

网络环境中的数据安全问题和对策

张晓卓

天津市医学科学技术信息研究所

DOI:10.12238/pe.v2i4.8348

[摘要] 目前,网络环境复杂多变,计算机数据安全问题较为突出,比如容易出现数据丢失、篡改等现象,从而对个人、组织等带来严重的经济损失。因此,本文主要阐述了网络环境中数据安全的意义,并基于数据安全问题,提出了相应的解决对策,以期为相关人员提供有效参考。

[关键词] 网络环境; 数据安全; 问题; 对策

中图分类号: TN711 文献标识码: A

Data Security Issues and Countermeasures in Network Environment

Xiaozhuo Zhang

Tianjin Health Information Research Center

[Abstract] The network environment is complex and ever-changing, and computer data security issues are prominent, which can easily lead to data loss, tampering, and other phenomena, causing serious economic losses to individuals, organizations, and others. Therefore, this article mainly elaborates on the significance of data security in the network environment, and proposes corresponding solutions based on data security issues, in order to provide effective reference for relevant personnel.

[Key words] network environment; Data security; Problem; countermeasure

在计算机网络环境中,数据安全面临着严峻的挑战,因此,相关从业人员必须加大数据安全力度,采取多样化的数据安全防护策略和技术,以筑牢数据安全的防线。此外,还需更新观念,对数据安全问题给予高度重视,结合现实情境,积极探寻并实施有效的解决方案,以确保数据安全保护工作更具针对性和实效性,从而营造一个更为安全可靠的网络环境。

1 网络环境中数据安全的意义

1.1 提升网络环境的安全性

在新时代的发展浪潮中,人们在工作和生活中对网络技术的依赖日益增强,这要求我们务必不断优化网络环境,严密保护数据安全,以提供更加便捷的服务。网络作为人们沟通交流的核心平台,其高效的信息传递能力和数据共享功能显得尤为关键。一个安全的网络环境,能有效预防数据丢失、泄露和篡改的风险,显著提升数据传输的安全性。因此,强化网络环境中数据安全的保护工作,不仅有助于保障网络系统的稳定运行,还能营造一个安全的网络环境,防止不法分子的入侵,进而充分发挥网络在社会发展中的重要作用。

1.2 确保财产安全

随着科技的进步,网络支付手段及平台日益多样化,规模持续扩大。其中,支付宝、微信支付等支付软件凭借其卓越的发展速度和广泛的普及度,已深受社会大众的青睐,成为支付的首选

方式。然而,网络支付在提供便捷性的同时,也伴随着不容忽视的安全隐患,这些隐患可能威胁到用户的财产安全。例如,部分不法分子利用先进的网络技术,入侵个人支付账号,窃取用户财产。因此,加强网络环境中的数据安全保护工作显得尤为重要。这不仅能够有效规范并监管网络不法行为,还能通过多种网络安全预防技术,切实保障人民群众的财产安全^[1]。

1.3 促进社会和谐发展

网络环境的数据安全保障工作的高质量实施,对于社会的和谐稳定发展起着至关重要的推动作用。它不仅是维护网络安全、保障信息安全的基石,更是构建数字社会、推动经济社会持续健康发展的必要条件。在新时代,人们对于大数据、计算机等技术的研究力度显著增强,技术水平的提升为网络环境中的数据安全提供了更为坚实的保障。这不仅有效避免了黑客恶意攻击、病毒入侵等风险,还高效保护了国家机密文件等重要数据,确保了政府等相关关键单位的各项工作能够安全、有序地推进。

此外,网络数据传递的高速和广泛特性无疑给网络监管工作带来了更大的挑战。部分人员通过网络肆意传播负面、消极、有害的信息,导致谣言泛滥,对社会和谐稳定构成了直接威胁。因此,我们需要对网络数据进行全方位的管控,提升网络监管水平,以便及时发现并制止这些不良信息的传播,改

善网络环境,净化网络信息,为社会的和谐稳定发展提供更有力的保障。

2 网络环境中数据安全问题

2.1 黑客恶意攻击

黑客一词原指那些精通计算机编程,能够独立开发计算机程序的专业人士。然而,随着我国科学技术的飞速发展,市场上涌现出多种黑客软件与工具,它们借助互联网迅速传播,使得“黑客”一词逐渐带有贬义色彩。不少热衷于计算机技术的人员,利用这些黑客工具与软件,对他人或组织的计算机系统实施非法访问,这不仅对计算机系统的安全稳定性构成直接威胁,还可能引发重大的经济损失。更为严重的是,黑客借助非法软件与工具,恶意侵入计算机系统,窃取重要数据或篡改信息,这进一步加剧了网络数据安全的隐患^[2]。

2.2 木马病毒入侵

网络因其开放性的特质,随着技术的持续革新,涌现出多种木马病毒,对计算机网络的数据安全构成了显著威胁。不法分子为窃取重要信息,将木马病毒植入个人和企业的计算机网络中,这些病毒在入侵时,隐匿地布置了大量软件和网址,诱导用户下载软件、访问网址,悄无声息地将木马植入网络系统,从而实现了对网络数据的操控。木马病毒潜伏性增强,其隐蔽性使得人们难以察觉,长期潜伏在计算机网络设备中,并选择关键时机进行大规模爆发,严重威胁网络数据安全,甚至导致带有木马病毒的计算机网络设备损坏,引发网络系统的大面积瘫痪。

此外,部分用户在使用计算机网络时,缺乏必要的网络安全保障技术应用,未能按照规范安装木马病毒查杀软件,导致计算机设备安全防护不足,出现了数据访问、残留数据等安全问题。而一些个人或企业在使用计算机设备时,虽然安装了病毒查杀软件和防火墙等防护措施,但由于长时间未进行更新升级,其防护效果大打折扣,难以有效抵御不断更新的木马病毒,仍然面临着诸多数据安全问题。

2.3 专业人员技术能力有待提高

网络环境的数据安全保障工作,对专业技术人员的综合能力和素养提出了极高的要求。为了维护网络安全,防止不法分子侵袭,保障网络系统稳定运行,并优化网络环境,技术人员需运用先进技术,结合丰富的实践经验。然而,当前部分网络技术人员在综合能力和素质方面尚待提升,缺乏具备高水平、高素养的专业人才。

网络环境的数据安全保障工作之所以复杂,是因为其涉及范围广泛,要求严格且难度大。此外,不断更新的木马病毒和多元化的隐藏方式,为网络技术人员带来了极大的挑战。因此,我们需要持续加强技术人员的培训和能力提升,以应对日益复杂的网络环境安全挑战。

3 网络环境中数据安全的保障措施

3.1 强化网络数据安全意识

网络数据安全管理工作的重要性不言而喻,要求相关人员必须给予高度的重视,并深刻认识到其在当前信息时代的关键

作用。为了确保网络数据的安全性,我们需要主动出击,通过多样化的途径,积极学习并掌握网络安全防护的专业知识和技能。因此,在网络环境中开展数据安全保护工作,相关部门必须采取一系列切实有效的措施。这包括合理开展网络数据安全信息的宣传工作,以增强公众的网络数据安全意识。具体而言,相关部门可以利用线上平台如微信、微博、短视频等新媒体工具,广泛传播网络数据安全知识;同时,也可以通过线下方式,如组织专题讲座、开展教育培训、发放宣传手册等,来进一步提升宣传工作的质量和效率。通过这些努力,我们能够共同构建一个更加安全、稳定的网络环境。例如:人们在日常工作、学习和生活中会使用多种类型的网络平台,包含部分邮箱、电脑系统账户、银行账户等多种个人私密账户,这就需要人们合理设置账户密码,尽量选择多种复杂元素设置密码,组合使用数据、符号、英文字母大小写等,增强个人私密账户的安全可靠性,降低数据安全问题发生概率。同时,相关人员在网络数据安全宣传工作中,引导人们不能随意点击来路不明的链接、网址,减少木马病毒入侵现象。此外,做好网络使用各类法律法规的宣传,增强人们的法律意识,引导人员在日常使用计算机网络的过程中自觉遵守相关法律规定,保证操作行为的合规合法性,最大限度降低网络环境中数据安全问题发生概率,进一步保证网络数据的安全可靠性^[3]。

3.2 加强网络数据安全保护技术的应用

在网络环境中,为确保网络数据安全的全方位提升,我们需对内部信息数据、软硬件设备及程序进行细致的综合管理。同时,加大各类保护技术的应用力度,以进一步增强网络数据的安全性。通过这样的全面管理与技术应用,我们能够更好地保护网络数据安全,降低潜在风险。

3.2.1 数据加密技术。计算机设备使用中,用户通过计算进行数据传递,从而促进不同终端互相通信。计算机在网络环境中容易受到多种类型病毒的侵袭,从而破坏、篡改数据,产生文件数据传输中出现的问题。而多源数据加密技术的应用,能够在很大程度上避免这些问题的发生,进一步保障数据安全。例如:(1)链路数据加密技术:该技术在实际应用过程中,用户发现部分计算机系统运行中出现病毒入侵的问题,可以充分发挥该技术的模糊性功能,提高数据的安全可靠性。同时,人们利用具体的链路技术,全方位包含网络数据传输过程,并优化不同数据,保障数据安全。在此过程中,出现外来者突破防火墙,非法侵入计算机系统,难以在较短时间内及时、准确地发现传输数据,避免数据问题。(2)软件加密技术:网络环境复杂多变,为了进一步保护个人或者相关组织的各类关键数据,就需要相关专业人员科学使用多种类型的杀毒软件,并在实际应用中,确保杀毒软件的针对性和有效性,定期进行更新升级,从而更好地应对多种类型的木马病毒等。通过结合软件加密技术,充分发挥杀毒软件的重要作用,更加高效地预防多种网络病毒入侵。同时,进行防病毒软件的全面检测、控制工作,从而有序控制计算机,增强加密功能,确保网络数据安全^[4]。

3.2.2 入侵检测技术。相关专业网络技术人员不断加大入侵检测技术的研究和开发,促进其逐渐发展成多元化的应用系统。新时期,网络环境中的数据安全问题频繁发生,为人们带来较大损失,而入侵检测技术水平不断提升,逐渐成为网络数据安全保护工作中不可缺少的关键技术。该技术在实际应用过程中,能够增强计算机系统对网络攻击的抵御能力,增强管理者的网络安全保护和管理能力,进一步保证数据安全基础设施的完整性。该技术能够对网络、系统内的大量信息数据进行全面采集并分析,综合判定其有无受到外来网络的攻击,并及时进行响应,迅速启动防御机制,进一步保证网络系统运行的安全稳定性。此外,在技术开发的产品能够在无人监控的环境下安全运行,具有良好的网络数据安全保护作用,甚至在计算机系统全面瘫痪的条件下持续运行,在不同网络系统中具有较好的适用性,增强网络数据安全防护性能。

3.2.3 防火墙技术。该技术在应用中,能够将内外网进行有效隔离,构建完全有效的防护屏障,防止网络数据受到外来攻击。同时,内部人员在没有相应权限的情况下,不能进行网络数据查询、使用等操作,避免人员非法修改、窃取。(1)合理设置访问权限:访问权限机制,能够保证计算机网络安全、稳定地运行,营造良好的网络数据访问条件。在此过程中,需要利用防火墙技术提供有力的保障。通常,人们在合理分配计算机功能后,利用防火墙技术优化资源分配,从而对于多种类型的网络数据进行合理分发,使得数据自动归档,针对性分配给相应的单位,并严格按照网络环境中数据内容、属性进行全方位保护,避免数据传输中出现安全问题^[5]。(2)身份认证:相关人员借助防火墙技术,对计算机设备使用者的身份进行认证,并引导其在通过身份认证后,安全进行数据传递、共享,全面保障网络通信安全,提高网络通信质量和效率。通过防火墙技术,更好地保护网络数据,防止其在传递中受到多种外部因素的影响,出现数据安全问

题。(3)系统监控。计算机网络系统在实际运行中存在较多安全问题。这就需要技术人员全方位监控计算机网络日志文件,及时发现各类问题,并制定针对性地解决措施,提升计算机网络保护效果。同时,利用防火墙技术,高质量监管日志文件,发挥其抵御病毒的功能。用户利用多样化方式,合理设置并优化分配多种程序编码,就能有效监控日志。

4 结语

互联网技术的持续创新与广泛应用,极大地便利了人们的生活,但同时也带来了前所未有的挑战与威胁。在享受计算机网络带来的种种便利时,不得不面对黑客攻击、病毒入侵等安全风险,这些风险可能导致数据的泄露、被非法修改或滥用。

为了应对这些挑战,相关人员必须加大网络环境中数据安全保护的宣传力度,提升全民的网络数据安全意识。同时,还应积极利用多元化的网络数据保护技术,构建坚实的数据安全防线,从而有效应对并解决网络环境中的数据安全问题。

[参考文献]

[1]蒋冬冬,孙允恒.基于大数据云计算网络环境的数据安全问题研究[J].通信与信息技术,2023,(05):79-82.

[2]李冬月.计算机网络的数据安全策略重点分析[J].信息系统工程,2022,(11):108-111.

[3]王珂.开放网络环境下隐私数据安全防护模型研究[J].长江信息通信,2022,35(06):150-153.

[4]凌旺,闵啸,赵亮.基于大数据云计算网络环境的数据安全问题研究[J].电子元器件与信息技术,2022,6(01):238-239.

[5]李燕.基于大数据云计算网络环境的数据安全问题分析[J].无线互联科技,2022,18(15):19-20.

作者简介:

张晓卓(1980--),男,汉族,天津市人,本科,天津市医学科学技术信息研究所,研究方向:信息网络安全。