防范病毒入侵,用户需安装可靠的防病毒软件,并定期更新病毒库,以确保系统免受病毒侵害。防病毒软件不仅应部署在服务终端操作平台上,还应覆盖界面操作系统,形成全面的防护体系。一些高级病毒能够篡改系统数据,导致计算机无法正常运行或启动。用户在遭遇病毒感染时,迅速采取措施隔离病毒源,并利用防病毒软件进行彻底清除。定期备份重要数据,以防数据丢失或损坏。

3.4 强化防火墙技术应用

在计算机运行维护中,合理且有效地应用防火墙技术不仅能够为计算机筑起一道坚实的防护屏障,还能有效抵御网络攻击,确保计算机及数据的安全。应做好以下几方面:(1)计算机用户需深刻认识到防火墙技术的重要性,充分利用其对网络访问进行严格的安全防护。通过防火墙技术的部署,能够有效阻止黑客对计算机的非法入侵,防止重要信息数据被破坏或泄露。这要求用户在计算机运行期间,始终保持防火墙技术的开启状态,并定期检查其配置与运行状态,确保其发挥最大效用。(2)防火墙技术具备智能预警功能。当计算机浏览存在风险的网页时,防火墙会立即发出警告,提醒用户注意潜在威胁,并对计算机内部的重要信息和文件进行保护。这一功能能够显著提升用户的安全意识,促使用户及时采取措施应对潜在风险。(3)防火墙技术还具备

强大的网络信息检测能力。它能够对网络中的数据包进行实时监测与分析,一旦发现存在危险性的信息,防火墙会自动将其屏蔽或阻挡,防止其进入计算机系统。这一功能能够有效过滤掉网络中的恶意流量,降低计算机遭受攻击的风险。

3.5 强化程序设计语言应用

在计算机工程安全管理中,程序设计语言直接关系到计算机网络的安全性。传统的低级语言虽易于维护,便于技术人员快速解决问题,但其安全性相对较低,易受网络攻击。为提升计算机网络安全,必须掌握并应用更高级的语言,应做好以下几方面:(1)需要对不同种类的程序设计语言进行深入学习和了解。每种语言都有其独特的设计理念和优势,通过对比分析,可以更好地把握它们各自的特点和适用场景。在此基础上,针对不同语言的设计难度进行合理的研究,明确其安全性能和维护要求。(2)制定具有针对性的维护措施。根据各种语言的特点,制定相应的安全策略和维护计划,确保在实际应用中能够充分发挥其优势,同时有效避免潜在的安全风险。(3)将高级语言合理地运用到计算机网络系统中。在系统设计阶段,就应充分考虑安全性因素,选择合适的程序设计语言,并优化其应用方式。通过高级语言的运用,可以构建更加安全、稳定的计算机系统,为网络安全提供有力保障。

3.6 强化安全防范技术

计算机网络在运行过程中面临着来自内外的多重威胁,提高安全防范技术成为确保计算机稳定运行、保障其安全性的关键。以下是一系列针对性的技术措施:

(1)计算机设备和软件的升级与更新。随着技术的不断进步,新的安全漏洞和威胁层出不穷。定期升级计算机硬件和软件,以确保它们具备最新的安全功能和修复补丁,是防范安全风险的第一步。操作人员需不断提升自身的防范意识,通过日常的系统查杀和漏洞检查,及时发现并修复潜在的安全问题。(2)实施定期的安全检查。这包括检查计算机的硬件配置、软件运行状态以及网络连接情况,以确保它们处于正常且安全的状态。通过定期检查,可以及时发现并解决可能因外界因素导致的软硬件损坏或异常,从而有效避免安全事件的发生^[4]。

(3)提高个人安全防范意识。对于各类不明链接和邮

件,应保持高度警惕,避免点击或下载可能携带恶意软件的内容。积极安装并定期更新杀毒软件,对计算机进行全面杀毒,以清除可能存在的病毒和恶意程序。这些措施将有助于构建一个更加安全、可靠的计算机使用环境,有效抵御网络安全问题的侵扰。

3.7 定期检测与安全使用策略

计算机工程系统存在漏洞,常为病毒和黑客提供可乘之机。为确保系统安全,应采取以下策略:(1)定期检测预防系统漏洞被利用。利用专业的安全工具和技术,对系统进行全面扫描和分析,确保每一个细节都不被遗漏。一旦发现漏洞,应立即进行修复,并加强安全防护,防止类似问题再次发生。(2)提高安全使用意识。避免访问不明来源或存在安全隐患的网站,以减少病毒和恶意软件的感染风险。在浏览正规网站时,也需警惕个人信息的保护,切勿轻易留下身份证号、银行卡号等敏感数据。(3)定期更新和升级系统补丁。通过更新系统补丁,可以确保系统具备最新的安全功能和防护能力,从而有效抵御新的安全威胁。

结束语:计算机工程的安全维护是保障其稳定运行和数据安全的关键。通过构建全面的安全防护体系,实施有效的安全维护措施,我们可以有效应对计算机工程面临的各类安全威胁。未来,随着技术的不断进步和应用的不断深化,计算机工程的安全维护将面临更多挑战和机遇。我们应持续关注安全技术的发展动态,不断提升安全维护水平,为计算机工程的可持续发展提供有力保障。

参考文献

- [1]孙海玲.计算机网络安全隐患及有效维护措施分析[J].信息与电脑(理论版),2018(09).
- [2]张文锦.计算机的软硬件维护和网络安全防护问题与策略[J].信息通信,2019(09):140-141.
- [3]生飞.网络安全技术在计算机维护中的应用及作用[J].电脑知识与技术,2019,15(25):29-30.
- [4]王永华,张岩.基于计算机工程的安全维护措施[J].计算机与网络,2021,47(10):55-58