计算机系统网络和电信 2022【4】4
ISSN:2661-3719(Print);2661-3727(Online)

大数据时代中的网络数据安全问题与策略思考

常　青
中国电信股份有限公司陕西分公司　陕西西安　710061

摘　要：大数据时代的到来促使互联网成为人们日常生活和生产活动的重要组成部分，但是在人们使用互联网的范围不断扩大情况下，网络安全问题也日渐被暴露出来。近年来，网络病毒攻击事件、信息资源泄露事件层出不穷，尽管人们享受着大数据时代所带来的信息便利，但也因网络安全问题而开始产生对互联网的怀疑。本文以大数据时代为依托，先概述大数据时代的网络数据安全，然后分析当前网络数据安全存在的具体问题。最后，本文给出针对性应对策略，期望能够更好的治理网络环境。

关键词：大数据时代；网络数据安全；网络信息

Network data security problems and strategic thinking in the era of big data

Qing Chang
China Telecom Company Limited Shaanxi Branch, Xi’an, 710061

Abstract: The advent of the era of big data makes the Internet become an important part of People’s Daily life and production activities. However, as the range of people using the Internet continues to expand, network security problems are increasingly exposed. In recent years, network virus attack events, and information resource leakage events emerge one after another. Although people enjoy the information convenience brought by the era of big data, they also begin to have doubts about the Internet because of the problem of network security. Based on the era of big data, this paper first summarizes the network data security in the era of big data and then analyzes the specific problems existing in the current network data security. Finally, this paper gives specific countermeasures, hoping to better manage the network environment.

Key words: The era of big data; Network data security; Network Information

前言

尽管目前很多企事业单位正在采取多元化措施保护数据安全，但是从具体的应用上来看，大数据时代的逐步深化使得网络数据安全面临着更加严峻的挑战，数据安全问题较为突出。大数据时代背景下对于网络数据的治理一直是国内外政府关注的焦点，而主要研究集中在大数据定义、大数据技术应用以及大数据安全隐患等方面，很少从网络数据安全和对策这一研究角度出发来进行具体宏观的分析。基于此，本文从大数据时代这一背景出发，对数据安全治理过程中的网络安全策略进行深入分析。

一、大数据时代的网络数据安全概述

当今时代，我国社会经济的发展路径已经越来越明确，大数据和互联网都是国家经济发展重要方向。不仅如此，国际市场当中，越来越多的企业看中大数据技术的重要性，并将其与自身经营管理业务融合，突出大数据技术的价值，认可大数据时代对于企业发展产生的影响。从人们的生活角度来讲，大数据时代的到来对于人们的生活品质产生诸多正向影响，但是，大数据技术本身是一把双刃剑，人们在从网络中获得生活的便捷同时，也失去了边界性，诸多网络浏览记录遗留在网络当中，形成网络安全隐患[1]。如果国家所制定的网络监管治理制度不够完善，网络环境丧失保护与管理，大量用户信息就会被窃取甚至是损毁。除此之外，大数据时代所形成的数据量庞大，对于数据存储技术也提出更高要求。原本的信息技术在海量数据资源面前显现出局限性，待解决的网络安全问题不断出现。总体来讲，大数据时代，网络安全问题复杂且多变，不仅可能会出现数据被错误添加的情况，也有可能因为数据被篡改或肆意浏览而出现个人信息泄露问题[2]。

网络数据安全具有两个层面的含义，第一个层面主要指对数据本身所开展的防护措施，该种措施需要确保数据本身的完整性和保密性，且要延续数据的可用性。第二个层面主要指数据在存储方面的安全，通过一系列安全手段的保护，规避数据被盗用或肆意备份的问题[3]。本文所讨论的数据安全包含了数据本身的安全以及数据存储方面的安全。

二、大数据时代的网络数据安全威胁

大数据时代，网络数据安全呈现出下述几个方面的威胁：

首先，内部机密遭到破坏，威胁可能来自于内部人员。从事网络数据安全工作的员工群体当中，少部分人并不具备足够的职业道德素养水平，受到外界利益的诱惑与干扰，这些人被收买并以有意或无意的方式泄露内部机密，导致网络配置被篡改，记录信息出现错误或遗漏的情况。

其次，非法访问威胁。此处所讨论的非法访问主要指在未经过用户本人授权同意的情况下擅自使用用户的私人网络资源或者是将用户私人网络资源共享到网络平台当中[4]。非法访问行为包含用户个人或者是黑客擅自进入到某网络或系统当中并且展开了非法操作，也包括合法的网络用户在未经授权情况下擅自进行违法操作。

最后，信息完整性被破坏。网络安全受到威胁的情况下，信息的完整性很容易被破坏，该种情况主要体现在下述几个方面：第一，信息受到篡改，原本的信息流顺序和时间都发生改变，信息的内容以及形式受到影响。第二，信息被删除，删除全部信息或者是部分信息是一些恶意网络攻击行为最常见的手段，信息被删除以后，信息已经不复完整[5]。第三，信息插入。部分不法分子会在恶意攻击网络数据以后，在原有的信息中穿插一些其他消息，让信息的接收方无法读懂信息或者是直接读取错误信息。

三、大数据时代的网络数据安全治理问题

科学技术处于飞速发展状态，在网络用户数量不断增多情况下，网络系统中所形成的数据信息也在不断增多，这些信息不仅复杂且涉及面比较广泛。不同类型的数据形成了数据流，在数据筛选与提取的情况下，最终形成可以为人们提供信息服务的数据资源，这些信息就是有价值的信息[6]。在互联网已经普及的情况下，人们获取信息的速度不断加快，可以从网络中筛选对于自己有用的信息资源，人们都具有一定的数据管理能力，但也因为人们接触到的数据信息更多，数据安全问题对于人们产生的影响也越来越明显。此次对网络数据安全进行研究，发现虽然我国重视网络数据安全治理，但却依然存在诸多明显的问题：

（一）黑客攻击网络问题

大数据背景下，人们所掌握的安全技术水平显著提高，可以说该种情况促使网络数据的安全治理得到保障。但是，网络技术水平提升并不是用户单方面的提升，黑客的技术水平也在提升状态下，尽管现有网络系统中安装的各类防护系统类别和质量都有所改善，但在黑客寻找到网络漏洞以后，能够对安全防护系统进行专业攻击[7]。黑客通过数据信息篡改的方式破坏数据的保密性和准确性。事实上，最能对网络安全形成威胁的因素就是黑客攻击，黑客本身具有专业的计算机知识，掌握的计算机技术水平高于普通用户，常年混迹于网络当中促使黑客了解一些网络安全防护系统的漏洞以及关键点，该情况促使黑客能够轻易的攻占用户的电脑，促使用户的数据信息遭到泄露。黑客从网络中窃取信息并用于不法获利，严重情况下，因黑客的攻击行为可能会促使某些网络直接处于瘫痪状态[8]。

（二）网络病毒攻击问题

网络病毒一般是指，通过把破坏类数据直接嵌入到计算机程序中，导致电脑在操作过程中可以进行特性或者功能上的改变，比如进行简单指令复制后就可以直接修改高性能程序等，通常这种情况都具备较大破坏性。但如今，由于信息技术的飞速发展，网络病毒更加多样，并且具备了很大的破坏性，极大影响着网络的安全运营。网络中如果有病毒进入，将会使得电脑出现部分功能或者全部功能的破坏，内部资料会遭到盗窃或者修改，更有甚者可能会使得整个网络出现崩溃[9]。比如“熊猫烧香”病毒正是利用文档下载的方式传播病毒，因此使得不少用户的文档遭到非法删除，使用者个人信息也遭到泄漏，带来了巨大的经济损失。

（三）网络系统自身问题

网络中存在着形形色色的软件程序，而这些应用软件自身在安全使用中也存在着各种问题，再加上系统自身的漏洞，导致了不法分子们更多的使用漏洞来对数据信息系统进行攻击。很多软件在使用第一阶段之后，往往都会忽视安全防护问题

每一种系统都配备了一定的系统维护人员，他们在整个系统中履行着保障安全的基本工作。不过在实践工作中，有不少中小型系统的人员由于技术水平能力并不高，训练又不够严格，从而造成了整个系统漏洞较多[10]。从实际状况分析而言，由于参与系统维护的人员大多还没有信息系统和安全的意识，可能会出现某些信息系统存在的安全隐患。同时人为操控而产生的系统漏洞也在日渐增加，数据存储安全性无法得以保证。

四、大数据时代的网络数据安全问题的改进策略

（一）全周期治理数据安全问题

计算机监控系统可以提供给整个网络系统更有效的安全保护，同时也能够在全过程形成一个防御机制。只要网络系统中存在了有危险性的片段时刻，系统都能够给予整个生命周期的监视与防御。系统的安全管理过程还可采用 PDCA 管理理念，每月给出总的安全管理工作总体目标，每月根据总体目标进行分析，并给出安全管理工作小目标，在实施层面结合安全管理体系开展工作任务管理、定期或不定期地开展数据信息安全和隐患排查。针对风险预警与检测的成果加以完善，并按照系统管理要求给出下一次安全管理工作小目标，从而进人全新的 PDCA 循环。

（二）充分利用鉴别技术

鉴别的主要目的是为了验明客户或消息的真正身分。对企业所宣称的身份信息加以真正地鉴别，从而证

实其访问请求有效、并确保消息来自并达到特定的信息源和目的。识别技术也能够证明消息的安全性，从而有效地抵御假冒、非法访问、重演等危险。根据识别对象的不同，识别技术也可以包括消息源识别和通讯各方相互辨别；根据辨别内容的不同，识别技术也可以包括用户身份识别和消息内容辨识。鉴别的方式也多种多样：使用鉴别码证明消息的安全性；使用数通行字、加密、访问控制机制等手段辨识用户身份信息，防范假冒、非法访问；当今最好的识别方法就是数字签名。使用单边数字签名，可完成消息源识别，进行双边身分辨别、消息完整性辨别。而利用收发双边数字签名，可同时完成收发双边身分辨别、消息完整性辨别。

（三）重视网络防火墙作用

防火墙，顾名思义就是针对外界侵入而具有屏蔽功能的一种“墙”。在网络防火墙应用下，整个系统就被分为了内、外两部分，由这两部分人手来完成即时的、长周期系统监控工作，而在设计中对于人工智能技术的融入也让防火墙被赋予了智能特性。可以说明，网关防火墙通过自身对有害信息的准确辨别和高效拦截，以及在信息分析、智能管理上所具备的突出优点，使得系统遭受侵入和威胁的风险大大减小，使安全系统获得了有力的保护。同时，网关的设置也能够使杀毒功能更为完备。网关杀毒的方式也更为多样，从而能够更加全面地对系统进行杀毒管理。

在大数据处理时代背景下，防护墙能够对内部和外围的信息系统进行实时监测。运用先进的计算机技术，智能管理网络，有效辨识病毒，迅速拦截危险程序，并正确分类和管理数据，从而减少了病毒侵入风险，确保网络可以安全运转。同时建立了入侵监测体系，利用专门软件和硬件监测网络运转状况，以及时发生的非法威胁活动，以保证系统数据的安全性和保密性。入侵侦测管理系统就如同大厦内的监控管理系统，防火墙如同大厦门锁，一旦小偷踏入大厦中，则监控管理系统将适时发布警报，并主动进行防御对策。当攻击检测信息系统产生警报，数据安全监测部门可及时通过预警信号迅速解决问题，制定针对性举措防范攻击，维护网络数据安全，保障网络安全平稳运营。

（四）构建信任模型

随着计算机网络容量的日渐扩大，体系结构的日趋复杂化，网络入侵检测遇到的困难将日益多。目前，国内针对入侵检测领域的主要研发重点集中于入侵检测系统数据的获取和信息处理技术、分布式节点之间通信机制研究、利用多种入侵检测技术协同测试和保护入侵监测信息系统的安全性等领域。传统的入侵监测管理系统采用了分布式方法进行入侵数据监测，然后再将分析数据汇总至中心服务器进行进一步的深入分析。这种分布的、集中管理方式容易在信息处理和系统扩展上产生问题，同时还会由于单节点故障而导致整个系统瘫痪。采用华盛顿大学的对等网方式可以实现人侵监测和安全保护，并运用对等网中各个服务器相互信任的机制，进行守护程序之间的消息交流与攻击检测负载均衡，其对等网络结构如图 1 所示。

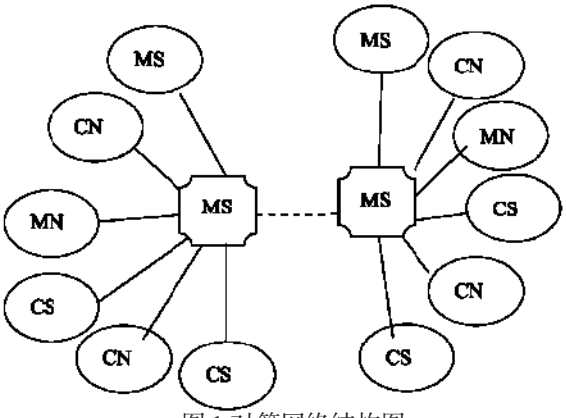

图 1 对等网络结构图

五、结束语

综上所述，在大数据时代下，不论是政府行业或是金融行业，甚至是日常生活中的各行各业，都存在着网络安全变革所造成的风险，而在此情况下，为了应对网络安全问题，不但必须提高对网络安全的意识，更必须建立健全信息安全保障体系，加快推动网络安全技术变革，从意识、制度、技能三方面维护大数字时代下所有产业和个人的安全。

参考文献：

[1] 王振中 . 大数据时代网络信息安全存在的问题及对策 [J]. 软件 , 2021.

[2] 雷学智 . 大数据时代网络信息安全存在的问题及对策 [J]. 信息与电脑 , 2020, 32(1):2.

[3] 马东君 . 浅谈大数据时代网络信息安全问题及其解决策略 [J]. 数码世界 , 2020.

[4] 张心祥 . 基于大数据视角下计算机网络信息安全防护策略的思考 [J]. 计算机产品与流通 , 2020(4):1.

[5] 加永次仁 . 基于”互联网 +”时代下的网络安全思考 [J]. 中国新通信 , 2020.

[6] 李晓红 . 大数据时代财务分析领域面临的相关问题思考 [J]. 今日财富 , 2020(1):2.

作者简介：常青，1977.1，男，汉，陕西渭南，本科，工程师，研究方向：网信安全