

基于大数据的计算机网络安全研究

董光毅*

济南革命烈士陵园, 山东 250002

摘要: 随着社会不断进步, 科学技术的发展, 人们的生活水平也有了很大的提高, 由于计算机的普及和发展, 人们对科技也越来越重视, 对互联网技术也有了更高的要求。人们对于隐私的要求也日益增加, 越来越多人关注计算机网络安全问题, 在很多时候即使选择各种方式去保护自己的隐私, 但总是会出现计算机盗取隐私的事件出现。仍然需要不断改进、优化计算机网络安全技术, 结合目前优秀的先进技术真正把保护计算机隐私安全, 有效提高计算机网络的工作效率, 促进计算机网络的发展。

关键词: 大数据; 计算机网络; 安全; 防护

一、前言

大数据时代, 互联网上的数据和信息不断井喷, 为人类提供了更为丰富的发展信息, 也为人类的发展提供了便利。但是随之而来的是, 如何保证计算机网络信息的安全, 避免出现信息安全问题, 影响正常的网络秩序。

二、计算机网络安全概念

随着计算机的出现, 互联网的普及早已使计算机网络成为人们生活中不可缺少的一部分, 人们通过网络满足各种需求, 无论是在生活中, 学习中还是娱乐中计算机网络都起到很重要的作用。因为计算机网络具有科学性便捷性, 速度也很快, 所以受到人们的喜爱, 在各行各业都受到了广泛的应用。虽然计算机网络可以为人们带来很多信息, 但这些信息被各种有害信息干扰, 所以很多人都会担心由于计算机网络的信息共享性, 隐私安全问题会产生威胁, 尤其在病毒, 有害信息也会实时更新, 入侵电脑盗取信息无处不在, 为人们的生活带来很大的威胁和风险^[1]。所以需要在计算机网络安全中投入更多的精力, 从各种角度中加强防范, 保护计算机网络安全。

三、大数据环境下计算机网络安全存在的问题

(一) 外界因素

由于计算机网络具有开放性和公开性, 所有人得到的信息都是通过信息共享实现的, 所以外界客观因素就导致了会有些不怀好意的人利用这个特质, 侵犯计算机网络安全。外界因素是在整个计算机网络中都存在的现象, 会根据不同的位置, 不同的设备, 所应用的不同场合有不同的表现, 出现不同的问题。比如可能在一些网站注册信息时候, 因为这个网站在网络安全中存在漏洞这就导致用户的信息会被共享, 姓名、电话号码等信息会被别人利用, 以此来谋取自己的利益。这种现象损害了用户的利益, 一旦产生刑事犯罪会产生巨大的损失, 所以需要有关部门加强管控, 所设计到的网站等积极维护计算机网络安全, 出现漏洞及时解决, 尽全力降低外界因素对计算机网络安全带来的影响^[2]。

(二) 网络管理不完善引发的安全问题

网络管理是保障计算机网络信息问题的关键所在, 特别是对于行业性的网络信息管理而言, 一旦出现安全问题就有可能引发蝴蝶效应, 最终造成不可挽回的损失。因而无论是企业还是政府机构, 对于网络信息安全都要予以充分的重视。甚至是个人家庭网络都需要重视网络安全问题, 而对于那些涵盖范围较广的大型广域网就更加需要重视安全管理。根据研究可知, 很多网络安全问题都是由于计算机系统漏洞所致, 而网络用户又没有及时更新防火墙设置和杀毒软件, 使得一系列安全问题发生。因而, 网络管理不完善也是引发网络信息安全的重要原因。

(三) 木马病毒攻击

木马病毒是破坏计算机系统的重大危害, 也是日常计算机网络安全维护的重点内容。木马病毒给计算机安全带来的危害非常大, 并且随着大数据技术不断发展的情况下, 木马病毒的数量和类型也在不断增多, 其危害程度也越来越高。在更多的技术支持下, 计算机木马病毒会基于更为多样化的方式存在和传输, 这使得一些病毒无法第一时间被发觉并加以制止。在这种情况下, 防控病毒侵害的效率自然会受到影响, 进而就会造成大量信息丢失, 甚至会让系统瘫痪。

* 通讯作者: 董光毅, 1981年2月, 男, 汉族, 山东济南人, 现就职于济南革命烈士陵园, 中级工程师, 本科。研究方向: 计算机。

四、数据环境下强化计算机网络安全的方法及应用

(一) 人工智能技术在防火墙技术的应用

人工智能技术在很多领域都有很多应用,其中在计算机中的一个部分就有很多应用,其中在计算机中的防护墙技术和一些防入侵技术中的应用格外重要。防火墙技术以及一些入侵检测技术等等是主要保护计算机安全的重要技术,可以保证计算机不被一些外来病毒入侵干扰,或是非法盗取一些信息,保证了计算机隐私安全和正常运行。信息安全现在是人们重点关注的热门话题,信息盗取入侵无处不在,在人工智能融入防火墙技术和防入侵技术后,智能防火墙技术可以有效加强计算机的安全指数,保障了信息安全,确保计算机可以正常运行不被入侵。智能防火墙技术可以自动识别计算机中的一些有害信息,然后自动进行拦截,这几减少了计算机被病毒入侵的可能。一些病毒通过包装很难被人们分辨识别,但通过智能防火墙可以通过智能分析技术轻易识别出一些病毒等有害信息,这样就减少了电脑入侵的可能性,保证了计算机的安全,智能防火墙技术和之前传统防火墙技术相比性能上有很大的提高,尤其是分析信息的技术,可以更加精准、快速。除此之外在防入侵技术以及检测入侵技术的能力相比传统技术也有很大的提升,相比传统更加智能化,类似一个简单的防御系统,即使计算机浏览到了病毒网页病毒也可以保护计算机不被病毒有害的信息侵扰^[3]。所以将人工智能技术融入防火墙技术以及防入侵等技术中可以有效提高了计算机的安全指数,保证计算机正常安全运行。

(二) 强化访问权限管理

访问权限能够有效保障计算机网络安全,因此,在大数据时代,为了应对数据不断增多的情况,用户需要强化方位权限管理。基于计算机网络安全的需求,做针对性设计。可以通过充分设置访问控制机制加以管理,决定是否准许服务请求,强化正常安检程序的保护效果,通过对服务请求源进行检查提升保护的效果。同时,也可以借助访问控制进行权限管理,当计算机系统收到访问要求后,询问验证口令,然后进行访问在目录当中授权的用户标志号。通过这种管控,以特定网络段和服务构建访问控制体系,从而合理控制登录的数量和时间,达到保护计算机网络安全的目的。

(三) 加强网络监控

网络监控技术能够监控局域网的计算,包括上网行为的监控,还能够使数据信息安全管理效率得到提高。通过内网监控软件能够管理“内网行为”和计算机屏幕,还能够对计算机软硬件信息数据及设备资产的安全性进行监控,包括打印监控、屏幕监控录像和应用软件限制^[4]。

(四) 完善网络管理

为确保在大数据时代下不丢失数据,保障数据安全,就要制定完善的网络管理方案,以及设施配置设备。而强化计算机网络安全控制需要全社会的共同努力来实现。社会保障是计算机网络安全的基本保障。网络安全管理部门要提高对网络的治理能力,可以从以下几方面出发:提高网络安全管理专业的技术,加强对他们的专业培训;引导网络用户和个人正确安全地使用网络,涉及网络安全问题的事情都要慎重考虑,及时处理;进行有关网络安全宣传活动,开展社区网络安全宣讲活动,提高人们的网络安全意识,共同为网络安全做出贡献;国家和政府部门还可以完善相关法律制度,为网络安全提供最根本、最有力的法律支持;互联网企业及时提高网络应用平台安全级别,指导企业用户网络安全维护以及应急方案,并针对突发事件制定有效应对方案。完善网络相关管理,才能进一步保证计算机网络安全信息的安全可靠。

(五) 规避管理疏忽,提升信息安全性

很多网络安全问题的出现往往都是由于计算机管理人员对各类管理行为疏忽所致,继而使得计算机出现安全漏洞,导致破坏者趁虚而入。基于此方面分析,无论是对于个人还是机构而言,作为网络管理员必须加强对计算机的管理,做好日常维护工作。对于个人用户,在使用计算机的过程中,需要充分重视网络安全问题,熟悉大数据时代下的数据安全保障措施,对各类网络数据进行系统性的安全管理,更加关注大数据时代下计算机网络信息的安全防范,通过行之有效的网络安全管理措施来实现大数据模式下的安全管理工作。对于网络信息机构而言,在使用计算机的过程中,需要站在宏观的角度上考虑问题,充分重视网络安全的重要性,建立动态的系统管理机制,依据网络安全防护措施来组建计算机技术平台,保证系统得以安全运行。最后,还需要从主观上形成一种网络安全认知,养成文明规范的计算机使用习惯,让网络用户认识到钓鱼网站、非法链接的危害,并且通过单个计算机为中心,与各类机构单位相联合,共同消灭当前计算机网络中的安全隐患,避免部分具有隐患的链接地址和不良信息得以传播。

(六) 强化网络监控手段

想要有效提升计算机网络信息的安全性,就需要相应地强化网络监控手段,特别是一些企业和机关单位,要充分借助网络监控技术手段,全面提升计算机网络安全性能,强化对网络系统安全的监控,要定期进行排查操作,严格

查询是否存在安全隐患。在应用过程中,可以基于签名标记法以及统计研究法等方法,对于计算机网络系统内部存在的一系列信息风险因素进行及时查询和处理。同时,相关用户也需要借助相应的知识手段,结合计算机网络信息系统运行的情况,分析系统内部是否存在信息风险因素,并找出可能存在安全风险的网络文件,并做及时清除处理,从而有效保障网络信息的安全性及可靠性。

五、结语

综上所述,优化计算机网络安全技术,结合目前优秀的先进技术真正把保护计算机隐私安全,有效提高计算机网络的工作效率,促进计算机网络的发展。

参考文献:

- [1]欧丽红.关于信息安全的计算机网络应用的研究[J].电子世界,2020(15):193-194.
- [2]彭礼平,傅嘉辉.计算机网络安全问题及其防范对策探析[J].计算机产品与流通,2020(09):59.
- [3]朱茜.网络背景下计算机电子商务信息安全的探讨[J].北京印刷学院学报,2020,28(6):139-142.
- [4]郭吉生.对计算机软件技术在大数据时代下应用探讨[J].计算机产品与流通,2019(7):30