

计算机硬件与网络安全研究

万 兵

中国电子科技集团公司第三十研究所 四川 成都 610041

摘 要: 计算机网络技术已经在人类的生活中, 占有了日益重要的地位它不但为中国人民的正常生活创造了便利条件, 还为整个中国经济社会的发展提供了新的动力与机会。计算机技术对于人类的生存及其对社会的危害将日益巨大, 将越来越深入到行业当中。由于计算机网络技术的迅速发展, 计算机系统的安全问题始终是计算机网络技术的核心。而且计算机安全是互联网中的很大组成部分。对电脑的硬件进行适时维修和更换是防止其发生安全问题的关键所在。同时还能够从一定意义上保障电脑的安全。

关键词: 计算机硬件维护; 网络安全; 研究

引言: 伴随发展脚步的不断加快, 计算机网络逐步渗透到日常生活的方方面面之中, 给生活带来诸多便利。但不可否认, 网络系统的安全问题也成为用户最为困扰的对象, 因为计算机网络复杂性较高, 可能会受到诸多因素干扰, 导致安全问题时有发生, 同时网络数据存在一定的安全漏洞, 可能会直接影响到用户的财务安全。由此来说, 如何提升网络系统安全程度, 优化硬件系统的维护方式, 创建更加稳定的网络环境, 为计算机运行提供保障就成为重要的研究方向。

1 计算机网络安全中硬件维护的重要意义

对电脑的网络安全问题来说, 由于硬件设备工作状态不稳定或所处环境比较不良, 会造成硬件设备的使用寿命较短, 从而对其正常工作功能、计算机功能等产生负面影响, 从而对安全控制系统形成直接或间接的威胁。如此一来, 在计算机等硬件设备中的电子检测设备也就变成了极其重要的设备。在机器工作环境中, 对环境因素所产生的影响至关重要, 当消除了湿度、静电、电磁波等的影响以后, 电磁场强度很快就可以对电脑中的集成电路设计产生重大影响, 甚至还能够导致计算机部件的氧化腐蚀, 进而会影响计算机的工作状态, 以影响正常的网络安全工作^[1]。另外, 当空气污染物、温度湿度条件等环境参数都不能满足计算机硬件的要求时, 硬件装置内的金属元素很容易和其他材料进行化学反应, 甚至发生金属氧化问题, 干扰电子元件的正常工作、影响机器的正常工作。而计算机硬件设施在网络安全构建中又有着关键的角色, 在这些硬件设施的运营过程中, 唯有确保系统所有信息及选项的满足需求, 方可起到有效的安全防护效果, 以保证计算机软件及系统的顺畅、安全应用。

2 计算机硬件维护与网络安全的相关性

2.1 硬件外部环境维护与计算机网络安全的相关性

计算机网络系统的运行同硬件系统有着紧密关联, 因此日常对硬件设备的维护工作就显得至关重要。同时运行环境也对硬件系统的使用周期有着直接影响, 如果长期运行在恶劣环境中, 就可能导致硬件设备出现异常, 无法达到预期功能, 进而影响网络系统的安全性。确保外部环境同实际需求相匹配是硬件系统维护工作中的重要环节。当计算机硬件装置处于良好的环境中, 其性能可以达到最佳状态, 为网络安全奠定坚实基础。温湿度、磁场强弱均会对硬件系统运行产生干扰, 也决定着计算机能否正常运转^[2]。由于南方地区常年湿润, 计算机长期运行于该环境中, 硬件设备的集成电路就可能受到影响, 导致无法正常工作, 影响整体的系统运行。此外, 如果计算机设备周围环境的磁场强度过高, 一旦用户直接同显示器设备接触就会造成触电问题, 其原因是显示器设备所携带的电荷同人体之间出现静电反应, 该反应会严重损害计算机系统安全, 甚至造成计算机整体瘫痪, 给用户带来难以弥补的经济亏损。

2.2 硬件设施中网络电缆、网卡与网络安全的相关性

除了外部环境的影响以外, 电缆线路和网卡同计算机网络系统是否安全也有着直接关联。其中网卡是保证计算机网络运行的基础所在, 如果在运行中网卡发生问题, 网络系统就会异常, 出现无法连接的情况, 同时也会造成用户传输数据的中断, 严重影响用户使用体验^[3]。由此来说, 技术人员在装设网络系统时应特别注意, 首先需要全面熟悉网络系统部署安装的各个环节和具体操作, 确保装设完成后可以正常运行, 为计算机安全提供有利保证, 真正优化网络服务, 增强系统的安全性。

3 影响网络安全和计算机硬件安全的重要因素

3.1 环境因素

受到电磁波、高温和潮湿等环境因素的干扰,计算机硬件系统在工作环境中容易出现异常工作的情况,这非常不利电脑的安全。因此,在高温情况下操作电脑,容易使计算机硬件设计中的数据产生偏差,实际的数据会背离事先设置好的正常数据,并造成电子元件损坏、内部逻辑发生紊乱的故障问题。如果长期在低温条件下操作电脑,则计算机的硬件设备会长时间暴露于温度条件下,将会导致计算机的硬件设备产生腐蚀、生锈等故障问题,可以减少计算机的硬件工作时间^[4]。此外,计算机硬件系统如果受到电磁波的干扰,其产生的故障现象就十分明显。如果计算机工作中,在数据传送的过程中遇到电磁波干扰,计算机传递的数据也可能产生信号失真。所以,在电脑工作过程中,注意观察电脑的所处环境,要保证电脑在正常工作温度以下进行操作,并且要避免电磁波,防止电脑遭受其影响。

3.2 网卡和网络电缆因素

危害网络安全的另一种原因,是网卡和网络电缆。人们在配置网卡的过程中,如果对网卡的设置不合理,则电脑将无法顺利地实现联网工作,使得互联网信号传递产生了阻碍。所以客户在挑选网卡的过程中,往往需要针对计算机的工作方式进行具体分析的选择,并针对不同的信息传送场合进行相应的选型工作^[5]。

4 计算机硬件维护提升网络安全的策略建议

4.1 做好数据的存储以及输出的安全性

在当前的数字化社会,现有的互联网技术手段能够为互联网信息的保存和传递创造足够的环境,以保证数据的安全保存,高效传输。而目前,计算机在网络处理与传输过程中的保密工作重要性也正随着当前信息化社会的进步发展,而变得越来越突出^[6]。在消息传递过程中,必须对重要部分加以保密。而数据加密的思想,早在二战时期就开始被发明并广泛应用,这项技术可以有效克服数据在保存和传播过程中出现的危险和缺陷,不法分子可以在没有密文的前提下无法对截获的数据实施解密,从而保证了数据在传播和利用过程中的机密性、完整性和可用性。

4.2 合理的运用杀毒软件

局域网状态下计算机硬盘的安全隐患,有很多可能是遭到了网络病毒的入侵。在这些前提下,为电脑下载安装一个良好的杀毒软件,是普通用户在进行日常的计算机操作中最易于实现的电脑安全措施。杀毒的工作原理也相当简单,它就是通过对电脑上一直出现的文件进行逐个地排查,来判断电脑内是不是真的存在着网络病毒的。网络病毒的实质上,是一串程序代码,而杀毒软

件在经过检查后如果找到了病毒,就会自发启动将病毒的程序代码删除。这一系列的动作虽然繁琐,必须花费较多的功夫,然而实际并非如此。杀毒软件对所有数据的逐一检查,无论是及时性、准确性均远远胜过了人工排查^[7]。所以,对长期暴露于网络安全环境下的电脑而言,通过安装杀毒系统能够更有效地发现并试图伪装潜入电脑内的网络病毒,还能够对已完成潜入的网络病毒加以排除与粉碎,是普通用户用来对抗网络病毒攻击的最好途径。

4.3 不断提升相关技术人员的专业水平

当前,计算机技术愈来愈高,互联网愈来愈成熟。这就需要相应的科技工作者进一步提高自身专业知识的技能,才能有效的管理计算机系统,并使用户享受良好的售后服务。因为技术人员操作的失误可能造成整个网络发生问题,使计算机发生了安全问题。要想保障计算机系统的硬件设备,维护计算机系统安全,还需要人员应该具备良好的职业道德素质和正确维护计算机网络的基本知识和安全运行上网的技能^[8]。要经常组织有关科技工作者开展技术培训与考察,不断提升自身的网络管理技术水平,熟练掌握各种计算机病毒,并掌握其攻击手段的基本特征,准确找出解决之方法,及时采取防范措施与解决方案,并严格进行网络安全保护操作,以维护整个计算机的安全。

4.4 定期对计算机硬件系统进行维护

在维修计算机硬件设备中,重点要对网络设备、网卡以及计算机本身的各方面加以检查和维修。正确的操作方法应该是安装防火墙:因为在计算机系统上,防火墙是重要的防护措施。通过安装防火墙等于在电脑和互联网之间建立一个坚固的安全墙,控制对电脑内部的侵犯,以提高机器的自身稳定性。设置防火墙就好比在计算机中设置了一个锁,能够有效的防止不法人员对一个局域网的存取访问,这样减少了个人信息窃取与破坏的事件几率。此外,通过设置防火墙也如同给整个计算机系统自动地设置了一种可以进行监视的操作系统,它能够随时地为人们反馈入侵消息,并同时也有效地保存着整个计算机系统内的所有程序,可以更有效的报警,并记下所有入侵数据。安装防火墙也是计算机网络的安全性保障^[1]。一旦电脑不能安装防火墙,那么,电脑的安全将存在相当大的安全隐患存在。

4.5 安装防火墙装置

在防火墙正常工作流程中,会设置相应的防护体系,在数据的交换和传输中遵守一定的要求和标准,以防止内部数据外露,组织不良信息传播。在电脑实际操

作活动中,存在着各种的威胁影响,许多犯罪人员会通过互联网非法窃取或删除他人数据资料,这是影响计算机安全和网络安全的主要方面,还可能出现计算机瘫痪的各种问题,由此导致电脑没有了安全保护^[2]。防火墙装置便是硬件和软件结合的有效措施,一方面能够通过防火墙技术手段构建计算机网络防御系统,对计算机网络进行实时监控和防护;另外则通过设置的权限体系,有效防止外部信息和病毒的攻击,从而在软硬件协调下建立完善的安全保障体系。

4.6 采用先进的技术

人们在使用电脑和互联网的环境当中,防火墙技术能够供人们适当使用。防火墙技术可以设定网站的访问授权,控制没有通过许可的非法浏览活动,防止外界人士无法接触到的信息来源,可以较好的减少数据被丢失的可能性,进行适当预防。而且防火墙功能可以从一定意义上提高互联网运行的稳定性,给在互联网上的客户信息资料的安全性带来必要的安全保护,确保了信息在传送过程中的安全。而访问权限的设定也增加了对数据的安全。不能进行授权就不能对客户数据进行存取^[3]。防火墙能够监视互联网的工作情况,所以,我们能够去使用这个功能。之后,我们能够去使用入侵侦测功能。防火墙功能的不足可以通过入侵侦测功能去补足。通过这些方法对电脑中已有的数据以及正在访问或使用的数据进行监测和分析,网络上的异常欣喜和电脑硬件可以迅速的识别这些情况,从而对问题做出有效的解决,最后去改善电脑的硬件安全和网络安全。

4.7 利用硬件优化计算机网络的性能

在使用互联网过程中,要产生大量的重要信息,同时数据的传递过程中也会出现大量的垃圾信息,这种垃圾信息将会降低整个互联网的安全性,会减少节点设备和局域网间的宽带,从而增加了带宽输出,但同时清除数据垃圾也要耗费不少时间和清理的时间。想要更有效的保护计算机数据安全,提升电脑的使用性能,就必须实时的对计算机产生的垃圾信息进行处理,也可以修改原有的程序算法,或者通过对硬件模块的加速技术来处

理问题^[4]。其加速的手段是技术目标硬件加速技术,提高设计效能,释放了CPU时间,进一步增加应用软件的工作能力,使应用软件的可靠性提高。另外,它还可以扩大数据包的允许范围,使得计算机系统的稳定性保持良好的程度,对于整个计算机系统的安全起着十分关键的作用。

结语

综上所述,在现代社会中,电脑和互联网早已成为了当代人类日常生活与工作环境的必要条件,而网络安全问题也逐渐成为了危及人类正常生存的关键因子。而硬件是计算机设备的核心所在,对安全具有直接的作用效应,所以必须充分认识硬件对安全的作用,从而掌握相应的运用方法和保护技术,以确保硬件设施的平稳工作,保证互联网的永久安全性。

参考文献

- [1]黄家永.计算机硬件维护技术及故障解决[J].电子世界, 2020(1): 196-197.
- [2]张伟.计算机硬件故障分析与维护处理策略[J].信息与电脑(理论版), 2020, 32(9): 29-31.
- [3]王旭.计算机硬件组装及维护的关键技术研究[J].南方农机, 2020, 51(1): 217, 219
- [4]崔丽娟.浅析硬件维护在计算机网络安全中的重要性——评《计算机硬件基础与维护技术》[J].现代雷达, 2021, 43(6): 107.
- [5]郑恒河.信息时代计算机网络安全管理策略探索——评《计算机网络安全原理》[J].中国安全科学学报, 2021, 31(10): 200.
- [6]廖桂芳, 刘鹏.计算机硬件维护在网络安全中的重要性研究[J].电脑知识与技术, 2020, 16(2): 12-13.
- [7]刘鹏, 廖桂芳.网络环境下计算机硬件安全保障和维护策略研究[J].卫星电视与宽带多媒体, 2019(24): 50-51.
- [8]安积慧.计算机硬件维护与网络安全的相关性探析[J].卫星电视与宽带多媒体, 2020(14):3.