

新形势下计算机网络通信中存在的问题及改进策略

张智勇 谭智敏*

北京计算机技术及应用研究所 北京 100089

摘要: 随着信息时代的到来,信息网络通讯和计算机应用技术也在不断发展。新时代的计算机网络通信技术具有共享和大数据处理的特点,人们利用其可以进行更为高效的工作。但是在新形势下计算机网络通信技术仍然存在许多问题。

关键词: 计算机;信息网络数据;通信信号;通信安全

一、引言

在科学技术的不断发展背景下,计算机通信网络技术得到快速的发展,人们的生活和工作中已经离不开计算机通信网络技术,然而,在具体的应用过程当中,计算机网络技术还存在一些安全问题,对计算机通信网络技术产生了很大的影响,不利于计算机通信网络技术的发展。

二、计算机网络通信安全防范的意义

1. 有助于推动人们正常工作

当今社会,计算机技术早已全面普及,人类生活、工作都高度依赖于计算机信息系统。各个单位与企业为了更加方便、高效地开展工作的,都大量应用计算机网络实现对工作资料与数据的传输、处理与保存。但是,由于计算机网络通信安全问题一直存在,个别不法分子时常利用技术漏洞盗取企业机密,这就使得部分企业根基受到严重威胁,让企业难以健康、可持续发展,有的企业甚至因此丢失核心数据不得不面临破产的艰难处境^[1]。

2. 能够维护人们的个人利益

计算机网络通信涉及人们生活的方方面面,其不关系着人们的工作效率,更在人类日常生活中扮演着重要角色。例如,人们利用微信进行沟通联系、利用电子邮件传输资料信息等。然而,部分不法分子依然会攻破网络防护盗取聊天信息、冒充他人骗取钱财、窃取机密文件……这些行为使得个人的利益与安全受到了严重威胁,所以加强计算机网络通信安全防范迫在眉睫^[2]。

三、计算机网络信息通信安全问题

1. 病毒入侵威胁

网络信息时代对计算机信息安全来说,病毒是非常大的威胁。计算机病毒不仅能够对计算机系统当中的文件进行恶意篡改,还能获取计算机中的数据信息。计算机病毒最大的特点就是传染性和隐蔽性,其可以借助硬盘或软件系统快速扩散,利用计算机操作系统或管理程序中的漏洞来攻击用户。一旦计算机被病毒攻击,就会产生运行问题,如运行迟缓、死机等,遭受病毒攻击程度较深时甚至会造成系统瘫痪^[3]。

2. 数据信息失窃

计算机网络十分开放,用户可以访问各种网站,因此用户操作不当或误点非法网站,都有可能造成计算机中毒,威胁计算机的信息安全。就目前而言,还没有形成十分健全的网络安全防护体系,用户端必须严格执行安全防护措施,才能确保计算机网络信息安全。然而,不少计算机用户都未树立起高度的安全意识,没有进行应有的安全防护,造成网络安全问题时有发生。除此之外,用户的错误操作,也会损害网络运行安全,导致个人隐私信息泄露,当被不法分子窃取了重要信息后,有可能会借此开展攻击,给用户带来严重损失^[4]。

3. 通信信号问题

计算机网络通信过程中,固定网络和移动网络端口之间的信息传输主要取决于空中接口。但是由于空中接口始终是开放的,因此当其他人使用该开放接口来非法传输由发送器发送的信息时,如果不能及时地删除或纠正故障,发送的信息将被公共接口窃取。这种行为称为数据攻击,是通过开放接口对发送器发送的信息进行的非法操作,例如删除、更改、窃取和其他不当行为。作为移动网络的固定网络端口和主要信息传输通道,无线接口处于同时向外部和内部开放的位置。面对数据攻击,

*通讯作者简介:谭智敏,1977年10月,男,汉族,湖南衡阳人,现任北京计算机技术及应用研究所副主任,高级工程师,硕士研究生。研究方向:计算机技术。

第一作者简介:张智勇,1989年04月,男,汉族,山西阳高人,设计师,本科,研究方向:计算机技术。

网络通信开发者需要采取相应的措施避免发生这一现象,以免信息因处理不当而影响正常操作^[1]。

4. 通讯技术问题

硬件错误和软件错误是计算机网络通信技术问题的两个最重要的方面。其中,硬件错误很容易发现。一般情况下,当计算机网络通信硬件设备出现故障时,会出现一些相关的提示,例如网络连接错误,以减少网络通信出现故障的情况。然后,计算机的异常通信通常是由软件错误引起的。如果发生计算机软件问题,将影响网络通信的质量。硬件和软件是通信技术中影响较大的因素,因此,为了尽可能降低通信风险,需要针对该问题提出相应的解决方案。计算机网络通信技术经常面临硬件或软件错误。使用者通过计算机发出的提示,可以清楚地判断计算机的硬件错误。如果计算机硬件出现问题,它将影响用户的可用性。因此,由于在用户使用过程中无法显示页面,或者网络速度迅速下降,将导致网络通信的质量下降,此时就可以考虑是否是计算机软件出现了问题^[4]。

四、探究计算机网络通信安全的有效防护措施

1. 应用信息加密技术

通过对网络信息进行加密,能有效的维护计算机的安全。一方面可以保证信息数据的安全,另一方面也能在第一时间保证数据的完整性。计算机网络加密技术是对相关数据的信息转化,从而形成带有密码的数据,通过对于加密技术的使用,能更好的将一些密文转换为明文数据。应用信息加密技术可以分为对称式的加密技术和非对称式的加密技术,两者在使用过程有着明显的不同,前者的加密密钥和解密密钥是相同的,优点在于算法实现后的效率高,速度快;后者的加密和解密会使用两把不同的密钥,加密密钥是向社会公开的,私匙是秘密保存的,只有私匙的所有者才能利用私匙对密文进行解密^[3]。

2. 管理措施

(1) 加强网络信息安全防护意识的宣传

加强网络通信安全的宣传,努力增强人们对网络安全的认识,提高相关工作人员的专业技能,强化网络信息安全防护意识,是保障计算机网络通信安全的前提条件。相关单位应当积极开展有关培训工作,不断强化工作人员的计算机技能,帮助用户掌握计算机防护办法,努力优化管理结构,全面提升人们保护个人信息、企业机密和国家信息的意识^[2]。

(2) 加强技术研发

计算机网络通信安全离不开高新技术的支持,所以,我们要加强相关技术的研发,努力研究安全性能强的新型通信技术,不断填补系统漏洞,加强安全防卫,从硬件、软件各方面想办法提高计算机网络信息安全防范能力和通信设备的抗灾能力。

3. 利用网络防火墙技术

防火墙作为计算机网络的第一道安全屏障,将计算机和网络间连接在一起,传输个人和网络信息,都应该通过防火墙。当下,防火墙技术是应用最普遍的,也是比较有效的一种防护技术。一些比较严谨的计算机代理服务,已经把防火墙技术和包滤技术结合在一起,发挥二者的共同作用,更有力地保障了计算机系统的可靠性。防火墙技术能够检测和阻挡网络中的病毒,或是降低病毒的攻击性,来保证网络通信安全不受损害。设定防火墙功能,可以对一些不常用的窗口进行统一管理,封锁病毒,同时也可以禁止用户访问非法网站,以避免计算机信息受到损害^[1]。

4. 通讯信号问题的改进策略

为避免由于物理因素而导致的计算机网络连接失败,可以选择一个稳定性强的电路,以最大程度减少电磁波对计算机造成的影响。对于家用计算机,请检查电源电压,更换稳定的电源,并执行合理的操作,以最大程度减少扩展模块和其他模块的故障。有许多情况会导致网络连接问题,并且在许多情况下是由于物理因素引起的。因此,有必要每天对硬件设施进行测试,并确保其质量符合标准要求。除了选择具有高检测精度的设备调试,如光纤电缆、路由器和集线器之类的设备外,还必须选择合适的计算机网络通信路径,以避免在计算机使用过程中由于电磁干扰而引起通信干扰^[2]。

5. 加强网络系统监控

在计算机使用过程中,网络病毒入侵体系检测是一门综合性较强的防护技术,通过使用这项技术,能大大的降低木马病毒的入侵,追逐时间,网络正常运行的状态。通过结合这项技术,能够对一些不法入侵的病毒进行查看和分析,再将其进行统计分析和签名分析。在具体使用过程中,统计分析法是对网络正常使用状态进行监测,从而辨明这个使用过程中是否存在非法入。签名分析的方式,是对网络已知的弱点进行管理和检测。这两种办法综合使用起来能从根本上降低计算机病毒入侵的概率^[1]。

五、结束语

总的来说,计算机网络通信技术的大力发展和普及

是新时代的趋势。从计算机网络通信技术发展程度和与社会适应程度的角度来看,新形势下的计算机网络通信技术仍然存在较多问题,这就需要相关研究人员对其中存在的问题加以分析和探究,并探索出相应的解决策略。在此背景下,本文对计算机网络通信中存在的问题进行分析,并提出了新形势下计算机网络通信的优化对策,能够为提升计算机网络通信质量打下良好的基础。相信随着计算机网络通信技术的发展,其能够为人们提供更为方便快捷的通讯方式,不断提高人们的生活质量。

参考文献:

- [1]曾帅.计算机通信网络安全维护措施探究[J].中国新通信, 2020, 22 (03): 29-30.
- [2]黄磊.新形势下计算机通信网络安全隐患及其对策探讨[J].中国新通信, 2020, 22 (05): 30.
- [3]胡中雨.计算机网络通信安全问题及防范措施分析[J].
- [4]谢润超, 刘龙.新形势下计算机网络通信中存在的问题及改进策略[J].数字通信世界, 2020 (10): 158.