基于大数据云计算环境下的数据安全分析

◆吴珊云
（广西工业职业技术学院）

摘要：在网络环境中也是存在一些危险的，计算机病毒、木马等恶意程序都会影响到信息安全，一些重要信息被他人窃取，敏感信息造成外泄，这给企业及个人都带来了重大的影响，严重时会带来巨大的经济损失。因此，为了应对网络环境的特点，应该加强信息安全的保护工作，利用相应的措施提高数据信息在网络环境中的安全性，可以有效地保护企业或个人的利益。下面就来对大数据云计算背景下的数据安全问题进行一下简要分析，并且提出一些相应的数据安全应对策略，以供参考。
关键词：大数据；数据安全；策略；分析

一、大数据时代数据安全面临的问题

随着网络的普及，掌握计算机技术和网络技术的人员越来越多，人们也认识到了信息资源的重要价值，这也让不法分子发现了网络中的潜在利益。在我国利用网络从事犯罪活动的事件逐年上升，许多违法人员利用病毒、木马程序，恶意盗取一些企业网站中的个人信息、商业信息，给企业带来了重大经济损失。这种高科技犯罪，因为其盗用的计算机数据是可以拷贝的，因此在窃取数据信息时，往往不易被察觉，等到发现重要信息被窃取时，已经很难对犯罪人员进行搜寻，这也是目前数据安全面临的重要问题之一。同时，近年来违法人员在网络犯罪中，专业水平越来越高，而在大数据背景下，大量庞杂的数据以多元的形式被发送接收，数据在传输过程中有很多环节会出现数据外泄，这也让违法人员更容易寻找漏洞，同时违法人员因为掌握更加专业的知识，让作案后的追溯更加困难，所以当下数据安全管理工作，必须要提高对数据的各环节管理，提高对访客的审核力度，这也是数据安全管理工作需要重视的问题。

二、云计算的优势

1、投入成本较低。传统的数据中心需要较高的成本投入，很多小型企业因为难以支付昂贵的费用，使其不能建立自己的数据中心。但是，云计算的出现为小型企业提供了良好的条件，可以通过云计算服务租用自己需要的服务，使得整体成本降低，也不用参与复杂的管理，有利于企业的进一步完善和发展。

2、涵盖资源量极大。云计算资源是一个巨大的资源池，主要是由大量的计算机资源组成的，并可以进行资源共享。它主要是通过对互联网进行访问，用户可以使用云计算资源池中的硬件和软件。这种超大规模的资源可以有效的提高用户的数据访问能力，而数据的存储和计算能力也得到了有效的加强。

3、数据动态化。云计算中的的数据可以进行动态扩展，用户可以根据自己的需求进行扩展，也就是说云计算中的数据资源具有很强的伸缩性。

4、数据虚拟化。云计算中，虚拟化技术是其中的核心，可以利用底层架构进行抽象化，使得设备之间的差异和兼容对上层应用进行透明化，从而使得云对底层数据实现统一管理。

5、 数据的按需服务。在整体的云计算中，用户可以按照自己的需求来选择云计算服务，并且根据实际需求的服务使用量来计算费用。

三、大数据时代保障数据安全的策略

（一）建立完整的数据安全管理体系

数据安全管理是为了保证计算机系统的正常运转，保证计算机网络中，不会因为偶然或恶意攻击而出现数据信息的泄露或破坏，不会因为木马程序被恶意攻击者操纵，进而对数据信息作出篡改。数据信息安全主要是要保证信息的不被破坏，保证信息的正常传输和接收，以及保证信息的私密性。因此想要做好数据信息的安全管理工作，就需要建立完整的数据安全管理体系，这样才能通过技术、人员等相结合的方式，提高数据安全保障效果。数据安全体系主要是需要从管理到技术的提高，进而保证数据安全策略得以完成，最终实现大数据时代背景下对数据安全保障的要求标准。因此，数据安全体系需要从安全保障功能、数据安全保护技术、数据保护流程等方面，分多个层次的进行有效配合，这样才能够建立有效的数据信息安全体系。

因为在大数据时代的背景下，数据信息的获取途径较多，因此恶意攻击者对企业内部核心数据服务器的攻击途径和攻击可能也增多了。恶意攻击者一般通过在网络中搜寻大量的网络浏览信息，对其中关键信息进行筛选，分析用户的成分、客户端的防御能力、客户端内部的组织构架等信息；根据需要从中挑选出具有价值的目标，在通过不同的手段进行攻击，使用试探性攻击防火墙，在用户常用网站中放置诱惑性信息，在连接中植入木马程序、病毒程序等手段；通过侵入客户端的方式，恶意攻击者可以逐步侵入企业内部的核心数据服务器，再根据需要选择窃取核心资产或潜伏在数据服务器内部长期威胁企业数据安全。所以建立大数据信息安全管理体系时，应该根据恶意攻击者的攻击方式，将所有可能被攻击的途径进行相应的防护，加强网络浏览的安全扫表，加大杀毒软件的投放力度，通过多个环节的防护措施，让企业内部网络形成完整的整体，最终防止恶意攻击者的渗透。

（二）进行大数据安全的技术研究

在大数据时代背景下，应该提高数据安全方面的相关技术研究，例如：完善客户端的操作系统，减少客户端操作系统的系统漏洞，提高相应的加密技术研究，设定更加完善的访问权限审核等。相关技术研究的最终目的在于，最大限度的保证大数据在开放性传输、接受过程中，保证数据信息安全，避免数据泄露、损坏、更改等问题的发生，通过先进的安全防护技术，减少恶意攻击者绕过访问权限侵入核心服务器，防止客户端成为恶意攻击者的傀儡机，最终保证企业核心数据资源的数据安全。

随着科学技术的快速发展，数据存储方式越来越多，而移动设备携带便捷的优势使其快速并广泛应用到广大用户中，这就加大了数据被破坏的可能性。某些情况下，数据是不能被恢复的。因此，加大移动设备的数据备份和安全管理具有重要意义。用户可以将相关数据上传至云服务器中，但是云服务器不能保证数据的绝对安全。每个云服务器都存在很多可靠的数据分发中心，其中一些 PC 端较为陈旧， 因此，这种数据备份方法只能作为一个计划方案来备用。

（三）大数据安全技术的应用研究

对于所采使用的相关安全防护技术，企业应该进项相应的技术分析，保证这些技术在应用时可以达到相应的安全预警和防护标准。应该在大数据的获取方面，根据数据的重要性进行分级采集，将获得的大数据进行二次分析提取，进而将数据设定出不同的指标，根据指标的不同进行关联，最终形成完整的安全评估机制，有助于掌握信息安全状态。

结束语：综上所述，面对大数据时代的特点，数据安全管理需要从体系到技术进行完善，只有保证数据安全体系建立与数据安全技术共同发展，才能真正达到大数据安全的要求标准。提高大数据安全管理水平，有助于维护企业利益，是大数据时代下企业在数据安全管理方面需要重视的工作。

参考文献：

[1]刘佳祎.云计算与大数据环境下的信息安全技术[J].电子技术与软件工程,2019(02):204.
[2]赵丁,宋刚.大数据云计算语境下的数据安全应对策略[J].电子技术与软件工程,2019(02):210.
[3]刘静.基于安全云计算的大数据信息管理框架研究[J].信阳农林学院学报,2018,28(04):118-120+124.
[4]王鹏.基于大数据与云计算环境的个人信息安全协同保护研究[J].信息与电脑(理论版),2018(22):204-205.

作者简介：吴珊云（1974. 08—），男，广西南宁，壮族，硕士研究生，讲师，研究方向：电子信息工程。

基金项目：2018 年度广西高校中青年教师基础能力提升项目–智能制造领域云计算技术应用的研究（2018KY1104）。