

数字化时代下计算机网络安全问题及对策研究

顾 涛

(杭州朗和科技有限公司, 浙江 杭州 310051)

摘 要 随着数字技术的不断发展, 数字化时代下计算机网络安全问题越来越多。结合近年来网络安全的发展现状, 分析网络安全技术的发展带来的新挑战, 探讨数字化时代下计算机网络安全面临的问题, 包括计算机病毒、黑客攻击以及网络盗窃等。因此, 本文认为只有加强网络安全建设, 提高计算机网络安全水平、保障信息安全, 才能构建一个健康的网络环境, 为各行业网络安全保驾护航。

关键词 数字化; 网络安全; 计算机网络

中图分类号: TP393.08

文献标识码: A

文章编号: 1007-0745(2023)04-0025-03

数字经济时代的到来, 互联网的普及率越来越高, 由此对计算机网络安全保护问题也提出了更高的要求, 如何解决好网络安全问题是当下重点研究的课题, 本文针对目前的计算机网络现状提出对应的策略, 以期推动计算机网络安全健康有序发展。

1 计算机网络安全的发展现状

1.1 计算机网络安全的发展状况

计算机网络安全是当今信息社会的重要组成部分, 也是世界上日益受重视的问题。由于计算机网络安全系统可以保护网络系统免受外部威胁, 因此它在保护网络系统安全方面发挥着重要作用。计算机网络安全的发展状况^[1]非常复杂, 主要原因是它的发展正在跟上信息技术的发展步伐, 而且安全技术本身就是一个动态发展的领域。例如, 随着信息技术的发展, 网络攻击已经变得更加复杂, 更具针对性, 因此需要不断加强网络安全技术, 以便能够应对新型网络攻击。因此, 计算机网络安全的发展状况不仅受到信息技术发展的影响, 还受到网络攻击的发展状况的影响。

另外, 安全技术的发展也受到了政府的重视, 许多国家的政府都会采取一系列的措施, 以促进计算机网络安全的发展。例如政府可以通过制定相关的法律和法规来维护网络安全; 政府也可以投资科研, 开发新的安全技术; 政府还可以加强对网络安全的审查, 加强对网络攻击的惩罚。计算机网络安全的发展状况受到信息技术发展水平、网络安全技术的发展水平和政府监管政策的影响。随着信息技术的发展, 计算机网络安全的技术也在不断发展, 政府也在不断加强对网络安全的管理, 所以计算机网络安全的发展状况是一个复杂而又动态的过程。

1.2 数字化时代下计算机网络安全的挑战

网络安全技术在数字化时代下的发展也带来了新的挑战。数字时代下, 计算机网络安全技术面临着计算机病毒、黑客攻击^[2]以及网络盗窃等问题的挑战。计算机病毒的发展越来越快, 而黑客也越来越多, 他们利用技术手段对网络进行攻击, 窃取数据, 破坏网络系统, 严重影响网络安全。另外, 网络盗窃是一个重要问题, 不少网络用户因为未能保护自己的网络安全而成为网络盗窃的受害者。

数字化时代下计算机网络安全是一个重大挑战。随着计算机技术的发展, 网络安全面临着越来越大的挑战。随着互联网的发展, 网络空间的攻击者越来越多。由于网络空间的复杂性, 攻击者可以利用技术工具实施攻击, 从而破坏网络安全。例如, 攻击者可以利用恶意软件进行攻击, 从而窃取重要信息或影响正常的网络活动。另外, 由于网络安全性的缺失, 攻击者还可以利用网络漏洞进行攻击, 从而破坏网络安全。

网络安全技术发展迅速, 但安全挑战仍然存在。因此, 政府应该采取有效的措施来加强网络安全, 包括实施完善的法律法规、加强网络安全管理、投资网络安全研究等。同时, 各种企业和机构也应该加强网络安全管理, 实施安全措施, 如安全审计、安全测试等, 以确保网络安全。数字化时代下计算机网络安全是一个重大挑战。政府、企业和机构都应该采取有效措施, 加强网络安全管理, 以确保网络安全, 维护网络安全和保护网络系统完整性。

2 计算机网络安全问题的有效对策分析

2.1 加强网络安全管理

网络安全管理是网络安全的重要组成部分, 它是实现网络安全的关键。为了提高网络安全水平, 应该

建立健全的网络安全管理体系,并加强网络安全规定的制定及实施,强化网络安全意识。同时,应该建立完善网络安全管理机制^[3],制定出合理的网络安全政策,加强对网络安全的监督,以确保网络安全技术的有效运用。加强网络安全管理是当今社会中越来越受到重视的一个话题,随着网络应用的不断深入,网络安全问题也日益突出,如何更好地保证网络安全,是一个值得深入研究的问题。

第一,建立一套完善的网络安全管理体系。这套体系包括安全策略、安全技术、安全审计等几个方面,各部分之间相互协调,形成一个完整的安全管理框架,从而确保网络安全管理工作的有效性和可操作性。

第二,提高网络安全意识。网络安全意识是指用户对安全的认知和意识,一般来说,网络安全意识可以分为两个层次,一个是网络安全知识,即掌握常见的网络安全技术,如安全访问控制、身份认证、加密和访问控制等;另一个是网络安全行为,即能够准确判断和采取正确的网络安全行动。因此,提升网络安全意识,对于加强网络安全管理至关重要。

第三,重视网络安全审计。网络安全审计是对网络安全管理体系的一种定期监督,它是对网络安全管理的有效性进行评估的重要手段。只有定期开展网络安全审计,才能及时发现网络安全问题,为安全管理工作提供有力的支撑。

第四,加强网络安全管理还要依靠科学的安全技术。安全技术是网络安全管理的核心,也是最重要的部分。应当采取合理的安全技术措施,及时应对各种网络安全攻击,加强网络安全防护。加强网络安全管理是一项艰巨而又重要的任务,必须建立完善的安全管理体系,提高网络安全意识,定期开展安全审计,采用合理的安全技术措施,才能有效地保障网络安全。

2.2 完善网络安全技术

网络安全技术的发展也为网络安全提供了新的可能性和挑战。为了提高网络安全水平,应该完善网络安全技术,加强网络安全技术的研发和应用,开发出更加安全的技术,比如病毒检测技术、防火墙技术、加密技术^[4]等,以有效地防止网络攻击和网络盗窃。网络安全技术是当前社会中一个重要的热点,其重要性无可厚非。网络安全技术的发展不仅涉及网络的安全性,还涉及网络环境的安全可控性,因此,完善网络安全技术理论是迫在眉睫的问题。

第一,要完善网络安全技术理论,需要加强网络安全培训。网络安全培训不仅要培养网络安全人员的

知识和技能,还要加强网络安全的意识。只有培养出专业的网络安全人员,才能保障网络的安全。

第二,要完善网络安全技术理论,需要加强网络安全技术的研究。当前,网络安全技术已经发展到一定阶段,但仍有很多不完善的地方。因此,要想进一步完善网络安全技术理论,就必须进行更深入的科学研究,寻找新的理论,提出新的安全技术,以提高网络安全性。

第三,要完善网络安全技术理论,还需要推广网络安全技术的应用。目前,网络安全技术的应用仍然比较有限,有很多企业和用户还没有真正意识到网络安全的重要性,因此,要想完善网络安全技术理论,就必须将网络安全技术推广到更多的企业和用户中去。

第四,要完善网络安全技术理论,需要加强网络安全的监管。由于网络安全技术的发展步伐较快,安全技术的应用还不够普及,因此,必须加强监管,规范网络安全的行为,使网络安全能够得到有效的保护。要完善网络安全技术理论,需要做好多方面的工作,需要社会各方面的支持。只有加强网络安全培训、加强网络安全技术的研究、推广网络安全技术的应用和加强网络安全的监管,才能让网络安全技术理论更加完善,从而保障网络安全环境的安全可控性。

2.3 加强网络安全教育

网络安全教育^[5]是网络安全工作的重要组成部分。为了让更多的人了解网络安全,应该加强网络安全教育、普及网络安全知识、增强网络用户的网络安全意识,以便他们能够正确地使用网络,从而减少网络安全问题的发生。随着科技的发展,网络已经成为我们日常生活中不可或缺的一部分,同时也带来了许多安全问题。比如网络诈骗、网络恶意软件、网络身份盗用等,这些问题不仅给我们带来财产损失,还可能让我们陷入严重的法律纠纷中。因此,加强网络安全教育显得尤为重要。

第一,要让全体网民认识到网络安全的重要性,提高网络安全的认知水平,让大家能够正确认识和理解网络安全,从而做出正确的安全行为。其次,要加强网络安全常识的教育,让网民熟悉网络安全的各种风险,及其防范措施。此外,要加强网络安全法律法规的宣传教育,让网民更加了解网络安全的法律法规,以保障自身的权益和网络安全。

第二,要加强网络安全技术的教育,让网民更加深入地了解网络安全技术,并能够正确使用网络安全技术来保护自己的网络安全。此外,还要加强对网络

安全教育的认可、支持和监督,让网民能够更加认真地学习和理解网络安全,从而做到更加安全地使用网络。

加强网络安全教育非常重要。通过认知、常识、法律法规、技术、认可、支持和监督等多种措施,我们可以提高网民的网络安全意识,并让网民能够更加安全地使用网络。只有通过系统性的网络安全教育,我们才能真正做到真正地保障网络安全,让网络成为我们生活中安全、有效的工具。

2.4 提高网络安全防御能力

随着网络技术的发展,网络安全防御能力也越来越重要。网络安全防御能力的提高可以有效地预防网络安全攻击,保护网络数据安全,确保数据安全,保护网络系统的安全稳定运行,以及提高网络运行效率。

第一,提高网络安全防御能力,必须采用有效的防火墙技术,防止未授权的访问、未经授权的修改和未经授权的攻击。另外,需要实施严格的安全策略,严格限制系统资源的访问,控制对系统资源的访问,限制对网络上敏感信息的访问,以及采用安全审计技术,定期对网络系统进行审计,发现和修复网络系统中的漏洞。

第二,采取主动防御措施,利用网络监测技术,及时发现网络安全攻击,采取应急措施,确保网络安全。同时,还要对网络安全技术进行定期更新,确保网络系统的安全性。

第三,加强安全培训,提高用户的安全意识,让用户正确使用网络,避免发生网络安全事件。同时,还要及时发布安全知识,让用户了解网络安全的重要性,并及时采取有效的安全措施。提高网络安全防御能力是一项非常重要的工作,要想有效地保护网络安全,就必须采取有效的技术措施,采用有效的安全策略,加强安全培训,定期更新网络安全技术,以及及时发布安全知识,以确保网络安全。

2.5 提高网络安全素养

当今社会,网络成为人们生活中不可或缺的重要部分。网络安全素养的重要性也越来越受到重视,特别是在网络不断发展的今天,如何提高网络安全素养就成为一个重要的课题。

第一,要提高网络安全素养,必须从普及网络知识开始。实际上,大部分人对网络安全知之甚少,而这也是网络安全素养提升的最大障碍。因此,提高网络安全素养的第一步就是通过教育和宣传,向公众普及网络安全知识,让大家能够更好地了解网络安全的重要性。

第二,要想提高网络安全素养,就要采取一些有效的安全措施,以防止网络安全事件的发生。比如,安装杀毒软件和防火墙软件,并及时更新他们;建立良好的用户权限管理机制,限制用户对系统的访问;使用强密码,并定期更换;建立网络安全培训机制,定期对网络安全进行培训;定期对网络安全进行审查,及时发现、解决问题等。

第三,为了更好地提高网络安全素养,要建立安全文化,让网络安全概念深入人心。这就要求企业要为员工提供安全意识培训,让员工能够更好地理解网络安全的重要性,及时发现网络安全风险,提高网络安全防御能力。而政府部门也要加大网络安全宣传力度,通过新闻媒体、社交媒体等渠道,宣传正确的网络安全知识,增强公众的网络安全意识。

第四,提高网络安全素养非常重要。它要求我们从普及网络知识开始,采取有效的安全措施,建立安全文化,加强网络安全宣传,以此来提高网络安全素养,更好地保护自身和他人的网络安全。

3 结语

网络安全是数字化时代的重要问题,也是社会发展的重要内容。为了提高网络安全水平,应该加强网络安全管理,完善网络安全技术,加强网络安全教育,以有效地保障信息安全。数字化时代下,计算机网络安全是一个重要问题,主要有三个方面需要解决:一是加强对网络设备的安全性管理;二是加强系统安全性管理;三是提高网络安全防御能力。在解决这些问题的同时,还要建立完善的网络安全监督机制,加强网络安全管理,强化网络安全技术研究,构建安全的网络应急处理机制,加强与社会其他部门的合作,加强教育和培训,建立有效的网络安全管理体系,提高网络安全素养,有助于防止和遏制计算机网络安全攻击。

参考文献:

- [1] 李卫峰. 大数据背景下计算机网络安全及解决策略[J]. 电脑知识与技术, 2021, 17(22): 42-43.
- [2] 李天轮. 关于计算机网络安全防范措施研究[J]. 数码世界, 2020(02): 253.
- [3] 但凝云. 基于云计算环境下计算机网络安全问题的研究[J]. 计算机产品与流通, 2017(10): 71.
- [4] 郭翰科, 黄源. 大数据时代背景下计算机网络安全防范应用与运行[J]. 数字通信世界, 2018(11): 170.
- [5] 周玉锁. 计算机网络安全技术的影响因素与防范措施探讨[J]. 网络安全技术与应用, 2023(01): 159-161.