

大数据背景下计算机信息技术在网络安全中的应用

张军善

华电青岛发电有限公司 山东青岛 266031

摘要: 由于科技的发展,电子计算机及其他前沿设施的使用越来越普遍,它们已经深刻地影响着人们的日常生活,并且深刻地改变着人们的思考方式。然而,由于大数据的兴起,提高计算机信息系统的可靠性显得尤为必要,为此,我们应该加倍重视并加固网络安全技术的应用,从而提高计算机信息系统的可靠性与可操作性。因应这一点,我们将重点研究如何利用大数据来改善互联网的安全,并给出有效的建议。

关键词: 大数据; 计算机; 计算机信息技术; 网络安全

一、计算机网络安全技术的概述与应用

由于科技的飞速进展,当前,互联网和电商领域的兴起日新月异。然而,由于操作不当、硬件缺陷等原因,电脑可能会受到损害,从而给使用者造成巨大的麻烦,甚至可能造成重大的个人信息损失。近年来,由于各种漏洞的存在,导致了网络安全的问题,这些漏洞的存在给使用者的安全造成了巨大的威胁,他们的个人隐私和敏感信息很可能被非法侵犯,从而导致大量的财产和敏感的个人资料被盗。随着社会的进一步发展,必须加强对网络安全的认识,并且积极研究、开发出更加有效的方法来管理、维护、控制、监控、管理,从而有效地提高使用者的体验,维护良好的网络环境。随着时间的推移,越来越多的新型的电脑和数据库系统涌现。其中,电脑和数据库系统的安全技术尤为重要,它们不仅能够提供高效的服务,而且还具有易于维护和更新的功能。例如,电脑的防病毒和黑客攻击能力,它们能够对电脑进行实时监测,并且能够对电脑进行预警,从而为电脑的运行提供更高的安全保障。

二、分析大数据运用的优势

尽管大数据有着潜在的风险,如果不加防范,它的使用将会受到严厉的限制。然而,它的强大之处却不仅仅体现在这一点上,而且它的优越性更加明显,它不仅仅是云计算技术的衍生,而且它更加强调了它的实际应用,比如通过收集、处理、传输、共享等方式,更加有效地满足了不断变化的社会需求,更加符合了保护隐私的原则。随着科技的发展,网络早已变得无所不有,它

是生活和工作的一部分。人们通过它获取大量的个人和商业资讯,这些资讯很难被遗忘或损坏,同时,它的便捷性和灵活性让它变得更加强大,它既无须任何物质资源,又无论是时间、地点、复杂性都无所畏惧。尽管采用大数据云储存技术的方法具有更多的优势,如更加稳健的系统、更加灵活的操作、更加强劲的访问速度、更低的维修成本等,它们仍然具有极强的安全性,能够更加完善地保障用户的隐私,同时,它们还能够通过账号访问和更新,使得任何时候都能够及时发现和处理被泄露的隐私。

三、大数据下信息管理技术在网络安全中存在的常见问题

1. 信息安全管理体制不完善

随着科技的进步,越来越多的企业开始采用CIO机制,以提高管理效率和提升服务质量。然而,根据我国企业发展数据显示,大多数企业仍然坚持传统的管理模式,缺乏灵活性,各部门之间的分工与协调处理效果不佳,网络信息安全也存在一定的风险。因此,企业应该加强对信息安全管理,提升网络管理水平,以确保企业的长期发展。由于缺乏有效的法律法规和约束机制,加上企业对信息技术和网络安全建设的认知不足,使得我国企业的网络安全建设和管理受到严重影响,导致网络安全问题日益突出。

2. 对信息系统安全管理建设和投入不足

随着科学技术的进步,许多发展中的经济体都开始加强对网络信息安全的管控,以确保公司的可持续性。然而,相比之下,我们仍然缺乏足够的资源,以支撑这一领域的发展。尤其是对于那些规模不断扩张的大型公司,他们的信息化投入只占他们的总销售额的2%,而一些小型、微型、民间的公司,他们的信息化投入更是不

作者简介: 张军善(1987.11--),男,汉族,山东省青岛市人,本科,助理工程师,主要研究方向:网络安全管理、信息技术。

足1%。根据最近的统计数据,可以看到,许多企业仅仅把精力放在追求短期的经济增长上,而忽视了基本的网络安全保障。由此产生的结果,即内部的网络安全管理机构缺乏实际的作用,而且缺乏必要的技术支持,导致网络安全漏洞频繁,给企业带来巨大的挑战。

四、大数据时代下网络安全发生的主要因素

1. 互联网的开放性

随着网络科学的飞速进步,大数据时代已经迅猛降临,深刻地影响着人们的日常生活。由于其具备的开放性,它已经被普遍应用于多种领域,为企业和政府提供了极具价值的信息。尽管当今的互联网技术正推动着社会的迅猛发展,但同样存在着许多的网络安全挑战。有些非法份子受到财富和其他诱惑,会越界侵入,从而导致严重的后果。尽管大型电脑可以通过IP协议来实施自我保护,但当病毒入侵的时候,它们的效果将会大打折扣,从而影响到整个系统的稳健性和可靠性。随着科学发展的不断推动,信息的可靠性日益提升,而信息的可靠性却受到了严重的影响。因此,有必要加强信息的可靠性,以及开发更加先进的信息安全防御技术,以有效地防止各种网络攻击。

2. 计算机网络操作者的使用方式有误

对于计算机网络而言,其实质性的安全性取决于其使用者,因此,他们必须具备良好的专业知识和能力,才能够有效地掌握和运行计算机,从而实现最大限度地利用资源,避免由于不当的行为而导致的严重的网络攻击。由于技术的发展和技术的普及,许多新型的电脑可以通过简单的编写和配置来实时监控和控制系统的运行状态,从而有效防止电脑的异常运行。此外,正确的电脑操作也能够保护电脑的安全性,避免电脑被盗取、篡改、破坏,从而保护电脑的正常运转和数据的完整性。通过深入研究和实践,我们应该努力提高对使用流程的掌握,以避免此类问题的出现。只有通过正确的方式进行操作,才能够维护系统的正常运行。

五、大数据背景下计算机网络安全防范对策

1. 强化对计算机病毒的防范

随着网络科学的飞速进步,计算机的病毒攻击能力显著增加,然而,病毒的复杂性与多样化仍然存在,因此,病毒的清理任务日益艰巨。为此,我们应当采取更加先进的预警措施,以最大限度地维护电脑的安全。为了有效地处理电脑安全隐患,我们必须采取积极的措施,首先,我们必须采取预防措施,比如建立完善的防火墙系统,配备多种多样的保护程序,阻止恶意攻击。另外,

我们的网络安全管理者也必须加强个人的专业知识,增加电脑的抗病毒和抗黑客攻击的能力,及时发现和处理电脑上的恶意程序,加固电脑的硬件和软件,及时采取有效的措施,有效地抵抗恶意攻击,最终达成有效的电脑安全。通过加固电脑网络的防护措施,大大提高了系统的稳定性。

2. 修补与完善计算机漏洞

用户在进行计算机系统的工作过程中会生成许多数据,在这一背景之下,网络资源的存储量也会迅速增加,乃至呈现出爆发式的增加,这一现状在对我们日常生活和管理工作带来方便的基石上也会使得互联网网络存在许多缺陷。所以,在用户进行互联网网络信息系统的工作过程中,必须修补形形色色的缺陷,为充分适应信息化背景之下互联网网络信息技术的迅速的发展,有关应用人士必须认知和意识到网络漏洞修补的必要性,而且科技人员也应加大对网络系统缺陷复原应用软件的研究,这样的话既有利于很好地解决互联网网络缺陷问题,还有利于规避信息的泄漏。利用网络渗透恢复软件能否快速修复互联网网络渗透,对应于研发人员与科技工作者来说,必须在保证计算机网络系统安全稳定运行的背景增强系统对病毒的防御,进而优化原有渗透回复工具。此外,为更进一步提高网络系统渗透回复技巧,使用人员必须在关心计算机系统运作情况的时候,注意网络系统非正常运作时及早利用回复技巧,这将对进一步提高网络运行效率非常重要。

六、阐述计算机网络安全技术及在网络安全维护中的运用

1. 防火墙技术

防火墙作为一种重要的电脑网络安全措施,已经成为普遍的现象。无论是私营还是商业电脑,几乎每台电脑都配备了防火墙,它的类型包括应用层防火墙、包过滤防火墙等,它们的功能各不相同,前者意在阻止未经许可许可的使用,而后者则在于阻止非法行为,从而保护电脑系统的正常运行。应用层的防火墙通常会被部署到服务器上,它们可以从根本上检测出网络上的恶意软件,并采取有力措施阻止它们的蔓延。尽管采取的方法有所差异,两种防御技术的结合可以有效地减少网络病毒的威胁,从而保护网络的正常运行。

2. 加密技术

通过采用先进的加密算法,能够把原本的文件加密,使其具备更高的隐私和完整性。加密后的文件无法被任何外部攻击者破解,从而大大增加了数据的安全性。随

着技术的飞速发展，数据加密技术也取得了长足的进步，技术专家们能够轻松实施对称加密，即加密与解密的密码相同，从而有效地防止数据的外泄。此外，非对称加密也能够提供更加完善的数据加密服务，它的密码更加灵活，更加稳定，更加有效。

3. 杀毒软件

杀毒软件在保护计算机网络安全方面发挥着重要作用，它们能够有效地检测并阻止恶意攻击，几乎每一台电脑都安装并配备了360杀毒软件，它们能够有效地保护电脑中的数据，因此受到越来越多的人的青睐。为了让杀毒软件发挥最大的功效，我们必须定期更新病毒库，以便及时发现并清除新型病毒。只有这样，我们才能够持续提高计算机网络安全性和稳定性。

七、结语

由于科学的蓬勃发展，当前的计算机科学技术日益

完善，它被应用于方方面面，然而，我们必须警惕，因为它具备开放、交流、可靠和自主的优势，许多恶意攻击者可以通过它们的漏洞窃取他们所拥有的敏感个人信息，从而对人民的隐私和财物造成极大的危害。所以，为了确保计算机的安全与稳健，我们必须采取有力的措施，不仅仅是加强网络安全，还必须更好地掌握大数据及其相关的计算机网络技术，进而实现更高层次的管控。

参考文献：

[1]夏鹏.浅谈大数据背景下计算机信息技术在网络安全中的运用[J].网络安全技术与应用, 2022 (08): 164-165.

[2]张晨.“大数据”背景下计算机信息技术在网络安全中的应用[J].科技资讯, 2022, 20 (12): 4-6.DOI: 10.16661/j.cnki.1672-3791.2202-5042-2221.