 DOI: https://doi.org/10.12349/iser.v6i6.6019

Discussion on Cybersecurity Strategies for Data Security Governance in the Era of Big Data

Junyong Jiang

Shanghai Digital Security Technology Co., Ltd., Shanghai, 200000, China

Abstract

Driven by the rapid development of the information age, China has also entered the era of big data. The development speed of the Internet of Things, industrial Internet and other technologies has been significantly enhanced. At the same time, the application of big data technology in people's production and life has become increasingly widespread and in-depth, which has also given rise to big data information processing tools such as Hadoop, Hive, Spark and flink. As well as the circulation of data elements and the application of data through large model training, the application value of data information has been enhanced. The geometric explosive growth of data information has brought about more serious data security problems, and phenomena such as data theft and misappropriation have become increasingly common. Therefore, in the context of the big data era, while emphasizing the exploration of data potential, it is also necessary to continuously enhance data security awareness, adopt effective network security strategies to strengthen data security governance, safeguard people's privacy security and prevent the leakage of enterprise business information, and improve the level of data security governance and network security in the big data era. Based on this, the article provides a relevant overview of big data, analyzes the common network security problems in data security governance in the era of big data, and then effectively discusses the relevant response strategies for reference.

Keywords

The era of Big Data Data security governance Cyber security Strategy

大数据时代数据安全治理的网络安全策略探讨

江均勇

上海数字安全科技有限公司，中国 · 上海 200000

摘　要

在信息化时代快速发展的推动下，我国也进入了大数据时代，物联网、工业互联网等的发展速度也得到了大幅提升，同时大数据技术在人们的生产、生活中的应用也越发广泛、深入，也催生了Hadoop、Hive、Spark、flink等大数据信息处理工具，以及数据要素流通、大模型训练对数据的应用，提高了数据信息的应用价值。数据信息的几何式暴增带来了更为严峻的数据安全问题，数据遭到窃取、盗用等现象越发常见。因此，大数据时代背景下，在重视对数据潜力的挖掘的同时，也必须不断强化数据安全意识，采用有效的网络安全策略强化数据安全治理，保障人们的隐私安全与避免企业商业信息的泄漏，提高大数据时代数据安全治理与网络安全水平。基于此，文章对大数据进行了相关概述，分析了大数据时代数据安全治理中常见的网络安全问题，进而对相关应对策略进行了有效探讨，以供参考。

关键词

大数据时代；数据安全治理；网络安全；策略

1 引言

在计算机技术，尤其是互联网技术、大数据技术、云计算等现代信息技术的快速发展推动下，各个领域的信息化发展水平也得到了大幅提升，互联网网络成为人们生产生活不可或缺的重要元素，随着信息化与数字化的深入发展与广泛普及，各个行业、领域的数据呈现出暴涨发展趋势，其中涉及许多隐私、敏感数据信息，成为“有心之人”争相获取的对象，也成了许多企业、个人的隐患所在。因此，大数据时代背景下的数据安全已然成为社会各界广泛关注与高度重视的话题。人们的生产、生活对于计算机网络的依赖性不断增强，许多数据的整合、分析、利用都需要借助计算机网络技术来完成。信息化建设也成了现代企业提高核心竞争力，创造新的利润增长点，推动企业实现持续发展的重要战略。面对复杂的发展形势，大数据技术等现代信息技术的价值创造，必须以高水平的数据安全、网络安全为前提。因此，加强对大数据时代数据安全治理的网络安全策略探讨有着十分重要的现实意义。

【作者简介】江均勇（1981–），男，中国重庆人，硕士，技术总监，从事云计算、大数据、网络安全、数据安全、人工智能及人工智能安全研究。

2 大数据的相关概述

就广义而言，大数据指的是对大量互联网数据的处理的统称。而在信息科技领域，大数据则是指从某一数据源中快速便捷地、不间断地、大量地获取不重复的数据信息，这一技术的应用成为推动互联网进入新一轮革命的重要推手，分布式计算框架也成了互联网行业对于大数据处理技术应用的主流框架。在信息化发展的当下，大数据的发展趋势较为明显。数据科技也成了互联网发展的重要方向，同时也凸显出了大数据在互联网发展中的重要性。企业基于大数据进行可用信息的精确筛选，以此准确甄别其潜在客户，掌握客户需求变化等。此外，电子政务、电子商务、智慧交通、科教领域等，大数据都有着十分重要的应用。尤其是基于互联网对信息数据发展起来的电子商务，在大数据的助推下，实现了划时代意义的转型。大数据技术在电子商务中的应用，实现了对用户需求的精准分析，以及能够在大量数据中挖掘出准确的竞争情报的功能，使得电子商务企业占据明显的市场优势。但同时这些企业也面临着信息泄露、盗用、窃取等数据安全管理问题。可以说，大数据背景下各个行业领域的发展迎来了新的机遇与契机，但同时也带来了严峻的数据安全治理和网络安全问题，稍有不慎，企业也会陷入万劫不复的绝境。

3 大数据时代数据安全治理网络安全面临的主要问题

3.1 缺乏安全意识的人为因素引起的安全问题

在大数据时代背景下，只要人们接触互联网，就可能出现个人或者集体信息暴露的情况。由此可见，大数据背景下的网络安全管理最不容忽视的便是人为因素。比如，某些网络平台的注册登录，或者是通讯工具上的聊天，都可能会出现个人身份证、家庭住址、手机号等重要信息在网络中暴露、流传，进而使得人们的信息、财产安全等受到不确定威胁的情况。即便是现行的网络系统“承诺”会保护个人信息，但是这也并非“百分百”的安全，尤其是个人信息保护意识普遍欠缺的当下，许多诸如弱口令等的行为，为不法分子盗取信息提供了可乘之机，许多个人信息安全受到威胁。还有就是许多人在进行网购、网聊等过程中往往会输出大量信息，这些信息在大数据背景下可以说是“透明的”，这些信息存在过的痕迹也会导致一些秘密信息遭到泄漏。此外，网络黑客等通过将病毒、恶意信息植入网络连接上，诱使用户点击，进而导致信息泄露等安全问题。

3.2 网络病毒入侵导致的安全问题

互联网环境的安全、稳定，会受到网络病毒的较大影响。许多网络病毒在网络终端中的植入以及在网络环境中的传播，会形成对网络信息交互的监听、截获等作用，使得人们的信息安全受到威胁。网络病毒是人为的、出于某种目的而进行编写的能够对计算机系统、软件程序等进行破坏、干扰等的程序，通过将病毒程序复制到网络终端上，形成病毒侵入，进而获取终端上的各种信息，严重威胁用户的信息安全。网络病毒具备传染性，能够借助网络通道感染成千上万的计算机终端，统一暴发将会导致整个网络系统的运行瘫痪，造成难以估计的损失。比如，著名的“熊猫烧香”病毒，不仅对感染的电脑上的文件进行加密，还会以网络共享、U 盘等多重途径迅速传播，扩大病毒感染的范围，给众多个人用户和企业造成难以估量的损失。又比如在伊朗爆发的“超级工厂”病毒，更是对其核电站的正常运行造成了严重影响，危害甚大。

3.3 黑客攻击导致的安全问题

在大数据时代背景下，数据安全治理还需集中加强对黑客攻击的打击治理。许多黑客掌握着较为先进的网络攻击手段，通过攻击大量计算机来窃取数据信息，甚至能够在互联网上准确找到安全漏洞进行攻击，获取或者篡改用户信息，这也是大数据环境在数据安全治理面临的最为严峻的网络安全问题。黑客攻击网络的技术手段各种各样，防不胜防，即便是再高级的防火墙，稍有不慎，也会被攻破，进而导致信息泄露，企业、用户等数据信息遭到拦截、贩卖，引发难以估计的后果。

4 大数据时代数据安全治理的网络安全策略

4.1 加强对账号的安全管理与保护

大数据时代背景下，各种社交媒体、软件百花齐放，争相发展。大数据特点也赋予了这些平台庞大的信息集群特征。用户对于平台使用的管理不当，导致出现数据传输漏洞，个人信息遭到泄漏、篡改等。对此，需要进一步加强对账户与数据安全管理的意识与保护力度，尤其是企业的数据库管理必须设计专门的数据保护方案，确保企业数据安全。首先，不同的社交媒体平台账号需要做好分类管理，结合平台使用、运行的特征实施差异化、个性化的数据保护策略。比如，对于银行、网银等账户需要采用更为复杂的安全保护措施，通过设置强口令、多重验证等方式来提高安全保护级别，最大限度地降低财产损失风险。其次，在提高社交媒体平台中个人信息安全水平方面，需要在进行密码编程时做好对密码保护模块的强化设计，杜绝在身份验证环节出现安全漏洞，实施高难度的密码安全加密，提高不法手段的密码破解难度水平。

4.2 强化认证和授权机制

大数据时代背景下，人们的生产生活产生的网络信息交互更为频繁、信息体量也在不断增大，做好网络信息安全保护迫在眉睫，其中加强信息传递的认证与授权管理至关重要。首先，在信息认证方面，需要强化对信息完整性的验证机制。通过严格、完善的信息认证机制，确保和明确信息由认证目标发出，以及信息的发送与相关要求相符，包括信息发送时间、顺序等，都做到数据验证上的充分明确。其次，

在身份认证方面，需要强化账号、系统登录的密钥验证、人脸识别认证等体系，采用多元化的身份认证方式，确保登录的唯一性、安全性。此外，在完善认证协议方面，针对消息认证、身份认证等建立完善的协议机制，提高消息认证的可靠性，准确识别和避免病毒欺骗、节点误导等问题。认证内容越是明确，协议要求也应越为清晰，以此确保信息的安全性、隐私性得到有效保护。

4.3 加强对设备接入的严格控制

数据安全、网络安全问题大多是由网络攻击引起，而大部分的网络攻击都需要借助设备接入口完成入侵。比如，许多计算机病毒都是由于外接 U 盘或者其他硬件遭到病毒入侵，这些病毒隐藏在外接设备中，一旦有与计算机连接的机会就会使得计算机感染病毒。受限于安全意识与资金投入等的影响，我国许多企业的大部分外接设备在连接安全性较低，进而引发了各种网络安全问题。因此，需要重视加强对外接设备接入模式的改善，提高接入安全性能。比如，在接入前进行全盘病毒查杀，或者是采用“安全 U 盘”模式，降低病毒的感染能力。除此之外，通过无线网络连接的方式也存在信息遭到盗取、篡改等风险，因此针对无线网络的应用构建防火墙也是十分钟，借助其他安全软件来对接入网络的设备进行安全扫描，准确识别和阻挡各种接入病毒的入侵。

4.4 强化网络安全意识

大数据时代背景下，互联网的使用已然成为人们生产、生活不可或缺的组成部分，因此加强对网络安全，数据安全保护的宣传力度，提高人们的网络安全意识至关重要，这也是从意识源头避免高危信息泄露问题发生的重要措施。大数据下网络技术的应用提高了人们生活、工作的便利性，而大部分人缺乏对计算机、网络运行原理的了解，在日常使用过程中诸多“无意识”行为，为不法分子提供可乘之机，用户信息遭到窃取、泄露。因此，网络安全问题需要从强化用户安全意识的根源上进行解决。比如，企业需要加强内部教育培训，针对各种典型案例与自身实际运行相结合，为员工剖析各种网络安全隐患，强化全员的网络安全意识，针对企业机密信息做好特殊保护，在接入网络的状态下杜绝点击不明连接等不安全行为，必要时做好物理上的安全隔离，以此阻止信息数据的泄露与盗用。

4.5 加强对杀毒软件与防火墙的构建

大数据时代背景下，各种病毒隐藏在数据传播当中，需要借助杀毒软件对不安全的网络信息进行有效过滤，实现对网络安全的有效保护。因此，对于数据安全治理，需要重视加强对计算机杀毒系统、杀毒软件的合理选择，并与防火墙技术相结合，提高对病毒的识别、防控能力。防火墙的构建能够起到对网络安全问题的有效缓冲，在数据传输过程中实现对访问策略以外的路由信息进行拦截的作用。大数据时代背景下的防火墙技术也得到了较好提升，融合了服务控制、用户控制、方向控制、行为控制等功能，在有效阻挡黑客攻击的同时实现对数据信息的安全保护，保障网络安全。

5 结语

综述可知，大数据时代背景下互联网的高度发展为各个行业、领域提供了新的发展机遇，企业的核心竞争力也因此得到显著提升。而先进的信息技术发展带来各种便利的同时，也加剧了网络安全风险。这就要求相关企业、用户加强对大数据时代下数据安全治理的特殊性的深入认识，准确把握大数据运行下的各种网络安全问题，进而采取有效措施提高网络安全运行效益，提高大数据时代下数据安全治理水平。

参考文献

[1] 庄益娈.大数据时代数据安全治理的网络安全策略分析[J].科学与信息化, 2021(12):72-72.

[2] 陈鹏东.大数据时代数据安全治理的网络安全研究[J].数字通信世界, 2021, 000(002):167-169.

[3] 马骁.大数据时代数据安全治理的网络安全策略[J].科学大众, 2021, 000(009):P.63-64.

[4] 张晶,李洪洋,张智钧,等.大数据时代数据安全治理的网络安全策略[J].网络安全技术与应用, 2021.

[5] 王路遥.大数据时代的网络信息安全及防范措施[J].电子技术与软件工程, 2019(5):1.