 DOI: https://doi.org/10.26549/bdai.v4i1.12361

Exploration on the Path of Network Information Security under the Background of Big Data

Chenxi Guo[1] Huanyin Shi[1] Xiaoxuan Xu[1] Tianhong Du[2]

1. Comprehensive Information Support Center of Staff Department of Shanxi Armed Police Corps, Taiyuan, Shanxi, 030000, China
2. Shanxi Armed Police Corps Hospital, Taiyuan, Shanxi, 030000, China

Abstract

The era of big data can facilitate the information interaction, improve the efficiency and quality of the information interaction, but the network information security has gradually attracted attention and attention. This paper also focuses on this, mainly discusses the influencing factors of network information security under the background of big data, and analyzes the strategy of big data. It is hoped that through the discussion and analysis of this article, the technical advantages of big data technology can be better played to ensuring people's information security.

Keywords

big data era; network information technology; network information security; guarantee path

大数据背景下网络信息安全保障路径探索

郭晨禧[1] 石桓印[1] 徐晓璇[1] 杜天虹[2]

1. 武警山西总队参谋部综合信息保障中心，中国 · 山西 太原 030000
2. 武警山西总队医院，中国 · 山西 太原 030000

摘　要

大数据时代的到来让现阶段的人们在信息交互上得到了极大的便捷，人们信息交互的效率和质量都得到了明显的提升，但是大数据时代下网络信息安全问题也逐渐引起了人们的关注和重视。论文也将目光集中于此，主要讨论了大数据背景下网络信息安全的影响因素，分析了大数据背景下网络信息安全保障策略。希望通过论文的探讨和分析可以更好地发挥大数据技术的技术优势，同时保障人们的信息安全。

关键词

大数据时代；网络信息技术；网络信息安全；保障路径

1 引言

网络技术和信息技术的飞速推广和普及为现阶段人们的工作和生活带来了极大的便捷，人们在享受时代红利享受技术红利的同时也逐渐认识到了网络信息安全保障的必要性与影响，提高网络信息安全性是发挥网络技术优势过程中必须着重考量的一大问题，网络信息安全如果无法得到保障，人民的财产安全和人们的个人隐私都容易受到侵犯，而想要明确在大数据背景下网络信息安全的保障策略首先需要了解大数据背景下网络信息安全的影响因素。

2 大数据背景下网络信息安全的影响因素

大数据时代下影响网络信息安全的因素是相对较多的，但是从实际情况以及社会中各种经典案例来看，网络信息安全的影响因素主要可以从病毒入侵、黑客攻击和自然灾害三个角度来着手展开分析，如图 1 所示。

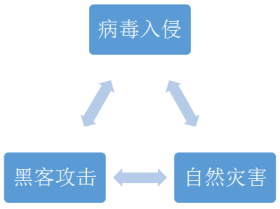

图 1 网络信息安全的影响因素

2.1 病毒入侵

网络技术可以更好地便捷人们的信息交互，因此其本身就具备着一定的开放性特征。在大数据时代下，网络技术被广泛应用于人们日常工作和生活的各个角落，这就导致网络信息的开放性特征变得更加明显，而在这样的背景下，很

【作者简介】郭晨禧（1996–），男，中国山西吕梁人，本科，助理工程师，从事网络运维、网络安全等研究。

多不法分子也利用网络信息的开放性特征谋取利益。一般情况下，计算机的 IP 或 tcp 协议自我保护能力都是相对较差的，这就让网络信息安全性受到了一定的影响，不法分子可以通过病毒入侵的方式来破坏计算机系统，并且随着时间的推移影响计算机正常操作，进而达到窃取数据或破坏系统的目的。而病毒传播的形式也是相对较多的，除了利用网络加载页面和小程序以外，光盘、软盘、硬盘等相应的形式都可以传播病毒进而导致计算机系统数据运输受到极大影响，如木马病毒、CIM 病毒等，病毒入侵是影响网络信息安全的重要因素，也是较为常见的问题，波及范围相对较广，出现频率也相对较高 [1]。

2.2 黑客攻击

计算机、手机等智能终端设备的飞速推广与普及，因此相应的专业型人才并不在少数，为系统维护和升级提供服务，但是也同样滋生了新的违法犯罪方式和专业技术人群，即人们口中常说的黑客。黑客攻击是较为常见且影响相对较大的网络信息安全威胁，不法分子可以通过计算机技术影响其他用户系统的正常运行。一般情况下，黑客攻击主要包含以下几种类别：第一，黑客可以对用户端系统进行针对性攻击，进而在系统中截取相应的数据信息，同时破坏系统，影响系统的正常运转。第二，黑客可以在计算机系统信息传输的过程当中进行信息拦截破解，进而导致信息无法正常传输，同时信息也会面临着泄漏风险。第三，黑客还可以指针对计算机系统通过计算机操作的方式攻击用户端系统，进而导致系统崩溃，影响系统的正常运转，黑客攻击也同样是网络信息安全威胁相对较大的因素，且一般情况下黑客攻击所造成的损失和影响也是相对较大的 [2]。

2.3 自然灾害

黑客攻击和病毒入侵是网络信息安全的重要影响因素也是常见问题，但是除此之外，自然灾害对于网络信息安全也会产生一定的影响，如电击、火灾、涝灾、地震等。同时受自然灾害影响，系统在后期维护使用的过程中面临着重重问题。做好防灾措施，提升防护意识，避免网络信息受到自然灾害因素影响导致系统中保存信息受到不可挽回的损害也是需要着重考量的一大问题。但是相较前两种问题，自然灾害所造成的影响和出现的频率是相对较低的。

3 大数据背景下网络信息安全保障策略

大数据时代下网络信息技术已经覆盖于人们日常生活和工作的各个角落，而网络信息安全涉及个人隐私与个人财产，需要尤为引起关注和重视，明确网络信息安全保障策略十分必要，如图 2 所示，可以从以下几点着手加强控制与管理。

3.1 合理运用防护技术，增加信息保障效果

利用信息防护技术来保障网络信息安全是较为常见的一种网络信息安全保护策略，应用效果也是相对较好的，就现阶段来看，应用效果相对较好且应用范围相对较广的技术主要包含以下几种。

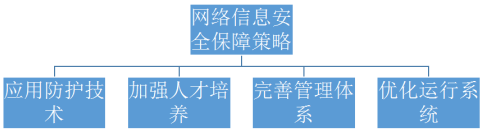

图 2 网络信息安全保障策略

3.1.1 防火墙技术

防火墙技术是现阶段网络信息安全的基本保障技术，可以通过对外界信息的判断和分析来有效地判断信息的安全性，进而保障内部信息的可靠性，人们可以将重要信息数据设置在防火墙之内，这样在出现外界信息时防火墙可以第一时间阻隔信息并且实时检测信息，有效地避免病毒入侵问题，进而保障网络信息的安全性。

3.1.2 数据加密技术

数据加密技术同样是应用范围相对较广且信息安全保护效果相对较好的一种技术，尤其是随着时间的推移，数据加密技术已经得到了不断的完善和优化，其信息安全保障能力也在不断上升，一般情况下数据加密技术可以分为对称加密技术和非对称加密技术两个主要类别，其密钥形式有所区别，在数据加密技术支持下信息数据需要在具体解密算法指导下才可以正常应用、正常显示，因此可以有效地解决信息截取或信息丢失问题，保障网络信息安全 [3]。

3.1.3 入侵检测技术

入侵检测技术可以对外来信息数据进行有效的检测和识别，通过建立入侵检测系统以有效解决信息被窃取的问题，保障网络信息安全。

3.1.4 信息安全审计技术

信息安全审计技术可以通过信息分析与检测的方式及时发现计算机系统当中存在的漏洞，同时及时发现非法入侵行为，进而提高信息安全风险的预测能力、监测能力和控制能力，保障计算机系统的正常运行。

以上几种技术都可以较好地解决病毒入侵问题，保障信息数据的安全，可以结合实际情况做出科学的选择。

3.2 强化网络信息运行系统的防攻击性能

黑客攻击是网络信息安全的重要影响因素，也是必须引起关注和重视的一大重点问题，要想更好地提升网络信息的安全性，就需要强化网络信息运行系统的防攻击性，进而有效地应对黑客攻击行为。一般情况下，黑客攻击行为的目标对象多为企业，而从这一特性上来看可以从以下几点着手进行解决：首先，相应的企业需要加强调查和分析了解黑客网络攻击的常用技术和常见手法，在此基础上对企业信息系统漏洞做出有效地分析，引入杀毒软件，如 360 安全卫士或建立大数据安全信息管理平台，将数据进行集中管理、集中保存、集中防护，进而有效地保障信息的安全性，降低黑客

攻击所带来的影响。其次，企业可以通过认证可行性加强的方式来有效地应对黑客攻击问题，加强对于外部数据访问流程的监督与控制，有效地避免黑客盗取信息的情况出现。最后，企业的网络系统管理工作人员需要提高关注和重视，认识到黑客攻击对于企业所带来的影响，加强技术培训，规范计算机操作，并且要求其他部门各工作人员学会利用防攻击软件，提前做好网络信息的安全保障工作，进而避免网络信息丢失、被窃取等相应情况的出现 [4]。

3.3 建立完善的网络信息安全管理体系

首先，可以通过限制访问信息用户数量的方式来更好地保障网络信息安全，相应人员在登陆系统后需要通过实名验证才可以获取相应的数据信息，而实名验证可以通过指纹识别、密码识别等多种方式进行身份识别，这样没有得到授权的用户则无法登陆到对应系统来浏览信息。如果系统监测到存在用户强行登录等情况时可以通过自动化关闭的方式执行封闭管理指令，进而有效地避免信息被窃取的问题，保障信息安全。其次，随着大数据时代的到来，网络信息安全已然成为了社会公众性问题，因此相关职能单位也需要加强法律法规建设，尤其是针对恶意传播病毒、恶意攻击他人系统网络等相应的法律法规更需要作出进一步的完善，如果发现不法分子利用病毒等多种方法破坏他人计算机系统或截取他人信息时应当及时地予以法律制裁，通过法律建设的方式营造良好的社会氛围，提高人们的关注和重视，提升不法分子的违法成本，进而净化网络运行环境 [5]。

3.4 培养专业的网络信息安全保障队伍

想要更好地保障网络信息安全，专业型人才队伍往往起到了至关重要的影响，加强人才队伍打造和培训可以为网络系统的优化升级以及相应的软件优化升级提供更多的保障，进而更好地发挥网络技术、大数据技术的技术优势，便捷人们的生活。而培养专业的网络信息安全保障队伍具体可以从以下几点展开分析：

首先，需要调节专业型人才培养方向，在人才培养的过程中，不仅要让受教育者掌握专业的技术，了解最新技术方法，同时也需要强化实践应用能力和创新意识的培养，推动技术优化升级，为中国信息安全保障工作的开展提供人才基础。其次，需要根据不同情况、不同实践需求针对性地调节人才培养方案，在提高人才创新能力、应变能力的同时提高培训方案的针对性、可行性与有效性。最后，还需要在人才队伍培养和建设的过程当中提升相应人员的自我管理意识、自我教育能力和自我审视能力，主动学习最新的技术方法，不断更新自身的知识储备。事实上，大数据技术作为一种普及率相对较广且渗透性相对较强的技术，其信息安全问题已经引起了社会的普遍重视，因此不断地更新迭代网络信息安全相关的技术理念，提升自我学习自我管理能力十分必要，只有这样才可以更好地适应时代和社会的变化，更好地解决实际问题 [6]。

4 结语

大数据时代下想要更好地发挥网络技术信息技术的技术优势，提高人们的工作效率和工作质量，让人们享受技术和时代带来的红利，就需要加强网络信息安全管理和建设，明确大数据背景下网络信息安全的影响因素，并在此基础之上合理运用防护技术，增加信息保障效果，加强人才培养，强化信息运行系统的防攻击性能，并且通过建立完善网络信息安全管理体系的方式有效地解决网络信息安全问题。

参考文献

[1] 沈春马.大数据背景下计算机网络信息安全问题分析[J].网络安全技术与应用,2022(12):167-169.

[2] 雷梦玲.大数据背景下中国网络信息安全管理对策研究[J].网络安全技术与应用,2022(12):166-167.

[3] 郑秀毅.大数据背景下的计算机网络信息安全问题及防护措施[J].网络安全技术与应用,2022(8):161-162.

[4] 杜传胜.大数据背景下的网络信息安全技术体系的构建[J].软件,2022,43(1):77-79.

[5] 唐瑞鹏,孙国玺,张锋.大数据背景下船舶移动网络信息安全风险预测模型[J].舰船科学技术,2021,43(20):163-165.

[6] 高红军.大数据背景下如何保证计算机网络信息安全[J].网络安全技术与应用,2021(9):168-169.