大数据时代网络信息安全与防护研究

刘志滨 [1]，潘海珠 [1]，张继升 [2]

[1] 齐齐哈尔大学计算机与控制工程学院　黑龙江齐齐哈尔
[2] 哈尔滨师范大学计算机科学与信息工程学院　黑龙江哈尔滨

【摘要】当今大数据时代，数据、网络技术和计算机技术的应用越来越普及，为人们的日常工作和学习提供了很多方便。而大数据时代下的网络信息安全问题也越来越受到人们的重视。在这个越来越重要的计算机网络安全时代，黑客、病毒以及计算机技术人员在安全方面上的缺乏在很大程度上降低了计算机网络的安全性，这些危机在一定程度上扰乱了社会秩序。因此，本文针对当前大数据时代的计算机网络信息安全因素进行研究，探索网络信息安全的保护措施。

【关键词】大数据时代；网络安全；信息安全；软件安全；防护措施

Research on Computer Network Information Security and Protection in big Data Era

LiuZhi Bin[1], PanHai Zhu[1], ZhangJi Sheng[2]

[1]School of Computer and Control Engineering, Qiqihar University, Qiqihar
[2]School of Computer Science and Information Engineering, Harbin Normal University, Harbin

【Abstract】In today's era of big data, the application of data, network technology and computer technology is becoming more and more popular, providing a lot of convenience for People's Daily work and study. The problem of network information security in the era of big data is getting more and more attention. In this increasingly important era of computer network security, hackers, viruses and computer technicians in the lack of security to a large extent reduced the security of computer network, these crises to a certain extent soft chaos of social order. Therefore, this paper studies the factors of computer network information security in the current era of big data, and explores the protection measures of network information security.

【Keywords】Big data era; Network security; Information security; Software security; Protective measures

引言

用户通过访问 Internet 获得自己需要的信息，同时利用计算机的数据传输功能实现信息资源的共享和交互，人们的生活和工作基本全面步入大数据网络时代。用户访问和数据传输过程中的信息安全问题也引起了社会各界的广泛关注[1]。在时代背景下，如何加强计算机网络信息安全已成为社会需要解决的主要问题。一些网络黑客或病毒会利用计算机网络中的漏洞和数据入侵计算机系统，对个人数据信息进行买卖， 对特定对象发动主动或被动攻击，从而实现对信息和数据的盗窃、破坏和泄露，对网络信息安全构成严重威胁。通过加强对计算机网络信息安全的管理，分析影响信息安全的因素，寻求相应的解决方案，可以有效提高计算机网络安全保护水平。

1 大数据时代特点

大数据时代特点：数据量大、类型多、处理速度快、值密度低。

大数据背景下的网络信息和用户行为特点，被互联网实时监控，进行分析数据，根据数据所反映的数据的趋势和状态，我们可以以相关图像和趋势图的形式呈现给决策者，帮助用户做出更准确的判断[2]。一些不法分子会利用这些大数据进行数据整理，进行针对恶略性分析和利用，并且可以进一步利用这些大数据实施非法的社工行为。

2 计算机网络信息安全特点

（1）信息安全风险的隐蔽性。在计算机网络环境下，各种数据和信息的操作方式和操作人员将打

破过去信息传播的空间和时间的限制，是整个信息传播行为中的一种隐藏手段，使其无法及时追溯网络犯罪的源头。

（2）信息安全风险的智能化特征。在大数据时代，数据信息产生的各种数据信息源和行为具有多样化的特点。如果不法人员利用计算机网络安全漏洞逐一破解，很容易对整个数据系统产生严重的影响。准智能源于非法人员拥有的专业技能，通过专业调查和突破，可以对计算机设备造成一定的破坏。

（3）信息安全风险的突发性。对于计算机病毒而言，其传播性和隐蔽性会在运行过程中造成整个计算机网络的突然的、不可预测的瘫痪和崩溃。这必然会降低整个计算机网络的安全性能，造成严重的数据破坏。

3 计算机网络信息安全三大影响因素

3.1 用户操作不当

在计算机操作过程中，由于个人操作不当，也会造成计算机网络信息安全问题。计算机中存储着大量的用户数据信息[3]。如果用户在操作过程中造成操作错误，比如错手删除，没有及时保存等不当操作，也会影响信息的安全。此外，由于一些用户的安全意识相对较低，在浏览网页时，会错误地打开一些含有病毒的链接，导致计算机受到病毒的入侵，从而威胁计算机信息的安全。

3.2 系统本身问题

到目前为止，计算机网络仍然存在较大的问题，各种安全问题层出不穷，这在一定程度上不利于计算机技术应用的更好发展。同时，实际分析表明，计算机在实际操作过程中容易出现隐藏的软件漏洞，这将大大增加安全风险，严重阻碍计算机网络的正常运行。换句话说，如果计算机网络存在漏洞，必然会导致计算机网络系统安全功能的削弱。黑客很容易窃取计算机网络系统的核心信息和数据。严重的计算机网络安全问题将在很大程度上影响人们的生活[4]。

3.3 硬件配置不协调

第一，使用网卡的工作站选择不正确导致网络不稳定。第二，文件服务器不是很稳定。作为全网的核心，其运行的稳定性和功能的完善对全网的质量起着重要的作用。网络应用的要求没有得到足够的重视，网络的设计和选择不合理，会阻碍网络的正常运行，影响网络的可靠性、可扩展性和升级性[5]。另外，由于缺乏安全策略，很多网站在不知不觉中扩大了防火墙的使用，忽略了那些可能被他人使用的权限。

4 大数据下网络信息安全防护措施

4.1 提升用户安全意识

广大计算机用户应树立良好的信息安全意识。例如，在使用电脑处理个人事务或工作事务时，在输入相关信息时，应设置一个相对复杂的密码，以提高账户的安全性，避免被一些不法分子利用，有效地保护了自己信息的安全。此外，随着智能手机的广泛使用，许多公共场所目前都有无线网络。使用者在公众地方连接公共无线网络时，应小心谨慎，以减少资料泄漏的可能性。为了有效提高家庭网络的安全性，防止黑客入侵家庭网络，用户可以设置用户对家庭网络的访问权限。随着大数据发展下的计算机技术和网络技术的飞速发展，已全面的走入了人们生活和工作的方方面面。要保护网络信息安全，广大用户必须树立强烈的安全意识，着力提高自身安全水平。技术进一步提高了计算机网络的安全程度。

4.2 病毒防护软件

目前常见的病毒识别技术包括特征编码、校验和、行为测试、软件仿真等。根据其使用特点可分为两种：一种是单机版，另一种是网络版。目前，由于病毒防护的普及，大多数病毒都可以被有效地分离和消除。但在病毒防护方面还存在一些问题，如病毒防护始终滞后于病毒的出现和木马病毒的传播。在未来的杀毒应用中加入杀毒软件将大大提高杀毒能力。例如，利用云计算技术进行云杀，通过强大的分布式服务器组成的云计算，可以快速升级病毒样本，并快速准确检测。动态仿真系统采用主动防御技术，实现对病毒的自动监控、分析和判断，及时拦截危险行为，实现对病毒的主动防护。

4.3 提高网络安全技术

加强网络防火墙技术的应用，既可以控制网络内部的访问，又可以有效地避免外部用户的入侵，从而保护计算机网络的安全。在使用防火墙技术时，系统会自动检查计算机网络数据，及时发现计算机中潜在的病毒，并及时进行杀毒清除。此外，工作人员还应加强入侵检测技术的应用，加强对计算机网络的检测，防止计算机网络受到外界的非法入侵。目前常用的网络检测技术主要有两种，即统计分析

法和特征分析法。统计分析主要是利用统计学的理论来计算计算机的运行方式，从而推断计算机的运行是否在安全范围内。特征分析法主要是对计算机薄弱区域的攻击行为进行分析，利用入侵检测技术，及时发现计算机系统中的漏洞和非法入侵，采取一系列的对策，防止黑客入侵。切实保护计算机网络信息安全[6]。

4.4 提高软件系统防护

软件维护是软件中非常重要的一部分。无论是修改错误、提高性能，还是升级版本，都是改善软件生命周期的重要操作。软件是现实世界的产物，所以当我们的市场环境发生变化时，软件的功能也必须发生变化，以适应不断变化的市场趋势，这就对开发人员提出了更高的要求。

（1）加固软件安全体系

为了提高已开发软件产品的安全性，可以选择使用成熟的加固软件对自己开发的软件进行保护，为软件筑起一道安全防护墙。加强软件、保护软件中的关键代码和提高软件反向反编译的阈值主要有两件事。严格检查软件系统的逻辑结构，对软件中的数据和密码进行严格严格的限制和过滤，必要时采用多层次、多风格的加密方法。

（2）充分利用帮助台

没有任何一个应用程序比帮助台更了解软件的使用。帮助台可以从用户那里收集软件故障、bug或需要改进的地方，因此负责帮助台的员工可以从这些反馈中总结出哪些应用程序目前存在问题，哪里出了问题。应用的帮助台设施还不完善，但有一个“用户反馈”区，用户可以使用电子邮件或软件和产品运营商附带的通讯窗口报告软件问题。此部分充当帮助台。如果技术公司能够将收集到的用户反馈整理起来，发送给开发团队进行讨论，开发人员就可以根据反馈集中在软件中可能出现错误的地方，从而提高软件的性能。更重要的是，这些教训可以延续到新的软件开发过程中，减少软件再次出现故障的机会。

（3）及时更新和删除应用程序

由于系统是可以继续的，所以不可能每个系统都是 100%安全的，如果你想持续使用这个应用程序，功能和算法一般都会持续更新。当旧系统不再提供价值，不需要与其他应用程序集成，它可以被替换为一个新的系统，和维护的一部分责任的新系统可以启动到供应商，减少维护时间和维护工作有时 developers。

（4）严格的质量控制

当任务非常紧，开发人员不能完成 ddl 即使他们努力工作一分钟，他们会缩短质量检验的时间，并且只能在最后一次将产品送到质量检验处做一个简短的测试。如果质量检验做得不好，就会给产品的使用带来隐患。每个应用程序都经过严格的测试。当产品没有经过严格的测试就发布时，软件在几周内就会面临各种各样的错误和问题，开发人员必须花费大量的精力进行维护。但是，如果在最初的质量检查中就完成 bug 检测、兼容性、可用性等问题，则会大大减少软件使用初期的维护工作量。因此，开发者必须有足够的时间进行开发和软件测试。

（5）安装程序建立的标准化程序

很多应用程序没有标准化的安装，有些系统甚至没有官方的安装渠道。在这种情况下，盗版安装软件会猖獗，甚至会在安装包中插入病毒，严重影响产品的信誉和质量。因此，无论使用什么设备或系统，无论是安卓还是苹果，无论是电脑还是 ipad，安装的程序都应该尽可能的正式和标准化。最好建立统一的认证官网提供下载方法。同时，官方网站还应实时更新补丁，以适应各种安装方式和安装包。在这种情况下，无论软件以何种渠道在何处发布，软件都会被有序地下载安装，这大大减少了帮助台和维护人员的工作压力。

5 结束语

大数据既能帮助人们提高效率，找到不足，改善生活，促进发展，也能成为我们方方面面的威胁。在新时代背景下，威胁计算机网络信息安全的病毒、黑客等越来越隐蔽，攻击手段也越来越复杂多样。硬件配置、引入新技术加强数据和信息监管、建立和完善网络安全代理服务器、合理设置防火墙和杀毒软件等措施确保网络信息安全[7]。

参考文献

[1] 黄斌.大数据时代下计算机网络信息安全问题探究[J].通信电源技术,2021,38(04):149-151.DOI:10.19399/j.cnki.tpt.2021.04.049.

[2] Guan Yi,Chen Qian,Jain Deepak Kumar. Research on Intelligent Perception and Cognitive Computing of Information Security System Based on Computer Big Data

[J]. Wireless Communications and Mobile Computing,2021,2021.

[3] 刘嵩鹤,梁俊.大数据时代下的计算机网络信息安全[J].电子技术与软件工程,2018(16):199.

[4] 张元喆. 大数据时代计算机网络安全及防范的策略分析[J]. 网络安全技术与应用,2021(9):167-168. DOI:10.3969/j.issn.1009-6833.2021.09.096.

[5] 陈迈.计算机网络安全防范技术的研究及应用[J].网络安全技术与应用,2017(12):6-7.

[6] 李孝莉,武雪芹. 大数据背景下计算机网络信息安全风险和解决对策研究[J]. 数码设计（下）,2020,9(9):14-15.

[7] 何帅,王海洋,赵力.露天煤矿智慧化建设关键技术及智能管控理念[J].煤矿安全,2020,51(10):298-304.DOI:10.13347/j.cnki.mkaq.2020.10.052.

收稿日期：2022 年 3 月 18 日
出刊日期：2022 年 6 月 30 日
引用本文：刘志滨，潘海珠，张继升，大数据时代网络信息安全与防护研究[J]. 国际计算机科学进展, 2022, 2(1) : 29-32.
DOI: 10.12208/j. aics.20220008

检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据 （WANFANG DATA）、Google Scholar 等数据库收录期刊